报告编号：44090243008-00008-23-0234-01

网络安全等级保护
OA 系统等级测评报告



被测单位：茂名职业技术学院

测评单位：广东中科实数科技有限公司

报告时间：2023 年 08 月 15 日

说明：

一、每个备案系统单独出具测评报告。

二、测评报告编号为四组数据。各组含义和编码规则如下：

第一组为系统备案表编号，由 2 段 16 位数字组成，可以从公安机关颁发的系统备案证明（或备案回执）上获得。第 1 段即备案证明编号的前 11 位（前 6 位为受理备案公安机关代码，后 5 位为受理备案的公安机关给出的备案单位的顺序编号）；第 2 段即备案证明编号的后 5 位（系统编号）。

第二组为年份，由 2 位数字组成。例如 09 代表 2009 年。

第三组为机构代码，由网络安全等级测评与检测评估机构服务认证证书编号最后四位数字组成。

第四组为本年度系统测评次数，由两位构成。例如 02 表示该系统本年度测评 2 次。

网络安全等级测评基本信息表

被测对象					
被测对象名称	OA 系统			安全保护等级	第二级（S2A2）
备案证明编号	44090243008-00008				
被测单位					
单位名称	茂名职业技术学院				
单位地址	茂名市文明北路 232 号			邮政编码	525300
联系人	姓名	罗良宏	职务/职称	综合科科长	
	所属部门	学院办公室	办公电话	0668-2920122	
	移动电话	17820191383	电子邮件	mmzyb@126.com	
测评单位					
单位名称	广东中科实数科技有限公司			机构代码	SC202327130010234
单位地址	广东省广州市南沙区海滨路 1121 号 A9 栋 4 层			邮政编码	511466
联系人	姓名	钟宁	职务/职称	办公室负责人	
	所属部门	办公室	办公电话	020-84686743	
	移动电话	13902309071	电子邮件	zhongning@realdatachina.com	
审核批准	编制人	朱思源	编制日期	2023.8.14	
	审核人	丁丽萍	审核日期	2023.8.15	
	批准人	丁丽萍	批准日期	2023.8.15	

声明

本报告是 OA 系统的等级测评报告。

本报告测评结论的有效性建立在被测评单位提供相关证据的真实性基础之上。

本报告中给出的测评结论仅对被测对象当时的安全状态有效。当测评工作完成后，由于被测对象发生变更而涉及到的系统构成组件（或子系统）本报告不再适用。

本报告中给出的测评结论不能作为对被测对象内部部署的相关系统构成组件（或产品）的测评结论。

在任何情况下，若需引用本报告中的测评结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。

广东中科实数科技有限公司

2023 年 08 月 15 日

等级测评结论

测评结论和综合得分			
被测对象名称	OA 系统	安全保护等级	第二级（S2A2）
扩展要求 应用情况	☐云计算 ☑移动互联 ☐物联网 ☐工业控制系统 ☐大数据		
被测对象描述	OA 系统是由茂名职业技术学院统一组织规划建设，由北京致远互联软件有限公负责开发，于 2018 年 10 月正式投入运行，由教育信息与网络中心负责运行维护。OA 系统网络主要分为 4 个区域，分别为外网边界区域、安全管理区域、服务器区域、办公区域，主要由网络设备、安全设备组成，OA 系统为 B/S 结构，主要由 Linux 平台的操作系统，Oracle 平台的数据库系统，及 Tomc 中间件系统组成。单位采用自主运维模式，通过部署运维及管理终端提供专用运维管理，采用运维安全管理系统实现设备的统一管理，并进行操作运维审计，使用日志审计系统进行设备日志统一收集存储与分析。在安全管理方面，茂名职业技术学院已建立了较为完善的安全管理体系，建立了相应的安全组织，设立了相应的安全部门和岗位，制定了安全管理制度并参照落实。		
安全状况描述	本次测评共发现安全问题数总计 36 个，其中高风险问题 0 个，中风险问题数 30 个，低风险问题 6 个。主要存在的问题：机房未提供机房验收文档，无法明确建筑材料的耐火等级。机房未部署湿度控制设备，不能防止水蒸气结露。备份服务器、UIS 超融合管理平台未配置口令有效期策略。运维终端未配置屏幕保护程序。备份服务器未配置登录失败处理策略及登录连接超时策略。运维终端进行远程管理时，鉴别信息通过不安全的协议进行传输，数据库、中间件、UIS 超融合管理平台日志留存时间不足 6 个月，未进行定期备份。		
等级测评结论	中	综合得分	78.39

总体评价

茂名职业技术学院在网络安全技术防护措施的建设和安全管理制度体系建设方面，已采取了相应的安全机制和管理措施，初步建立了一套满足自身业务发展的网络安全防护体系，能够基本保障 OA 系统日常有效的运行。其中：

1.安全物理环境

机房部署 1 组科华品牌 UPS 电源系统，正常负荷情况下能保证机房内设备正常运行 30 分钟以上，具有 UPS 巡检和维护记录。机房通信线缆和强电线缆采用桥架方式部署，桥架位于机柜上方，强弱电桥架分开部署，可避免互相干扰。信息机房部署 1 组科华 UPS 电源系统，UPS 运行正常，可起到稳压和过电压防护作用。信息机房出入口已安装了福鑫电子门禁系统，通过手机蓝牙和门禁卡对进入人员进行身份鉴别，且机房入口安排了专人值守，门禁系统存在机房进出电子记录表，记录内容包括开门时间、操作人员和打开方式。信息机房内服务器、网络设备及安全设备是用螺丝固定在机柜上，能够有效防止设备从机柜上脱落，重要设备和主要部件、线缆设置明显的机打标签，标签内容包括：设备名称、设备编号、项目名称、本端、对端。但仍存在部分安全问题如：机房未铺设防静电地板。未部署机房专用精密空调,不能设置湿度自动调节。未部署湿度控制设备，不能防止水蒸气结露。未提供火灾自动消防系统的定期巡检和维护的记录。

2.安全通信网络

服务器、安全设备、网络设备采用 https 协议或 ssh 协议进行远程管理、数据库采用 ssl 协议进行远程管理，应用系统、超融合管理平台采用 https 协议，均可保证通信过程中数据的完整性。网络拓扑图与实际网络运行环境一致，被测网络已在外网边界处有部署出口防火墙，并配置了访问控制策略，重要网段部署在

出口防火墙内部,未与外部网络直接相连,已在服务器区部署 WEB 应用防火墙，配置了访问控制策略，可避免非授权的访问。学校已依据工作职能、重要性、信息重要程度等划分对网络划分多个区域，并为各网络区域分配地址，安全管理区为 172.16.*.0/24，服务器区为 10.1.*.0/22，办公区为 192.168.*.0/24，网络区域与划分原则一致 。但仍存在部分安全问题如：未基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

3.安全区域边界

安全管理区边界处在核心交换机上配置了与办公区、服务器区、外网边界之间的访问控制策略，最后一条策略默认拒绝所有。安全管理区边界的核心交换机访问控制策略中已设置源地址、目的地址、源端口、目的端口、协议，管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝。办公区边界处已部署核心交换机，并开启了访问控制策略，能够保证跨越边界的访问和数据流通过受控接口进行通信，不存在绕过边界的途径。出口防火墙 1、出口防火墙 2 已开启访问控制策略对源区域、源地址、目的地址、协议、端口等进行检测，以允许/拒绝数据包进出。服务器边界处已部署 WEB 应用防火墙，已对重要节点进行审计，包括流量检测和行为检测，审计覆盖到每个用户，已对重要的用户行为和重要安全事件进行审计。但仍存在部分安全问题如：不能对边界的流量和边界的安全事件进行审计,故缺少边界的流量审计和安全事件审计记录。不能对边界的流量和边界的安全事件进行审计,故无法对审计记录进行保护和备份。未部署有防病毒网关或者有防病毒模块的防火墙，因而未能对恶意代码进行检测和清除。未根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能

力。

4.安全计算环境

网络设备：核心交换机采 ssh 远程登录，已禁用 telnet 远程通信，可防止鉴别信息在网络传输过程中被窃听。核心交换机采用 ssh 协议进行通信，能保证重要数据在传输过程中的完整性。核心交换机采用用户名+口令方式对登录的用户进行身份标识和鉴别，不存在同名账户，身份标识具有唯一性，交换机已设置口令策略，口令长度为 8 位，由数字、小写字母、大写字母和特殊字符组合而成，已开启口令 180 天定期更换策略。核心交换机已对管理终端地址进行限制，限制地址为 192.168.*.32-192.168.*.47 ，192.168.*.0-192.168,*.31。汇聚交换机 1 已开启登录失败处理功能，失败 10 次锁定 5 分钟，已设置超时 15 分钟自动退出。

安全设备：WEB 应用防火墙在通信过程中采用 https 协议传输数据，用户口令信息加密传输，可防止鉴别信息在网络传输过程中被窃听。WEB 应用防火墙遵循最小安装原则，未安装不必要的组件和应用程序。出口防火墙 1 采用用户名+口令的方式进行身份鉴别；不存在空口令用户；以用户名作为用户身份唯一性标识；已配置符合复杂度要求的密码策略（口令长度设置至少 8 位，必须包含数字、大写字母、小写字母、特殊字符其中 3 种），已设置口令最长使用天数为 90 天。出口防火墙 2 不存在不必要的默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的服务。上网行为管理系统存在默认账户 admin 无法修改、删除，但口令已修改为复杂口令。

服务器和终端:备份服务器已开启 rsyslog 系统日志和 auditd 安全审计功能，审计覆盖到每个用户，可对重要的用户行为和重要安全事件进行审计。备份服务器已配置系统管理员账户：sangfor，审计管理员账户：shenji，安全管理员账户：

anquan，普通账户：peanut001，账户权限已分离，分别拥有其工作所需的最小权限，超级管理员账户 root 要经过授权审批才能使用，可实现管理用户的权限分离。备份服务器在通信过程中采用 ssh 协议传输数据，可保证重要数据在传输过程中的完整性。数据库服务器登录失败 5 次锁定 3 分钟，已设置超时 5 分钟自动退出。已通过服务器区防火墙限制仅 10.1.15.*、192.168.*.0/27 可远程登录应用服务器。

系统管理软件平台：UIS 超融合管理平台登录失败 3 次锁定 1 分钟，操作员闲置 60 分钟自动退出。UIS 超融合管理平台设置了系统管理员账户 super、安全管理员账户 anquanguanliyuan、审计管理员账户 shenjiguanliyuan，账户权限已分离，分别拥有其工作所需的最小权限。数据库仅采集和保存必需的用户个人信息，如职工的姓名、部门、岗位、职级、人员类型、人员状态等。数据库已对登录的用户分配账户和权限，已配置系统管理员账户 SYS、SYSTEM，业务账户 OAUSER、WXUSER、ETL_USER，备份账户：OABACKUP。

业务应用系统平台：OA 系统、AAP 端在通信过程中采用 https 协议传输数据，用户口令信息加密传输，可防止鉴别信息在网络传输过程中被窃听。OA 系统、APP 端登录时不自动保存和显示历史账号和口令，在用户退出后及时清空会话信息，无法通过回退操作访问退出前界面，用户的鉴别信息所在的存储空间被释放或重新分配前能够得到完全清除。OA 系统、APP 端已采用 https 进行通信，能保证重要数据在传输中的完整性。OA 系统保存的个人信息仅授权用户可访问，非授权用户无法访问及使用，且具备个人信息保护的相关管理要求和流程规定。OA 系统的登录日志包括人员、登录名、部门、岗位、登录时间、退出时间、在线时长、IP 地址；应用日志包括操作人员、操作人员登录名、操作类型、操作描

述、操作时间、IP 地址、所在单位、操作结果、操作模块；APP 端审计日志包括人员、登录名、部门、岗位、登录时间、退出时间、在线时长、IP 地址。

数据资源：OA 系统、APP 端已采用 https 进行通信，能保证重要业务数据、重要个人信息在传输中的完整性。OA 系统保存的个人信息仅授权用户可访问，非授权用户无法访问及使用，单位具备个人信息保护的相关管理要求和流程规定。OA 系统用户输入框有姓名，手机号、性别、所属部门等信息，均为业务必需的个人信息，未发现超范围采集情况，单位具备个人信息保护的相关管理要求和流程规定。

5.安全管理中心

安全设备、网络设备、服务器均配置审计管理员账户，并对审计管理员账户进行身份鉴别，只允许其通过日志审计系统进行安全审计操作，并且设备已开启安全审计对审计管理员的操作行为进行审计。安全设备、网络设备、服务器均有建立系统管理员账户，并对系统管理员进行身份鉴别，只允许系统管理员通过特定的命令或操作界面进行系统管理操作，服务器通过堡垒机进行身份鉴别，仅允许系统管理员进行操作和管理，并且各设备已开启安全审计对系统管理员的操作行为进行审计。该单位已配置系统管理员，并且安全设备、网络设备、服务器均由系统管理员负责系统的资源和运行，包括用户身份，系统资源配置、系统加载和启动、系统运行的异常处理，数据和设备的备份恢复。该单位已设置审计管理员岗位并配置相应的人员，并且有部署日志审计系统收集各设备的日志审计记录进行分析、处理。

6.安全管理制度

该单位《信息安全制度管理规范》已规定总体安全管理制度和规定以及安全

技术标准和规范须经信息安全领导小组审批确认，方可发布，已通过 OA 系统正式发文通知，制度版本为 V2.0，具备“收发文登记记录”。该单位《信息安全制度管理规范》已指定信息化办公室负责主持制定茂名职业技术学院信息化技术规范和有关规章制度,安全管理制度由信息化办公室发布。该单位秉承“积极防御，综合防范”的信息安全方针,根据国家信息安全等级保护等有关政策和标准要求，建立“三个体系，一个中心，三重防护”的安全保障体系框架，已在《信息安全总体策略》中阐明机构安全工作的总体目标、范围、原则和安全框架等。该单位已对安全活动中的主要内容建立了管理制度，已制定《数据安全管理规范.》、《网络安全管理规范》、《网络安全管理规范》、《应用安全管理规范》。该单位已建立《设备操作规程》、《 软件操作手册》、《防火墙配置和操作手册》等操作规程，相关文档中包含对网络安全、系统运行维护、系统配置、用户操作等方面的规定。但仍存在部分安全问题如：未具有管理制度评审记录和修订记录。

7.安全管理机构

该单位《安全审核与检查管理制度》规定学校部门每月进行一次安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况，详见《安全检查报告 20230321》。该单位《安全组织机构-沟通合作》规定各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通机制,每年组织一次工作会议进行沟通合作，共同协调处理信息安全相关问题，具有“沟通会议记录表”。该单位《安全组织机构-沟通合作》已规定通过聘请信息安全专家和外部顾问成员，指导茂名职业技术学院信息安全建设，规定服务中心有关部门建立沟通、合作机制，定期组织相关单位、部门召开内部协调会议，具备“B005 信息安全会议记录”。该单位《安全组织及职责管理规定》已设立办公室为网络安全管理职能部门，《岗

位安排及岗位职责》中已明确了各岗位负责人的职责，包括安全管理员、系统管理员、网络管理员、应用管理员、资料管理员、安全主管等方面的岗位职责。该单位《岗位安排及岗位职责》已设置系统管理员为黄海东、安全审计管理员为麦才赞、安全管理员为龙恒，网络管理员为吴国华、机房管理员为陈思凡、资产管理员为黄健。

8.安全管理人员

该单位《安全教育和培训制度》规定由学院教育信息与网络中心负责人员的安全意识教育和岗位培训，明确考核结果由信息中心进行备案，具备“学院信息管理人员培训签到记录”，具备“C014 专业培训考核记录表”。该单位《内部人员信息安全管理规定》规定信息安全相关岗位人员上岗前必须经人力资源保障科进行身份、背景、专业资格和资质的审查和考查，教育信息与网络中心进行技术和业务技能考核，具备“C002 人员信息审查记录”。该单位《外部接入受控网络访问系统管理规范》要求外部人员接入受控网络前由对接人在 OA 提出申请，教育信息与网络中心负责人批准后由系统管理员开设账户、分配权限，并登记备案，记录外部人员访问的权限、时限、账户等信息的规定，具有相关登记记录。该单位规定离职人员职工离职时需要回收涉密资料、账号口令、钥匙、资产等以及其他任何形式的载体，具有人员离岗终止权限、交还软硬件设备的记录。

9.安全建设管理

该单位《工程管理制度》明确规定由信息中心负责系统建设管理和工程实施管理。该单位《系统交付管理》规定了系统建设完成后，需要项目承建方向信息中心交付项目相关清单，详见“系统交付清单”。该单位 OA 系统定级结果经过当地公安部门批准，已取得备案证，备案证明编号为：444090243008-00008。该

单位在系统上线前已对负责系统运行维护的技术人员进行技能培训，具有“D009 技能培训记录”。该系统具有“茂名职业技术学院 OA 系统定级报告”，报告中明确了系统的安全保护等级为第 2 级（S2A2），且描述了安全保护等级确定的方法和理由。但仍存在部分安全问题如：单位缺乏相关测试验收报告。单位未对外包开发人员进行资格审查，未有相应的考核记录。该单位未在上线前进行安全性测试，未有相关安全测试报告。未在软件交付前通过第三方检测工具或人工检测软件包中可能存在的恶意代码。未组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，未有相关的方案评审记录。

10.安全运维管理

该单位《恶意代码防范管理制度》已规定须定期组织召开恶意代码宣传培训，并对外来计算机或存储设备接入系统前进行恶意代码检查，具有“E004 防恶意代码意识培训记录”。该单位《恶意代码防范管理制度》已指定教育信息与网络中心负责对截获的危险恶意代码进行分析处理，定期每月对恶意代码软件病毒库升级更新，未发生过病毒攻击行为，未截获到恶意代码。该单位《机房安全管理制度》明确规定不可在重要区域接待来访人员和不随意放置含有敏感信息的移动介质，明确办公桌上不准摆放机要文件，机要文件的草稿纸应立即销毁，不准乱丢，各类记录本不准乱放，一律置于文件柜内或其他固定地方。该单位《系统安全管理规定》已指定教育信息与网络中心负责账户管理，创建账户、修改账户权限、删除账户等操作需经过审批后在 OA 系统上填写在审批申请，经过审批后方可执行，OA 系统具有相关审批记录，审批记录中包含审批内容如申请账户、建立账户、删除账户等，审批人，审批时间等。该单位具备系统运维日志记录，具有“机房巡检记录”、“系统维护记录表”等记录文档。但仍存在部分安全问题如：

未定期进行漏洞扫描，缺少漏洞扫描报告和修复记录。未提供变更方案和评审记录。

在本次测评中，茂名职业技术学院 OA 系统测评项符合率为 75.41%，其中部分符合率为 11.99%，不符合率为 12.60%，其中测评项总数 631 个，符合项总数 371 个，部分符合项总数 59 个，不符合项总数 62 个，不适用项总数 139 个。问题数总计 36 个，其中高风险问题 0 个，中风险问题数 30 个，低风险问题 6 个。综合上述评价结果：茂名职业技术学院 OA 系统在网络安全等级保护第 2 级（S2A2）保护要求中综合得分 78.39，测评结论为中。

主要安全问题及整改建议

经过单项测评结果判定和整体测评发现，OA 系统存在的主要问题及整改建议如下：

一、安全物理环境方面

（1）低风险，未提供机房验收文档，机房防震等级不明确。

涉及测评对象：信息机房。

整改建议：建议提供机房防震证明文档，确定机房防震等级，以备日后查看。

（2）低风险，未提供火灾自动消防系统的定期巡检和维护的记录。

涉及测评对象：信息机房。

整改建议：建议对消防设备进行定期巡检维护，并保存巡检记录。

（3）中风险，未提供机房验收文档，无法明确建筑材料的耐火等级。

涉及测评对象：信息机房。

整改建议：建议妥善保留机房装饰设计验收文档，以证明主机房及辅助区采用具有耐火等级的建筑材料。

（4）中风险，未部署湿度控制设备，不能防止水蒸气结露。

涉及测评对象：信息机房。

整改建议：建议部署湿度控制设备（如精密空调），能防止水蒸气结露。

（5）中风险，机房未铺设防静电地板。

涉及测评对象：信息机房。

整改建议：建议机房统一使用防静电地板，以防止静电对电子设备和人员造成伤害。

（6）低风险，未部署机房专用精密空调，不能设置湿度自动调节。

涉及测评对象：信息机房。

整改建议：建议机房部署湿度控制装置（如精密空调，湿度控制装置）进行控制机房内的湿度。

二、安全通信网络方面

（1）低风险，未基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

涉及测评对象：安全通信网络。

整改建议：建议基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

三、安全区域边界方面

（1）中风险，未根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。

涉及测评对象：办公区边界、安全管理区边界。

整改建议：建议边界处部署下一代防火墙，根据会话状态信建立访问控制策略，为进出数据流提供明确的允许/拒绝访问能力。

（2）中风险，未部署入侵防御系统或者有入侵防御模块的防火墙，因而不可对网络攻击行为进行监视。

涉及测评对象：安全管理区边界、办公区边界。

整改建议：建议部署网络入侵检测设备，在关键网络节点处对可能潜在的

攻击行为进行监视。

（3）中风险，未部署有防病毒网关或者有防病毒模块的防火墙，因而未能对恶意代码进行检测和清除。

涉及测评对象：办公区边界、安全管理区边界。

整改建议：建议网络层部署恶意代码防范设备对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

（4）中风险，无法对边界的流量和边界的安全事件进行审计。

涉及测评对象：安全管理区边界、办公区边界。

整改建议：建议边界处部署下一代防火墙，并且配置应用访问策略和启用入侵防御、病毒防护功能，使得能对边界的流量和边界的安全事件进行审计。

（5）中风险，不能对边界的流量和边界的安全事件进行审计，故缺少边界的流量审计和安全事件审计记录。

涉及测评对象：办公区边界、安全管理区边界。

整改建议：建议办公区边界处部署下一代防火墙，使得能对边界的流量和边界的安全事件进行审计，审计记录至少包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

（6）中风险，不能对边界的流量和边界的安全事件进行审计，故无法对审计记录进行保护和备份。

涉及测评对象：安全管理区边界、办公区边界。

整改建议：建议安全管理区边界处部署下一代防火墙，并且配置应用访问策略和启用入侵防御、病毒防护功能，使得能对边界的流量和边界的安全事件进行审计，且应将审计记录上传至日志审计系统保存备份。

（7）低风险，未基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

涉及测评对象：办公区边界、外网区边界、服务器区边界、安全管理区边界。

整改建议：建议基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

四、安全计算环境方面

（1）中风险，未配置口令有效期策略。

涉及测评对象：备份服务器、UIS 超融合管理平台。

整改建议：建议配置口令的有效期策略，定期 90 天更换口令，防止口令被轻易破解。

（2）中风险，未配置屏幕保护程序。

涉及测评对象：运维终端。

整改建议：建议配置屏幕保护程序，闲时 5 分钟自动退出，降低设备被非授权访问的风险。

（3）中风险，未配置登录失败处理策略及登录连接超时策略。

涉及测评对象：备份服务器。

整改建议：建议配置登录失败处理策略，如失败 5 次锁定 5 分钟，防止恶意人员暴力破解账户口令。并配置登录连接超时策略，降低设备被非授权访问的风险。

（4）中风险，进行远程管理时，鉴别信息通过不安全的协议进行传输。

涉及测评对象：运维终端。

整改建议：建议配置“远程（RDP）连接要求使用指定的安全层”为“SSL”和配置“设置客户端连接加密级别”为“高级别”，防止鉴别信息在传输过程中被窃听。

（5）中风险，未禁止 root 账户远程登录。

涉及测评对象：数据库服务器、应用服务器、备份服务器。

整改建议：建议严格限制 root 账户的远程访问权限，禁止其进行远程登录。

（6）中风险，未设置审计管理、安全管理员账户，未实现管理用户的权限分离。

涉及测评对象：数据库。

整改建议：建议设置审计管理、安全管理员账户，并根据业务需要设置各账户的权限，实现管理权限最小化，实现管理用户三权分立。

（7）中风险，审计记录保存时间不足六个月。

涉及测评对象：数据库服务器、应用服务器、数据库、UIS 超融合管理平台、中间件、终端安全管理系统（EDR）。

整改建议：建议对日志进行集中存放，并确保保存时间能够达到半年以上。

（8）中风险，审计记录仅保存在本机，未进行定期备份。

涉及测评对象：运维终端。

整改建议：建议对日志进行集中存放，定期备份日志，并确保保存时间能

够达到半年以上。

（9）中风险，未严格限制终端登录地址范围。

涉及测评对象：运维终端。

整改建议：建议对接入终端的网络地址范围进行限制。

（10）中风险，未定期进行漏洞扫描。

涉及测评对象：核心交换机、汇聚交换机 1、汇聚交换机 2、运维安全管理系统、基线核查系统、出口防火墙 1、出口防火墙 2、日志审计系统、WEB 应用防火墙、上网行为管理系统、UIS 超融合管理平台、OA 系统、终端安全管理系统（EDR）。

整改建议：建议定期进行漏洞扫描，并在测试通过的前提下，及时修复风险漏洞，并保留漏洞修复记录

（11）低风险，未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

涉及测评对象：核心交换机、汇聚交换机 1、汇聚交换机 2、运维安全管理系统、基线核查系统、出口防火墙 1、出口防火墙 2、日志审计系统、WEB 应用防火墙、上网行为管理系统、数据库服务器、应用服务器、备份服务器、运维终端、UIS 超融合管理平台、终端安全管理系统（EDR）。

整改建议：建议基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

（12）中风险，未配置“远程（RDP）连接要求使用指定的安全层”为

“SSL”和未配置“设置客户端连接加密级别”为“高级别”，不能保证重要数据在传输过程中的完整性。

涉及测评对象：运维终端。

整改建议：建议配置“远程（RDP）连接要求使用指定的安全层”为“SSL”和配置“设置客户端连接加密级别”为“高级别”保证重要数据在传输过程中的完整性。

（13）中风险，未有备份恢复测试记录。

涉及测评对象：核心交换机、汇聚交换机 1、汇聚交换机 2、运维安全管理系统、基线核查系统、出口防火墙 1、出口防火墙 2、日志审计系统、WEB 应用防火墙、上网行为管理系统、数据库服务器、应用服务器、备份服务器、数据库、UIS 超融合管理平台、OA 系统、重要业务数据、重要个人信息、终端安全管理系统（EDR)、中间件。

整改建议：建议建立备份恢复机制，定期对备份的数据进行恢复测试，确保在出现数据破坏时，可利用备份数据进行恢复。并妥善保存相关记录。

（14）中风险，未利用通信网络将关键数据定时批量传送至备用场地。

涉及测评对象：核心交换机、汇聚交换机 1、汇聚交换机 2、运维安全管理系统、基线核查系统、出口防火墙 1、出口防火墙 2、日志审计系统、WEB 应用防火墙、上网行为管理系统、数据库服务器、应用服务器、备份服务器、数据库、UIS 超融合管理平台、OA 系统、重要业务数据、重要个人信息、中间件、终端安全管理系统（EDR)。

整改建议：建议利用通信网络将重要数据定时批量传送至备用场地，两地相距 30 公里以上。

五、安全管理制度方面

（1）中风险，未具有管理制度评审记录和修订记录。

涉及测评对象：制度或记录类文档。

整改建议：建议在制度中明确对安全管理制度需进行定期或不定期的论证和审定工作，并在实际工作中遵照相关制度执行。

六、安全建设管理方面

（1）中风险，未组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，未有相关的方案评审记录。

涉及测评对象：制度或记录类文档。

整改建议：建议组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，并进行论证后实施。

（2）中风险，未在软件交付前通过第三方检测工具或人工检测软件包中可能存在的恶意代码。

涉及测评对象：制度或记录类文档。

整改建议：建议在交付前对开发单位提供软件源代码中可能存在的恶意代码通过第三方的检查工具或人工进行审查，并保留相关检查报告。

（3）中风险，单位缺乏相关测试验收报告。

涉及测评对象：制度或记录类文档。

整改建议：建议对测试结果进行详细的记录，形成测试验收报告。

（4）中风险，该单位未在上线前进行安全性测试，未有相关安全测试报告。

涉及测评对象：制度或记录类文档。

整改建议：建议系统在上线前进行安全性测试，并具有相关安全测试报告。

（5）中风险，单位未对外包开发人员进行资格审查，未有相应的考核记录。

涉及测评对象：移动互联安全扩展要求。

整改建议：建议在移动业务应用软件开发前就对开发者进行资格审查。

七、安全运维管理方面

（1）中风险，未定期进行漏洞扫描，缺少漏洞扫描报告和修复记录。

涉及测评对象：制度或记录类文档。

整改建议：建议指定专人定期对网络和主机、应用进行漏洞扫描并保存检测记录。

（2）中风险，未提供变更方案和评审记录。

涉及测评对象：制度或记录类文档。

整改建议：建议制定系统变更相关制度，规定变更方案的申报审批程序，应要求方案包含变更类型、变更原因、变更过程、变更前评估等内容。

目录

网络安全等级测评基本信息表 I
声明 II
等级测评结论 III
总体评价 IV
主要安全问题及整改建议 XIII
目录 XXII
1 测评项目概述 1
1.1 测评目的 1
1.2 测评依据 1
1.3 测评过程 2
1.4 报告分发范围 3
2 被测对象描述 4
2.1 被测对象概述 4
2.1.1 定级结果 4
2.1.2 业务和采用的技术 4
2.1.3 网络结构 5
2.2 测评指标 6
2.2.1 安全通用要求指标 6
2.2.2 安全扩展要求指标 9
2.2.3 其他安全要求指标 9
2.2.4 不适用安全要求指标 9
2.3 测评对象 11
2.3.1 测评对象选择方法 11
2.3.2 测评对象选择结果 13
3 单项测评结果分析 18
3.1 安全物理环境 19
3.1.1 已有安全控制措施汇总分析 19
3.1.2 主要安全问题汇总分析 20

3.2 安全通信网络.....21
3.2.1 已有安全控制措施汇总分析.....21
3.2.2 主要安全问题汇总分析.....21
3.3 安全区域边界.....22
3.3.1 已有安全控制措施汇总分析.....22
3.3.2 主要安全问题汇总分析.....24
3.4 安全计算环境.....26
3.4.1 网络设备.....26
3.4.2 安全设备.....29
3.4.3 服务器和终端.....34
3.4.4 系统管理软件/平台.....39
3.4.5 业务应用系统/平台.....44
3.4.6 数据资源.....46
3.4.7 其他系统或设备.....47
3.4.8 安全扩展要求.....47
3.5 安全管理中心.....48
3.5.1 已有安全控制措施汇总分析.....48
3.5.2 主要安全问题汇总分析.....48
3.6 安全管理制度.....49
3.6.1 已有安全控制措施汇总分析.....49
3.6.2 主要安全问题汇总分析.....49
3.7 安全管理机构.....50
3.7.1 已有安全控制措施汇总分析.....50
3.7.2 主要安全问题汇总分析.....51
3.8 安全管理人员.....52
3.8.1 已有安全控制措施汇总分析.....52
3.8.2 主要安全问题汇总分析.....53
3.9 安全建设管理.....53
3.9.1 已有安全控制措施汇总分析.....53

3.9.2 主要安全问题汇总分析.....55
3.10 安全运维管理.....56
3.10.1 已有安全控制措施汇总分析.....56
3.10.2 主要安全问题汇总分析.....61
3.11 其他安全要求指标.....61
3.12 验证测试.....62
3.12.1 漏洞扫描.....63
3.12.2 渗透测试.....66
3.13 单项测评小结.....71
3.13.1 控制点符合情况汇总.....71
3.13.2 安全问题汇总.....74
4 整体测评.....83
4.1 安全控制点间安全测评.....83
4.2 区域间安全测评.....83
4.3 整体测评结果汇总.....85
5 安全问题风险分析.....87
6 等级测评结论.....95
7 安全问题整改建议.....97
附录 A 被测对象资产.....106
A.1 物理机房.....106
A.2 网络设备.....106
A.3 安全设备.....106
A.4 服务器.....107
A.5 终端设备.....108
A.6 其他系统或设备.....108
A.7 系统管理软件/平台.....108
A.8 业务应用系统/平台.....109
A.9 数据资源.....109
A.10 密码产品.....109

A.11 安全相关人员.....110
A.12 安全管理文档.....110
附录 B 上次测评问题整改情况说明.....112
附录 C 单项测评结果汇总.....114
C.1 安全物理环境.....114
C.2 安全通信网络.....115
C.3 安全区域边界.....115
C.4 安全计算环境.....116
C.4.1 网络设备.....116
C.4.2 安全设备.....117
C.4.3 服务器和终端.....119
C.4.4 系统管理软件/平台.....120
C.4.5 业务应用系统/平台.....121
C.4.6 数据资源.....121
C.4.7 其他系统或设备.....122
C.4.8 安全扩展要求.....122
C.5 安全管理中心.....122
C.6 安全管理制度.....123
C.7 安全管理机构.....123
C.8 安全管理人员.....123
C.9 安全建设管理.....124
C.10 安全运维管理.....124
C.11 其他安全要求指标.....125
附录 D 单项测评结果记录.....125
D.1 安全物理环境.....125
D.1.1 安全通用要求部分.....125
D.1.2 安全扩展要求部分.....127
D.2 安全通信网络.....128
D.2.1 安全通用要求部分.....128

D.3 安全区域边界.....129
D.3.1 安全通用要求部分.....129
D.3.2 安全扩展要求部分.....136
D.4 安全计算环境.....137
D.4.1 安全通用要求部分.....137
D.4.2 安全扩展要求部分.....200
D.5 安全管理中心.....201
D.5.1 安全通用要求部分.....201
D.6 安全管理制度.....201
D.7 安全管理机构.....203
D.8 安全管理人员.....205
D.9 安全建设管理.....206
D.9.1 安全通用要求部分.....206
D.9.2 安全扩展要求部分.....210
D.10 安全运维管理.....210
D.10.1 安全通用要求部分.....210
D.10.2 安全扩展要求部分.....216
D.11 其他安全要求.....216
附录 E 漏洞扫描结果记录.....216
附录 F 渗透测试结果记录.....218
F.1 项目实施摘要.....218
F.1.1 测试时间.....218
F.1.2 测试方式.....218
F.1.3 测试对象.....218
F.1.4 测试工具.....219
F.2 渗透测试概述.....219
F.2.1 渗透测试目的.....220
F.2.2 渗透测试风险管理.....221
F.2.3 渗透测试收益.....221

F.2.4 渗透测试流程.....222
F.2.5 渗透测试技术方法.....222
F.3 测试结果综述.....223
F.3.1 漏洞等级分布.....223
F.3.2 漏洞信息摘要.....223
F.4 漏洞详情.....224
F.4.1 茂名职业技术学院 OA 系统漏洞详情.....224
F.5 整体建议.....227
附录 G 威胁列表.....228

1 测评项目概述

1.1 测评目的

安全等级测评的目的是通过对目标系统在安全技术及管理方面的测评,对目标系统的安全技术状态及安全管理状况做出初步判断,给出目标系统在安全技术及安全管理方面与其相应安全等级保护要求之间的差距。测评结论作为委托方进一步完善系统安全策略及安全技术防护措施依据。

为进一步提高信息的保障能力，根据《信息安全等级保护管理办法》（公通字 2007【43】号）的精神，茂名职业技术学院委托广东中科实数科技有限公司（0234）对 OA 系统实施等级测评，以期发现被测评对象和等级保护标准的差距以及存在的安全隐患，为后续的安全整改工作提供参考依据。

1.2 测评依据

测评过程中主要依据的标准:

（1） 《中华人民共和国网络安全法》

（2） GB 17859—1999 《计算机信息系统 安全保护等级划分准则》

（3） GB/T 22239—2019 《信息安全技术 网络安全等级保护基本要求》

（4） GB/T 28448—2019 《信息安全技术 网络安全等级保护测评要求》

（5） GB/T 28449—2018 《信息安全技术 网络安全等级保护测评过程指南》

（6） GB/T36627-2018 《信息安全技术 网络安全等级保护测试评估技术指南》

（7） GB/T25058-2019 《信息安全技术 网络安全等级保护实施指南》

（8） GB/T 20984—2022 《信息安全技术 信息安全风险评估方法》

1.3 测评过程

本次测评项目自 2023 年 07 月 14 日起至 2023 年 08 月 15 日结束，等级测评过程分为四个基本测评活动：测评准备阶段、方案编制阶段、现场测评阶段、分析与报告编制阶段。测评双方之间的沟通与洽谈贯穿整个等级测评过程。

2023 年 07 月 14 日至 2023 年 07 月 19 日期间为测评准备阶段，测评项目组通过调查表格等方式，完成了茂名职业技术学院 OA 系统基本情况的调查，并针对调研结果进行了静态分析。测评项目组成员熟悉被测定级对象、调试测评工具、准备各种表单等。

2023 年 07 月 20 日至 2023 年 07 月 23 日期间为方案编制阶段，测评项目组编制完成《茂名职业技术学院 OA 系统网络安全等级保护测评方案》，并得到茂名职业技术学院现场测评授权。

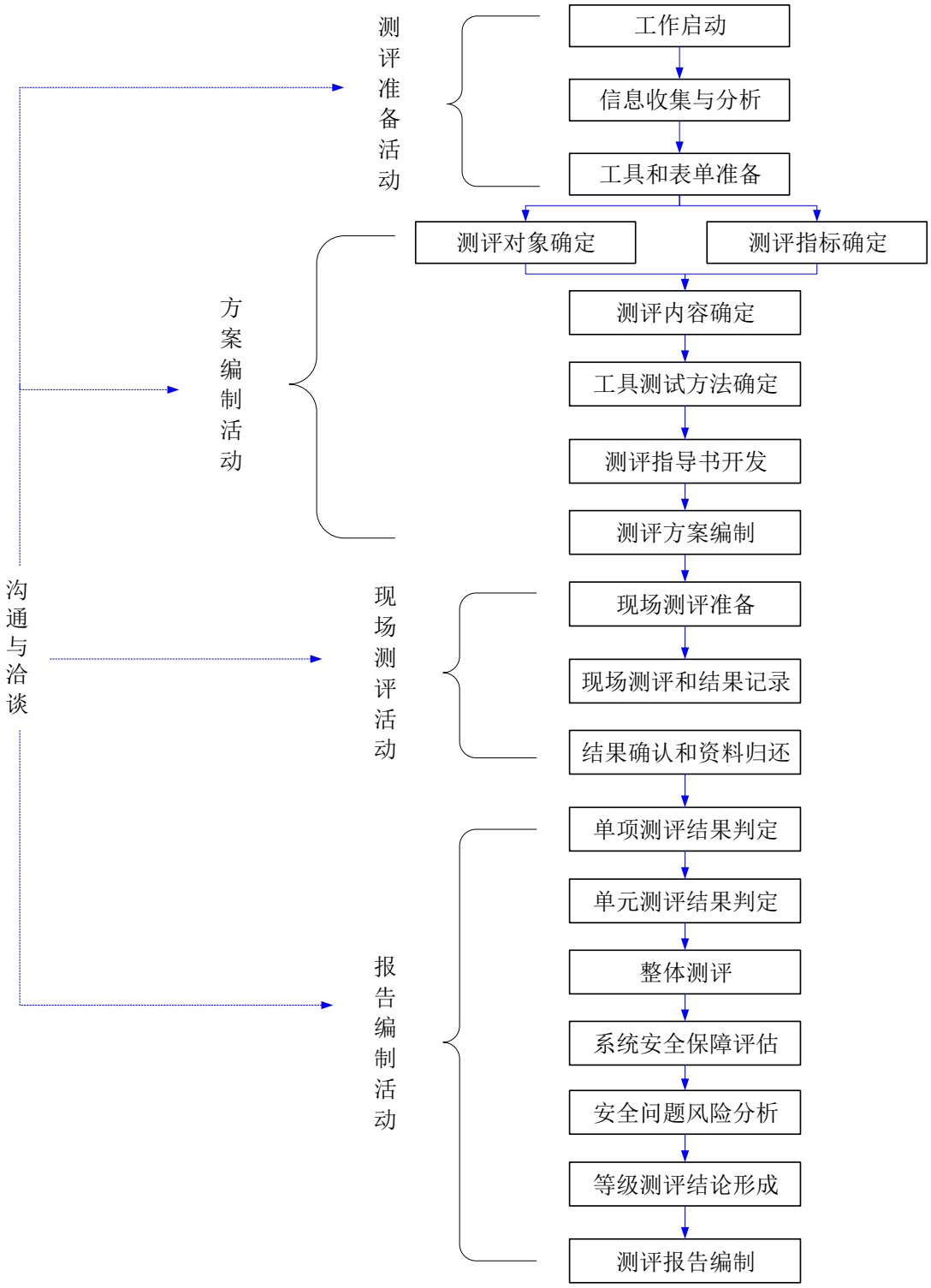
2023 年 07 月 24 日至 2023 年 07 月 27 日期间为现场测评阶段，网络安全等级测评小组按照测评现场工作计划，在茂名职业技术学院开展了网络安全等级保护测评工作。测评组投入相关测试人员，完成了安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面的网络安全等级保护测评。

2023 年 07 月 27 日，测评项目组同茂名职业技术学院召开了网络安全等级保护测评问题会议，就现场安全等级保护测评情况进行了总结，讨论并确认了管理和技术方面所发现的问题，编制问题汇总表。

2023 年 07 月 28 日至 2023 年 08 月 15 日期间为分析与报告编制阶段，测评项目组对现场测评结果进行整理，并与等级保护要求进行差距分析、整体测评，对发现问题进行风险分析和评价，依据此次测评指标完成网络安全等级测评报告

编制工作。

具体流程如下图所示：



1.4 报告分发范围

本报告一式 4 份，其中，2 份提交茂名职业技术学院，1 份提交当地等级保

护工作监管部门，1 份由广东中科实数科技有限公司留存。

2 被测对象描述

2.1 被测对象概述

2.1.1 定级结果

表 2-1 定级结果

被测对象名称	安全保护等级	业务信息安全保护等级	系统服务安全保护等级
OA 系统	2 级	2 级	2 级

2.1.2 业务和采用的技术

茂名职业技术学院 OA 系统是学院实现办公流程话的系统，包括了公文管理、会议管理、流程管理、移动管理、全文检索、高级 office 套件等模块，OA 系统实现了学校办文、办会、办事的规范化，实现了规范流程管理、内控合规管理、标准高效管理。被测对象采用移动互联技术。

2.1.3 网络结构

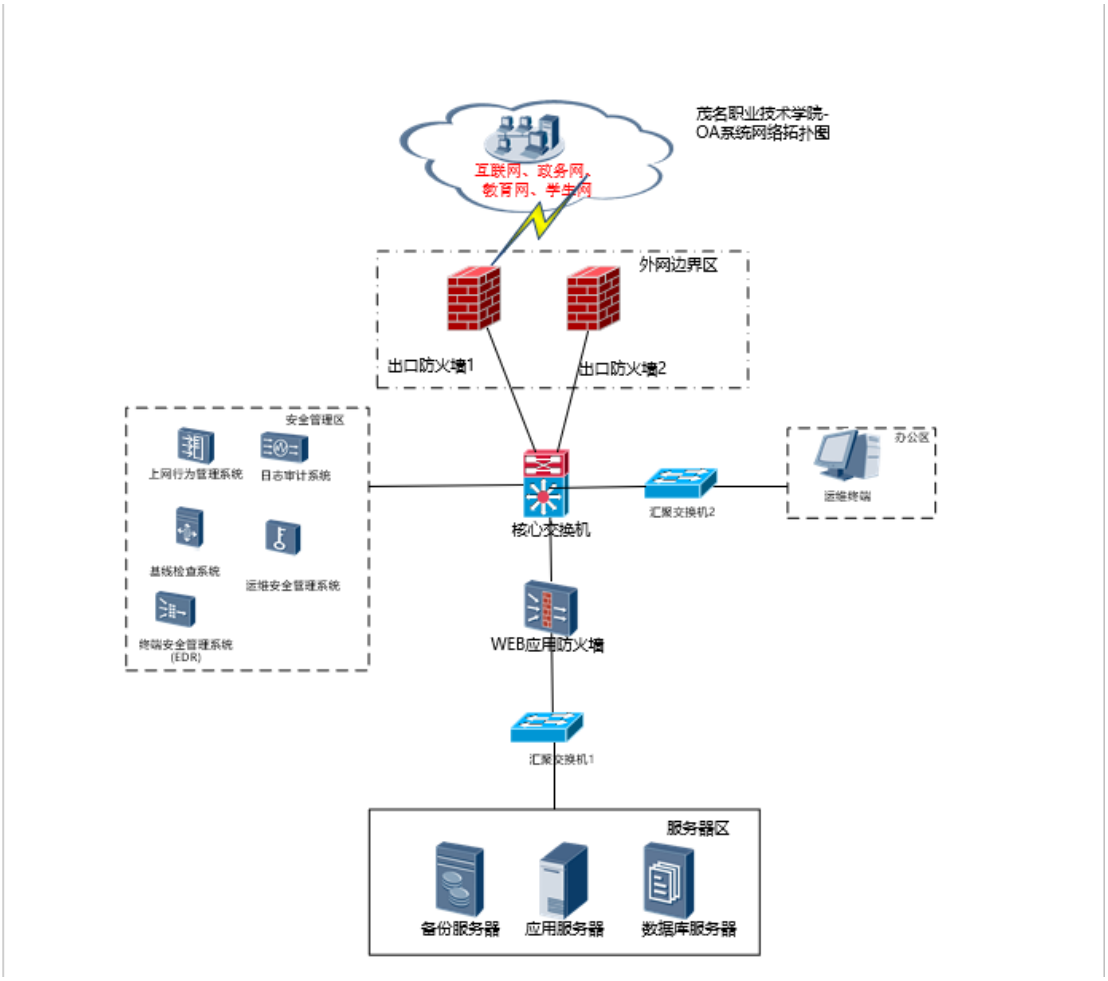


图 2-1 茂名职业技术学院 OA 系统网络拓扑图

被测系统网络出口已采用出口防火墙 1、出口防火墙 2 进行边界防护和访问控制。整体网络根据业务功能/安全需求不同，在核心交换机上划分了安全管理区、服务器区、外网边界区、办公区，并且区域与区域之间的访问通信也在核心交换机上配置较为严格的访问控制策略。

外网边界处已部署出口防火墙具有入侵检测，病毒防护功能，能对系统进出流量进行检测和防护，安全管理区已部署日志审计系统、上网行为管理系统对网络中的安全事件和用户行为进行集中审计；已部署运维安全管理系统对用户的远程登录行为进行审计。办公区已通过核心交换机、上网行为管理系统等

设备实施网络访问控制。服务器区已部署 WEB 应用防火墙对 web 入侵行为进行检测，已部署终端安全管理系统对 OA 系统服务器进行恶意代码防护。

2.2 测评指标

2.2.1 安全通用要求指标

表 2-2 安全通用要求指标

安全类	控制点	测评项数
安全物理环境	物理位置选择	2
	物理访问控制	1
	防盗窃和防破坏	2
	防雷击	1
	防火	2
	防水和防潮	2
	防静电	1
	温湿度控制	1
	电力供应	2
	电磁防护	1
安全通信网络	网络架构	2
	通信传输	1
	可信验证	1
安全区域边界	边界防护	1
	访问控制	4
	入侵防范	1
	恶意代码防范	1
	安全审计	3
	可信验证	1

安全类	控制点	测评项数
安全计算环境	身份鉴别	3
	访问控制	4
	安全审计	3
	入侵防范	5
	恶意代码防范	1
	可信验证	1
	数据完整性	1
	数据备份恢复	2
	剩余信息保护	1
	个人信息保护	2
安全管理中心	系统管理	2
	审计管理	2
安全管理制度	安全策略	1
	管理制度	2
	制定和发布	2
	评审和修订	1
安全管理机构	岗位设置	2
	人员配备	1
	授权和审批	2
	沟通和合作	3
	审核和检查	1
安全管理人员	人员录用	2
	人员离岗	1
	安全意识教育和培训	1
	外部人员访问管理	3

安全类	控制点	测评项数
安全建设管理	定级和备案	4
	安全方案设计	3
	产品采购和使用	2
	自行软件开发	2
	外包软件开发	2
	工程实施	2
	测试验收	2
	系统交付	3
	等级测评	3
	服务供应商选择	2
安全运维管理	环境管理	3
	资产管理	1
	介质管理	2
	设备维护管理	2
	漏洞和风险管理	1
	网络和系统安全管理	5
	恶意代码防范管理	3
	配置管理	1
	密码管理	2
	变更管理	1
	备份与恢复管理	3
	安全事件处置	3
	应急预案管理	2
	外包运维管理	2

安全类	控制点	测评项数
安全通用要求指标数量统计		135

2.2.2 安全扩展要求指标

表 2-3 安全扩展要求指标

扩展类型	安全类	控制点	测评项数
移动互联安全扩展要求	安全物理环境	无线接入点的物理位置	1
	安全区域边界	边界防护	1
	安全区域边界	访问控制	1
	安全区域边界	入侵防范	5
	安全计算环境	移动应用管控	2
	安全建设管理	移动应用软件采购	2
	安全建设管理	移动应用软件开发	2
安全扩展要求指标数量统计			14

2.2.3 其他安全要求指标

本次测评不包含其他安全要求指标。

2.2.4 不适用安全要求指标

表 2-4 不适用安全要求指标

安全类	控制点	不适用项	不适用原因
安全建设管理	产品采购和使用	b)应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。	经核查，该系统未使用密码产品，不适用。
	自行软件开发	a)应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；	经核查，该单位系统为外包软件开发，本项不适用。
		b)应在软件开发过程中对安全	

安全类	控制点	不适用项	不适用原因
		性进行测试，在软件安装前对可能存在的恶意代码进行检测。	
安全运维管理	密码管理	b)应使用国家密码管理主管部门认证核准的密码技术和产品。	经核查，该系统未使用任何密码产品。
	外包运维管理	a)应确保外包运维服务商的选择符合国家的有关规定；	经核查，该单位目前未涉及任何外包运维服务，不适用。
		b)应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。	
安全物理环境（移动互联安全扩展要求）	无线接入点的物理位置	应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。	经核查，OA 系统仅使用 APP，用户通过互联网访问，未采用无线网络组网，该测评项不适用。
安全区域边界（移动互联安全扩展要求）	边界防护	应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。	被测系统 APP 端部署在通用手机上，通过互联网接入，不存在无线接入设备，此项不适用。
	访问控制	无线接入设备应开启接入认证功能，并且禁止使用 WEP 方式进行认证，如使用口令，长度不小于 8 位字符。	
	入侵防范	a)应能够检测到非授权无线接入设备和非授权移动终端的接入行为；	
		b)应能够检测到针对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为；	
		c)应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态；	
		d)应禁用无线接入设备和无线	

安全类	控制点	不适用项	不适用原因
		接入网关存在风险的功能，如：SSID 广播、WEP 认证等；	
		e)应禁止多个 AP 使用同一个认证密钥。	
安全计算环境（移动互联安全扩展要求	移动应用管控	a)应具有选择应用软件安装、运行的功能；	经核查，OA 系统 APP 采用通用手机，不涉及专用移动终端，此项不适用。
		b)应只允许可靠证书签名的应用软件安装和运行。	
表中不适用指标数量			16

2.3 测评对象

2.3.1 测评对象选择方法

本次等级测评中采用抽查的方法兼顾类别与数量，测评原则包括：

- **重要性原则**：应抽查对被测定级对象来说重要的服务器、数据库和网络设备等；
- **安全性原则**：应抽查对外暴露的网络边界；
- **共享性原则**：应抽查共享设备和数据交换平台/设备；
- **全面性原则**：抽查应尽量覆盖系统各种设备类型、操作系统类型、数据库系统类型和应用系统类型；
- **符合性原则**：选择的设备、软件系统等应能符合相应等级的测评强度要求。

茂名职业技术学院 OA 系统为第二级系统。第二级定级对象的等级测评，测评对象的种类和数量都较多，重点抽查重要的设备、设施、人员和文档等，抽查

的测评对象种类主要考虑以下几个方面：

——主机房(包括其环境、设备和设施等)，如果某一辅机房中放置了服务于整个定级对象或对定级对象的安全性起决定作用的设备、设施，那么也应该作为测评对象；

——存储被测定级对象重要数据的介质的存放环境；

——整个系统的网络拓扑结构；

——安全设备，包括防火墙、入侵检测设备、防病毒网关等；

——边界网络设备(可能会包含安全设备)，包括路由器、防火墙和认证网关等；

——对整个定级对象或其局部的安全性起决定作用的网络互联设备，如核心交换机、汇聚层交换机、核心路由器等；

——承载被测定级对象核心或重要业务、数据的服务器(包括其操作系统和数据库)；

——重要管理终端；

——能够代表被测定级对象主要使命的业务应用系统；

——信息安全主管人员、各方面的负责人员；

——涉及到定级对象安全的所有管理制度和记录。

在本级定级对象测评时，定级对象中配置相同的安全设备、边界网络设备、网络互联设备以及服务器应至少抽查两台作为测评对象。

2.3.2 测评对象选择结果

2.3.2.1 物理机房

表 2-5 物理机房

序号	机房名称	物理位置	重要程度
1	信息机房	广东省茂名市文明北路 232 号综合楼 5 楼 501	关键

2.3.2.2 网络设备

表 2-6 网络设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度
1	核心交换机	否	Comware V7	H3C S7500E-X	数据交换、访问控制	关键
2	汇聚交换机 1	否	Release 1119P11	S5560X-30C-EI	数据交换	重要
3	汇聚交换机 2	否	Release 1119P11	S5560X-30C-EI	数据交换	重要

2.3.2.3 安全设备

表 2-7 安全设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度
1	运维安全管理系统	否	深信服 OS V3.0.6	深信服 AC-1000-D603-PT	运维管理	重要
2	基线核查系统	否	深信服 OS V3.0.3	深信服 AC-1000-D602-PT	漏洞扫描	重要
3	出口防火墙 1	否	深信服 OS AF 8.0.23	深信服 AF-2000-H642	访问控制	关键
4	出口防火墙 2	否	深信服 OS AF 8.0.23	深信服 AF-2000-H642	访问控制	关键
5	日志审计	否	深信服 OS	深信服 AC-	日志	重要

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度
	系统		LAS 3.0.5	1000-D601-PT	审计	
6	WEB 应用防火墙	否	深信服 OS AF 8.0.9	深信服 WAF-2000-H642	安全防护	关键
7	终端安全管理系统(EDR)	否	深信服 3.7.2	深信服 AC-1000-D603-PT	病毒查杀	重要
8	上网行为管理系统	否	深信服 OSAC12.0.26.076 Build20190725	深信服 AC-1000-D600-PT	上网行为管理	重要

2.3.2.4 服务器

表 2-8 服务器

序号	设备名称	所属业务应用系统/平台	是否虚拟设备	操作系统及版本	数据库管理系统及版本	中间件及版本	重要程度
1	数据库服务器	OA 系统	是	CentOS 7.9	Oracle 19.3	Tomcat 8.5.82	关键
2	应用服务器	OA 系统	是	CentOS 7.9	-	Tomcat 7.0.69	关键
3	备份服务器	OA 系统	否	CentOS 6.8	-	-	重要

2.3.2.5 终端设备

表 2-9 终端设备

序号	设备名称	是否虚拟设备	操作系统及版本	用途	重要程度
1	运维终端	否	Windows 10 专业版	运维专用	一般

2.3.2.6 其他系统或设备

本次测评不涉及其他系统或设备。

2.3.2.7 系统管理软件/平台

表 2-10 系统管理软件/平台

序号	系统管理软件/平台名称	主要功能	版本	所在设备名称	重要程度
1	中间件 1	信息发布	Tomcat 8.5.82	数据库服务器	关键
2	中间件 2	信息发布	Tomcat 7.0.69	应用服务器	关键
3	数据库	数据存储	Oracle 19.3	数据库服务器	关键
4	UIS 超融合管理平台	搭建云计算环境，实现仅服务器和交换机的极简的硬件架构平台和统一的软件定义数据中心资源池。	V7.0 (E0750P09)	-	关键

2.3.2.8 业务应用系统/平台

表 2-11 业务应用系统/平台

序号	业务应用系统/平台名称	主要功能	业务应用软件及版本	开发厂商	重要程度
1	OA 系统	办公无纸化，流程化	A8+企业版 V8.1	广州致远互联软件有限公司	关键

2.3.2.9 数据资源

表 2-12 数据资源

序号	数据类别	所属业务应用	安全防护需求	重要程度
1	重要配置数据	OA 系统	完整性、可用性	重要
2	重要业务数据	OA 系统	保密性、完整性、可用性	关键
3	重要鉴别数据	OA 系统	保密性、完整性、可用性	关键
4	重要审计数据	OA 系统	完整性、可用性	重要

序号	数据类别	所属业务应用	安全防护需求	重要程度
5	重要个人信息	OA 系统	保密性、完整性、可用性	关键

注：鉴别数据和重要配置数据分别在对应测评对象（网络设备、安全设备、服务器和终端、系统管理软件/平台、业务应用系统/平台）中汇总测评数据，重要审计数据在安全管理中心层面汇总测评数据，本节只汇总重要业务数据、重要个人信息和大数据资源的测评记录。

2.3.2.10 安全相关人员

表 2-13 安全相关人员

序号	姓名	岗位/角色	联系方式	所属单位
1	叶永利	安全主管	0668-2920122	茂名职业技术学院
2	龙恒	安全管理员	13377766618	茂名职业技术学院
3	黄海东	系统管理员	-	茂名职业技术学院
4	麦才赞	审计管理员	-	茂名职业技术学院
5	陈思凡	机房管理员	-	茂名职业技术学院
6	吴国华	网络管理员	-	茂名职业技术学院
7	黄健	资产管理员	-	茂名职业技术学院

2.3.2.11 安全管理文档

表 2-14 安全管理文档

序号	文档名称	主要内容
1	《信息安全总体策略》	单位总体安全策略方针和目录、安全保障体系框架等。
2	《数据安全管理规范.》	数据安全方面的管理规定，包括数据的存放环境、使用规定。
3	《网络安全管理规范》	单位网络方面的管理，包括杀毒，计算机使用等内容。
4	《应用安全管理规范》	关于单位应用系统的日常使用规范文档。
5	《设备操作规程》	关于设备日常操作规范和流程文档。
6	《软件操作手册》	关于单位安全设备操作、Linux 服务器配置手

序号	文档名称	主要内容
		册、主机运维操作手册、软件操作手册、数据库日常运维操作手册等指导文档。
7	《防火墙配置和操作手册》	深信服防火墙配置和操作流程介绍。
8	《信息安全制度管理规范》	关于单位安全管理制度的修订、发布等管理要求。
9	《安全组织及职责管理规定》	关于单位安全管理机构、人员安全管理等内容。
10	《岗位安排及岗位职责》	关于单位人员岗位的配置，包含系统管理员、安全管理员、审计管理员等。
11	《授权和审批管理规定》	单位网络活动的日常审批和授权。
12	《安全组织机构-沟通合作》	日常运维与外部的交流合作。
13	《安全审核与检查管理制度》	关于单位安全检查、审查工作规范制度文档。
14	《安全检查报告 20230321》	单位系统的安全检测报告。
15	《内部人员信息安全管理规定》	关于单位内部员工日常的安全管理。
16	《人员管理制度》	关于单位人员录用、调岗、离岗管理制度文档。
17	《安全教育和培训制度》	关于单位安全培训、安全交流工作制度文档。
18	《外部人员访问管理制度》	关于单位针对外来人员访问管控制度文档。
19	《外部接入受控网络访问系统管理规范》	关于外部人员接入网络的规定和接入流程。
20	《OA 系统专家评审意见表》	关于 OA 系统的专家评审意见表。
21	《信息系统信息安全管理制度汇编 V2.0》	包含单位网络安全、信息安全、人员管理、设备管理等规定的文档。
22	《工程管理制度》	关于单位工程管理工作的文档。
23	《建设方案》	针对 OA 系统开发阶段建设的方案。
24	《测试及验收方案》	单位工程实方案，对时间、进度、质量等进行管理和限制。
25	《系统交付管理》	关于第三方交付系统时的管理文档。

序号	文档名称	主要内容
26	《OA 系统-需求规格说明书 》	关于 OA 系统开发业务需求、功能需求、用户需求等说明。
27	《系统变更管理制度》	关于系统变更流程和变更内容的管理规定。
28	《设备采购合同》	安全设备的采购合同。
29	《机房安全管理制度》	关于单位信息机房的管理文档，包含日常的运维和进出规定内容。
30	《介质安全管理规定》	关于单位介质的存储和传输规范文档。
31	《设备安全管理制度》	关于配套设施、软硬件维护管理方面的管理制度。
32	《网络安全管理规定》	关于网络和系统安全的管理文档。
33	《系统安全管理规定》	关于网络和系统安全的管理文档。
34	《恶意代码防范管理制度》	关于恶意代码防范的管理文档，包括防恶意代码软件的授权使用、恶意代码升级、定期查杀等内容。
35	《密码管理制度》	关于密码方面的管理文档，包括密码的使用和采购内容。
36	《变更控制管理制度》	单位变更管理文档，覆盖了变更管理更方面的要求。
37	《备份与恢复管理制度》	单位备份策略和周期的规定，重要数据日常备份管理。
38	《网络安全事件报告制度》	关于单位网络安全事件管理报告文档。
39	《校园网络信息安全应急预案》	校园应急事件处置流程的文档。

3 单项测评结果分析

单项测评内容包括“2.2.1 安全通用要求指标”、“2.2.2 安全扩展要求指标”和“2.2.3 其他安全要求指标”中涉及的安全类，由已有安全控制措施汇总分析和主要安全问题汇总分析两部分构成，单项测评结果汇总、单项测评结果记录参见报告附录。

3.1 安全物理环境

3.1.1 已有安全控制措施汇总分析

（1）物理位置选择

1）信息机房位于综合楼 5 层 501 室，大楼共 7 层，未设置在建筑物顶层或地下室。

（2）物理访问控制

1）信息机房出入口已安装了福鑫电子门禁系统，通过手机蓝牙和门禁卡对进入人员进行身份鉴别，且机房入口安排了专人值守，门禁系统存在机房进出电子记录表，记录内容包括开门时间、操作人员和打开方式。

（3）防盗窃和防破坏

1）信息机房内服务器、网络设备及安全设备是用螺丝固定在机柜上，能够有效防止设备从机柜上脱落，重要设备和主要部件、线缆设置明显的机打标签，标签内容包括：设备名称、设备编号、项目名称、本端、对端。

2）信息机房采用桥架方式，将通信线缆铺设于机柜上方的线架中。

（4）防雷击

1）信息机房内所有机设施进行了安全接地。

（5）防水和防潮

1）信息机房位于大楼 5 层，机房为封闭式机房，墙壁采用防水防潮建筑材料；机房内未发现渗水漏水等现象。

（6）电力供应

1）信息机房部署 1 组科华 UPS 电源系统，UPS 运行正常，可起到稳压和过电压防护作用。

2）机房部署 1 组科华品牌 UPS 电源系统，正常负荷情况下能保证机房内设备正常运行 30 分钟以上，具有 UPS 巡检和维护记录。

（7）电磁防护

1）机房通信线缆和强电线缆采用桥架方式部署，桥架位于机柜上方，强弱电桥架分开部署，可避免互相干扰。

3.1.2 主要安全问题汇总分析

安全物理环境存在的安全问题有：

（1）未提供机房验收文档，机房防震等级不明确。

无法确认机房所处物理环境是否满足相关要求，不能及时发现机房存在的风险隐患，涉及测评对象：**信息机房。**

（2）未提供火灾自动消防系统的定期巡检和维护的记录。

不能及时了解消防系统的可用性，导致火灾发生时火势不能第一时间被控制并扑灭，可能对机房重要设备造成严重损害，涉及测评对象：**信息机房。**

（3）未提供机房验收文档，无法明确建筑材料的耐火等级。

无法确认机房建筑材料是否具有耐火等级，不能及时发现机房是否存在的火灾隐患，涉及测评对象：**信息机房。**

（4）未部署湿度控制设备，不能防止水蒸气结露。

在机房出现漏水事故时，可能形成积水，如水势蔓延至机房其他区域，造成重要设备损坏，涉及测评对象：**信息机房。**

（5）机房未铺设防静电地板。

可能导致静电无法得到有效释放，静电放电可能会影响数据传输，并可能对精密电子元件造成损害，涉及测评对象：**信息机房。**

（6）未部署机房专用精密空调，不能设置湿度自动调节。

导致机房不能做到恒湿,不利于电子设备的稳定运行,增加了设备故障几率,涉及测评对象：**信息机房。**

3.2 安全通信网络

3.2.1 已有安全控制措施汇总分析

（1）网络架构

1）学校已依据工作职能、重要性、信息重要程度等划分对网络划分多个区域，并为各网络区域分配地址，安全管理区为 172.16.*.0/24，服务器区为 10.1.*.0/22，办公区为 192.168.*.0/24，网络区域与划分原则一致 。

2）网络拓扑图与实际网络运行环境一致，被测网络已在外网边界处有部署出口防火墙，并配置了访问控制策略，重要网段部署在出口防火墙内部，未与外部网络直接相连，已在服务器区部署 WEB 应用防火墙，配置了访问控制策略，可避免非授权的访问。

（2）通信传输

1）服务器、安全设备、网络设备采用 https 协议或 ssh 协议进行远程管理、数据库采用 ssl 协议进行远程管理，应用系统、超融合管理平台采用 https 协议，均可保证通信过程中数据的完整性。

3.2.2 主要安全问题汇总分析

安全通信网络存在的安全问题有：

（1）未基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

无可信链和可信验证，不能通过可信验证技术提高系统自身安全防护能力，不能实现积极主动防御，涉及测评对象：**安全通信网络。**

3.3 安全区域边界

3.3.1 已有安全控制措施汇总分析

（1）边界防护

1）办公区边界处、服务器区边界、安全管理区界处已部署核心交换机，互联网边界处已部署出口防火墙 1、出口防火墙 2 并开启了访问控制策略，能够保证跨越边界的访问和数据流通过受控接口进行通信，不存在绕过边界的途径。

（2）访问控制

1）安全管理区边界处、服务器区边界、办公区边界处在核心交换机上配置了与办公区、服务器区、外网边界之间的访问控制策略，互联网边界处已部署有出口防火墙 1、出口防火墙 2，已配置并启用访问控制策略，最后一条策略默认拒绝所有。

2）核心交换机、出口防火墙 1、出口防火墙 2、web 应用防火墙不存在多余和无效的访问控制策略,设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾，设备的访问控制策略实现最小化。

3)安全管理区边界的核心交换机访问控制策略中已设置源地址、目的地址、源端口、目的端口、协议，管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝。

5）服务器区边界在核心交换机、web 应用防火墙配置了服务器区与安全管理区、边界接入区之间的访问控制策略，策略可对源地址、源端口、目的地址、目的端口、协议进行检测，能对数据包的进出进行检测。

6）出口防火墙 1、出口防火墙 2 已开启访问控制策略对源区域、源地址、目的地址、协议、端口等进行检测，以允许/拒绝数据包进出。

7）办公区边界核心交换机访问控制策略中已设置源地址、目的地址、源端口、目的端口、协议，管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝。

8）出口防火墙 1、出口防火墙 2、WEB 应用防火墙已启用会话认证的访问控制策略，能为进出数据流提供明确的允许/拒绝访问的能力。

（3）入侵防范

1）服务器区边界的 WEB 应用防火墙支持对网络攻击行为防范，设备规则库已更新到最新，支持对端口扫描、强力攻击、木马后门攻击、应用漏洞攻击、网络蠕虫等攻击进行检测和监视。

2）出口防火墙 1、出口防火墙 2 已启用入侵防御策略，入侵防御特征库版本已自动更新至：20230722，可在关键网络节点处监视网络攻击行为。

（4）恶意代码防范

1）出口防火墙 1、出口防火墙 2 已启用病毒防护功能，并且病毒库已自动更新至 20230722，可对恶意代码进行检测和清除。

2）已在服务器边界部署 WEB 应用防火墙，WEB 应用防火墙具备防恶意代码功能，恶意代码规则库已更新至最新，可对网络节点的恶意代码进行检测和清除。

（5）安全审计

1）服务器边界处已部署 WEB 应用防火墙，已对重要节点进行审计，包括流量检测和行为检测，审计覆盖到每个用户，已对重要的用户行为和重要安全事件

进行审计。

2）外网边界部署了出口防火墙 1、出口防火墙 2，已开启安全审计功能，并且防火墙已制定详细的访问控制规则和启用入侵防御和恶意代码检测功能，可对边界的流量进行审计和对边界的安全事件进行审计，审计覆盖到每个用户。

3）出口防火墙 1、出口防火墙 2 的流量事件审计记录包括：用户、应用、策略类型、处理动作、终端类型、级别、事件；入侵防御日志审计记录包括：攻击源、攻击时间、攻击描述、影响服务器、所处阶段，病毒防护审计记录包括：时间、日志级别、用户名称、源地址、源端口、目的地址、目的端口、归属地、病毒名称。

4）WEB 应用防火墙审计记录包括事件日期、时间、用户、攻击类型、攻击源 IP 等内容。

5）WEB 应用防火墙审计日志仅授权用户可进行访问，对审计记录进行保护，测评时间为 2023 年 7 月 24 日，可查看到 2022 年 11 月 8 日之前的审计日志，保存周期大于 6 个月，审计日志已传输至日志审计系统审计和保护，避免受到未预期的删除、修改或覆盖。

6）出口防火墙 1、出口防火墙 2 日志记录已配置上传至日志审计系统保存备份，审计日志仅授权用户可进行访问，对审计记录进行保护，日志记录无法删除、修改或覆盖，测评时间为 2023 年 7 月 24 日，可查看到 2022 年 11 月 08 日之前的审计日志，保存周期大于 6 个月。

3.3.2 主要安全问题汇总分析

安全区域边界存在的安全问题有：

（1）未根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。

无法对来自外部非可信网络的网络通信进行控制，极易存在被网络攻击的风险，涉及测评对象：**办公区边界、安全管理区边界。**

（2）未部署入侵防御系统或者有入侵防御模块的防火墙，因而不可对网络攻击行为进行监视。

增加了应用系统受到网络攻击的风险，涉及测评对象：**安全管理区边界、办公区边界。**

（3）未部署有防病毒网关或者有防病毒模块的防火墙，因而未能对恶意代码进行检测和清除。

无法检测潜在的恶意代码，可能会造成恶意代码流入系统造成破坏的风险，涉及测评对象：**办公区边界、安全管理区边界。**

（4）无法对边界的流量和边界的安全事件进行审计。

安全审计功能不完善可能导致安全审计员无法利用审计日志对部分安全事件予以准确定位和追溯，涉及测评对象：**安全管理区边界、办公区边界。**

（5）不能对边界的流量和边界的安全事件进行审计，故缺少边界的流量审计和安全事件审计记录。

安全审计功能不完善可能导致审计员无法利用审计记录对安全事件予以准确定位和追溯，涉及测评对象：**办公区边界、安全管理区边界。**

（6）不能对边界的流量和边界的安全事件进行审计，故无法对审计记录进行保护和备份。

未对审计记录进行保护可能导致审计员无法利用审计记录对安全事件予以准确定位和追溯，涉及测评对象：**安全管理区边界、办公区边界。**

（7）未基于可信根对边界设备的系统引导程序、系统程序、重要配置参数

和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

无可信链和可信验证，不能通过可信验证技术提高系统自身安全防护能力，不能实现积极主动防御，涉及测评对象：**办公区边界、外网区边界、服务器区边界、安全管理区边界。**

3.4 安全计算环境

3.4.1 网络设备

3.4.1.1 已有安全控制措施汇总分析

（1）身份鉴别

1）核心交换机、汇聚交换机 1、汇聚交换机 2 采用用户名+口令对登录的用户进行身份标识和鉴别，不存在同名账户，身份标识具有唯一性，交换机已设置口令长度为 8 位，由数字、小写字母、大写字母和特殊字符组合而成，已开启口令 180 天定期更换策略。

2）核心交换机、汇聚交换机 1、汇聚交换机 2 已开启登录失败处理功能，失败 10 次锁定 5 分钟，已设置超时 15 分钟自动退出。

3）核心交换机、汇聚交换机 1、汇聚交换机 2 采 ssh 远程登录，已禁用 telnet 远程通信，可防止鉴别信息在网络传输过程中被窃听。

（2）访问控制

1）汇聚交换机 1、汇聚交换机 2 分配了系统管理员 super、安全管理员 long，审计管理员 shenjiyuan，已对登录的用户分配账户和权限，并且不存在默认账户和匿名账户。

2）核心交换机已对登录的用户分配权限，存在网络管理员 super、操作管理

员 long、 操作管理员 nwctrl。

3）核心交换机、汇聚交换机 1、汇聚交换机 2 不存在默认账户，不存在默认口令。

4）核心交换机、汇聚交换机 1、汇聚交换机 2 不存在多余、过期账户，无共享账户。

5）汇聚交换机 1、汇聚交换机 2 存在系统管理员 super、安全管理员 long，审计管理员 shenjiyuan，不同用户具备不同的访问权限，已授予管理用户最小权限，实现管理用户的权限分离。

6）核心交换机已授予用户最小权限，已建立存在网络管理员 super、操作管理员 long、操作管理员 nwctrl，网络审计员 shenjiyuan，不同账户具备不同的访问权限，已实现管理用户的权限分离。

（3）安全审计

1)核心交换机、汇聚交换机 1、汇聚交换机 2 已开启日志 Information Center、Security log 审计功能，审计覆盖到每个用户，已对重要的用户行为和重要安全事件进行审计。

2）汇聚交换机 1、汇聚交换机 2 审计记录包括事件的日期、时间、类型、主体标识、客体标识，结果、身份鉴别时间请求的来源。

3）核心交换机的审计记录包括日期时间、用户、登录 ip、登录是否成功、操作命令记录等审计信息。

4）汇聚交换机 1、汇聚交换机 2、核心交换机审计记录已上传到日志审计系统进行备份审计，仅审计管理员可以查看日志，审计记录最早可以查看 20220630，日志保存时间少于六个月，日志记录无法删除、修改或覆盖。

（4）入侵防范

1）核心交换机、汇聚交换机 1、汇聚交换机 2 不存在默认共享，已关闭不需要的系统服务：Telnet、http、ftp 等，已关闭不需要的高危端口：445、137、138、139、21 等。

2）核心交换机、汇聚交换机 1、汇聚交换机 2 已对管理终端地址进行限制，限制地址为 192.168.*.32-192.168.*.47 ，192.168.*.0-192.168,*.31。

（5）数据完整性

1）核心交换机、汇聚交换机 1、汇聚交换机 2 采用 ssh 协议进行通信，能保证重要数据在传输过程中的完整性。

3.4.1.2 主要安全问题汇总分析

安全计算环境网络设备存在的安全问题有：

（1）未定期进行漏洞扫描。

不能及时发现系统中存在的漏洞，并对漏洞进行修补，可能导致恶意人员利用系统漏洞对系统进行攻击，涉及测评对象：**核心交换机、汇聚交换机 1、汇聚交换机 2。**

（2）未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

无可信链和可信验证，不能通过可信验证技术提高系统自身安全防护能力，不能实现积极主动防御，涉及测评对象：**核心交换机、汇聚交换机 1、汇聚交换机 2。**

（3）未有备份恢复测试记录。

一旦出现故障，可能无法恢复数据，造成重要数据丢失，涉及测评对象：**核心交换机、汇聚交换机 1、汇聚交换机 2。**

（4）未利用通信网络将关键数据定时批量传送至备用场地。

如机房遭受严重破坏,可能导致数据完全丢失,涉及测评对象:**核心交换机、汇聚交换机 1、汇聚交换机 2。**

3.4.2 安全设备

3.4.2.1 已有安全控制措施汇总分析

（1）身份鉴别

1）基线核查系统、日志审计系统、安全运维管理系统、终端安全管理系统、WEB 应用防火墙、出口防火墙 1、上网行为管理系统、出口防火墙 2 采用用户名加口令的方式对用户登录进行身份鉴别；不存在空口令用户；以用户名作为用户身份唯一性标识;已配置符合复杂度要求的密码策略(口令长度设置至少 8 位，必须包含数字、大写字母、小写字母、特殊字符其中 3 种)，已开启口令超过 90 天强制修改。

2）出口防火墙 1、出口防火墙 2 已配置非法登录 10 次后锁定账户 5 分钟，已配置登录连接超时自动退出时长为 30 分钟。

3）上网行为管理系统已配置非法登录 5 次后锁定账户 1 分钟，已配置登录连接超时自动退出时长为 20 分钟。

4）WEB 应用防火墙已配置非法登录 10 次后锁定账户 5 分钟，已配置登录连接超时自动退出时长为 100 分钟。

5）运维安全管理系统已配置非法登录 5 次后锁定账户 2 分钟，已配置登录连接超时自动退出时长为 30 分钟。

6）终端安全管理系统、日志审计系统、基线核查系统已配置非法登录 5 次后锁定账户 5 分钟，已配置登录连接超时自动退出时长为 10 分钟。

7）基线核查系统、日志审计系统、终端安全管理系统、运维安全管理系统、WEB 应用防火墙、出口防火墙 1、上网行为管理系统、出口防火墙 2 在通信过程中采用 https 协议传输数据，用户口令信息加密传输，可防止鉴别信息在网络传输过程中被窃听。

（2）访问控制

1）出口防火墙 1、出口防火墙 2、上网行为管理系统、运维安全管理系统、WEB 应用防火墙、终端安全管理系统、日志审计系统、基线核查系统对可登录用户进行了账户和权限分配，包括超级管理员 admin、系统管理员 systemadmin、审计管理员 auditadmin、安全管理员 securityadmin 等账户，不同账户具备不同的访问权限。

2）出口防火墙 1、出口防火墙 2、上网行为管理系统、运维安全管理系统、WEB 应用防火墙、终端安全管理系统、日志审计系统、基线核查系统存在默认账户 admin 无法修改、删除，但口令已修改为复杂口令。

3）出口防火墙 1、出口防火墙 2、上网行为管理系统、运维安全管理系统、WEB 应用防火墙、终端安全管理系统、日志审计系统、基线核查系统未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。

4）出口防火墙 1、出口防火墙 2、上网行为管理系统、运维安全管理系统、WEB 应用防火墙、终端安全管理系统、日志审计系统、基线核查系统设置了超级管理员 admin、系统管理员 systemadmin、审计管理员 auditadmin、安全管理员 securityadmin 等账户，不同账户具备不同的访问权限，且各账户权限均为工作所

需最小权限。并且已限制超级管理员 admin 的使用，admin 需要经过审批才能使用。

（3）安全审计

1）出口防火墙 1、出口防火墙 2、上网行为管理系统、运维安全管理系统、WEB 应用防火墙、终端安全管理系统、日志审计系统、基线核查系统已开启安全审计功能，可对所有重要的用户行为和重要安全事件进行审计，审计范围覆盖系统内所有用户。

2）基线核查系统日志审计记录包括：序号、组件名称、日志级别、日志内容、日志产生时间。

3）日志审计系统审计记录包括用户日志和系统日志，用户日志：序号、日志级别、日志内容、日志产生时间；系统日志：序号、组件名称、日志级别、日志内容、日志产生时间。

4）终端安全管理系统日志审计记录包括：序号、操作时间、用户、ip 地址、操作类型、操作对象、操作描述、操作结果。

5）运维安全管理系统日志审计记录包括：序号、时间、账号、登录地址、用户、模块、操作、操作结果等信息。

6）WEB 应用防火墙日志审计记录包括：序号、管理员、账号类型、操作方式、主机 IP、操作对象、操作、日期时间、描述、详情等信息。

7）上网行为管理系统日志审计记录包括：序号、来源、类型、时间、详细信息等信息。

8）出口防火墙 2、出口防火墙 1 日志审计记录包括：序号、管理员、账号类型、操作方式、主机 IP、操作对象、操作、日期时间、描述、详情等信息。

9）出口防火墙 1、出口防火墙 2、上网行为管理系统、WEB 应用防火墙、日志审计系统、基线核查系统、运维安全管理系统审计日志仅授权用户可进行访问，对审计记录进行保护，测评时间为 2023 年 07 月 24 日，可查看到 2022 年 11 月 8 日之前的审计日志，保存周期大于 6 个月，审计日志已传送至日志审计系统进行审计。

（4）入侵防范

1）基线核查系统、日志审计系统、运维安全管理系统、上网行为管理系统、WEB 应用防火墙、出口防火墙 1、出口防火墙 2、终端安全管理系统遵循最小安装原则，未安装不必要的组件和应用程序。

2）基线核查系统、日志审计系统、运维安全管理系统、上网行为管理系统、WEB 应用防火墙、出口防火墙 1、出口防火墙 2、终端安全管理系统不存在不必要的默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的服务。

17）已对基线核查系统、日志审计系统、运维安全管理系统、上网行为管理系统、WEB 应用防火墙、出口防火墙 1、出口防火墙 2、终端安全管理系统的终端地址范围进行了限制，仅有 10.253.*.0-10.253.*.255、192.168.*.31-192.168.*.47、192.168.*.0-192.168.*.31 网段地址能够访问。

（5）数据完整性

基线核查系统、日志审计系统、运维安全管理系统、上网行为管理系统、WEB 应用防火墙、出口防火墙 1、出口防火墙 2、终端安全管理系统在通信过程中采用 https 协议传输数据，可保证重要数据在传输过程中的完整性。

3.4.2.2 主要安全问题汇总分析

安全计算环境安全设备存在的安全问题有：

（1）审计记录保存时间不足六个月。

无法对安全事件进行追溯和分析，同时无法及时了解设备实际运行状况以及可能存在的安全隐患，涉及测评对象：**终端安全管理系统（EDR)。**

（2）未定期进行漏洞扫描。

不能及时发现系统中存在的漏洞，并对漏洞进行修补，可能导致恶意人员利用系统漏洞对系统进行攻击，涉及测评对象：**运维安全管理系统、基线核查系统、出口防火墙 1、出口防火墙 2、日志审计系统、WEB 应用防火墙、上网行为管理系统、终端安全管理系统（EDR)。**

（3）未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

无可信链和可信验证，不能通过可信验证技术提高系统自身安全防护能力，不能实现积极主动防御，涉及测评对象：**运维安全管理系统、基线核查系统、出口防火墙 1、出口防火墙 2、日志审计系统、WEB 应用防火墙、上网行为管理系统、终端安全管理系统（EDR)。**

（4）未有备份恢复测试记录。

一旦出现故障，可能由于各种原因无法利用备份数据进行恢复，造成重要数据丢失，涉及测评对象：**运维安全管理系统、基线核查系统、出口防火墙 1、出口防火墙 2、日志审计系统、WEB 应用防火墙、上网行为管理系统、终端安全管理系统（EDR)。**

（5）未利用通信网络将关键数据定时批量传送至备用场地。

如机房遭受严重破坏，可能导致数据完全丢失，涉及测评对象：**运维安全管理系统、基线核查系统、出口防火墙 1、出口防火墙 2、日志审计系统、WEB 应用防火墙、上网行为管理系统、终端安全管理系统（EDR）。**

3.4.3 服务器和终端

3.4.3.1 已有安全控制措施汇总分析

（1）身份鉴别

1）应用服务器、数据库服务器采用账户名+口令方式进行登录，身份标识唯一，不存在空口令账户；已配置口令复杂度策略，口令须包含数字、大写字母、小写字母，长度不少于 8 位；已配置口令有效期为 90 天。

2）运维终端采用账户名+口令方式进行登录，身份标识唯一，不存在空口令账户；已启用“密码必须符合复杂性要求”，口令须包含数字、大写字母、小写字母和特殊字符中三类，“密码长度最小值”为 8 个字符，“密码最长使用期限”为 180 天。

3）数据库服务器、应用服务器登录失败 5 次锁定 3 分钟，操作闲置 5 分钟自动退出。

4）应用服务器、备份服务器、数据库服务器未启用 Telnet 服务，采用 SSH 协议进行远程管理，可防止鉴别信息在网络传输过程中被窃听。

（2）访问控制

1）运维终端已对登录的用户分配账户和权限，已为登录的用户配置系统管理员账户：admin、mmzy、安全管理员账户：anquan、审计管理员账户：shenji。

2）应用服务器、备份服务器、数据库服务器系统默认账户 root 不宜重命名，

登录口令已修改为复杂口令。

3）运维终端不存在默认账户。

4）应用服务器、备份服务器、数据库服务器、运维终端已禁用多余账户，不存在过期账户 ，不存在共享账户的情况。

5）备份服务器、应用服务器、超级管理员账户、数据库服务器已配置系统管理员账户：sangfor，审计管理员账户：shenji，安全管理员账户：anquan，普通账户：peanut001，账户权限已分离。运维终端已为登录的用户配置系统管理员账户：admin/mmzy、安全管理员账户：anquan、审计管理员账户：shenji，账户权限已分离分别拥有其工作所需的最小权限。

（3）安全审计

1）运维终端审计服务 Windows Event Log 运行正常，运维终端本地审核策略均已设置为“成功、失败”，审计覆盖每个用户，可对重要的用户行为和安全事件进行审计。

2）应用服务器、备份服务器、数据库服务器已开启 rsyslog 系统日志和 auditd 安全审计功能，守护进程运行正常， 审计覆盖到每个用户，可实现对重要的用户行为和重要安全事件的安全审计。

3）应用服务器、备份服务器、数据库服务器审计记录包括 message、audit 等审计记录，message 日志及 secure 日志包括：日期、时间、服务器、进程、详细信息等内容；wtmp 日志包括：账户名、登录方式、日期、时间、终端 IP 地址等内容；audit 日志包括：类型、时间戳、事件 ID、进程 ID、用户名、执行命令、是否成功等内容。

4）运维终端审计记录包含：级别、日期和时间、来源、事件 id、任务类别、

关键字等审计相关信息。

5）备份服务器重要日志文件及日志配置文件权限值均未超过 644，仅授权用户可管理，已纳入日志审计系统的审计范围，可避免日志受到未预期的删除、修改或覆盖等，现场测评时间为 2023 年 7 月 24 日，日志最早可查询时间为 2023 年 1 月 3 日，日志留存时间满足六个月。

（4）入侵防范

1）应用服务器、备份服务器、数据库服务器、运维终端遵循最小安装原则，未安装多余的组件和应用程序。

2）应用服务器、备份服务器、数据库服务器、运维终端不存在不必要的默认共享，已通过系统防火墙严格限制 80、21、23、25、135、139、445 等端口的访问规则，已禁用不必要的服务。

3）已通过服务器区防火墙限制仅 10.1.15.*、192.168.*.0/27 可远程登录应用服务器、备份服务器、数据库服务器。

4）已部署深信服终端安全管理系统，应用服务器、备份服务器、数据库服务器已安装深信服终端安全管理系统 Agent，漏洞库更新于 2023 年 07 月 22 日，已设置自动扫描任务，每天 0 点对备份服务器进行一次漏洞扫描，近期扫描记录中未发现安全漏洞，且在本次漏洞扫描中未发现已知的风险漏洞。

5）已安装 360 安全卫士，可对运维终端进行漏洞管理，近期漏洞扫描结果未发现已知漏洞，有系统补丁安装记录。在本次漏洞扫描中未发现存在已知的风险漏洞。

（5）恶意代码防范

1）运维终端已安装 360 杀毒，能及时识别和防范病毒行为，已通过互联网

自动实时更新病毒库，360 杀毒病毒库版本：5.0.0.8170，更新时间 2023 年 7 月 22 日，现场测评时间：2023 年 7 月 24 日。

2）应用服务器、备份服务器、数据库服务器已部署深信服终端安全管理系统，已安装深信服终端安全管理系统 Agent，能及时识别入侵和病毒行为，病毒库最近更新时间为 2023 年 07 月 22 日，现场测评时间为 2023 年 07 月 24 日。

（6）数据完整性

1）应用服务器、备份服务器、数据库服务器在通信过程中采用 ssh 协议传输数据，可保证重要数据在传输过程中的完整性。

（7）剩余信息保护

1）应用服务器、备份服务器、数据库服务器为 Linux 操作系统，用户的鉴别信息所在的存储空间由操作系统自动分配， Linux 自身资源回收机制可满足剩余信息保护。

2）运维终端已启用“交互式登录：不显示上次登录”和“关机：清除虚拟内存页面文件”，可能保证鉴别数据被释放前得到完全清除。

3.4.3.2 主要安全问题汇总分析

安全计算环境服务器和终端存在的安全问题有：

（1）未配置口令有效期策略。

账户口令可能被长时间使用，恶意人员可通过猜解或暴力破解的方式获取账户口令，存在非授权访问的风险，涉及测评对象：**备份服务器。**

（2）未配置登录失败处理策略及登录连接超时策略。

恶意人员可通过暴力破解的方式获取账户口令。且设备易被非授权人员恶意操作，存在非授权访问的风险，涉及测评对象：**备份服务器。**

（3）未配置屏幕保护程序。

设备易被非授权人员恶意操作，存在非授权访问的风险，涉及测评对象：**运维终端。**

（4）进行远程管理时，鉴别信息通过不安全的协议进行传输。

账号、口令等通过不安全的协议进行传输，可能导致敏感信息被恶意人员嗅探并盗用，存在非授权访问的风险，涉及测评对象：**运维终端。**

（5）未禁止 root 账户远程登录。

恶意人员可能利用默认账户对系统进行试探攻击，存在潜在的安全隐患，涉及测评对象：**数据库服务器、应用服务器、备份服务器。**

（6）审计记录保存时间不足六个月。

无法对安全事件进行追溯和分析，同时无法及时了解设备实际运行状况以及可能存在的安全隐患，涉及测评对象：**数据库服务器、应用服务器。**

（7）审计记录仅保存在本机，未进行定期备份。

日志记录容易受到恶意篡改、删除，不便于对安全事件进行追踪和分析，涉及测评对象：**运维终端。**

（8）未严格限制终端登录地址范围。

恶意用户可从网内任意地址尝试对设备进行访问、攻击，存在非授权访问的风险，涉及测评对象：**运维终端。**

（9）未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

无可信链和可信验证，不能通过主动免疫可信验证技术提高系统自身安全防

护能力，不能实现积极主动防御，涉及测评对象：**数据库服务器、应用服务器、备份服务器、运维终端。**

（10）未配置“远程（RDP）连接要求使用指定的安全层”为“SSL”和未配置“设置客户端连接加密级别”为“高级别”，不能保证重要数据在传输过程中的完整性。

可能导致重要数据在传输过程中被攻击者劫持、篡改，使重要数据的完整性遭到破坏，涉及测评对象：**运维终端。**

（11）未有备份恢复测试记录。

一旦出现故障，可能由于各种原因无法利用备份数据进行恢复，造成重要数据丢失，涉及测评对象：**数据库服务器、应用服务器、备份服务器。**

（12）未利用通信网络将关键数据定时批量传送至备用场地。

如机房遭受严重破坏，可能导致数据完全丢失，涉及测评对象：**数据库服务器、应用服务器、备份服务器。**

3.4.4 系统管理软件/平台

3.4.4.1 已有安全控制措施汇总分析

（1）身份鉴别

1）数据库采用账户名＋口令的方式登录，身份标识具有唯一性，不存在空口令账户；已配置口令复杂度策略，口令须包含数字、大写字母和小写字母，不少于 8 位；口令有效期为 180 天。

2）数据库登录失败 5 次锁定一天，超时退出时间为 10 分钟。

3）UIS 超融合管理平台登录失败 3 次锁定 1 分钟，操作员闲置 60 分钟自动退出。

4）UIS 超融合管理平台采用 HTTPS 协议进行远程管理，可防止鉴别信息在网络传输过程中被窃听。

5）数据库已采用 ssl 协议进行远程管理，可防止鉴别信息在网络传输过程中被窃听。

（2）访问控制

1）数据库已对登录的用户分配账户和权限，已配置系统管理员账户 SYS、SYSTEM，业务账户 OAUSER、WXUSER、ETL_USER，备份账户：OABACKUP。

2）UIS 超融合管理平台已对登录的用户分配账户和权限，已配置系统管理员账户 super、安全管理员账户 anquanguanliyuan、审计管理员账户 shenjiguanliyuan。

3）系统不存在默认账户，不存在默认口令。

4）数据库未重命名默认账户 SYS、SYSTEM、SYSMAN、SCOTT、DBSNMP，但账户 SYSMAN、SCOTT、DBSNMP 已被锁定，账户 SYS、SYSTEM 不宜重命名，口令已修改为复杂口令。

5）数据库已禁用多余账户，不存在过期账户 ，不存在共享账户的情况。

6）UIS 超融合管理平台无多余账户，不存在过期账户 ，不存在共享账户的情况。

7）UIS 超融合管理平台设置了系统管理员账户 super、安全管理员账户 anquanguanliyuan、审计管理员账户 shenjiguanliyuan，账户权限已分离，分别拥有其工作所需的最小权限。

（3）安全审计

1）数据库已对普通用户开启审计功能，已启用对所有用户的重要行为进行

审计，已启用对 SYSDBA 或 SYSOPER 特权连接时直接发出的 SQL 语句进行审计。

2）中间件 1、中间件 2 已开启安全审计功能，在日志配置中已开启 Cataline 引擎日志、控制台输出日志、manager 应用日志和内部代码丢出的日志，审计覆盖到每个用户，能对重要的用户行为和重要安全事件进行审计。

3）UIS 超融合管理平台已开启操作日志和安全审计功能，审计功能运行正常， 审计覆盖到每个用户，可实现对重要的用户行为和重要安全事件的安全审计。

4）UIS 超融合管理平台审计记录包括登录名、操作员名称、完成时间、登录地址、操作分类、操作对象、操作描述、执行结果、失败原因、风险级别和事件类型。

5）中间件 1、中间件 2 的日志审计结果包含：事件的日期和时间、用户、事件类型、操作 IP、动作、结果等。 中间件所在的服务器的操作系统时间与北京时间一致。

6）数据库告警日志记录了 id、日期、时间、用户、操作、事件、结果等信息。

（4）入侵防范

1）UIS 超融合管理平台在数据输入界面提供有效性校验功能，可对无效或非法数据、字符长度和有效性进行校验。

2）已部署深信服终端安全管理系统，中间件 1、中间件 2、数据库所在服务器已安装深信服终端安全管理系统 Agent，已设置自动扫描任务，每天 0 点对应用服务器进行一次漏洞扫描，近期扫描记录中未发现安全漏洞，且在本次漏洞扫

描中未发现已知的风险漏洞。

（5）数据完整性

1）数据库已采用 ssl 协议进行远程管理，可保证重要数据在传输过程中的完整性。

2）中间件 1、中间件 2 未提供独立的登录管理界面，数据的传输完整性由应用服务器操作系统实现，应用服务器在通信过程中采用 ssh 协议传输数据，可保证重要数据在传输过程中的完整性。

3）UIS 超融合管理平台在通信过程中采用 HTTPS 协议传输数据，可保证重要数据在传输过程中的完整性。

（6）剩余信息保护

1）UIS 超融合管理平台登出后不保存上次登录信息，资源回收机制可满足剩余信息保护。

2）数据库登出后不记录账号和口令，数据库系统资源释放或清除机制正常且满足要求。

（7）个人信息保护

1）数据库仅采集和保存必需的用户个人信息，如职工的姓名、部门、岗位、职级、人员类型、人员状态等。

2）系统中保存的个人信息仅授权用户可访问，非授权用户无法访问及使用，已制定相关制度明确个人信息保护的相关管理要求和流程规定。

3.4.4.2 主要安全问题汇总分析

安全计算环境系统管理软件平台存在的安全问题有：

（1）未配置口令有效期策略。

账户口令可能且长时间使用，存在非授权访问的风险，涉及测评对象：**UIS 超融合管理平台。**

（2）未设置审计管理、安全管理员账户，未实现管理用户的权限分离。

无法实现不同权限角色间的监督,存在管理账户越权管理或滥用权限的风险，涉及测评对象：**数据库。**

（3）审计记录保存时间不足六个月。

日志记录容易受到恶意篡改、删除，不便于对安全事件进行追踪和分析，涉及测评对象：**中间件 1、中间件 2、数据库、UIS 超融合管理平台。**

（4）未定期进行漏洞扫描。

不能及时发现系统中存在的漏洞，并对漏洞进行修补，可能导致恶意人员利用系统漏洞对系统进行攻击，涉及测评对象：**UIS 超融合管理平台。**

（5）未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

无可信链和可信验证,不能通过主动免疫可信验证技术提高系统自身安全防护能力，不能实现积极主动防御，涉及测评对象：**UIS 超融合管理平台。**

（6）未有备份恢复测试记录。

一旦出现故障，可能由于各种原因无法利用备份数据进行恢复，造成重要数据丢失，涉及测评对象：**中间件 1、中间件 2、数据库、UIS 超融合管理平台。**

（7）未利用通信网络将关键数据定时批量传送至备用场地。

如机房遭受严重破坏，可能导致数据完全丢失，涉及测评对象：**中间件 1、中间件 2、数据库、UIS 超融合管理平台。**

3.4.5 业务应用系统/平台

3.4.5.1 已有安全控制措施汇总分析

（1）身份鉴别

1）OA 系统采用用户名+口令+验证码后台登录或通过统一身份验证平台登录（账号登录：用户名+口令；动态码登录：用户名+验证码+动态码；微信扫描登录)；APP 端采用用户名+口令+验证码进行身份鉴别，身份标识唯一，不存在同名用户，不存在空口令用户；系统已开启密码安全设置功能，密码强度设置为中，由大写字母，小写字母和字符中的任意两种组成，长度不小于 8 位，口令设置 180 天定期更换。

2）OA 系统、AAP 端已开启登录失败处理功能，失败 5 次锁定 3 小时，系统和 AAP 端已有超时自动退出功能，30 分钟超时自动退出。

3）OA 系统、AAP 端在通信过程中采用 https 协议传输数据，用户口令信息加密传输，可防止鉴别信息在网络传输过程中被窃听。

（2）访问控制

1）OA 系统已对登录的用户分类账户和权限，系统角色包括系统管理员、安全审计员、单位管理员、普通人员、编外人员等角色，不同角色具备不同的权限。

2）OA 系统用户采用实名登录，不存在默认账户，用户首次登录需要强制修改口令，不存在默认口令。

3）OA 系统用户为学校的教师、领导，已设置 60 天账号不登录自动停用，不存在多余、过期的账户，账户对应到学校教师个人，不存在共享账户。

4）OA 系统已授予管理用户最小权限，包括系统管理员、单位管理员、安全审计员，实现管理用户的权限分离。

（3）安全审计

1）OA 系统、APP 端已开启安全审计功能，包括登录日志、应用日志，审计覆盖到每个用户，已对重要的用户行为和事件进行审计。

2）OA 系统的登录日志包括人员、登录名、部门、岗位、登录时间、退出时间、在线时长、IP 地址；应用日志包括操作人员、操作人员登录名、操作类型、操作描述、操作时间、IP 地址、所在单位、操作结果、操作模块；APP 端审计日志包括人员、登录名、部门、岗位、登录时间、退出时间、在线时长、IP 地址。

3）OA 系统、APP 端已对审计记录进行保护，仅安全审计员和系统管理员能进行查看，已定期每天备份日志到数据库服务器，日志一直保存，测评时间为 2023 年 7 月 24 日，可查看到 2022 年 11 月 8 日之前的日志，保存周期大于 6 个月。

（4）入侵防范

1）OA 系统、APP 端已设置上传文件的后缀，对 aps、jsp、jspx、HTML、ascx、ashx、cer 等格式进行限制。输入框禁止*、？、 、%等特殊字符的输入。

（5）数据完整性

1）OA 系统、APP 端已采用 https 进行通信，能保证重要数据在传输中的完整性。

（6）剩余信息保护

1）OA 系统、APP 端登录时不自动保存和显示历史账号和口令，在用户退出后及时清空会话信息，无法通过回退操作访问退出前界面，用户的鉴别信息所在的存储空间被释放或重新分配前能够得到完全清除。

（7）个人信息保护

1）OA 系统用户输入框有姓名，手机号、性别、所属部门等信息，均为业务必需的个人信息，未发现超范围采集情况，单位具备个人信息保护的相关管理要求和流程。

2）OA 系统保存的个人信息仅授权用户可访问，非授权用户无法访问及使用，且具备个人信息保护的相关管理要求和流程规定。

3.4.5.2 主要安全问题汇总分析

安全计算环境业务应用系统平台存在的安全问题有：

（1）未定期进行漏洞扫描。

不能及时发现系统中存在的漏洞，并对漏洞进行修补，可能导致恶意人员利用系统漏洞对系统进行攻击，涉及测评对象：**OA 系统。**

（2）未有备份恢复测试记录。

一旦出现故障，可能由于各种原因无法利用备份数据进行恢复，造成重要数据丢失，涉及测评对象：**OA 系统。**

（3）未利用通信网络将关键数据定时批量传送至备用场地。

如机房遭受严重破坏，可能导致数据完全丢失，涉及测评对象：**OA 系统。**

3.4.6 数据资源

3.4.6.1 已有安全控制措施汇总分析

（1）数据完整性

1）OA 系统、APP 端已采用 https 进行通信，能保证重要业务数据在传输中的完整性。

2）OA 系统、APP 端已采用 https 进行通信，能保证重要个人信息在传输中的完整性。

（2）个人信息保护

1）OA 系统用户输入框有姓名，手机号、性别、所属部门等信息，均为业务必需的个人信息，未发现超范围采集情况，单位具备个人信息保护的相关管理要求和流程规定。

2）OA 系统保存的个人信息仅授权用户可访问，非授权用户无法访问及使用，单位具备个人信息保护的相关管理要求和流程规定。

3.4.6.2 主要安全问题汇总分析

安全计算环境数据资源存在的安全问题有：

（1）未有备份恢复测试记录。

一旦出现故障，可能由于各种原因无法利用备份数据进行恢复，造成重要数据丢失，涉及测评对象：**重要业务数据、重要个人信息。**

（2）未利用通信网络将关键数据定时批量传送至备用场地。

如机房遭受严重破坏，可能导致数据完全丢失，涉及测评对象：**重要业务数据、重要个人信息。**

3.4.7 其他系统或设备

3.4.7.1 已有安全控制措施汇总分析

本次测评不包含安全计算环境其他设备的测评内容。

3.4.7.2 主要安全问题汇总分析

本次测评不包含安全计算环境其他设备的测评内容。

3.4.8 安全扩展要求

3.4.8.1 已有安全控制措施汇总分析

本次测评不包含安全计算环境扩展要求的测评内容。

3.4.8.2 主要安全问题汇总分析

经安全计算环境扩展要求检测结果分析,所有检测项均符合相应级别的网络安全等级保护要求。

3.5 安全管理中心

3.5.1 已有安全控制措施汇总分析

（1）系统管理

1）安全设备、网络设备、服务器均有建立系统管理员账户，并对系统管理员进行身份鉴别,只允许系统管理员通过特定的命令或操作界面进行系统管理操作，服务器通过堡垒机进行身份鉴别，仅允许系统管理员进行操作和管理，并且各设备已开启安全审计对系统管理员的操作行为进行审计。

2）该单位已配置系统管理员，并且安全设备、网络设备、服务器均由系统管理员负责系统的资源和运行,包括用户身份,系统资源配置、系统加载和启动、系统运行的异常处理，数据和设备的备份恢复。

（2）审计管理

1）安全设备、网络设备、服务器均配置审计管理员账户，并对审计管理员账户进行身份鉴别，只允许其通过日志审计系统进行安全审计操作，并且设备已开启安全审计对审计管理员的操作行为进行审计。

2）该单位已设置审计管理员岗位并配置相应的人员，并且有部署日志审计系统收集各设备的日志审计记录进行分析、处理。

3.5.2 主要安全问题汇总分析

经安全管理中心检测结果分析,所有检测项均符合相应级别的网络安全等级保护要求。

3.6 安全管理制度

3.6.1 已有安全控制措施汇总分析

（1）安全策略

1）该单位秉承“积极防御，综合防范”的信息安全方针，根据国家信息安全等级保护等有关政策和标准要求，建立“三个体系，一个中心，三重防护”的安全保障体系框架,已在《信息安全总体策略》中阐明机构安全工作的总体目标、范围、原则和安全框架等。

（2）管理制度

1）该单位已对安全活动中的主要内容建立了管理制度，已制定《数据安全管理规范.》、《网络安全管理规范》、《网络安全管理规范》、《应用安全管理规范》。

2）该单位已建立《设备操作规程》、《 软件操作手册》、《防火墙配置和操作手册》等操作规程，相关文档中包含对网络安全、系统运行维护、系统配置、用户操作等方面的规定。

（3）制定和发布

1）该单位《信息安全制度管理规范》已指定信息化办公室负责主持制定茂名职业技术学院信息化技术规范和有关规章制度,安全管理制度由信息化办公室发布。

2）该单位《信息安全制度管理规范》已规定总体安全管理制度和规定以及安全技术标准和规范须经信息安全领导小组审批确认，方可发布，已通过 OA 系统正式发文通知，制度版本为 V2.0，具备“收发文登记记录”。

3.6.2 主要安全问题汇总分析

安全管理制度存在的安全问题有:

（1）未具有管理制度评审记录和修订记录。

可能导致安全管理体系与现实情况不符，导致管理文档无法落地，涉及测评对象：**制度或记录类文档。**

3.7 安全管理机构

3.7.1 已有安全控制措施汇总分析

（1）岗位设置

1）该单位《安全组织及职责管理规定》已设立办公室为网络安全管理职能部门，《岗位安排及岗位职责》中已明确了各岗位负责人的职责，包括安全管理员、系统管理员、网络管理员、应用管理员、资料管理员、安全主管等方面的岗位职责。

2）该单位《安全组织及职责管理规定》已进行安全管理岗位的划分，包括网络管理员、系统管理员、安全管理员、安全审计员、数据库管理员、机房管理员等管理岗位，文档中明确了部门及各个工作岗位的职责，详见《岗位安排及岗位职责》。

（2）人员配备

1）该单位《岗位安排及岗位职责》已设置系统管理员为黄海东、安全审计管理员为麦才赞、安全管理员为龙恒，网络管理员为吴国华、机房管理员为陈思凡、资产管理员为黄健。

（3）授权和审批

1）该单位《授权和审批管理规定》规定由信息安全领导小组办公室确定审批内容后，报送信息安全领导小组批准。

2）该单位《授权和审批管理规定》明确审批的内容，重大事项应由信息安

全领导小组办公室确定后，报送信息安全领导小组批准。重大事项至少包括网络系统、应用系统、数据库管理系统、重要服务器和设备等重要资源的变更、操作、访问和接入等。

（4）沟通和合作

1）该单位《安全组织机构-沟通合作》规定各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通机制，每年组织一次工作会议进行沟通合作，共同协调处理信息安全相关问题，具有“沟通会议记录表”。

2）该单位《安全组织机构-沟通合作》已规定通过聘请信息安全专家和外部顾问成员，指导茂名职业技术学院信息安全建设，规定服务中心有关部门建立沟通、合作机制，定期组织相关单位、部门召开内部协调会议，具备“B005 信息安全会议记录”。

3）该单位已建立“外部联系表”，内容包含外联单位名称、合作内容、联系人和联系方式等信息。

（5）审核和检查

1）该单位《安全审核与检查管理制度》规定学校部门每月进行一次安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况，详见《安全检查报告 20230321》。

3.7.2 主要安全问题汇总分析

经安全管理机构检测结果分析，所有检测项均符合相应级别的网络安全等级保护要求。

3.8 安全管理人员

3.8.1 已有安全控制措施汇总分析

（1）人员录用

1）该单位已指定由人力资源保障科负责本学院职工聘用与录用。

2）该单位《内部人员信息安全管理规定》规定信息安全相关岗位人员上岗前必须经人力资源保障科进行身份、背景、专业资格和资质的审查和考查，教育信息与网络中心进行技术和业务技能考核，具备“C002 人员信息审查记录”。

（2）人员离岗

1）该单位规定离职人员职工离职时需要回收涉密资料、账号口令、钥匙、资产等以及其他任何形式的载体，具有人员离岗终止权限、交还软硬件设备的记录。

（3）安全意识教育和培训

1）该单位《安全教育和培训制度》规定由学院教育信息与网络中心负责人员的安全意识教育和岗位培训，明确考核结果由信息中心进行备案，具备“学院信息管理人员培训签到记录”，具备“C014 专业培训考核记录表”。

（4）外部人员访问管理

1）该单位已制定《外部人员访问管理制度》，已规定外部人员进场前，需要出示盖章申请，由学校项目负责人批准后陪同，并登记个人资料留底。单位已通过 OA 系统保留进出审批记录。

2）该单位《外部接入受控网络访问系统管理规范》要求外部人员接入受控网络前由对接人在 OA 提出申请，教育信息与网络中心负责人批准后由系统管理员开设账户、分配权限，并登记备案，记录外部人员访问的权限、时限、账户等

信息的规定，具有相关登记记录。

3）该单位《外部接入受控网络访问系统管理规范》规定在外部人员离场后应及时清除其所有的访问权限，并保留清除记录，具备“C020 离场信息资料交接表”。

3.8.2 主要安全问题汇总分析

经安全管理人员检测结果分析,所有检测项均符合相应级别的网络安全等级保护要求。

3.9 安全建设管理

3.9.1 已有安全控制措施汇总分析

（1）定级和备案

1）该系统具有“茂名职业技术学院 OA 系统定级报告”，报告中明确了系统的安全保护等级为第 2 级（S2A2），且描述了安全保护等级确定的方法和理由。

2）该单位已组织上级部门及相关安全技术专家对系统定级结果的合理性和正确性进行论证评审，具备《OA 系统专家评审意见表》。

3）该单位 OA 系统定级结果经过当地公安部门批准，已取得备案证，备案证明编号为：444090243008-00008。

（2）安全方案设计

1）该系统的建设方案包含有总体安全设计方案，方案中已明确须根据等级保护二级的要求对系统实施安全防护,方案内容包括了:信息系统安全等级定级、信息系统安全风险分析、信息系统安全技术方案、信息安全设备选型等内容。

2）该系统根据建设方案中的安全规划设计方案中要求该系统的安全保护等为二级，并且根据二级标准制定了信息系统安全技术方案。

（3）产品采购和使用

1）该系统相关网络安全产品均采用公开招投标、邀请招标、单一来源等方式开展采购，招投标文件、流程符合国家《中华人民共和国招投标法》的有关要求，并且采购的网络安全产品都有提供公安部签署的销售许可证。

（4）外包软件开发

1）开发单位已提供交付清单，清单包括软件操作手册、系统测试文件及用户手册、需求说明文档、系统设计流程、系统使用指南等文档。

（5）工程实施

1）该单位《工程管理制度》明确规定由信息中心负责系统建设管理和工程实施管理。

2）该单位《建设方案》明确工程的实施过程，包括工程完成时间、进度、质量控制等方面的内容。

（6）系统交付

1）该单位《系统交付管理》规定了系统建设完成后，需要项目承建方向信息中心交付项目相关清单，详见“系统交付清单”。

2）该单位在系统上线前已对负责系统运行维护的技术人员进行技能培训，具有“D009 技能培训记录”。

3）该单位具有《OA 系统-需求规格说明书 》、《系统安装配置维护手册》、《用户使用手册（新增功能）》等运行维护文档，《软件需求说明书》等建设过程文档。

（7）等级测评

1）该系统每年进行等级测评，本次等级测评时间与上次等级测评时间间隔

符合制度规定，已针对上次网络安全等级保护测评结论进行了相应的整改，具备整改报告及整改记录文件。

2）该系统在确定该信息系统的安全保护等级后，并未发生较大变更，未调整安全保护级别，且已在《系统变更管理制度》中规定系统发生重大变更或级别发生变化时及时进行等级测评。

3）该系统于 2022 年由广东南方信息安全研究院进行了等级测评，本年度由广东中科实数科技有限公司负责测评工作，单位已选择符合国家有关规定的测评机构进行等级测评。

（8）服务供应商选择

1）该系统由深信服科技有限公司提供安全产品及服务，该服务供应商符合国家的有关规定。

2）该系统与深信服科技有限公司签订《设备采购合同》服务合同，服务合同中明确了甲乙双方的责任和义务。

（9）移动应用软件采购

1）APP 可通过微信扫描指定的二维码获取、安装、来自可靠的分发渠道。

2）单位已与外包开发人员签署有相关保密协议，可保证其可靠。

（10）移动应用软件开发

1）移动业务应用软件的签名证书由腾讯应用宝颁发，具备合法性。

3.9.2 主要安全问题汇总分析

安全建设管理存在的安全问题有：

（1）未组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，未有相关的方案评审记录。

无法确保方案设计的合理性和正确性，不能确保系统安全方案的正确实践，涉及测评对象：**制度或记录类文档。**

（2）未在软件交付前通过第三方检测工具或人工检测软件包中可能存在的恶意代码。

可能在上线前无法发现软件 BUG 和恶意代码未被发现，对组织的信息系统及声誉造成风险，涉及测评对象：**制度或记录类文档。**

（3）单位缺乏相关测试验收报告。

无法保证经过测试验收的系统达到既定的安全性等目标，涉及测评对象：**制度或记录类文档。**

（4）该单位未在上线前进行安全性测试，未有相关安全测试报告。

不能及时发现系统存在的安全性问题，造成系统的风险，涉及测评对象：**制度或记录类文档。**

（5）单位未对外包开发人员进行资格审查，未有相应的考核记录。

可能导致使用的人员未经严格的审查，无法满足岗位需求，涉及测评对象：**移动互联安全扩展要求。**

3.10 安全运维管理

3.10.1已有安全控制措施汇总分析

（1）环境管理

1）该单位《机房安全管理制度》规定教育信息与网络中心负责机房安全，已指定机房管理员负责对机房进行管理，对机房供配电、UPS 电源、空调、温湿度监控设备等进行管理，具有机房进出登记表、机房值班记录、机房设备维护记录表。

2）该单位《机房安全管理制度》规定所有进入机房的人员都需要向教育信息与网络中心提交进入机房的申请，说明进入机房的原因、操作内容、及访问时间，并填写《机房进出登记表》，并在操作过程中需要由运维工程师陪同和监督，在进行关键操作之前需请示主管，不可把外部人员单独留在设备旁；机房内应保持清洁，定期消毒、杀菌，保证机房的安全和卫生；机房禁止放置易燃、易爆、腐蚀、强磁性物品，禁止将机房内的电源引出挪做他用，确保机房安全。

3）该单位《机房安全管理制度》明确规定不可在重要区域接待来访人员和不随意放置含有敏感信息的移动介质，明确办公桌上不准摆放机要文件，机要文件的草稿纸应立即销毁，不准乱丢，各类记录本不准乱放，一律置于文件柜内或其他固定地方。

（2）资产管理

1）该单位已配置资产管理员定期对资产进行清点核查，具有“资产清单”，清单内容包括部门、重要程度、编号、类型、型号、编码、ip、入库时间、资产使用部门、资产归属部门等。

（3）介质管理

1）该单位存储介质由资产管理员统一管理，存储在带锁的介质保存柜中，并定期对介质进行盘点，具有“介质记录清单”。

2）该单位《介质安全管理规定》明确对涉密介质应实行集中编号登记，责任到人管理，防止失控，处理过涉密信息或者重要数据的存储介质，不得转让或者出借给无关人员使用，不得私自带出境外，不得送往无安全保密保障的机构修理，对需要送出维修或销毁的介质，首先清除其中的敏感数据，防止信息的非法泄漏；对介质归档和查询等过程进行记录，并根据存档介质的目录清单定期盘点；

具有“存储介质目录清单”。

（4）设备维护管理

1）该单位《设备安全管理制度》规定对信息系统相关的各种设备（包括备份和冗余设备)、线路等指定系统管理员定期进行维护管理；系统管理员在日常巡检过程中对设备和线路等进行维护，巡检记录含有相关维护记录。

2）该单位《设备安全管理制度》已规定由教育信息与网络中心负责相关的维护工作，已明确维护责任、维修和服务流程、维修过程的监督控制等内容。

（5）网络和系统安全管理

1）该单位已设立系统管理员、网络管理员、安全管理员等角色，已在制度和文档中划分各管理人员的职责，详见《网络安全管理规定》、“ 岗位安排及岗位职责”。

2) 该单位《系统安全管理规定》已指定教育信息与网络中心负责账户管理，创建账户、修改账户权限、删除账户等操作需经过审批后在 OA 系统上填写在审批申请，经过审批后方可执行，OA 系统具有相关审批记录，审批记录中包含审批内容如申请账户、建立账户、删除账户等，审批人，审批时间等。

3）该单位《系统安全管理规定》明确对账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定。

4）该单位具有网络安全设备、数据库、服务器操作系统等重要设备的配置操作手册，包含了设备的操作步骤，参数配置等内容。

5）该单位具备系统运维日志记录，具有“机房巡检记录”、“系统维护记录表”等记录文档。

（6）恶意代码防范管理

1）该单位《恶意代码防范管理制度》已规定须定期组织召开恶意代码宣传培训，并对外来计算机或存储设备接入系统前进行恶意代码检查，具有“E004 防恶意代码意识培训记录”。

2）该单位《恶意代码防范管理制度》规定凡接入单位网络的计算机都必须安装全局统一的恶意代码防范软件，并纳入全局统一的恶意代码防范管理体系，对外来人员的计算机或存储设备在接入单位网络系统之前应先进行恶意代码检查；安全员要定时检查入侵和恶意代码防范服务器的入侵特征库、恶意代码库、扫描引擎的更新情况，保持入侵特征库、恶意代码库、扫描引擎为最新状态。

3）该单位《恶意代码防范管理制度》已指定教育信息与网络中心负责对截获的危险恶意代码进行分析处理，定期每月对恶意代码软件病毒库升级更新，未发生过病毒攻击行为，未截获到恶意代码。

（7）配置管理

1）该单位已记录和保存系统的基本配置信息，包括系统名称、型号、版本、VLAN 信息、端口信息、网络结构等内容，详见“网络配置信息表格”。

（8）密码管理

1）该单位已在《密码管理制度》中明确信息系统采用密码技术应符合国家标准和行业标准。

（9）备份与恢复管理

1）该单位《备份与恢复管理制度》已明确备份策略和数据恢复策略，已根据业务重要程度，制定备份清单，具有“数据备份记录表”。

2）该单位已建立《备份与恢复管理制度》对备份方式、频度、介质、保存期等内容进行了规定。

3）该单位已建立《备份与恢复管理制度》规定对重要数据每周全量备份，已制定《E005 应用系统及数据库等重要数据备份和恢复管理办法》作为备份程序和恢复程序。

（10）安全事件处置

1）该单位《网络安全事件报告制度》规定了发生安全事件应向教育信息与网络中心报告，该单位未发生安全事件。

2)该单位已制定《网络安全事件报告制度》,制度中明确了安全事件的报告、处置和响应流程，明确不同安全事件的定义：一般、严重和重大三个事件级别、组织人员职责、安全事件处理流程处置和响应流程：发现事件、应急恢复、事件分析与处理事件记录、上报途径、恢复程序。

3）该单位已制定了安全事件报告模板，要求发生安全事件时，根据报告模板进行填报，安全事件报告包括了发生事件的时间、责任人、影响、影响范围、事件的类型、响应分级、事件描述、事件对业务的负面影响、攻击者的动机、已经采取的应对措施、初步判定事件的发展趋势、计划采取的应对措施、网络安全负责人签名等内容。

（11）应急预案管理

1）该单位《校园网络信息安全应急预案》，已明确重要事件的应急预案，包括机房火灾故障、停电事故、设备故障、应用系统故障和网络故障的应急处理流程及系统恢复流程等内容。

2）该单位《校园网络信息安全应急预案》规定每 6 个月对系统相关的人员进行应急预案培训，并进行应急预案的演练；具有《应急预案培训记录》和《应急预案演练记录》。

3.10.2主要安全问题汇总分析

安全运维管理存在的安全问题有：

（1）未定期进行漏洞扫描，缺少漏洞扫描报告和修复记录。

可能导致系统补丁升级不到位，存在信息系统高风险漏洞，从而导致信息泄露风险，涉及测评对象：**制度或记录类文档。**

（2）未提供变更方案和评审记录。

变更事件发生时，临时制定变更方案，导致对变更事项应对不及时或无法应对，可能出现变更失败，并且在变更过程中对系统造成软硬件故障或数据丢失等风险，涉及测评对象：**制度或记录类文档。**

3.11 其他安全要求指标

本次测评不包含其他安全要求指标。

3.12 验证测试

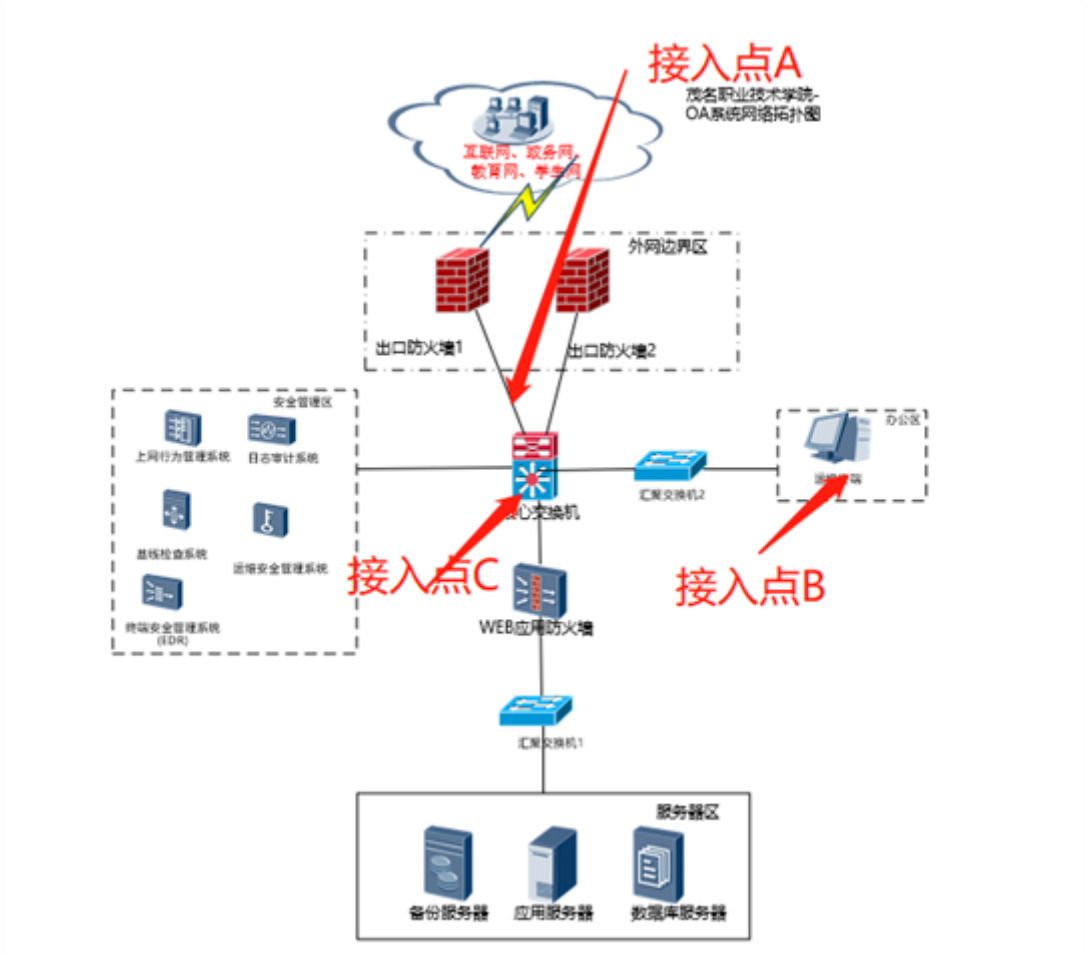


图 3-1 茂名职业技术学院 OA 系统漏洞扫描工具接入测试图

接入点 A：通过在互联网接入，模拟互联网发起的对应用系统等资产漏洞发现的过程，以及模拟黑客对应用系统软件本身进行黑盒测试，发现系统中存在的问题，例如暴力破解，xss 跨站脚本等，并尝试利用漏洞进行攻击行为。

接入点 B：通过在办公网，模拟从办公网网段内部发现操作系统、数据库、应用、中间件、网络设备、安全设备等资产漏洞的过程。

接入点 C：通过在核心交换机接入，模拟从核心区内部发现操作系统、数据库、应用、中间件、网络设备、安全设备等资产漏洞的过程。

3.12.1漏洞扫描

3.12.1.1 漏洞扫描结果统计

接入点的漏洞扫描结果汇总如下表所示。

表 3-1 接入点 A 漏洞扫描结果汇总表

序号	设备名称	系统及版本	安全漏洞数量			
			高	中	低	小计
-	-	--	-	-	-	--

表 3-2 接入点 B 漏洞扫描结果汇总表

序号	设备名称	系统及版本	安全漏洞数量			
			高	中	低	小计
1	172.16.1.2	Linux 2.4.20	0	0	4	4
2	172.16.1.50	-	0	0	4	4
3	172.16.2.1	-	0	0	4	4
4	10.1.4.27	-	0	0	4	4
5	10.1.4.28	-	0	0	4	4
6	192.168.10.3	-	0	0	2	2
7	172.16.1.1	Linux 2.4.37	0	0	2	2
8	172.16.1.18	-	0	0	2	2
9	172.16.1.14	Linux 2.4.20	0	0	4	4
10	10.2.1.2	Linux 2.4.20	0	0	4	4
11	10.2.1.3	Linux 2.4.20	0	0	2	2
12	10.1.4.16	-	0	0	1	1
13	10.2.1.4	-	0	0	1	1
14	OA 系统	A8+企业版 V8.1	0	1	4	5

表 3-3 接入点 C 漏洞扫描结果汇总表

序号	设备名称	系统及版本	安全漏洞数量			
			高	中	低	小计
1	10.1.4.27	-	0	0	4	4
2	10.1.4.28	-	0	0	4	4
3	10.1.15.253	-	0	0	1	1
4	10.2.1.2	-	0	0	2	2
5	10.2.1.3	Linux Windows	0	0	3	3
6	10.2.1.4	Linux Windows	0	0	2	2
7	172.16.1.1	Linux 2.4.37	0	0	2	2
8	172.16.1.2	-	0	0	4	4
9	172.16.1.14	-	0	0	1	1
10	172.16.1.18	-	0	0	1	1
11	172.16.1.50	-	0	0	4	4
12	172.16.2.1	-	0	0	4	4
13	192.168.10.25	-	0	0	1	1

3.12.1.2 漏洞扫描问题描述

通过对漏洞扫描结果进行分析，OA 系统存在的主要安全漏洞汇总如下表所示。

表 3-4 主要安全漏洞汇总表

序号	安全漏洞名称	关联资产/域名	严重程度
1	允许 Traceroute 探测	10.1.4.27 10.1.4.28 10.1.15.253 10.2.1.2 10.2.1.4 10.2.1.3 172.16.1.1 172.16.1.14	低

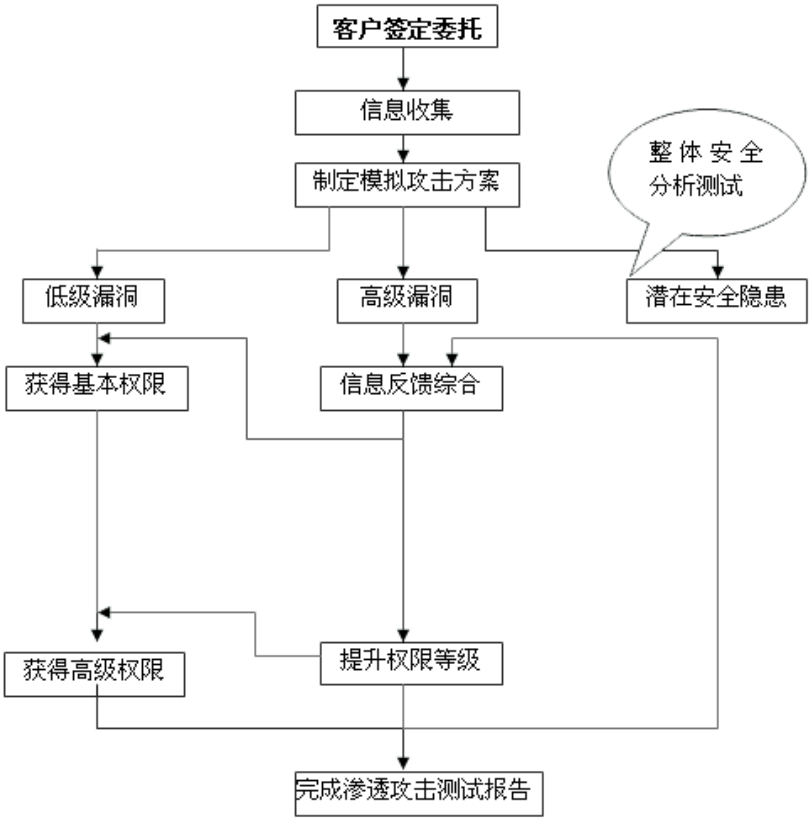
序号	安全漏洞名称	关联资产/域名	严重程度
		172.16.1.18 172.16.1.50 192.168.10.25 172.16.2.1 192.168.10.3 10.1.4.16	
2	SSH 版本信息可被获取	10.1.4.27 10.1.4.28 172.16.1.2 172.16.2.1 172.16.1.50	低
3	探测到 SSH 服务器支持的算法	10.1.4.27 10.1.4.28 172.16.2.1 172.16.1.50 172.16.1.2	低
4	OpenSSH CBC 模式信息泄露漏洞(CVE-2008-5161)【原理扫描】	10.1.4.27 10.1.4.28 172.16.1.2 172.16.1.50 172.16.2.1	低
11	服务器允许 SSL 会话恢复【原理扫描】	10.2.1.2 10.2.1.3 172.16.1.18	低
12	SMTP 服务器版本信息可被获取	10.2.1.3 10.2.1.4 172.16.1.1	低
13	可通过 NetBIOS 名字服务端口远程获取系统信息	192.168.10.3	低
14	可通过 HTTP 获取远端 WWW 服务信息	172.16.1.1 172.16.1.14	低
15	获取目标 SSL 证书过期时间【原理扫描】【可验证】	172.16.1.14 10.2.1.2	低
16	探测到服务器支持的 SSL 加密协议【原理扫描】【可	172.16.1.14 10.2.1.2	低

序号	安全漏洞名称	关联资产/域名	严重程度
	验证】	10.2.1.3	
17	远端 HSTS 服务运行中	10.2.1.2	低
18	检测到目标 URL 存在 http host 头攻击漏洞	OA 系统	中
19	检测到目标 X-Content-Type-Options 响应头缺失	OA 系统	低
20	检测到目标 X-XSS-Protection 响应头缺失	OA 系统	低
21	检测到目标 Content-Security-Policy 响应头缺失	OA 系统	低
22	点击劫持：X-Frame-Options 未配置	OA 系统	低

3.12.2渗透测试

3.12.2.1 渗透测试过程说明

1. 渗透测试基本流程



1） 实施方案制定、客户书面同意

合法性即客户书面授权委托，并同意实施方案是进行渗透测试的必要条件。渗透测试首先必须将实施方法、实施时间、实施人员、实施工具等具体的实施方案提交给客户，并得到客户的相应书面委托和授权。

应该做到客户对渗透测试所有细节和风险的知晓,所有过程都在的控制下进行，这也是专业渗透测试与黑客入侵本质的不同。

2） 内部计划制定、二次确认

根据客户设备范围和项目时间计划，并结合前一步的信息收集得到的设备存活情况、网络拓扑情况以及扫描得到的服务开放情况、漏洞情况制定内部的详细实施计划。具体包括每个地址下一步可能采用的测试手段，详细时间安排，并将以下一步工作的计划和时间安排与客户进行确认。

3） 取得权限、提升权限

通过初步的信息收集分析，存在两种可能，一种是目标系统存在重大的安全弱点，测试可能直接控制目标系统；另一种是目标系统没有重大的安全弱点，但是可以获得普通用户权限，这时可以通过该用户权限进一步收集目标系统信息。接下来尽最大努力取得超级用户权限、收集目标主机资料信息，寻求本地权限提升的机会。这样不停地进行信息收集分析、权限提升的结果形成了整个渗透测试过程。

4） 生成报告

渗透测试之后，测试者将会提供一份渗透测试报告。报告将会十分详细地说明渗透测试过程中得到的数据和信息，并且将会详细地记录整个渗透测试的全部操作。

2. 渗透测试内容

测试内容包括：业务漏洞测试与技术漏洞测试。

1) 业务漏洞测试

- 枚举用户信息类漏洞。如：测试系统在忘记密码、注册新用户等模块是否可枚举用户名、手机号、弱密码等敏感信息。
- 表单爆破。检测登陆、注册等模块是否有防撞库机制。
- 密码重置类漏洞。检测密码找回、密码修改、密码重置等模块是否可绕过验证直接重置或修改用户密码。
- 越权类漏洞。检测是否可以越权访问和操作系统内其他用户的敏感信息，如密码、账户信息、手机号、无权限的菜单或交易等。包括垂直越权、水平越权等。
- 薅羊毛类漏洞。检测是否可以绕过系统校验机制进行批量恶意注册账号、批

量发送短信、进行刷单薅羊毛等行为。

- 会话 session 类漏洞。查看网站 sessionid 会话是否存在安全漏洞，用户身份识别功能有无安全问题。如固定会话标识、未授权的访问、无 httpOnly 等
- 任意文件上传类漏洞。检测上传类接口等是否可上传任意文件。
- 任意文件下载类漏洞。检测下载文件模块是否存在任意文件下载漏洞。
- 其它业务 0Day 漏洞根据系统业务规则、边界值、不正确的数值等进行非常规输入测试，查看其是否有风险漏洞。

2) 技术漏洞测试

- 数据溢出类 检测系统接受的数据长度超出允许的范围时,是否会产生溢出风险。
- 文件包含或资源非法调用类漏洞。检查包括本地/远程文件包含、资源非法调用等漏洞。
- 注入类漏洞。对业务 http 请求中的各参数进行 sql 注入、XXE 注入、命令行注入等各种注入类风险检测。
- 跨站类漏洞。对业务 http 请求中的各参数进行 xss、csrf、ssrf 等测试，检测是否存在漏洞。
- 访问控制类漏洞。测试是否可以在未登陆或权限不足的情况下访问系统相关模块。
- 劫持类漏洞。检测系统是否存在界面劫持、js 劫持、json 劫持等漏洞。
- 敏感信息泄露类漏洞。检查系统是否存在敏感信息、代码泄露问题。
- 通讯安全类漏洞。检查系统通讯协议是否安全，通信数据是否加密、是否可被劫持、篡改、伪造等。

- 代码执行类漏洞。检测系统是否存在代码执行相关漏洞。
- 非法参数类漏洞。检测系统对特殊字符、非法长度或种类的参数是否进行了严格校验，是否因此引发安全漏洞。
- 第三方组件漏洞。检查系统使用的第三方库或组件是否存在风险。

3. 渗透测试工具

测试工具是指为实施测试活动而采用的工具。一切能够满足测试需求、协助测试活动发现问题的工具都是测试工具。在本项目中使用的工具包含但不限于以下工具:

工具名称	工具用途
RSAS	自动化主机扫描、自动化web扫描，漏洞探测，精准扫描“操作系统、应用服务、中间件、数据库、web应用、web 代码”等多种应用漏洞以及弱口令
Nessus	主机发现、高级扫描、基础网络扫描、高级动态扫描等功能
Burp Suite	拦截数据包、修改数据包、重放数据包、暴力破解、解码等功能
Nmap	端口扫描、快速扫描大型的网络、主机发现、版本侦测、操作系统侦测等功能
Sqlmap	自动化的SQL注入，布尔类型的盲注、时间的盲注、报错注入、联合查询注入、堆叠查询注入等方式对数据库进行检测

3.12.2.2 渗透测试问题描述

通过渗透测试发现，OA 系统存在的安全问题汇总如下表所示。

表 3-5 渗透测试结果汇总表

序号	安全问题	关联资产/域名	严重程度
1	无		

3.13 单项测评小结

3.13.1控制点符合情况汇总

根据单项测评结果汇总控制点符合情况如下表所示。

表 3-6 控制点符合情况汇总表

序号	通用/扩展	安全类	控制点	控制点符合情况		
				符合	部分符合	不符合
1	安全通用要求	安全物理环境	物理位置选择		√	
2			物理访问控制	√		
3			防盗窃和防破坏	√		
4			防雷击	√		
5			防火		√	
6			防水和防潮		√	
7			防静电		√	
8			温湿度控制		√	
9			电力供应	√		
10			电磁防护	√		
11		安全通信网络	网络架构	√		
12			通信传输	√		
13			可信验证			√
14		安全区域边界	边界防护	√		
15			访问控制		√	
16			入侵防范		√	
17			恶意代码防范		√	
18			安全审计		√	
19			可信验证			√

序号	通用/扩展	安全类	控制点	控制点符合情况		
				符合	部分符合	不符合
20		安全计算环境	身份鉴别		√	
21			访问控制		√	
22			安全审计		√	
23			入侵防范		√	
24			恶意代码防范	√		
25			可信验证			√
26			数据完整性		√	
27			数据备份恢复		√	
28			剩余信息保护	√		
29			个人信息保护	√		
30		安全管理中心	系统管理	√		
31			审计管理	√		
32		安全管理制度	安全策略	√		
33			管理制度	√		
34			制定和发布	√		
35			评审和修订		√	
36		安全管理机构	岗位设置	√		
37			人员配备	√		
38			授权和审批	√		
39			沟通和合作	√		
40			审核和检查	√		
41		安全管理人员	人员录用	√		
42			人员离岗	√		
43			安全意识教育和	√		

序号	通用/扩展	安全类	控制点	控制点符合情况		
				符合	部分符合	不符合
			培训			
44			外部人员访问管理	√		
45		安全建设管理	定级和备案	√		
46			安全方案设计		√	
47			产品采购和使用	√		
48			外包软件开发		√	
49			工程实施	√		
50			测试验收		√	
51			系统交付	√		
52			等级测评	√		
53			服务供应商选择	√		
54		安全运维管理	环境管理	√		
55			资产管理	√		
56			介质管理	√		
57			设备维护管理	√		
58			漏洞和风险管理		√	
59			网络和系统安全管理	√		
60			恶意代码防范管理	√		
61			配置管理	√		
62			密码管理	√		
63			变更管理		√	
64			备份与恢复管理	√		

序号	通用/扩展	安全类	控制点	控制点符合情况		
				符合	部分符合	不符合
65			安全事件处置	√		
66			应急预案管理	√		
67	移动互联安全扩展要求	安全计算环境	移动应用管控	√		
68		安全建设管理	移动应用软件采购	√		
69			移动应用软件开发		√	
控制点符合情况数量统计				44	22	3

3.13.2 安全问题汇总

针对单项测评结果中存在的部分符合项和不符合项进行汇总，形成安全问题如下表所示。

表 3-7 安全问题汇总表

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T1	未提供机房验收文档，机房防震等级不明确。	信息机房	安全通用要求	安全物理环境	物理位置选择	a)机房场地应选择在具有防震、防风和防雨等能力的建筑内；
T2	未提供火灾自动消防系统的定期巡检和维护的记录。	信息机房	安全通用要求	安全物理环境	防火	a)机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；
T3	未提供机房验收文档，无法明确建筑材料的耐火等级。	信息机房	安全通用要求	安全物理环境	防火	b)机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T4	未部署湿度控制设备，不能防止水蒸气结露。	信息机房	安全通用要求	安全物理环境	防水和防潮	b)应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。
T5	机房未铺设防静电地板。	信息机房	安全通用要求	安全物理环境	防静电	应采用防静电地板或地面并采用必要的接地防静电措施。
T6	未部署机房专用精密空调，不能设置湿度自动调节。	信息机房	安全通用要求	安全物理环境	温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。
T7	未基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	安全通信网络	安全通用要求	安全通信网络	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T8	未根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	办公区边界、安全管理区边界	安全通用要求	安全区域边界	访问控制	d)应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。
T9	未部署入侵	安全管理区	安全通	安全区	入侵防	应在关键网络节点

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
	防御系统或者有入侵防御模块的防火墙，因而不可对网络攻击行为进行监视。	边界、办公区边界	用要求	域边界	范	处监视网络攻击行为。
T10	未部署有防病毒网关或者有防病毒模块的防火墙，因而未能对恶意代码进行检测和清除。	办公区边界、安全管理区边界	安全通用要求	安全区域边界	恶意代码防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。
T11	无法对边界的流量和边界的安全事件进行审计。	安全管理区边界、办公区边界	安全通用要求	安全区域边界	安全审计	a)应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
T12	不能对边界的流量和边界的安全事件进行审计，故缺少边界的流量审计和安全事件审计记录。	办公区边界、安全管理区边界	安全通用要求	安全区域边界	安全审计	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
T13	不能对边界的流量和边界的安全事件进行审计，故无法对审计记录进行保护和	安全管理区边界、办公区边界	安全通用要求	安全区域边界	安全审计	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
	备份。					
T14	未基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	办公区边界、外网区边界、服务器区边界、安全管理区边界	安全通用要求	安全区域边界	可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T15	未配置口令有效期策略。	备份服务器、UIS 超融合管理平台	安全通用要求	安全计算环境	身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
T16	未配置屏幕保护程序。	运维终端	安全通用要求	安全计算环境	身份鉴别	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
T17	未配置登录失败处理策略及登录连接超时策略。	备份服务器	安全通用要求	安全计算环境	身份鉴别	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
						施；
T18	进行远程管理时，鉴别信息通过不安全的协议进行传输。	运维终端	安全通用要求	安全计算环境	身份鉴别	c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。
T19	未禁止 root 账户远程登录。	数据库服务器、应用服务器、备份服务器	安全通用要求	安全计算环境	访问控制	a)应对登录的用户分配账户和权限；
T20	未设置审计管理、安全管理员账户，未实现管理用户的权限分离。	数据库	安全通用要求	安全计算环境	访问控制	d)应授予管理用户所需的最小权限，实现管理用户的权限分离。
T21	审计记录保存时间不足六个月。	数据库服务器、应用服务器、中间件 1、中间件 2、数据库、UIS 超融合管理平台、终端安全管理系统（EDR）	安全通用要求	安全计算环境	安全审计	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
T22	审计记录仅保存在本机，未进行定期备份。	运维终端	安全通用要求	安全计算环境	安全审计	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
T23	未严格限制终端登录地址范围。	运维终端	安全通用要求	安全计算环境	入侵防范	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T24	未定期进行漏洞扫描。	核心交换机、汇聚交换机 1、汇聚交换机 2、运维安全管理系统、基线核查系统、出口防火墙 1、出口防火墙 2、日志审计系统、WEB 应用防火墙、上网行为管理系统、UIS 超融合管理平台、OA 系统、终端安全管理系统（EDR）	安全通用要求	安全计算环境	入侵防范	e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。
T25	未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	核心交换机、汇聚交换机 1、汇聚交换机 2、运维安全管理系统、基线核查系统、出口防火墙 1、出口防火墙 2、日志审计系统、WEB 应用防火墙、上网行为管理系统、数据库服务器、应	安全通用要求	安全计算环境	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
		用服务器、备份服务器、运维终端、UIS 超融合管理平台、终端安全管理系统（EDR）				
T26	未配置“远程（RDP）连接要求使用指定的安全层”为“SSL”和未配置“设置客户端连接加密级别”为“高级别”，不能保证重要数据在传输过程中的完整性。	运维终端	安全通用要求	安全计算环境	数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。
T27	未有备份恢复测试记录。	核心交换机、汇聚交换机 1、汇聚交换机 2、运维安全管理系统、基线核查系统、出口防火墙 1、出口防火墙 2、日志审计系统、WEB 应用防火墙、上网行为管理系	安全通用要求	安全计算环境	数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能；

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
		统、数据库服务器、应用服务器、备份服务器、中间件1、中间件2、数据库、UIS 超融合管理平台、OA 系统、重要业务数据、重要个人信息、终端安全管理系统（EDR）				
T28	未利用通信网络将关键数据定时批量传送至备用场地。	核心交换机、汇聚交换机 1、汇聚交换机 2、运维安全管理系统、基线核查系统、出口防火墙 1、出口防火墙 2、日志审计系统、WEB 应用防火墙、上网行为管理系统、数据库服务器、应用服务器、备份服务器、中间件1、中间件2、数据库、UIS 超	安全通用要求	安全计算环境	数据备份恢复	b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
		融合管理平台、OA 系统、重要业务数据、重要个人信息、终端安全管理系统（EDR）				
T29	未具有管理制度评审记录和修订记录。	制度或记录类文档	安全通用要求	安全管理制度	评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。
T30	未组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，未有相关的方案评审记录。	制度或记录类文档	安全通用要求	安全建设管理	安全方案设计	c)应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。
T31	未在软件交付前通过第三方检测工具或人工检测软件包中可能存在的恶意代码。	制度或记录类文档	安全通用要求	安全建设管理	外包软件开发	a)应在软件交付前检测其中可能存在的恶意代码；
T32	单位缺乏相关测试验收报告。	制度或记录类文档	安全通用要求	安全建设管理	测试验收	a)应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；
T33	该单位未在	制度或记录	安全通	安全建	测试验	b)应进行上线前的安

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
	上线前进行安全性测试，未有相关安全测试报告。	类文档	用要求	设管理	收	全性测试，并出具安全测试报告。
T34	单位未对外包开发人员进行资格审查，未有相应的考核记录。	移动互联安全扩展要求	移动互联安全扩展要求	安全建设管理	移动应用软件开发	a)应对移动业务应用软件开发者进行资格审查；
T35	未定期进行漏洞扫描，缺少漏洞扫描报告和修复记录。	制度或记录类文档	安全通用要求	安全运维管理	漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。
T36	未提供变更方案和评审记录。	制度或记录类文档	安全通用要求	安全运维管理	变更管理	应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。

4 整体测评

4.1 安全控制点间安全测评

本次测评不包含本类安全检测调整项。

4.2 区域间安全测评

安全区域边界层面的入侵防范中要求“应在关键网络节点处监视网络攻击行为”，检查中发现办公区边界、安全管理区边界未部署入侵防御系统或者有入侵防御模块的防火墙，因而不可对网络攻击行为进行监视。但在互联网边界处部署

的边界防火墙有启用入侵防御模块，并且入侵防御的特征库已更新到 20230722，能有效防御外部网络攻击行为，并且设备接入内网需要经过审批和杀毒后才能接入，网络环境可控。综合以上因素对该问题起到一定补偿作用，据此降低控制项不符合因素给系统造成的风险。

安全区域边界层面的恶意代码防范中要求“应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新”，检查中发现办公区边界、安全管理区边界未部署有防病毒网关或者有防病毒模块的防火墙，因而未能对恶意代码进行检测和清除。但在互联网边界处部署出口防火墙有启用病毒防火墙功能，且病毒库已更新到 20230722，可对来自外部的恶意代码进行检测和清除，服务器上也安装有终端威胁防御系统，病毒库也更新至 20230722，设备接入内网需要经过审批和杀毒后才能接入，网络环境可控。综合以上因素对该问题起到一定补偿作用，据此降低控制项不符合因素给系统造成的风险。

安全区域边界层面的安全审计中要求“a)应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计”，检查中发现办公区边界、安全管理区边界无法对边界的流量和边界的安全事件进行审计。但办公区边界、安全管理区边界处于内网区域，不与外网直接连接，外网边界处部署有出口防火墙，有配置应用访问策略和启用入侵防御、病毒防护功能，可对边界流量和边界的安全事件进行审计，并且审计记录已配置上传至日志审计系统进行保存备份、分析，并且设备接入内网需要经过审批和杀毒后才能接入，网络环境可控。综合以上因素对该问题起到一定补偿作用，据此降低控制项不符合因素给系统造成的风险。

安全区域边界层面的安全审计中要求“a)应在网络边界、重要网络节点进行

安全审计,审计覆盖到每个用户,对重要的用户行为和重要安全事件进行审计”，检查中发现办公区边界、安全管理区无法对边界的流量和边界的安全事件进行审计。但办公区边界处于内网区域，不与外网直接连接，互联网网边界处部署有出口防火墙，有配置应用访问策略和启用入侵防御、病毒防护功能，可对边界流量和边界的安全事件进行审计,并且审计记录已配置上传至日志审计系统进行保存备份、分析,并且设备接入内网需要经过审批和杀毒后才能接入,网络环境可控。综合以上因素对该问题起到一定补偿作用,据此降低控制项不符合因素给系统造成的风险。

安全计算环境层面的安全审计中要求“c)应对审计记录进行保护,定期备份,避免受到未预期的删除、修改或覆盖等”，检查中发现审计记录保存时间不足六个月。但设备已设置了日志留存六个月，且存储空间充足，可满足存储超过 180 天的要求，日志记录无法删除、修改或覆盖。综合以上因素对该问题起到一定补偿作用，据此降低控制项不符合因素给系统造成的风险。

4.3 整体测评结果汇总

经整体测评后安全问题严重程度变化情况如下表所示。

表 4-1 整体测评结果汇总表

问题编号	安全问题	测评对象	整体测评描述	严重程度变化
T9	未部署入侵防御系统或者有入侵防御模块的防火墙，因而不可对网络攻击行为进行监视。	安全管理区边界、办公区边界	虽然办公区边界、安全管理区边界未部署入侵防御系统或者有入侵防御模块的防火墙，不可对网络攻击行为进行监视，但在互联网边界处部署的边界防火墙有启用入侵防御模块，并且入侵防御的特征库已更新到20230722，能有效防御外部	□升高 ☑降低

问题编号	安全问题	测评对象	整体测评描述	严重程度变化
			网络攻击行为，并且设备接入内网需要经过审批和杀毒后才能接入，网络环境可控。	
T10	未部署有防病毒网关或者有防病毒模块的防火墙，因而未能对恶意代码进行检测和清除。	办公区边界、安全管理区边界	虽然办公区边界、安全管理区边界处未部署有防病毒网关或者有防病毒模块的防火墙，不可对恶意代码进行检测和清除，但在互联网边界处部署出口防火墙有启用病毒防火墙功能，且病毒库已更新到 20230722，可对来自外部的恶意代码进行检测和清除，服务器上也安装有终端威胁防御系统，病毒库也更新至 20230722，设备接入内网需要经过审批和杀毒后才能接入，网络环境可控。	□升高 ☑降低
T11	无法对边界的流量和边界的安全事件进行审计。	安全管理区边界、办公区边界	虽然办公区边界、安全管理区边界不能对边界的流量和边界的安全事件进行审计，但办公区边界、安全管理区边界处于内网区域，不与外网直接连接，外网边界处部署有出口防火墙，有配置应用访问策略和启用入侵防御、病毒防护功能，可对边界流量和边界的安全事件进行审计，并且审计记录已配置上传至日志审计系统进行保存备份、分析，并且设备接入内网需要经过审批和杀毒后才能接入，网络环境可控。	□升高 ☑降低
T21	审计记录保存时间不足六个月。	数据库服务器、应用服务器、中间件 1、中间件 2、数据	虽然设备审计记录保存时间不足六个月，但设备已设置了日志留存六个月，手动每周进行备份，且存储空间充足，可满足存储超过 180 天	□升高 ☑降低

问题编号	安全问题	测评对象	整体测评描述	严重程度变化
		库、UIS 超融合管理平台、终端安全管理系统（EDR）	的要求，日志记录无法删除、修改或覆盖。	

5 安全问题风险分析

针对等级测评结果中存在的所有安全问题,结合关联资产和威胁分别分析安全问题可能产生的危害结果，找出可能对系统、单位、社会及国家造成的最大安全危害（损失），并根据最大安全危害（损失）的严重程度进一步确定安全问题的风险等级，结果为“高”、“中”或“低”。最大安全危害（损失）结果应结合安全问题所影响业务的重要程度、相关系统组件的重要程度、安全问题严重程度以及安全事件影响范围等进行综合分析。

表 5-1 安全问题风险分析

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
1	安全物理环境	未提供机房验收文档，机房防震等级不明确。	信息机房	物理环境影响	无法确认机房所处物理环境是否满足相关要求，不能及时发现机房存在的风险隐患。	低
2		未提供火灾自动消防系统的定期巡检和维护的记录。	信息机房	物理环境影响	不能及时了解消防系统的可用性，导致火灾发生时火势不能第一时间被控制并扑灭，可能对机房重要设备造成严重损害。	低
3		未提供机房验收文档，无法明确建筑材料的耐火等级。	信息机房	物理环境影响	无法确认机房建筑材料是否具有耐火等级，不能及时发现机房是否存在的火灾隐患。	中

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
4		未部署湿度控制设备，不能防止水蒸气结露。	信息机房	物理环境影响	在机房出现漏水事故时，可能形成积水，如水势蔓延至机房其他区域，造成重要设备损坏。	中
5		机房未铺设防静电地板。	信息机房	物理环境影响	可能导致静电无法得到有效释放，静电放电可能会影响数据传输，并可能对精密电子元件造成损害。	中
6		未部署机房专用精密空调，不能设置湿度自动调节。	信息机房	物理环境影响	导致机房不能做到恒湿，不利于电子设备的稳定运行，增加了设备故障几率。	低
7	安全通信网络	未基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	安全通信网络	恶意攻击	无可信链和可信验证，不能通过可信验证技术提高系统自身安全防护能力，不能实现积极主动防御。	低
8	安全区域边界	未根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	办公区边界、安全管理区边界	恶意攻击	无法对来自外部非可信网络的网络通信进行控制，极易存在被网络攻击的风险。	中
9		未部署入侵防御系统或者有入侵防御模块的防火墙，因而不可对网络攻击行为进	安全管理区边界、办公区边界	恶意攻击	增加了应用系统受到网络攻击的风险。	中

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
		行监视。				
10		未部署有防病毒网关或者有防病毒模块的防火墙，因而未能对恶意代码进行检测和清除。	办公区边界、安全管理区边界	恶意攻击	无法检测潜在的恶意代码，可能会造成恶意代码流入系统造成破坏的风险。	中
11		无法对边界的流量和边界的安全事件进行审计。	安全管理区边界、办公区边界	恶意攻击	安全审计功能不完善可能导致安全审计员无法利用审计日志对部分安全事件予以准确定位和追溯。	中
12		不能对边界的流量和边界的安全事件进行审计，故缺少边界的流量审计和安全事件审计记录。	办公区边界、安全管理区边界	恶意攻击	安全审计功能不完善可能导致审计员无法利用审计记录对安全事件予以准确定位和追溯。	中
13		不能对边界的流量和边界的安全事件进行审计，故无法对审计记录进行保护和备份。	安全管理区边界、办公区边界	恶意攻击	未对审计记录进行保护可能导致审计员无法利用审计记录对安全事件予以准确定位和追溯。	中
14		未基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	办公区边界、外网区边界、服务器区边界、安全管理区边界	恶意攻击	无可信链和可信验证，不能通过可信验证技术提高系统自身安全防护能力，不能实现积极主动防御。	低

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
15	安全计算环境	未配置口令有效期策略。	备份服务器、UIS 超融合管理平台	恶意攻击	账户口令可能被长时间使用，恶意人员可通过猜解或暴力破解的方式获取账户口令，存在非授权访问的风险。	中
16		未配置屏幕保护程序。	运维终端	恶意攻击	设备易被非授权人员恶意操作，存在非授权访问的风险。	中
17		未配置登录失败处理策略及登录连接超时策略。	备份服务器	恶意攻击	恶意人员可通过暴力破解的方式获取账户口令。且设备易被非授权人员恶意操作，存在非授权访问的风险。	中
18		进行远程管理时，鉴别信息通过不安全的协议进行传输。	运维终端	敏感信息泄露	账号、口令等通过不安全的协议进行传输，可能导致敏感信息被恶意人员嗅探并盗用，存在非授权访问的风险。	中
19		未禁止 root 账户远程登录。	数据库服务器、应用服务器、备份服务器	恶意攻击	恶意人员可能利用默认账户对系统进行试探攻击，存在潜在的安全隐患。	中
20		未设置审计管理、安全管理员账户，未实现管理用户的权限分离。	数据库	越权或滥用	无法实现不同权限角色间的监督，存在管理账户越权管理或滥用权限的风险。	中
21		审计记录保存时间不足六个月。	数据库服务器、应用服务器、数据库、UIS 超融合管理平台、中间件、终端安全管理系统（EDR）	抵赖	日志记录容易受到恶意篡改、删除，不便于对安全事件进行追踪和分析。	中

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
22		审计记录仅保存在本机，未进行定期备份。	运维终端	抵赖	日志记录容易受到恶意篡改、删除，不便于对安全事件进行追踪和分析。	中
23		未严格限制终端登录地址范围。	运维终端	恶意攻击	恶意用户可从网内任意地址尝试对设备进行访问、攻击，存在非授权访问的风险。	中
24		未定期进行漏洞扫描。	核心交换机、汇聚交换机 1、汇聚交换机 2、运维安全管理系统、基线核查系统、出口防火墙 1、出口防火墙 2、日志审计系统、WEB 应用防火墙、上网行为管理系统、UIS 超融合管理平台、OA 系统、终端安全管理系统（EDR）	恶意攻击	不能及时发现系统中存在的漏洞，并对漏洞进行修补，可能导致恶意人员利用系统漏洞对系统进行攻击。	中
25		未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形	核心交换机、汇聚交换机 1、汇聚交换机 2、运维安全管理系统、基线核查系统、出口防火墙 1、出口防火墙	敏感信息泄露	无可信链和可信验证，不能通过主动免疫可信验证技术提高系统自身安全防护能力，不能实现积极主动防御。	低

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
		成审计记录送至安全管理中心。	2、日志审计系统、WEB 应用防火墙、上网行为管理系统、数据库服务器、应用服务器、备份服务器、运维终端、UIS 超融合管理平台、终端安全管理系统（EDR）			
26		未配置“远程（RDP）连接要求使用指定的安全层”为“SSL”和未配置“设置客户端连接加密级别”为“高级别”，不能保证重要数据在传输过程中的完整性。	运维终端	篡改	可能导致重要数据在传输过程中被攻击者劫持、篡改，使重要数据的完整性遭到破坏。	中
27		未有备份恢复测试记录。	核心交换机、汇聚交换机 1、汇聚交换机 2、运维安全管理系统、基线核查系统、出口防火墙 1、出口防火墙 2、日志审计系统、WEB 应用防火	软硬件故障	一旦出现故障，可能由于各种原因无法利用备份数据进行恢复，造成重要数据丢失。	中

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
			墙、上网行为管理系统、数据库服务器、应用服务器、备份服务器、数据库、UIS 超融合管理平台、OA 系统、重要业务数据、重要个人信息、终端安全管理系统（EDR）、中间件			
28		未利用通信网络将关键数据定时批量传送至备用场地。	核心交换机、汇聚交换机 1、汇聚交换机 2、运维安全管理系统、基线核查系统、出口防火墙 1、出口防火墙 2、日志审计系统、WEB 应用防火墙、上网行为管理系统、数据库服务器、应用服务器、备份服务器、数据库、UIS 超融合管理平台、OA 系	物理环境影响	如机房遭受严重破坏，可能导致数据完全丢失。	中

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
			统、重要业务数据、重要个人信息、中间件、终端安全管理系统（EDR）			
29	安全管理制度	未具有管理制度评审记录和修订记录。	制度或记录类文档	管理不到位	可能导致安全管理体系与现实情况不符，导致管理文档无法落地。	中
30	安全建设管理	未组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，未有相关的方案评审记录。	制度或记录类文档	管理不到位	无法确保方案设计的合理性和正确性，不能确保系统安全方案的正确实践。	中
31		未在软件交付前通过第三方检测工具或人工检测软件包中可能存在的恶意代码。	制度或记录类文档	管理不到位	可能在上线前无法发现软件 BUG 和恶意代码未被发现，对组织的信息系统及声誉造成风险。	中
32		单位缺乏相关测试验收报告。	制度或记录类文档	管理不到位	无法保证经过测试验收的系统达到既定的安全性等目标。	中
33		该单位未在上线前进行安全性测试，未有相关安全测试报告。	制度或记录类文档	管理不到位	不能及时发现系统存在的安全性问题，造成系统的风险。	中
34		单位未对外包开发人员进行资格审查，未有相应的考核记录。	移动互联安全扩展要求	管理不到位	可能导致使用的人员未经严格的审查，无法满足岗位需求。	中
35	安全运维管理	未定期进行漏洞扫描，缺少漏洞扫描报告和修复	制度或记录类文档	管理不到位	可能导致系统补丁升级不到位，存在信息系统高风险漏洞，从而导致	中

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
		记录。			信息泄露风险。	
36		未提供变更方案和评审记录。	制度或记录类文档	管理不到位	变更事件发生时，临时制定变更方案，导致对变更事项应对不及时或无法应对，可能出现变更失败，并且在变更过程中对系统造成软硬件故障或数据丢失等风险。	中

6 等级测评结论

等级测评结论由安全问题风险分析结果和综合得分共同确定,判定依据如下表所示。

表 6-1 等级测评结论判定依据

等级测评结论	判定依据
优	被测对象中存在安全问题，但不会导致被测对象面临中、高等级安全风险，且综合得分 90 分以上（含 90 分）。
良	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且综合得分 80 分以上（含 80 分）。
中	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且综合得分 70 分以上（含 70 分）。
差	被测对象中存在安全问题,且会导致被测对象面临高等级安全风险，或综合得分低于 70 分。

综合得分计算方法如下:

设M为被测对象的综合得分，$M=V_t+V_m$，V_t和V_m根据下列公式计算:

$$V_t=\begin{cases}100\cdot y-\sum_{k=1}^{t}f(\omega_k)\cdot(1-x_k)\cdot S, & V_t>0\\ 0, & V_t\le 0\end{cases}$$

$$V_m=\begin{cases}100\cdot(1-y)-\sum_{k=1}^{m}f(\omega_k)\cdot(1-x_k)\cdot S, & V_m>0\\ 0, & V_m\le 0\end{cases}$$

$$0 \le x_k \le 1, \quad S = 100 \cdot \frac{1}{n}, \quad f(\omega_k) = \begin{cases} 1, & \omega_k = \text{一般} \\ 2, & \omega_k = \text{重要} \\ 3, & \omega_k = \text{关键} \end{cases}$$

其中，y 为关注系数，取值在 0 至 1 之间，由等级保护工作管理部门给出，默认值为 0.5。n 为被测对象涉及的总测评项数（不含不适用项，下同），t 为技术方面对应的总测评项数，V_t 为技术方面的得分，m 为管理方面对应的总测评项数，V_m 为管理方面的得分，ω_k 为测评项 k 的重要程度（分为一般、重要和关键），X_k 为测评项 k 的得分，如果测评项 k 涉及多测评对象，则 X_k 取值为多测评对象得分的算术平均值。

X_k 的得分计算如下：

测评项 k 涉及对象 / 测评项 k 定性判定	只涉及单个对象	涉及多个对象
符合	1	1
部分符合	0.5	计算测评对象平均分，取值在 0 至 1 之间。
不符合	0	0

注：当测评项 k 涉及多个对象时，针对每个对象的得分取值为 1、0.5 和 0。

根据第 5 章安全问题风险分析结果统计高、中、低风险安全问题的数量，利用综合得分计算公式计算出被测对象的综合得分，并将相关结果填入下表。

表 6-2 安全问题统计和综合得分

被测对象名称	安全问题数量			综合得分
	高风险	中风险	低风险	
OA 系统	0	30	6	78.39

依据 GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》和 GB/T 28448—2019《信息安全技术 网络安全等级保护测评要求》的第 2 级要求，经对 OA 系统的安全保护状况进行综合分析评价后，等级测评结论如下：

OA 系统本次等级测评的综合得分为 78.39，且不存在高等级安全风险，等级测评结论为中。

7 安全问题整改建议

表 7-1 安全问题整改建议

序号	安全类	安全问题	关联资产	整改建议
1	安全物理环境	未提供机房验收文档，机房防震等级不明确。	信息机房	建议提供机房防震证明文档，确定机房防震等级，以备日后查看。
2		未提供火灾自动消防系统的定期巡检和维护的记录。	信息机房	建议对消防设备进行定期巡检维护，并保存巡检记录。
3		未提供机房验收文档，无法明确建筑材料的耐火等级。	信息机房	建议妥善保留机房装饰设计验收文档，以证明主机房及辅助区采用具有耐火等级的建筑材料。
4		未部署湿度控制设备，不能防止水蒸气结露。	信息机房	建议部署湿度控制设备（如精密空调），能防止水蒸气结露。
5		机房未铺设防静电地板。	信息机房	建议机房统一使用防静电地板，以防止静电对电子设备和人员造成伤害。
6		未部署机房专用精密空调，不能设置湿度自动调节。	信息机房	建议机房部署湿度控制装置（如精密空调，湿度控制装置）进行控制机房内的湿度。
7	安全通信网络	未基于可信根对通信设备的系统引导程	安全通信网络	建议基于可信根对通信设备的系统引导程序、系统程

序号	安全类	安全问题	关联资产	整改建议
		序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。		序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
8	安全区域边界	未根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	办公区边界、安全管理区边界	建议办公区边界处部署下一代防火墙，根据会话状态信建立访问控制策略，为进出数据流提供明确的允许/拒绝访问能力。
9		未部署入侵防御系统或者有入侵防御模块的防火墙，因而不可对网络攻击行为进行监视。	安全管理区边界、办公区边界	建议部署网络入侵检测设备，在关键网络节点处对可能潜在的攻击行为进行监视。
10		未部署有防病毒网关或者有防病毒模块的防火墙，因而未能对恶意代码进行检测和清除。	办公区边界、安全管理区边界	建议网络层部署恶意代码防范设备对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。
11		无法对边界的流量和边界的安全事件进行审计。	安全管理区边界、办公区边界	建议边界处部署下一代防火墙，并且配置应用访问策略和启用入侵防御、病毒防护功能，使得能对边界的流量

序号	安全类	安全问题	关联资产	整改建议
				和边界的安全事件进行审计。
12		不能对边界的流量和边界的安全事件进行审计，故缺少边界的流量审计和安全事件审计记录。	办公区边界、安全管理区边界	建议办公区边界处部署下一代防火墙，使得能对边界的流量和边界的安全事件进行审计，审计记录至少包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。
13		不能对边界的流量和边界的安全事件进行审计，故无法对审计记录进行保护和备份。	安全管理区边界、办公区边界	建议安全管理区边界处部署下一代防火墙，并且配置应用访问策略和启用入侵防御、病毒防护功能，使得能对边界的流量和边界的安全事件进行审计，且应将审计记录上传至日志审计系统保存备份。
14		未基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	办公区边界、外网区边界、服务器区边界、安全管理区边界	建议基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

序号	安全类	安全问题	关联资产	整改建议
15	安全计算环境	未配置口令有效期策略。	备份服务器、UIS 超融合管理平台	建议配置口令的有效期策略，定期 90 天更换口令，防止口令被轻易破解。
16		未配置屏幕保护程序。	运维终端	建议配置屏幕保护程序，闲时 5 分钟自动退出，降低设备被非授权访问的风险。
17		未配置登录失败处理策略及登录连接超时策略。	备份服务器	建议配置登录失败处理策略，如失败 5 次锁定 5 分钟，防止恶意人员暴力破解账户口令。并配置登录连接超时策略，降低设备被非授权访问的风险。
18		进行远程管理时，鉴别信息通过不安全的协议进行传输。	运维终端	建议配置“远程（RDP）连接要求使用指定的安全层”为“SSL”和配置“设置客户端连接加密级别”为“高级别”，防止鉴别信息在传输过程中被窃听。
19		未禁止 root 账户远程登录。	数据库服务器、应用服务器、备份服务器	建议严格限制 root 账户的远程访问权限，禁止其进行远程登录。
20		未设置审计管理、安全管理员账户，未实现管理用户的权限分离。	数据库	建议设置审计管理、安全管理员账户，并根据业务需要设置各账户的权限，实现管理权限最小化，实现管理用户三权分立。

序号	安全类	安全问题	关联资产	整改建议
21		审计记录保存时间不足六个月。	数据库服务器、应用服务器、数据库、UIS 超融合管理平台、中间件、终端安全管理系统（EDR）	建议对日志进行集中存放，并确保保存时间能够达到半年以上。
22		审计记录仅保存在本机，未进行定期备份。	运维终端	建议对日志进行集中存放，定期备份日志，并确保保存时间能够达到半年以上。
23		未严格限制终端登录地址范围。	运维终端	建议对接入终端的网络地址范围进行限制。
24		未定期进行漏洞扫描。	核心交换机、汇聚交换机 1、汇聚交换机 2、运维安全管理系统、基线核查系统、出口防火墙 1、出口防火墙 2、日志审计系统、WEB 应用防火墙、上网行为管理系统、UIS 超融合管理平台、OA 系统、终端安全管理系统（EDR）	建议定期进行漏洞扫描，并在测试通过的前提下，及时修复风险漏洞，并保留漏洞修复记录
25		未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信	核心交换机、汇聚交换机 1、汇聚交换机 2、运维安全管理系统、基线核查系统、出口防火墙 1、出口	建议基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到

序号	安全类	安全问题	关联资产	整改建议
		验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	防火墙 2、日志审计系统、WEB 应用防火墙、上网行为管理系统、数据库服务器、应用服务器、备份服务器、运维终端、UIS 超融合管理平台、终端安全管理系统（EDR）	破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
26		未配置“远程（RDP）连接要求使用指定的安全层”为“SSL”和未配置“设置客户端连接加密级别”为“高级别”，不能保证重要数据在传输过程中的完整性。	运维终端	建议配置“远程（RDP）连接要求使用指定的安全层”为“SSL”和配置“设置客户端连接加密级别”为“高级别”保证重要数据在传输过程中的完整性。
27		未有备份恢复测试记录。	核心交换机、汇聚交换机 1、汇聚交换机 2、运维安全管理系统、基线核查系统、出口防火墙 1、出口防火墙 2、日志审计系统、WEB 应用防火墙、上网行为管理系统、数据库服务器、应用服务器、备份服务器、	建议建立备份恢复机制，定期对备份的数据进行恢复测试，确保在出现数据破坏时，可利用备份数据进行恢复。并妥善保存相关记录。

序号	安全类	安全问题	关联资产	整改建议
			数据库、UIS 超融合管理平台、OA 系统、重要业务数据、重要个人信息、终端安全管理系统（EDR）、中间件	
28		未利用通信网络将关键数据定时批量传送至备用场地。	核心交换机、汇聚交换机 1、汇聚交换机 2、运维安全管理系统、基线核查系统、出口防火墙 1、出口防火墙 2、日志审计系统、WEB 应用防火墙、上网行为管理系统、数据库服务器、应用服务器、备份服务器、数据库、UIS 超融合管理平台、OA 系统、重要业务数据、重要个人信息、中间件、终端安全管理系统（EDR）	建议利用通信网络将重要数据定时批量传送至备用场地，两地相距 30 公里以上。
29	安全管理制度	未具有管理制度评审记录和修订记录。	制度或记录类文档	建议在制度中明确对安全管理制度需进行定期或不定期的论证和审定工作，并在实际工作中遵照相关制度执行。

序号	安全类	安全问题	关联资产	整改建议
30	安全建设管理	未组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，未有相关的方案评审记录。	制度或记录类文档	建议组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，并进行论证后实施。
31		未在软件交付前通过第三方检测工具或人工检测软件包中可能存在的恶意代码。	制度或记录类文档	建议在交付前对开发单位提供软件源代码中可能存在的恶意代码通过第三方的检查工具或人工进行审查，并保留相关检查报告。
32		单位缺乏相关测试验收报告。	制度或记录类文档	建议对测试结果进行详细的记录，形成测试验收报告。
33		该单位未在上线前进行安全性测试，未有相关安全测试报告。	制度或记录类文档	建议系统在上线前进行安全性测试，并具有相关安全测试报告。
34		单位未对外包开发人员进行资格审查，未有相应的考核记录。	移动互联安全扩展要求	建议在移动业务应用软件开发前就对开发者进行资格审查。
35	安全运维管理	未定期进行漏洞扫描，缺少漏洞扫描报告和修复记录。	制度或记录类文档	建议指定专人定期对网络和主机、应用进行漏洞扫描并保存检测记录。
36		未提供变更方案和评审记录。	制度或记录类文档	建议制定系统变更相关制度，规定变更方案的申报审批程序，应要求方案包含变更类型、变更原因、变更过

序号	安全类	安全问题	关联资产	整改建议
				程、变更前评估等内容。

【正文结束】

附录A 被测对象资产

A.1 物理机房

附录 A 表-1 物理机房

序号	机房名称	物理位置	重要程度	备注
1	信息机房	广东省茂名市文明北路 232 号综合楼 5 楼 501	关键	-

A.2 网络设备

附录 A 表-2 网络设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度	备注
1	核心交换机	否	Comware V7	H3C S7500E-X	数据交换、访问控制	关键	-
2	汇聚交换机 1	否	Release 1119P11	S5560X-30C-EI	数据交换	重要	-
3	汇聚交换机 2	否	Release 1119P11	S5560X-30C-EI	数据交换	重要	-

A.3 安全设备

附录 A 表-3 安全设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度	备注
1	运维安全管理系统	否	深信服 OS V3.0.6	深信服 AC-1000-D603-PT	运维管理	重要	-
2	基线核查系统	否	深信服 OS V3.0.3	深信服 AC-1000-D602-PT	漏洞扫描	重要	-
3	出口防火	否	深信服 OS	深信服	访问控制	关键	-

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度	备注
	墙 1		AF 8.0.23	AF-2000-H642			
4	出口防火墙 2	否	深信服 OS AF 8.0.23	深信服 AF-2000-H642	访问控制	关键	-
5	日志审计系统	否	深信服 OS LAS 3.0.5	深信服 AC-1000-D601-PT	日志审计	重要	-
6	WEB 应用防火墙	否	深信服 OS AF 8.0.9	深信服 WAF-2000-H642	安全防护	关键	-
7	终端安全管理系统(EDR)	否	深信服 3.7.2	深信服 AC-1000-D603-PT	病毒查杀	重要	-
8	上网行为管理系统	否	深信服 OSAC12.0.26.076 Build20190725	深信服 AC-1000-D600-PT	上网行为管理	重要	-

A.4 服务器

附录 A 表-4 服务器

序号	设备名称	所属业务应用系统/平台名称	是否虚拟设备	操作系统及版本	数据库管理系统及版本	中间件及版本	重要程度	备注
1	数据库服务器	OA 系统	是	CentOS 7.9	Oracle 19.3	Tomcat 8.5.82	关键	-

序号	设备名称	所属业务应用系统/平台名称	是否虚拟设备	操作系统及版本	数据库管理系统及版本	中间件及版本	重要程度	备注
2	应用服务器	OA 系统	是	CentOS 7.9	-	Tomcat 7.0.69	关键	-
3	备份服务器	OA 系统	否	CentOS 6.8	-	-	重要	-

A.5 终端设备

附录 A 表-5 终端设备

序号	设备名称	是否虚拟设备	操作系统及版本	用途	重要程度	备注
1	运维终端	否	Windows 10 专业版	运维专用	一般	192.168.10.25

A.6 其他系统或设备

本次测评不涉及其他系统或设备。

A.7 系统管理软件/平台

附录 A 表-6 系统管理软件/平台

序号	系统管理软件/平台名称	所在设备名称	版本	主要功能	重要程度	备注
1	中间件 1	数据库服务器	Tomcat 8.5.82	信息发布	关键	-
2	中间件 2	应用服务器	Tomcat 7.0.69	信息发布	关键	-
3	数据库	数据库服务器	Oracle 19.3	数据存储	关键	-
4	UIS 超融合管理平台	-	V7.0 (E0750P09)	搭建云计算环境，实现仅服务器和交换机的极简的硬件架构平台和统	关键	-

序号	系统管理软件/平台名称	所在设备名称	版本	主要功能	重要程度	备注
				一的软件定义数据中心资源池。		

A.8 业务应用系统/平台

附录 A 表-7 业务应用系统/平台

序号	业务应用系统/平台名称	主要功能	业务应用软件及版本	开发厂商	重要程度	备注
1	OA 系统	办公无纸化，流程化	A8+企业版 V8.1	广州致远互联软件有限公司	关键	-

A.9 数据资源

附录 A 表-8 数据资源

序号	数据类别	所属业务应用	安全防护需求	重要程度
1	重要配置数据	OA 系统	完整性、可用性	重要
2	重要业务数据	OA 系统	保密性、完整性、可用性	关键
3	重要鉴别数据	OA 系统	保密性、完整性、可用性	关键
4	重要审计数据	OA 系统	完整性、可用性	重要
5	重要个人信息	OA 系统	保密性、完整性、可用性	关键

注：鉴别数据和重要配置数据分别在对应测评对象（网络设备、安全设备、服务器和终端、系统管理软件/平台、业务应用系统/平台）中汇总测评数据，重要审计数据在安全管理中心层面汇总测评数据，本节只汇总重要业务数据、重要个人信息和大数据资源的测评记录。

A.10密码产品

附录 A 表-9 密码产品

序号	产品/模块名称	生产厂商	商密型号	密码算法	用途	重要程度
-	-	-	-	-	-	-

A.11安全相关人员

附录 A 表-10 安全相关人员

序号	姓名	岗位/角色	联系方式	所属单位
1	叶永利	安全主管	0668-2920122	茂名职业技术学院
2	龙恒	安全管理员	13377766618	茂名职业技术学院
3	黄海东	系统管理员	-	茂名职业技术学院
4	麦才赞	审计管理员	-	茂名职业技术学院
5	陈思凡	机房管理员	-	茂名职业技术学院
6	吴国华	网络管理员	-	茂名职业技术学院
7	黄健	资产管理员	-	茂名职业技术学院

A.12安全管理文档

附录 A 表-11 安全管理文档

序号	文档名称	主要内容
1	《信息安全总体策略》	单位总体安全策略方针和目录、安全保障体系框架等。
2	《数据安全管理规范.》	数据安全方面的管理规定，包括数据的存放环境、使用规定。
3	《网络安全管理规范》	单位网络方面的管理，包括杀毒，计算机使用等内容。

序号	文档名称	主要内容
4	《应用安全管理规范》	关于单位应用系统的日常使用规范文档。
5	《设备操作规程》	关于设备日常操作规范和流程文档。
6	《软件操作手册》	关于单位安全设备操作、Linux 服务器配置手册、主机运维操作手册、软件操作手册、数据库日常运维操作手册等指导文档。
7	《防火墙配置和操作手册》	深信服防火墙配置和操作流程介绍。
8	《信息安全制度管理规范》	关于单位安全管理制度的修订、发布等管理要求。
9	《安全组织及职责管理规定》	关于单位安全管理机构、人员安全管理等内容。
10	《岗位安排及岗位职责》	关于单位人员岗位的配置，包含系统管理员、安全管理员、审计管理员等。
11	《授权和审批管理规定》	单位网络活动的日常审批和授权。
12	《安全组织机构-沟通合作》	日常运维与外部的交流合作。
13	《安全审核与检查管理制度》	关于单位安全检查、审查工作规范制度文档。
14	《安全检查报告 20230321》	单位系统的安全检测报告。
15	《内部人员信息安全管理规定》	关于单位内部员工日常的安全管理。
16	《人员管理制度》	关于单位人员录用、调岗、离岗管理制度文档。
17	《安全教育和培训制度》	关于单位安全培训、安全交流工作制度文档。
18	《外部人员访问管理制度》	关于单位针对外来人员访问管控制度文档。
19	《外部接入受控网络访问系统管理规范》	关于外部人员接入网络的规定和接入流程。
20	《OA 系统专家评审意见表》	关于 OA 系统的专家评审意见表。
21	《信息系统信息安全管理制度汇编 V2.0》	包含单位网络安全、信息安全、人员管理、设备管理等规定的文档。
22	《工程管理制度》	关于单位工程管理工作的文档。
23	《建设方案》	针对 OA 系统开发阶段建设的方案。
24	《测试及验收方案》	单位工程实方案，对时间、进度、质量等进行管

序号	文档名称	主要内容
		理和限制。
25	《系统交付管理》	关于第三方交付系统时的管理文档。
26	《OA 系统-需求规格说明书 》	关于 OA 系统开发业务需求、功能需求、用户需求等说明。
27	《系统变更管理制度》	关于系统变更流程和变更内容的管理规定。
28	《设备采购合同》	安全设备的采购合同。
29	《机房安全管理制度》	关于单位信息机房的管理文档，包含日常的运维和进出规定内容。
30	《介质安全管理规定》	关于单位介质的存储和传输规范文档。
31	《设备安全管理制度》	关于配套设施、软硬件维护管理方面的管理制度。
32	《网络安全管理规定》	关于网络和系统安全的管理文档。
33	《系统安全管理规定》	关于网络和系统安全的管理文档。
34	《恶意代码防范管理制度》	关于恶意代码防范的管理文档，包括防恶意代码软件的授权使用、恶意代码升级、定期查杀等内容。
35	《密码管理制度》	关于密码方面的管理文档，包括密码的使用和采购内容。
36	《变更控制管理制度》	单位变更管理文档，覆盖了变更管理更方面的要求。
37	《备份与恢复管理制度》	单位备份策略和周期的规定，重要数据日常备份管理。
38	《网络安全事件报告制度》	关于单位网络安全事件管理报告文档。
39	《校园网络信息安全应急预案》	校园应急事件处置流程的文档。

附录B 上次测评问题整改情况说明

OA 系统上次测评完成时间为 2022 年 10 月，由广东南方信息安全研究院负责测评工作，等级测评结论为中，综合得分为 73.85。

附录 B 表-1 上次测评问题整改情况

序号	安全问题	整改结果	情况说明
1	机房出入口未配置电子门禁系统	☑已整改 ☐未整改	经核查，信息机房出入口已安装了福鑫电子门禁系统，通过手机蓝牙和门禁卡对进入人员进行身份鉴别，且机房入口安排了专人值守，检查门禁系统存在机房进出电子记录表，记录内容包括开门时间、操作人员和打开方式。
2	机房内缺乏防静电措施（如防静电地板或铺设防静电地毯 ）（如：信息化机房）。 存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。	☐已整改 ☑未整改	暂未整改。
3	关键的应用服务和数据库服务网段未独立进行子网划分的情况	☐已整改 ☑未整改	暂未整改。
4	网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为	☐已整改 ☑未整改	暂未整改。
5	现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面	☐已整改 ☑未整改	暂未整改。
6	操作系统及数据库存在较多中风险的漏洞。	☑已整改 ☐未整改	经核查，已对存在中风险进行整改，设备存在部分低风险漏洞。
7	未能提供数据库系统重要数据的异地定时数据备份功能	☐已整改 ☑未整改	暂未整改。
8	未能提供应用软件系统重要数据的异地定时数据备份功能	☐已整改 ☑未整改	暂未整改。
9	单位未具备完整的安全	☐已整改	暂未整改。

序号	安全问题	整改结果	情况说明
	设计方案相关的文档。单位相关方案的设计的内容不够完善（如：制度文件、执行／记录文件）	☑未整改	
10	单位不了解现有密码相关的国家标准和行业标准。单位缺乏密码管理要求的制度文档（如：制度文件、执行／记录文件）	☐已整改 ☑未整改	暂未整改。

附录C　单项测评结果汇总

C.1 安全物理环境

附录 C　表-1 安全物理环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			物理位置选择	物理访问控制	防盗窃和防破坏	防雷击	防火	防水和防潮	防静电	温湿度控制	电力供应	电磁防护
1	信息机房	符合	1	1	2	1	0	1	0	0	2	1
		部分符合	1	0	0	0	2	1	1	1	0	0
		不符合	0	0	0	0	0	0	0	0	0	0
		不适用	0	0	0	0	0	0	0	0	0	0

附录 C　表-2 安全物理环境单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况	安全扩展要求
			无线接入点的物理位置（移动互联）
1	移动互联安全扩展	符合	0
		部分符合	0
		不符合	0

序号	测评对象	符合情况	安全扩展要求
			无线接入点的物理位置（移动互联）
	要求	不适用	1

C.2 安全通信网络

附录 C 表-3 安全通信网络单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求		
			网络架构	通信传输	可信验证
1	安全通信网络	符合	2	1	0
		部分符合	0	0	0
		不符合	0	0	1
		不适用	0	0	0

C.3 安全区域边界

附录 C 表-4 安全区域边界单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求					
			边界防护	访问控制	入侵防范	恶意代码防范	安全审计	可信验证
1	办公区边界	符合	1	3	0	0	0	0
		部分符合	0	0	0	0	0	0
		不符合	0	1	1	1	3	1
		不适用	0	0	0	0	0	0
2	外网区边界	符合	1	4	1	1	3	0
		部分符合	0	0	0	0	0	0
		不符合	0	0	0	0	0	1
		不适用	0	0	0	0	0	0
3	服务器区边界	符合	1	4	1	1	3	0
		部分符合	0	0	0	0	0	0
		不符合	0	0	0	0	0	1
		不适用	0	0	0	0	0	0

序号	测评对象	符合情况	安全通用要求					
			边界防护	访问控制	入侵防范	恶意代码防范	安全审计	可信验证
4	安全管理区边界	符合	1	3	0	0	0	0
		部分符合	0	0	0	0	0	0
		不符合	0	1	1	1	3	1
		不适用	0	0	0	0	0	0

附录 C 表-5 安全区域边界单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况	安全扩展要求		
			边界防护（移动互联）	访问控制（移动互联）	入侵防范（移动互联）
1	移动互联安全扩展要求	符合	0	0	0
		部分符合	0	0	0
		不符合	0	0	0
		不适用	1	1	5

C.4 安全计算环境

C.4.1 网络设备

附录 C 表-6 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	核心交换机	符合	3	4	3	2	0	0	1	0	0	0
		部分符合	0	0	0	1	0	0	0	1	0	0
		不符合	0	0	0	0	0	1	0	1	0	0
		不适用	0	0	0	2	1	0	0	0	1	2
2	汇聚	符合	3	4	3	2	0	0	1	0	0	0

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
	交换机 1	部分符合	0	0	0	1	0	0	0	1	0	0
		不符合	0	0	0	0	0	1	0	1	0	0
		不适用	0	0	0	2	1	0	0	0	1	2
3	汇聚交换机 2	符合	3	4	3	2	0	0	1	0	0	0
		部分符合	0	0	0	1	0	0	0	1	0	0
		不符合	0	0	0	0	0	1	0	1	0	0
		不适用	0	0	0	2	1	0	0	0	1	2

C.4.2 安全设备

附录 C 表-7 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	运维安全管理系统	符合	3	4	3	3	0	0	1	0	0	0
		部分符合	0	0	0	1	0	0	0	1	0	0
		不符合	0	0	0	0	0	1	0	1	0	0
		不适用	0	0	0	1	1	0	0	0	1	2
2	基线核查系统	符合	3	4	3	3	0	0	1	0	0	0
		部分符合	0	0	0	1	0	0	0	1	0	0
		不符合	0	0	0	0	0	1	0	1	0	0
		不适用	0	0	0	1	1	0	0	0	1	2

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
3	出口防火墙 1	符合	3	4	3	3	0	0	1	0	0	0
		部分符合	0	0	0	1	0	0	0	1	0	0
		不符合	0	0	0	0	0	1	0	1	0	0
		不适用	0	0	0	1	1	0	0	0	1	2
4	出口防火墙 2	符合	3	4	3	3	0	0	1	0	0	0
		部分符合	0	0	0	1	0	0	0	1	0	0
		不符合	0	0	0	0	0	1	0	1	0	0
		不适用	0	0	0	1	1	0	0	0	1	2
5	日志审计系统	符合	3	4	3	3	0	0	1	0	0	0
		部分符合	0	0	0	1	0	0	0	1	0	0
		不符合	0	0	0	0	0	1	0	1	0	0
		不适用	0	0	0	1	1	0	0	0	1	2
6	WEB 应用防火墙	符合	3	4	3	3	0	0	1	0	0	0
		部分符合	0	0	0	1	0	0	0	1	0	0
		不符合	0	0	0	0	0	1	0	1	0	0
		不适用	0	0	0	1	1	0	0	0	1	2
7	上网行为管理系统	符合	3	4	3	3	0	0	1	0	0	0
		部分符合	0	0	0	1	0	0	0	1	0	0
		不符合	0	0	0	0	0	1	0	1	0	0
		不适用	0	0	0	1	1	0	0	0	1	2
8	终端安全	符合	3	4	2	3	0	0	1	0	0	0
		部分符合	0	0	1	1	0	0	0	1	0	0

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
	管理系统（EDR）	不符合	0	0	0	0	0	1	0	1	0	0
		不适用	0	0	0	1	1	0	0	0	1	2

C.4.3 服务器和终端

附录 C 表-8 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	数据库服务器	符合	3	3	2	4	1	0	1	0	1	0
		部分符合	0	1	1	0	0	0	0	1	0	0
		不符合	0	0	0	0	0	1	0	1	0	0
		不适用	0	0	0	1	0	0	0	0	0	2
2	应用服务器	符合	3	3	2	4	1	0	1	0	1	0
		部分符合	0	1	1	0	0	0	0	1	0	0
		不符合	0	0	0	0	0	1	0	1	0	0
		不适用	0	0	0	1	0	0	0	0	0	2
3	备份服务器	符合	1	3	3	4	1	0	1	0	1	0
		部分符合	1	1	0	0	0	0	0	1	0	0
		不符合	1	0	0	0	0	1	0	1	0	0
		不适用	0	0	0	1	0	0	0	0	0	2

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
4	运维终端	符合	1	4	2	3	1	0	0	0	1	0
		部分符合	1	0	1	0	0	0	0	0	0	0
		不符合	1	0	0	1	0	1	1	0	0	0
		不适用	0	0	0	1	0	0	0	2	0	2

C.4.4 系统管理软件/平台

附录 C 表-9 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	中间件 1	符合	0	0	2	1	0	0	1	0	0	0
		部分符合	0	0	1	0	0	0	0	1	0	0
		不符合	0	0	0	0	0	0	0	1	0	0
		不适用	3	4	0	4	1	1	0	0	1	2
2	中间件 2	符合	0	0	2	1	0	0	1	0	0	0
		部分符合	0	0	1	0	0	0	0	1	0	0
		不符合	0	0	0	0	0	0	0	1	0	0
		不适用	3	4	0	4	1	1	0	0	1	2
3	数据库	符合	3	3	2	1	0	0	1	0	1	2
		部分符合	0	0	1	0	0	0	0	1	0	0
		不符合	0	1	0	0	0	0	0	1	0	0

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
		不适用	0	0	0	4	1	1	0	0	0	0
4	UIS 超融合管理平台	符合	2	4	2	1	0	0	1	0	1	0
		部分符合	1	0	1	1	0	0	0	1	0	0
		不符合	0	0	0	0	0	1	0	1	0	0
		不适用	0	0	0	3	1	0	0	0	0	2

C.4.5 业务应用系统/平台

附录 C 表-10 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	OA 系统	符合	3	4	3	1	0	0	1	0	1	2
		部分符合	0	0	0	1	0	0	0	1	0	0
		不符合	0	0	0	0	0	0	0	1	0	0
		不适用	0	0	0	3	1	1	0	0	0	0

C.4.6 数据资源

附录 C 表-11 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求			
			数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	重要业务	符合	1	0	0	0
		部分符合	0	1	0	0

序号	测评对象	符合情况	安全通用要求			
			数据完整性	数据备份恢复	剩余信息保护	个人信息保护
	数据	不符合	0	1	0	0
		不适用	0	0	1	2
2	重要个人信息	符合	1	0	0	2
		部分符合	0	1	0	0
		不符合	0	1	0	0
		不适用	0	0	1	0

C.4.7 其他系统或设备

本次测评不包含“安全计算环境单项测评结果汇总表（安全通用要求部分）”。

C.4.8 安全扩展要求

附录 C 表-12 安全计算环境单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况	安全扩展要求
			移动应用管控（移动互联）
1	移动互联安全扩展要求	符合	0
		部分符合	0
		不符合	0
		不适用	2

C.5 安全管理中心

附录 C 表-13 安全管理中心单项测评结果汇总表

序号	测评对象	符合情况	安全通用要求	
			系统管理	审计管理
1	安全管理中心	符合	2	2
		部分符合	0	0
		不符合	0	0
		不适用	0	0

C.6 安全管理制度

附录 C 表-14 安全管理制度单项测评结果汇总表

序号	测评对象	符合情况	安全通用要求			
			安全策略	管理制度	制定和发布	评审和修订
1	制度或记录类文档	符合	1	2	2	0
		部分符合	0	0	0	1
		不符合	0	0	0	0
		不适用	0	0	0	0

C.7 安全管理机构

附录 C 表-15 安全管理机构单项测评结果汇总表

序号	测评对象	符合情况	安全通用要求				
			岗位设置	人员配备	授权和审批	沟通和合作	审核和检查
1	制度或记录类文档	符合	2	1	2	3	1
		部分符合	0	0	0	0	0
		不符合	0	0	0	0	0
		不适用	0	0	0	0	0

C.8 安全管理人员

附录 C 表-16 安全管理人员单项测评结果汇总表

序号	测评对象	符合情况	安全通用要求			
			人员录用	人员离岗	安全意识教育和培训	外部人员访问管理
1	制度或记录类文档	符合	2	1	1	3
		部分符合	0	0	0	0

序号	测评对象	符合情况	安全通用要求			
			人员录用	人员离岗	安全意识教育和培训	外部人员访问管理
		不符合	0	0	0	0
		不适用	0	0	0	0

C.9 安全建设管理

附录 C 表-17 安全建设管理单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			定级和备案	安全方案设计	产品采购和使用	自行软件开发	外包软件开发	工程实施	测试验收	系统交付	等级测评	服务供应商选择
1	制度或记录类文档	符合	4	2	1	0	1	2	0	3	3	2
		部分符合	0	0	0	0	1	0	1	0	0	0
		不符合	0	1	0	0	0	0	1	0	0	0
		不适用	0	0	1	2	0	0	0	0	0	0

附录 C 表-18 安全建设管理单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况	安全扩展要求	
			移动应用软件采购（移动互联）	移动应用软件开发（移动互联）
1	移动互联安全扩展要求	符合	2	1
		部分符合	0	0
		不符合	0	1
		不适用	0	0

C.10安全运维管理

附录 C 表-19 安全运维管理单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求													
			环境管理	资产管理	介质管理	设备维护管理	漏洞和风险管理	网络和系统安全管理	恶意代码防范管理	配置管理	密码管理	变更管理	备份与恢复管理	安全事件处置	应急预案管理	外包运维管理
1	制度或记录类文档	符合	3	1	2	2	0	5	3	1	1	0	3	3	2	0
		部分符合	0	0	0	0	1	0	0	0	0	1	0	0	0	0
		不符合	0	0	0	0	0	0	0	0	0	0	0	0	0	0
		不适用	0	0	0	0	0	0	0	0	1	0	0	0	0	2

本次测评不包含“安全运维管理单项测评结果汇总表（安全扩展要求部分）”。

C.11其他安全要求指标

本次测评不包含其他安全要求指标。

附录D 单项测评结果记录

D.1 安全物理环境

D.1.1 安全通用要求部分

D.1.1.1 信息机房

控制点	测评项	结果记录	符合情况
物理位置选择	a)机房场地应选择在具有防震、防风和防雨等能力的建筑内；	经核查，信息机房位于广东省茂名市文明北路 232 号茂名职业技术学院综合楼 5 楼 501 室，所在建筑具有防震、防风和防雨等能力，机房内窗户已密封处理，屋顶、墙体没有开裂和渗水情况，具备防风和防雨的能力，但未提供机房验收文档，机房防震等	部分符合

控制点	测评项	结果记录	符合情况
		级不明确。	
	b)机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	经核查，信息机房位于综合楼 5 层 501 室，大楼共 7 层，未设置在建筑物顶层或地下室。	符合
物理访问控制	机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。	经核查，信息机房出入口已安装了福鑫电子门禁系统，通过手机蓝牙和门禁卡对进入人员进行身份鉴别，且机房入口安排了专人值守，门禁系统存在机房进出电子记录表，记录内容包括开门时间、操作人员和打开方式。	符合
防盗窃和防破坏	a)应将设备或主要部件进行固定，并设置明显的不易除去的标识；	经核查，信息机房内服务器、网络设备及安全设备是用螺丝固定在机柜上，能够有效防止设备从机柜上脱落，重要设备和主要部件、线缆设置明显的机打标签，标签内容包括：设备名称、设备编号、项目名称、本端、对端。	符合
	b)应将通信线缆铺设在隐蔽安全处。	经核查，信息机房采用桥架方式，将通信线缆铺设于机柜上方的线架中。	符合
防雷击	应将各类机柜、设施和设备等通过接地系统安全接地。	经核查，信息机房内所有机设施进行了安全接地。	符合
防火	a)机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；	经核查，信息机房已部署火灾自动消防系统(悬挂式七氟丙烷气体灭火装置)、门口设置了手提式二氧化碳灭火器，能够自动检测火情、自动报警，自动消防系统工作状态正常，但未提供火灾自动消防系统的定期巡检和维护的记录。	部分符合
	b)机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。	经核查，信息机房内采用防火门、实体墙等具有耐火等级的建筑材料，但未提供机房验收文档，从而无法明确建筑材料的耐火等级。	部分符合
防水和防潮	a)应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	经核查，信息机房位于大楼 5 层，机房为封闭式机房，墙壁采用防水防潮建筑材料；机房内未发现渗水漏水等	符合

控制点	测评项	结果记录	符合情况
		现象。	
	b)应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。	经核查，信息机房部署了 3 台康佳挂壁式空调、2 台格力立式空调，设置温度为 20°C，已配置小米温湿度传感器监控，定期对机房温度进行检查，但未部署湿度控制设备，不能防止水蒸气结露。空调下方已铺设安装好挡水板和排水措施，已安装漏水检测绳检测地下积水，及时处理机房水蒸气结露和地下积水的转移与渗透。	部分符合
防静电	应采用防静电地板或地面并采用必要的接地防静电措施。	经核查，信息机房未铺设防静电地板，仅对机柜、配电柜、设备进行了接地。	部分符合
温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。	经核查，信息机房内部署了 3 台康佳挂壁式空调、2 台格力立式空调，设置温度为 20°C，室内实时温度为 23.6°C，未部署机房专用精密空调，不能设置湿度自动调节。	部分符合
电力供应	a)应在机房供电线路上配置稳压器和过电压防护设备；	经核查，信息机房部署 1 组科华 UPS 电源系统，UPS 运行正常，可起到稳压和过电压防护作用。	符合
	b)应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。	经核查，机房部署 1 组科华品牌 UPS 电源系统，正常负荷情况下能保证机房内设备正常运行 30 分钟以上，具有 UPS 巡检和维护记录。	符合
电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。	经核查，机房通信线缆和强电线缆采用桥架方式部署，桥架位于机柜上方，强弱电桥架分开部署，可避免互相干扰。	符合

D.1.2 安全扩展要求部分

D.1.2.1 移动互联安全扩展要求

测评指标	控制点	测评项	结果记录	符合情况
移动互联安全扩展要求	无线接入点的物理位置	应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。	经核查，OA 系统仅使用 APP，用户通过互联网访问，未采用无线网络组网，该测评项不适用。	不适用

D.2 安全通信网络

D.2.1 安全通用要求部分

D.2.1.1 安全通信网络

控制点	测评项	结果记录	符合情况
网络架构	a)应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；	经核查，学校已依据工作职能、重要性、信息重要程度等划分对网络划分多个区域，并为各网络区域分配地址，安全管理区为 172.16.*.0/24，服务器区为 10.1.*.0/22，办公区为 192.168.*.0/24，网络区域与划分原则一致 。	符合
	b)应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	经核查，网络拓扑图与实际网络运行环境一致，被测网络已在外网边界处有部署出口防火墙，并配置了访问控制策略，重要网段部署在出口防火墙内部，未与外部网络直接相连，已在服务器区部署 WEB 应用防火墙，配置了访问控制策略，可避免非授权的访问。	符合
通信传输	应采用校验技术保证通信过程中数据的完整性。	经核查，服务器、安全设备、网络设备采用 https 协议或 ssh 协议进行远程管理、数据库采用 ssl 协议进行远程管理，应用系统、超融合管理平台采用 https 协议，均可保证通信过程中数据的完整性。	符合
可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并	经核查，未基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后	不符合

控制点	测评项	结果记录	符合情况
	在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	进行报警，并将验证结果形成审计记录送至安全管理中心。	

D.3 安全区域边界

D.3.1 安全通用要求部分

D.3.1.1 办公区边界

控制点	测评项	结果记录	符合情况
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	经核查，办公区边界处已部署核心交换机，并开启了访问控制策略，能够保证跨越边界的访问和数据流通过受控接口进行通信，不存在绕过边界的途径。	符合
访问控制	a)应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	经核查，办公区边界处在核心交换机上配置了与安全管理区、服务器区、外网边界之间的访问控制策略，最后一条策略默认拒绝所有。	符合
	b)应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	经核查，办公区边界核心交换机不存在多余和无效的访问控制策略，设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾，设备的访问控制策略实现最小化。	符合
	c)应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	经核查，办公区边界核心交换机访问控制策略中已设置源地址、目的地址、源端口、目的端口、协议，管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝。	符合
	d)应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	经核查，办公区边界没有根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	不符合

控制点	测评项	结果记录	符合情况
入侵防范	应在关键网络节点处监视网络攻击行为。	经核查，办公区边界未部署入侵防御系统或者有入侵防御模块的防火墙，因而不可对网络攻击行为进行监视。	不符合
恶意代码防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	经核查，办公区边界网络层面未部署有防病毒网关或者有防病毒模块的防火墙，因而未能对恶意代码进行检测和清除。	不符合
安全审计	a)应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经核查，办公区边界无法对边界的流量和边界的安全事件进行审计。	不符合
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经核查，办公区边界不能对边界的流量和边界的安全事件进行审计，故缺少边界的流量审计和安全事件审计记录。	不符合
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	经核查，办公区边界不能对边界的流量和边界的安全事件进行审计，故无法对审计记录进行保护和备份。	不符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	经核查，未基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	不符合

D.3.1.2 外网区边界

控制点	测评项	结果记录	符合情况
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	经核查，外网区边界处已部署出口防火墙 1、出口防火墙 2，并且配置了详细的访问控制策略，使得跨越边界的访问和数据流均通过边界设备提供的受控接口进行通信，不存在绕过	符合

控制点	测评项	结果记录	符合情况
		边界的途径。	
访问控制	a)应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	经核查，互联网边界处已部署有出口防火墙 1、出口防火墙 2，已配置并启用访问控制策略，最后一条策略为拒绝所有通信的策略。	符合
	b)应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	经核查，出口防火墙 1、出口防火墙 2 不同的访问控制策略之间的逻辑关系及前后排列顺序合理，不存在多余或无效的访问控制策略。	符合
	c)应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	经核查，出口防火墙 1、出口防火墙 2 已开启访问控制策略对源区域、源地址、目的地址、协议、端口等进行检测，以允许/拒绝数据包进出。	符合
	d)应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	经核查，出口防火墙 1、出口防火墙 2 已启用会话认证的访问控制策略，能为进出数据流提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视网络攻击行为。	经核查，出口防火墙 1、出口防火墙 2 已启用入侵防御策略，入侵防御特征库版本已自动更新至：20230722，可在关键网络节点处监视网络攻击行为。	符合
恶意代码防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	经核查，出口防火墙 1、出口防火墙 2 已启用病毒防护功能，并且病毒库已自动更新至 20230722，可对恶意代码进行检测和清除。	符合
安全审计	a)应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经核查，外网边界部署了出口防火墙 1、出口防火墙 2，已开启安全审计功能，并且防火墙已制定详细的访问控制规则和启用入侵防御和恶意代码检测功能，可对边界的流量进行审计和对边界的安全事件进行审计，审计覆盖到每个用户。	符合
	b)审计记录应包括事件的	经核查，出口防火墙 1、出口防火墙	符合

控制点	测评项	结果记录	符合情况
	日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	2 的流量事件审计记录包括：用户、应用、策略类型、处理动作、终端类型、级别、事件；入侵防御日志审计记录包括：攻击源、攻击时间、攻击描述、影响服务器、所处阶段，病毒防护审计记录包括:时间、日志级别、用户名称、源地址、源端口、目的地址、目的端口、归属地、病毒名称。	
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	经核查，出口防火墙 1、出口防火墙 2 日志记录已配置上传至日志审计系统保存备份，审计日志仅授权用户可进行访问，对审计记录进行保护，日志记录无法删除、修改或覆盖，测评时间为 2023 年 7 月 24 日，可查看到 2022 年 11 月 08 日之前的审计日志，保存周期大于 6 个月。	符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	经核查，未基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	不符合

D.3.1.3 服务器区边界

控制点	测评项	结果记录	符合情况
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	经核查，服务器区边界在核心交换机上配置访问控制策略保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信，不存在绕过边界的途径。	符合
访问控制	a)应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒	经核查，服务器区边界在核心交换机上配置了办公区、安全管理区、边界接入区之间的访问控制策略，最后一条策略默认拒绝所有。	符合

控制点	测评项	结果记录	符合情况
	绝所有通信；		
	b)应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	经核查，服务器区边界在核心交换机上配置了安全管理区与服务器区、边界接入区之间的访问控制策略，不同的访问控制策略之间的逻辑关系及前后排列顺序合理，不存在多余或无效的访问控制策略。	符合
	c)应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	经核查，服务器区边界在核心交换机、web 应用防火墙配置了服务器区与安全管理区、边界接入区之间的访问控制策略，策略可对源地址、源端口、目的地址、目的端口、协议进行检测，能对数据包的进出进行检测。	符合
	d)应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	经核查，服务器边界已部署 WEB 应用防火墙已启用会话认证的访问控制策略，能为进出数据流提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视网络攻击行为。	经核查，服务器区边界 WEB 应用防火墙支持对网络攻击行为防范，设备规则库已更新到最新，支持对端口扫描、强力攻击、木马后门攻击、应用漏洞攻击、网络蠕虫等攻击进行检测和监视。	符合
恶意代码防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	经核查，已在服务器边界部署 WEB 应用防火墙，WEB 应用防火墙具备防恶意代码功能，恶意代码规则库已更新至最新，可对网络节点的恶意代码进行检测和清除。	符合
安全审计	a)应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经核查，服务器边界处已部署 WEB 应用防火墙，已对重要节点进行审计，包括流量检测和行为检测，审计覆盖到每个用户，已对重要的用户行为和重要安全事件进行审计。	符合
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与	经核查，WEB 应用防火墙审计记录包括事件日期、时间、用户、攻击类型、攻击源 IP 等内容。	符合

控制点	测评项	结果记录	符合情况
	审计相关的信息；		
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	经核查，WEB 应用防火墙审计日志仅授权用户可进行访问，对审计记录进行保护，测评时间为 2023 年 7 月 24 日，可查看到 2022 年 11 月 8 日之前的审计日志，保存周期大于 6 个月，审计日志已传输至日志审计系统审计和保护，避免受到未预期的删除、修改或覆盖。	符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	经核查，未基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	不符合

D.3.1.4 安全管理区边界

控制点	测评项	结果记录	符合情况
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	经核查，安全管理区界处已部署核心交换机，并开启了访问控制策略，能够保证跨越边界的访问和数据流通过受控接口进行通信，不存在绕过边界的途径。	符合
访问控制	a)应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	经核查，安全管理区边界处在核心交换机上配置了与办公区、服务器区、外网边界之间的访问控制策略，最后一条策略默认拒绝所有。	符合
	b)应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	经核查，安全管理区边界核心交换机不存在多余和无效的访问控制策略，设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾，设备的访问控制策略实现最小化。	符合

控制点	测评项	结果记录	符合情况
	c)应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	经核查，安全管理区边界的核心交换机访问控制策略中已设置源地址、目的地址、源端口、目的端口、协议，管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝。	符合
	d)应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	经核查，安全管理区边界没有根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	不符合
入侵防范	应在关键网络节点处监视网络攻击行为。	经核查，安全管理区边界未部署入侵防御系统或者有入侵防御模块的防火墙，因而不可对网络攻击行为进行监视。	不符合
恶意代码防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	经核查，安全管理区边界网络层面未部署有防病毒网关或者有防病毒模块的防火墙，因而未能对恶意代码进行检测和清除。	不符合
安全审计	a)应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经核查，安全管理区边界无法对边界的流量和边界的安全事件进行审计。	不符合
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经核查，安全管理区边界不能对边界的流量和边界的安全事件进行审计，故缺少边界的流量审计和安全事件审计记录。	不符合
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	经核查，安全管理区边界不能对边界的流量和边界的安全事件进行审计，故无法对审计记录进行保护和备份。	不符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至	经核查，未基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	不符合

控制点	测评项	结果记录	符合情况
	安全管理中心。		

D.3.2 安全扩展要求部分

D.3.2.1 移动互联安全扩展要求

测评指标	控制点	测评项	结果记录	符合情况
移动互联安全扩展要求	边界防护	应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。	被测系统 APP 端部署在通用手机上，通过互联网接入，不存在无线接入设备，此项不适用。	不适用
	访问控制	无线接入设备应开启接入认证功能，并且禁止使用 WEP 方式进行认证，如使用口令，长度不小于 8 位字符。	被测系统 APP 端部署在通用手机上，通过互联网接入，不存在无线接入设备，此项不适用。	不适用
	入侵防范	a)应能够检测到非授权无线接入设备和非授权移动终端的接入行为；	被测系统 APP 端部署在通用手机上，通过互联网接入，不存在无线接入设备，此项不适用。	不适用
		b)应能够检测到针对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为；	被测系统 APP 端部署在通用手机上，通过互联网接入，不存在无线接入设备，此项不适用。	不适用
		c)应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态；	被测系统 APP 端部署在通用手机上，通过互联网接入，不存在无线接入设备，此项不适用。	不适用
		d)应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID 广播、WEP 认证等；	被测系统 APP 端部署在通用手机上，通过互联网接入，不存在无线接入设备，此项不适用。	不适用
		e)应禁止多个 AP 使用同一个认证密钥。	被测系统 APP 端部署在通用手机上，通过互联网接入，不存在无线接入设备，此项不适用。	不适用

D.4 安全计算环境

D.4.1 安全通用要求部分

D.4.1.1 网络设备

D.4.1.1.1 核心交换机

控制点	测评项	结果记录	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	经核查，核心交换机采用用户名+口令方式对登录的用户进行身份标识和鉴别，不存在同名账户，身份标识具有唯一性，交换机已设置口令策略，口令长度为 8 位，由数字、小写字母、大写字母和特殊字符组合而成，已开启口令 180 天定期更换策略。	符合
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	经核查，核心交换机已开启登录失败处理功能，失败 10 次锁定 5 分钟，已设置超时 15 分钟自动退出。	符合
	c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	经核查，核心交换机采 ssh 远程登录，已禁用 telnet 远程通信，可防止鉴别信息在网络传输过程中被窃听。	符合
访问控制	a)应对登录的用户分配账户和权限；	经核查，核心交换机已对登录的用户分配权限，存在网络管理员 super、系统管理员 long、安全管理员 nwctrl，审计管理员 shenjiyuan，不存在匿名账户。	符合
	b)应重命名或删除默认账户，修改默认账户的默认口令；	经核查，核心交换机不存在默认账户，不存在默认口令。	符合
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在；	经核查，核心交换机不存在多余、过期的账户，无共享账户。	符合
	d)应授予管理用户所需的最小权限，实现管理用户的	经核查，核心交换机已授予用户最小权限，已建立存在网络管理员 super、	符合

控制点	测评项	结果记录	符合情况
	权限分离。	系统管理员 long、安全管理员 nwctrl，审计管理员 shenjiyuan，不同账户具备不同的访问权限，已实现管理用户的权限分离。	
安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经核查，核心交换机已开启日志 Information Center、Security log 审计功能，审计覆盖到每个用户，已对重要的用户行为和重要安全事件进行审计。	符合
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经核查，核心交换机的审计记录包括日期时间、用户、登录 ip、登录是否成功、操作命令记录等审计信息。	符合
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	经核查，核心交换机审计记录已上传到日志审计系统进行审计和保护，仅审计管理员可以查看日志，日志已设置每周六备份到备份服务器，避免受到未预期的删除、修改或覆盖；现场测评时间为 20230724，审计记录最早可以查看 20220630，日志保存时间不少于六个月。	符合
入侵防范	a)应遵循最小安装的原则，仅安装需要的组件和应用程序；	经核查，核心交换机系统为定制私有系统，不支持客户自行安装程序和组件，此测评项不适用。	不适用
	b)应关闭不需要的系统服务、默认共享和高危端口；	经核查，核心交换机不存在默认共享，已关闭不需要的系统服务：Telnet、http、ftp 等，已关闭不需要的高危端口：445、137、138、139、21 等。	符合
	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	经核查，核心交换机已对管理终端地址进行限制，限制地址为 192.168.*.32-192.168.*.47 ，192.168.*.0-192.168,*.31。	符合
	d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于网络设备。	不适用

控制点	测评项	结果记录	符合情况
	内容符合系统设定要求；		
	e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经核查，核心交换机未定期进行漏洞扫描，在本次漏洞扫描中未发现高、中危安全漏洞。	部分符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于网络设备。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	经核查，核心交换机未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	经核查，核心交换机采用 ssh 协议进行通信，能保证重要数据在传输过程中的完整性。	符合
数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能；	经核查，核心交换机已提供本地备份功能，通过备份脚本手动每周备份至备份服务器，未有备份恢复测试记录。	部分符合
	b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	经核查，核心交换机未利用通信网络将核心交换机的重要数据定时批量传送至备用场地。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于网络设备。	不适用
个人信息保护	a)应仅采集和保存业务必需的用户个人信息；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于网络设备。	不适用
	b)应禁止未授权访问和非法使用用户个人信息。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于网络	不适用

控制点	测评项	结果记录	符合情况
		设备。	

D.4.1.1.2 汇聚交换机 1

控制点	测评项	结果记录	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	经核查，汇聚交换机 1 采用用户名+口令对登录的用户进行身份标识和鉴别，不存在同名账户。身份标识具有唯一性，口令长度要求为 8 位，由数字、小写字母、大写字母和特殊字符组合而成，已开启口令 180 天定期更换策略。	符合
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	经核查，汇聚交换机 1 已开启登录失败处理功能，失败 10 次锁定 5 分钟，已设置超时 15 分钟自动退出。	符合
	c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	经核查，汇聚交换机 1 采 ssh 远程登录，已禁用 telnet 远程通信，可防止鉴别信息在网络传输过程中被窃听。	符合
访问控制	a)应对登录的用户分配账户和权限；	经核查，汇聚交换机 1 分配了系统管理员 super、安全管理员 long，审计管理员 shenjiyuan，已对登录的用户分配账户和权限，并且不存在默认账户和匿名账户。	符合
	b)应重命名或删除默认账户，修改默认账户的默认口令；	经核查，汇聚交换机 1 不存在默认用户名，不存在默认口令。	符合
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在；	经核查，汇聚交换机 1 不存在多余、过期账户，无共享账户。	符合
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离。	经核查，汇聚交换机 1 分配了系统管理员 super、安全管理员 long，审计管理员 shenjiyuan，不同账户具备不同的访问权限，且各账户权限均为工	符合

控制点	测评项	结果记录	符合情况
		作所需最小权限,已实现管理员用户的权限分离。	
安全审计	a)应启用安全审计功能，审计覆盖到每个用户,对重要的用户行为和重要安全事件进行审计;	经核查，汇聚交换机 1 已开启日志 Information Center、Security log 审计功能，审计覆盖到每个用户，已对重要的用户行为和重要安全事件进行审计。	符合
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息;	经核查,汇聚交换机 1 审计记录包括事件的日期、时间、类型、主体标识、客体标识，结果、身份鉴别时间请求的来源。	符合
	c)应对审计记录进行保护,定期备份,避免受到未预期的删除、修改或覆盖等。	经核查,汇聚交换机 1 审计记录已上传到日志审计系统进行备份审计,仅审计管理员可以查看日志,审计记录最早可以查看 20220630，日志保存时间不少于六个月,日志记录无法删除、修改或覆盖。	符合
入侵防范	a)应遵循最小安装的原则，仅安装需要的组件和应用程序;	经核查,汇聚交换机 1 系统为定制私有系统,不支持客户自行安装程序和组件，此测评项不适用。	不适用
	b)应关闭不需要的系统服务、默认共享和高危端口;	经核查,汇聚交换机 1 不存在默认共享，已关闭不需要的系统服务：Telnet、http、ftp 等，已关闭不需要的高危端口：445、137、138、139、21 等。	符合
	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制;	经核查,汇聚交换机 1 已对管理终端地址进行限制，限制地址为 192.168.*.32-192.168.*.47 ，192.168.*.0-192.168,*.31。	符合
	d)应提供数据有效性检验功能,保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求;	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于网络设备。	不适用
	e)应能发现可能存在的已知漏洞,并在经过充分测试	经核查,汇聚交换机 1 未定期进行漏洞扫描，在本次漏洞扫描中未发现	部分符合

控制点	测评项	结果记录	符合情况
	评估后，及时修补漏洞。	高、中危安全漏洞。	
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于网络设备。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	经核查，汇聚交换机 1 未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。汇聚交换机 1。	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	经核查，汇聚交换机 1 采用 ssh 协议进行通信，能保证重要数据在传输过程中的完整性。	符合
数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能；	经核查，汇聚交换机 1 已提供本地备份功能，通过备份脚本手动每周备份至备份服务器，未有备份恢复测试记录。	部分符合
	b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	经核查，未利用通信网络将汇聚交换机 1 的重要数据定时批量传送至备用场地。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于网络设备。	不适用
个人信息保护	a)应仅采集和保存业务必需的用户个人信息；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于网络设备。	不适用
	b)应禁止未授权访问和非法使用用户个人信息。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于网络设备。	不适用

D.4.1.1.3 汇聚交换机 2

控制点	测评项	结果记录	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	经核查，汇聚交换机 2 采用用户名+口令对登录的用户进行身份标识和鉴别，不存在同名账户，身份标识具有唯一性，交换机已设置口令长度为 8 位，由数字、小写字母、大写字母和特殊字符组合而成，已开启口令 180 天定期更换策略。	符合
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	经核查，汇聚交换机 2 已开启登录失败处理功能，失败 10 次锁定 5 分钟，已设置超时 15 分钟自动退出。	符合
	c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	经核查，汇聚交换机 2 采 ssh 远程登录，已禁用 telnet 远程通信，可防止鉴别信息在网络传输过程中被窃听。	符合
访问控制	a)应对登录的用户分配账户和权限；	经核查，汇聚交换机 2 已对登录的用户分配权限，存在系统管理员 super、安全管理员 long，审计管理员 shenjiyuan。	符合
	b)应重命名或删除默认账户，修改默认账户的默认口令；	经核查，汇聚交换机 2 不存在默认账户，不存在默认口令。	符合
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在；	经核查，汇聚交换机 2 不存在多余、过期账户，无共享账户。	符合
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离。	经核查，汇聚交换机 2 存在系统管理员 super、安全管理员 long，审计管理员 shenjiyuan，不同用户具备不同的访问权限，已授予管理用户最小权限，实现管理用户的权限分离。	符合
安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经核查，汇聚交换机 2 已开启日志 Information Center、Security log 审计功能，审计覆盖到每个用户，已对重要的用户行为和重要安全事件进行审计。	符合

控制点	测评项	结果记录	符合情况
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经核查，汇聚交换机 2 审计记录包括事件的日期、时间、类型、主体标识、客体标识，结果、身份鉴别时间请求的来源。	符合
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	经核查，汇聚交换机 2 审计数据已上传日志审计系统保存备份，仅审计管理员可以查看日志，审计记录最早可以查看 20220321，日志保留大于 6 个月以上，日志记录无法删除、修改或覆盖。	符合
入侵防范	a)应遵循最小安装的原则，仅安装需要的组件和应用程序；	经核查，汇聚交换机 2 系统为定制私有系统，不支持客户自行安装程序和组件，此测评项不适用。	不适用
	b)应关闭不需要的系统服务、默认共享和高危端口；	经核查，汇聚交换机 2 不存在默认共享，已关闭不需要的系统服务：Telnet、http、ftp 等，已关闭不需要的高危端口：445、137、138、139、21 等。	符合
	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	经核查，汇聚交换机 2 已对管理终端地址进行限制，限制地址为 192.168.*.32-192.168.*.47 ，192.168.*.0-192.168,*.31。	符合
	d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于网络设备。	不适用
	e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经核查，汇聚交换机 2 未定期进行漏洞扫描，在本次漏洞扫描中未发现高、中危安全漏洞。	部分符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于网络设备。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程	经核查，汇聚交换机 2 未基于可信根对计算设备的系统引导程序、系统程	不符合

控制点	测评项	结果记录	符合情况
	序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	经核查，汇聚交换机 2 采用 ssh 协议进行通信，能保证重要数据在传输过程中的完整性。	符合
数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能；	经核查，汇聚交换机 2 已提供本地备份功能，通过备份脚本手动每周备份至备份服务器，未有备份恢复测试记录。	部分符合
	b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	经核查，未利用通信网络将汇聚交换机 2 的重要数据定时批量传送至备用场地。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于网络设备。	不适用
个人信息保护	a)应仅采集和保存业务必需的用户个人信息；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于网络设备。	不适用
	b)应禁止未授权访问和非法使用用户个人信息。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于网络设备。	不适用

D.4.1.2 安全设备

D.4.1.2.1 运维安全管理系统

控制点	测评项	结果记录	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具	经核查，运维安全管理系统采用用户名+口令方式进行登录，身份标识唯一，口令长度要求 10 位以上，由大	符合

控制点	测评项	结果记录	符合情况
	有复杂度要求并定期更换；	写字母+小写字母+数字+特殊字符其中 3 种组成，具备口令复杂度要求，已设置口令有效期为 90 天。	
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	经核查，运维安全管理系统已配置非法登录 5 次后锁定账户 2 分钟，已配置登录连接超时自动退出时长为 30 分钟。	符合
	c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	经核查，运维安全管理系统在通信过程中采用 https 协议传输数据，用户口令信息加密传输，可防止鉴别信息在网络传输过程中被窃听。	符合
访问控制	a)应对登录的用户分配账户和权限；	经核查，运维安全管理系统对可登录用户进行了账户和权限分配，包括超级管理员 admin、系统管理员 systemadmin、审计管理员 auditadmin、安全管理员 securityadmin 等账户，不同账户具备不同的访问权限，不存在匿名账户。	符合
	b)应重命名或删除默认账户，修改默认账户的默认口令；	经核查，运维安全管理系统存在默认账户 admin 无法删除、修改，但口令已改为复杂口令。	符合
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在；	经核查，运维安全管理系统中未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。	符合
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离。	经核查，运维安全管理系统设置了超级管理员 admin、系统管理员 systemadmin、审计管理员 auditadmin、安全管理员 securityadmin 等账户，不同账户具备不同的访问权限，且各账户权限均为工作所需最小权限，并且已限制超级管理员 admin 的使用，admin 需要经过审批才能使用。	符合
安全审计	a)应启用安全审计功能，审	经核查，运维安全管理系统已开启安	符合

控制点	测评项	结果记录	符合情况
	计覆盖到每个用户,对重要的用户行为和重要安全事件进行审计;	全审计功能,可对所有重要的用户行为和重要安全事件进行审计,审计范围覆盖系统内所有用户。	
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息;	经核查,运维安全管理系统日志审计记录包括：序号、时间、账号、登录地址、用户、模块、操作、操作结果等信息。	符合
	c)应对审计记录进行保护,定期备份,避免受到未预期的删除、修改或覆盖等。	经核查，测评时间为 2023 年 7 月 24 日,可查看到 2022 年 11 月 8 日审计日志，审计日志保存时间大于 6 个月,审计日志每周手动全备份到备份服务器，避免受到未预期的删除、修改或覆盖等。	符合
入侵防范	a)应遵循最小安装的原则,仅安装需要的组件和应用程序;	经核查,运维安全管理系统遵循最小安装原则,未安装不必要的组件和应用程序。	符合
	b)应关闭不需要的系统服务、默认共享和高危端口;	经核查,运维安全管理系统不存在不必要的默认共享,已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的服务。	符合
	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制;	经核查,已对运维安全管理系统的终端地址范围进行了限制，仅有 10.253.*.0-10.253.*.255 、192.168.*.31-192.168.*.47 、192.168.*.0-192.168.*.31 网段地址能够访问。	符合
	d)应提供数据有效性检验功能,保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求;	依据《信息安全技术 网络安全等级保护测评要求》，此项测评对象为终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、移动终端、移动终端管理系统、移动终端管理客户端和控制设备等,不适用于安全设备。	不适用
	e)应能发现可能存在的已知漏洞,并在经过充分测试评估后，及时修补漏洞。	经核查,运维安全管理系统未定期进行漏洞扫描,在本次漏洞扫描中未发现高、中危的安全漏洞。	部分符合

控制点	测评项	结果记录	符合情况
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	依据《信息安全技术 网络安全等级保护测评要求》，此项测评对象为终端和服务器等设备中的操作系统(包括宿主机和虚拟机操作系统)、移动终端、移动终端管理系统、移动终端管理客户端和控制设备等,不适用于安全设备。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证,并在检测到其可信性受到破坏后进行报警,并将验证结果形成审计记录送至安全管理中心。	经核查,运维安全管理系统未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	经核查,运维安全管理系统在通信过程中采用 https 协议传输数据，可保证重要数据在传输过程中的完整性。	符合
数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能;	经核查,运维安全管理系统所有数据每周手动全量备份至备份服务器中,未有备份恢复测试记录。	部分符合
	b)应提供异地数据备份功能,利用通信网络将重要数据定时批量传送至备用场地。	经核查,运维安全管理系统备份数据仅在本地保存,未利用通信网络将关键数据定时批量传送至备用场地。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	依据《信息安全技术 网络安全等级保护测评要求》，此项测评对象为终端和服务器等设备中的操作系统、业务应用系统、数据库管理系统、中间件和系统管理软件,不适用于安全设备。	不适用
个人信息保护	a)应仅采集和保存业务必需的用户个人信息;	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
	b)应禁止未授权访问和非法使用用户个人信息。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全	不适用

控制点	测评项	结果记录	符合情况
		设备。	

D.4.1.2.2 基线核查系统

控制点	测评项	结果记录	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	经核查，基线核查系统采用用户名+口令对用户进行身份鉴别；不存在空口令用户；以用户名作为用户身份唯一性标识；已配置符合复杂度要求的密码策略（口令长度设置至少 8 位，必须包含数字、大写字母、小写字母、特殊字符），已配置口令更换周期为 90 天。	符合
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	经核查，基线核查系统已配置非法登录 5 次后锁定账户 15 分钟，已配置登录连接超时自动退出时长为 15 分钟。	符合
	c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	经核查，基线核查系统在通信过程中采用 https 协议传输数据，用户口令信息加密传输，可防止鉴别信息在网络传输过程中被窃听。	符合
访问控制	a)应对登录的用户分配账户和权限；	经核查，基线核查系统对可登录用户进行了账户和权限分配，包括超级管理员 admin、系统管理员 systemadmin、审计管理员 auditadmin、安全管理员 securityadmin 等账户，不同账户具备不同的访问权限，不存在匿名账户。	符合
	b)应重命名或删除默认账户，修改默认账户的默认口令；	经核查，基线核查系统存在默认账户 admin 无法修改、删除，但口令已修改为复杂口令。	符合
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在；	经核查，基线核查系统中未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。	符合

控制点	测评项	结果记录	符合情况
	d)应授予管理用户所需的最小权限,实现管理用户的权限分离。	经核查,基线核查系统设置了超级管理员 admin、系统管理员 systemadmin、审计管理员 auditadmin、安全管理员 securityadmin 等账户,不同账户具备不同的访问权限,且各账户权限均为工作所需最小权限。并且已限制超级管理员 admin 的使用, admin 需要经过审批才能使用。	符合
安全审计	a)应启用安全审计功能,审计覆盖到每个用户,对重要的用户行为和重要安全事件进行审计;	经核查,基线核查系统已开启安全审计功能,可对所有重要的用户行为和重要安全事件进行审计,审计范围覆盖系统内所有用户。	符合
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息;	经核查,基线核查系统日志审计记录包括:序号、组件名称、日志级别、日志内容、日志产生时间。	符合
	c)应对审计记录进行保护,定期备份,避免受到未预期的删除、修改或覆盖等。	经核查,基线核查系统审计日志仅授权用户可进行访问,对审计记录进行保护,测评时间为 2023 年 7 月 24 日,可查看到 2022 年 11 月 8 日之前的审计日志,保存周期大于 6 个月,已设置每周全量备份日志到备份服务器。	符合
入侵防范	a)应遵循最小安装的原则,仅安装需要的组件和应用程序;	经核查,基线核查系统遵循最小安装原则,未安装不必要的组件和应用程序。	符合
	b)应关闭不需要的系统服务、默认共享和高危端口;	经核查,基线核查系统不存在不必要的默认共享,已关闭不必要的端口,仅开启业务所需端口,已禁用不必要的服务。	符合
	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制;	经核查,已对基线核查系统的终端地址范围进行了限制,仅有 10.253.*.0-10.253.*.255、192.168.*.31-192.168.*.47、192.168.*.0-192.168.*.31 网段地址能够访问。	符合

控制点	测评项	结果记录	符合情况
	d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
	e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经核查，基线核查系统未定期进行漏洞扫描，在本次漏洞扫描中未发现中、高危安全漏洞。	部分符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	经核查，基线核查系统未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	经核查，基线核查系统在通信过程中采用 https 协议传输数据，可保证重要数据在传输过程中的完整性。	符合
数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能；	经核查，基线核查系统所有数据每周手动全量备份至备份服务器中，未有备份恢复测试记录。	部分符合
	b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	经核查，基线核查系统备份数据仅在本地保存，未利用通信网络将关键数据定时批量传送至备用场地。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
个人信息保护	a)应仅采集和保存业务必需的用户个人信息；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用

控制点	测评项	结果记录	符合情况
	b)应禁止未授权访问和非法使用用户个人信息。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用

D.4.1.2.3 出口防火墙 1

控制点	测评项	结果记录	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	经核查，出口防火墙 1 采用用户名+口令的方式进行身份鉴别；不存在空口令用户；以用户名作为用户身份唯一性标识；已配置符合复杂度要求的密码策略（口令长度设置至少 8 位，必须包含数字、大写字母、小写字母、特殊字符其中 3 种），已设置口令最长使用天数为 90 天。	符合
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	经核查，出口防火墙 1 已配置非法登录 10 次后锁定账户 5 分钟，已配置登录连接超时自动退出时长为 30 分钟。	符合
	c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	经核查，出口防火墙 1 在通信过程中采用 https 协议传输数据，用户口令信息加密传输，可防止鉴别信息在网络传输过程中被窃听。	符合
访问控制	a)应对登录的用户分配账户和权限；	经核查，出口防火墙 1 对可登录用户进行了账户和权限分配，包括超级管理员 admin、系统管理员 systemadmin、审计管理员 auditadmin、安全管理员 securityadmin 等账户，不同账户具备不同的访问权限，不存在匿名账户。	符合
	b)应重命名或删除默认账户，修改默认账户的默认口令；	经核查，出口防火墙 1 存在默认账户 admin 无法修改、删除，但口令已修改为复杂口令。	符合
	c)应及时删除或停用多余的、过期的账户，避免共享	经核查，出口防火墙 1 中未发现多余或过期的账户，管理员用户与账户之	符合

控制点	测评项	结果记录	符合情况
	账户的存在；	间一一对应，未发现共享账户的情况。	
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离。	经核查，出口防火墙 1 设置了超级管理员 admin、系统管理员 systemadmin、审计管理员 auditadmin、安全管理员 securityadmin 等账户，不同账户具备不同的访问权限，且各账户权限均为工作所需最小权限。	符合
安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经核查，出口防火墙 1 已开启安全审计功能，可对所有重要的用户行为和重要安全事件进行审计，审计范围覆盖系统内所有用户。	符合
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经核查，出口防火墙 1 日志审计记录包括：序号、管理员、账号类型、操作方式、主机 IP、操作对象、操作、日期时间、描述、详情等信息。	符合
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	经核查，出口防火墙 1 审计日志仅授权用户可进行访问，对审计记录进行保护，测评时间为 2023 年 7 月 24 日，可查看到 2022 年 11 月 8 日之前的审计日志，保存周期大于 6 个月，审计日志已传送至日志审计系统备份审计，避免受到未预期的删除、修改或覆盖等。	符合
入侵防范	a)应遵循最小安装的原则，仅安装需要的组件和应用程序；	经核查，出口防火墙 1 遵循最小安装原则，未安装不必要的组件和应用程序。	符合
	b)应关闭不需要的系统服务、默认共享和高危端口；	经核查，出口防火墙 1 不存在不必要的默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的服务。	符合
	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	经核查，已对出口防火墙 1 的终端地址范围进行了限制，仅有 10.253.*.0-10.253.*.255、192.168.*.31-192.168.*.47、192.168.*.0-	符合

控制点	测评项	结果记录	符合情况
		192.168.*.31 网段地址能够访问。	
	d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
	e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经核查，出口防火墙 1 未定期进行漏洞扫描，在本次漏洞扫描中未发现高、中危安全漏洞。	部分符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	经核查，出口防火墙 1 未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	经核查，出口防火墙 1 在通信过程中采用 https 协议传输数据，可保证重要数据在传输过程中的完整性。	符合
数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能；	经核查，出口防火墙 1 所有数据所有数据每周手动全量备份至备份服务器中，未有备份恢复测试记录。	部分符合
	b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	经核查，出口防火墙 1 备份数据仅在本地保存，未利用通信网络将关键数据定时批量传送至备用场地。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
个人信息保护	a)应仅采集和保存业务必需的用户个人信息；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全	不适用

控制点	测评项	结果记录	符合情况
		设备。	
	b)应禁止未授权访问和非法使用用户个人信息。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用

D.4.1.2.4 出口防火墙 2

控制点	测评项	结果记录	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	经核查，出口防火墙 2 采用用户名+口令的方式对用户登录进行身份鉴别；不存在空口令用户；以用户名作为用户身份唯一性标识；已配置符合复杂度要求的密码策略，口令长度设置至少 8 位，必须包含数字、大写字母、小写字母、特殊字符其中 3 种，已设置口令最长使用天数为 90 天。	符合
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	经核查，出口防火墙 2 已配置非法登录 10 次后锁定账户 5 分钟，已配置登录连接超时自动退出时长为 30 分钟。	符合
	c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	经核查，出口防火墙 2 在通信过程中采用 https 协议传输数据，用户口令信息加密传输，可防止鉴别信息在网络传输过程中被窃听。	符合
访问控制	a)应对登录的用户分配账户和权限；	经核查，出口防火墙 2 对可登录用户进行了账户和权限分配，包括超级管理员 admin、系统管理员 systemadmin、审计管理员 auditadmin、安全管理员 securityadmin 等账户，不同账户具备不同的访问权限，不存在匿名账户。	符合
	b)应重命名或删除默认账户，修改默认账户的默认口令；	经核查，出口防火墙 2 存在默认账户 admin 无法修改、删除，但口令已修改为复杂口令。	符合

控制点	测评项	结果记录	符合情况
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在；	经核查，出口防火墙 2 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。	符合
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离。	经核查，出口防火墙 2 设置了超级管理员 admin、系统管理员 systemadmin、审计管理员 auditadmin、安全管理员 securityadmin 等账户，不同账户具备不同的访问权限，且各账户权限均为工作所需最小权限，并且已限制超级管理员 admin 的使用，admin 需要经过审批才能使用，不存在匿名账户。	符合
安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经核查，出口防火墙 2 已开启安全审计功能，可对所有重要的用户行为和重要安全事件进行审计，审计范围覆盖系统内所有用户。	符合
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经核查，出口防火墙 2 日志审计记录包括：序号、管理员、账号类型、操作方式、主机 IP、操作对象、操作、日期时间、描述、详情等信息。	符合
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	经核查，出口防火墙 2 审计日志仅授权用户可进行访问，对审计记录进行保护，测评时间为 2023 年 7 月 24 日，可查看到 2022 年 11 月 8 日之前的审计日志，保存周期大于 6 个月，审计日志已传送至日志审计系统进行审计。	符合
入侵防范	a)应遵循最小安装的原则，仅安装需要的组件和应用程序；	经核查，出口防火墙 2 遵循最小安装原则，未安装不必要的组件和应用程序。	符合
	b)应关闭不需要的系统服务、默认共享和高危端口；	经核查，出口防火墙 2 不存在不必要的默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的服务。	符合
	c)应通过设定终端接入方式或网络地址范围对通过	经核查，已对出口防火墙 2 的终端地址范围进行了限制，仅有 10.253.*.0-	符合

控制点	测评项	结果记录	符合情况
	网络进行管理的管理终端进行限制；	10.253.*.255 、 192.168.*.31-192.168.*.47 、 192.168.*.0-192.168.*.31 网段地址能够访问。	
	d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
	e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经核查，出口防火墙 2 未定期进行漏洞扫描，在本次漏洞扫描中未发现高、中危安全漏洞。	部分符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	经核查，出口防火墙 2 未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	经核查，出口防火墙 2 在通信过程中采用 https 协议传输数据，可保证重要数据在传输过程中的完整性。	符合
数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能；	经核查，出口防火墙 2 所有数据每周手动全量备份至备份服务器中，未有备份恢复测试记录。	部分符合
	b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	经核查，出口防火墙 2 备份数据仅在本地保存，未利用通信网络将关键数据定时批量传送至备用场地。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用

控制点	测评项	结果记录	符合情况
个人信息保护	a)应仅采集和保存业务必需的用户个人信息;	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
	b)应禁止未授权访问和非法使用用户个人信息。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用

D.4.1.2.5 日志审计系统

控制点	测评项	结果记录	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换;	经核查，日志审计系统采用用户名+口令方式进行登录，身份标识唯一，口令长度要求 8 位以上，由大写字母+小写字母+数字+特殊字符其中 3 种组成，具备口令复杂度要求，已设置口令更换周期为 90 天。	符合
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施;	经核查，日志审计系统已配置非法登录 5 次后锁定账户 10 分钟，已配置登录连接超时自动退出时长为 10 分钟。	符合
	c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	经核查，日志审计系统在通信过程中采用 https 协议传输数据，用户口令信息加密传输，可防止鉴别信息在网络传输过程中被窃听。	符合
访问控制	a)应对登录的用户分配账户和权限;	经核查，日志审计系统对可登录用户进行了账户和权限分配，包括超级管理员 admin、系统管理员 systemadmin、审计管理员 auditadmin、安全管理员 securityadmin 等账户，不同账户具备不同的访问权限，不存在匿名账户。	符合
	b)应重命名或删除默认账户，修改默认账户的默认口令;	经核查，日志审计系统存在默认账户 admin 无法修改、删除，但口令已修改为复杂口令。	符合

控制点	测评项	结果记录	符合情况
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在；	经核查，日志审计系统中未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。	符合
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离。	经核查，日志审计系统设置了超级管理员 admin、系统管理员 systemadmin、审计管理员 auditadmin、安全管理员 securityadmin 等账户，不同账户具备不同的访问权限，且各账户权限均为工作所需最小权限，并且已限制超级管理员 admin 的使用，admin 需要经过审批才能使用和不存在匿名账户。	符合
安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经核查，日志审计系统已开启安全审计功能，可对所有重要的用户行为和重要安全事件进行审计，审计范围覆盖系统内所有用户。	符合
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经核查，日志审计系统审计记录包括用户日志和系统日志，用户日志：序号、日志级别、日志内容、日志产生时间；系统日志：序号、组件名称、日志级别、日志内容、日志产生时间。	符合
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	经核查，日志审计系统审计日志仅授权用户可进行访问，对审计记录进行保护，测评时间为 2023 年 7 月 24 日，可查看到 2022 年 11 月 8 日之前的审计日志，保存周期大于 6 个月，审计日志每周手动全备份到备份服务器，日志保存时间不少于六个月，日志记录无法删除、修改或覆盖。	符合
入侵防范	a)应遵循最小安装的原则，仅安装需要的组件和应用程序；	经核查，日志审计系统遵循最小安装原则，未安装不必要的组件和应用程序。	符合
	b)应关闭不需要的系统服务、默认共享和高危端口；	经核查，日志审计系统不存在不必要的默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的服务。	符合

控制点	测评项	结果记录	符合情况
	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	经核查，已对日志审计系统的终端地址范围进行了限制，仅有 10.253.*.0-10.253.*.255 、 192.168.*.31-192.168.*.47 、 192.168.*.0-192.168.*.31 网段地址能够访问。	符合
	d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
	e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经核查，日志审计系统未定期进行漏洞扫描，在本次漏洞扫描中未发现高、中危安全漏洞。	部分符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	经核查，日志审计系统未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	经核查，日志审计系统在通信过程中采用 https 协议传输数据，可保证重要数据在传输过程中的完整性。	符合
数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能；	经核查，日志审计系统所有数据每周手动全量备份至备份服务器中，未有备份恢复测试记录。	部分符合
	b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	经核查，系统备份数据仅在本地保存，未利用通信网络将关键数据定时批量传送至备用场地。	不符合
剩余信息保护	应保证鉴别信息所在的存	依据《信息安全技术 网络安全等级	不适

控制点	测评项	结果记录	符合情况
	储空间被释放或重新分配前得到完全清除。	保护测评要求》，此项不适用于安全设备。	用
个人信息保护	a)应仅采集和保存业务必需的用户个人信息；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
	b)应禁止未授权访问和非法使用用户个人信息。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用

D.4.1.2.6 WEB 应用防火墙

控制点	测评项	结果记录	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	经核查，WEB 应用防火墙采用用户名+口令方式进行登录，身份标识唯一，口令长度要求 8 位以上，由大写字母+小写字母+数字+特殊字符其中 3 种组成，具备口令复杂度要求，已设置密码最长使用天数为 90 天。	符合
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	经核查，WEB 应用防火墙已配置非法登录 10 次后锁定账户 5 分钟，已配置登录连接超时自动退出时长为 100 分钟。	符合
	c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	经核查，WEB 应用防火墙在通信过程中采用 https 协议传输数据，用户口令信息加密传输，可防止鉴别信息在网络传输过程中被窃听。	符合
访问控制	a)应对登录的用户分配账户和权限；	经核查，WEB 应用防火墙对可登录用户进行了账户和权限分配，包括超级管理员 admin、系统管理员 systemadmin、审计管理员 auditadmin、安全管理员 securityadmin 等账户，不同账户具备不同的访问权限，不存在匿名账户。	符合
	b)应重命名或删除默认账	经核查，WEB 应用防火墙存在默认	符合

控制点	测评项	结果记录	符合情况
	户，修改默认账户的默认口令；	账户 admin 无法修改、删除，但口令已修改为复杂口令。	
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在；	经核查，WEB 应用防火墙中未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。	符合
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离。	经核查，WEB 应用防火墙设置了超级管理员 admin、系统管理员 systemadmin、审计管理员 auditadmin、安全管理员 securityadmin 等账户，不同账户具备不同的访问权限，且各账户权限均为工作所需最小权限，并且已限制超级管理员 admin 的使用，admin 需要经过审批才能使用和不存在匿名账户。	符合
安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经核查，WEB 应用防火墙已开启安全审计功能，可对所有重要的用户行为和重要安全事件进行审计，审计范围覆盖系统内所有用户。	符合
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经核查，WEB 应用防火墙日志审计记录包括：序号、管理员、账号类型、操作方式、主机 IP、操作对象、操作、日期时间、描述、详情等信息。	符合
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	经核查，WEB 应用防火墙审计日志仅授权用户可进行访问，对审计记录进行保护，测评时间为 2023 年 7 月 24 日，可查看到 2022 年 11 月 8 日之前的审计日志，保存周期大于 6 个月，审计日志已传送至日志审计系统备份审计，避免受到未预期的删除、修改或覆盖等。	符合
入侵防范	a)应遵循最小安装的原则，仅安装需要的组件和应用程序；	经核查，WEB 应用防火墙遵循最小安装原则，未安装不必要的组件和应用程序。	符合
	b)应关闭不需要的系统服务、默认共享和高危端口；	经核查，WEB 应用防火墙不存在不必要的默认共享，已关闭不必要的端	符合

控制点	测评项	结果记录	符合情况
		口，仅开启业务所需端口，已禁用不必要的服务。	
	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	经核查，已对 WEB 应用防火墙的终端地址范围进行了限制，仅有 10.253.*.0-10.253.*.255 、192.168.*.31-192.168.*.47 、192.168.*.0-192.168.*.31 网段地址能够访问。	符合
	d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
	e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经核查，WEB 应用防火墙未定期进行漏洞扫描，在本次漏洞扫描中未发现高、中危安全漏洞。	部分符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	经核查，WEB 应用防火墙未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	经核查，WEB 应用防火墙在通信过程中采用 https 协议传输数据，可保证重要数据在传输过程中的完整性。	符合
数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能；	经核查，WEB 应用防火墙所有数据每周手动全量备份至备份服务器中，未有备份恢复测试记录。	部分符合
	b)应提供异地数据备份功能，利用通信网络将重要数	经核查，WEB 应用防火墙备份数据仅在本地保存，未利用通信网络将关	不符合

控制点	测评项	结果记录	符合情况
	据定时批量传送至备用场地。	键数据定时批量传送至备用场地。	
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
个人信息保护	a)应仅采集和保存业务必需的用户个人信息；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
	b)应禁止未授权访问和非法使用用户个人信息。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用

D.4.1.2.7 上网行为管理系统

控制点	测评项	结果记录	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	经核查，上网行为管理系统采用用户名加口令的方式对用户登录进行身份鉴别；不存在空口令用户；以用户名作为用户身份唯一性标识；已配置符合复杂度要求的密码策略(口令长度设置至少 8 位，至少包含数字、大写字母、小写字母、特殊字符其中 2 种，已配置口令定期 90 天更换。	符合
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	经核查，上网行为管理系统已配置非法登录 5 次后锁定账户 1 分钟，已配置登录连接超时自动退出时长为 20 分钟。	符合
	c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	经核查，上网行为管理系统在通信过程中采用 https 协议传输数据，用户口令信息加密传输，可防止鉴别信息在网络传输过程中被窃听。	符合
访问控制	a)应对登录的用户分配账户和权限；	经核查，上网行为管理系统对可登录用户进行了账户和权限分配，包括超级管理员 admin、系统管理员	符合

控制点	测评项	结果记录	符合情况
		systemadmin、审计管理员 auditadmin、安全管理员 securityadmin 等账户，不同账户具备不同的访问权限，不存在匿名账户。	
	b)应重命名或删除默认账户，修改默认账户的默认口令；	经核查，上网行为管理系统存在默认账户 admin 无法修改、删除，但口令已修改为复杂口令。	符合
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在；	经核查，上网行为管理系统中未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。	符合
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离。	经核查，上网行为管理系统设置了超级管理员 admin、系统管理员 systemadmin、审计管理员 auditadmin、安全管理员 securityadmin 等账户，不同账户具备不同的访问权限，且各账户权限均为工作所需最小权限，并且已限制超级管理员 admin 的使用，admin 需要经过审批才能使用和不存在匿名账户。	符合
安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经核查，上网行为管理系统已开启安全审计功能，可对所有重要的用户行为和重要安全事件进行审计，审计范围覆盖系统内所有用户。	符合
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经核查，上网行为管理系统日志审计记录包括：序号、来源、类型、时间、详细信息等信息。	符合
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	经核查，上网行为管理系统审计日志已传送至日志审计系统备份审计，仅授权用户可进行访问，可对审计记录进行保护，测评时间为 2023 年 7 月 24 日，最早可查看到 2022 年 12 月 01 日的审计日志，日志保存时间不少于六个月，日志记录无法删除、修改或覆盖。	符合

控制点	测评项	结果记录	符合情况
入侵防范	a)应遵循最小安装的原则，仅安装需要的组件和应用程序；	经核查，上网行为管理系统遵循最小安装原则，未安装不必要的组件和应用程序。	符合
	b)应关闭不需要的系统服务、默认共享和高危端口；	经核查，上网行为管理系统不存在不必要的默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的服务。	符合
	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	经核查，已对上网行为管理系统的终端地址范围进行了限制，仅有 10.253.*.0-10.253.*.255 、192.168.*.31-192.168.*.47 、192.168.*.0-192.168.*.31 网段地址能够访问。	符合
	d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
	e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经核查，上网行为管理系统未定期进行漏洞扫描，在本次漏洞扫描中发现高、中危安全漏洞。	部分符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	经核查，上网行为管理系统未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	经核查，上网行为管理系统在通信过程中采用 https 协议传输数据，可保证重要数据在传输过程中的完整性。	符合

控制点	测评项	结果记录	符合情况
数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能；	经核查，上网行为管理系统所有数据每周手动全量备份至备份服务器中，未有备份恢复测试记录。	部分符合
	b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	经核查，上网行为管理系统系统备份数据仅在本地保存，未利用通信网络将关键数据定时批量传送至备用场地。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
个人信息保护	a)应仅采集和保存业务必需的用户个人信息；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
	b)应禁止未授权访问和非法使用用户个人信息。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用

D.4.1.2.8 终端安全管理系统（EDR）

控制点	测评项	结果记录	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	经核查，终端安全管理系统采用用户名加口令的方式对用户登录进行身份鉴别；不存在空口令用户；以用户名作为用户身份唯一性标识；已配置符合复杂度要求的密码策略(口令长度设置至少 8 位，必须包含数字、大写字母、小写字母、特殊字符其中 3 种)，已开启口令超过 90 天强制修改。	符合
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	经核查，终端安全管理系统已配置非法登录 5 次后锁定账户 5 分钟，已配置登录连接超时自动退出时长为 10 分钟。	符合
	c)当进行远程管理时，应采	经核查，终端安全管理系统在通信过	符合

控制点	测评项	结果记录	符合情况
	取必要措施防止鉴别信息在网络传输过程中被窃听。	程中采用 https 协议传输数据，用户口令信息加密传输，可防止鉴别信息在网络传输过程中被窃听，不存在匿名账户。	
访问控制	a)应对登录的用户分配账户和权限；	经核查，终端安全管理系统对可登录用户进行了账户和权限分配，包括超级管理员 admin、系统管理员 systemadmin、审计管理员 auditadmin、安全管理员 securityadmin 等账户，不同账户具备不同的访问权限。	符合
	b)应重命名或删除默认账户，修改默认账户的默认口令；	经核查，终端安全管理系统存在默认账户 admin 无法修改、删除，但口令已修改为复杂口令。	符合
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在；	经核查，终端安全管理系统中未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。	符合
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离。	经核查，终端安全管理系统设置了超级管理员 admin、系统管理员 systemadmin、审计管理员 auditadmin、安全管理员 securityadmin 等账户，不同账户具备不同的访问权限，且各账户权限均为工作所需最小权限，并且已限制超级管理员 admin 的使用，admin 需要经过审批才能使用和不存在匿名账户。	符合
安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经核查，终端安全管理系统已开启安全审计功能，可对所有重要的用户行为和重要安全事件进行审计，审计范围覆盖系统内所有用户。	符合
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经核查，终端安全管理系统日志审计记录包括：序号、操作时间、用户、ip 地址、操作类型、操作对象、操作描述、操作结果。	符合
	c)应对审计记录进行保护，	经核查，终端安全管理系统审计日志	部分

控制点	测评项	结果记录	符合情况
	定期备份，避免受到未预期的删除、修改或覆盖等。	已传送至日志审计系统备份审计，仅授权用户可进行访问，对审计记录进行保护，测评时间为 2023 年 7 月 24 日，最早可查看到 2023 年 5 月 5 日的审计日志，日志保存时间小于 6 个月。	符合
入侵防范	a)应遵循最小安装的原则，仅安装需要的组件和应用程序；	经核查，终端安全管理系统遵循最小安装原则，未安装不必要的组件和应用程序。	符合
	b)应关闭不需要的系统服务、默认共享和高危端口；	经核查，终端安全管理系统不存在不必要的默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的服务。	符合
	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	经核查，已对终端安全管理系统的终端地址范围进行了限制，仅有 10.253.*.0-10.253.*.255 、192.168.*.31-192.168.*.47 、192.168.*.0-192.168.*.31 网段地址能够访问。	符合
	d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
	e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经核查，终端安全管理系统未定期进行漏洞扫描，在本次漏洞扫描中发现高 、中危安全漏洞。	部分符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形	经核查，终端安全管理系统未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。	不符合

控制点	测评项	结果记录	符合情况
	成审计记录送至安全管理中心。		
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	经核查，终端安全管理系统在通信过程中采用 https 协议传输数据，可保证重要数据在传输过程中的完整性。	符合
数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能；	经核查，终端安全管理系统所有数据每周手动全量备份至备份服务器中，未有备份恢复测试记录。	部分符合
	b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	经核查，终端安全管理系统数据仅本地备份保存，未利用通信网络将关键数据定时批量传送至备用场地。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
个人信息保护	a)应仅采集和保存业务必需的用户个人信息；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用
	b)应禁止未授权访问和非法使用用户个人信息。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于安全设备。	不适用

D.4.1.3 服务器和终端

D.4.1.3.1 数据库服务器

控制点	测评项	结果记录	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	经核查，数据库服务器采用账户名+口令方式进行登录，身份标识唯一，不存在空口令账户；已配置口令复杂度策略，口令须包含数字、大写字母、小写字母，长度不少于 8 位；已配置口令有效期为 90 天。	符合
	b)应具有登录失败处理功	经核查，数据库服务器登录失败 5 次	符合

控制点	测评项	结果记录	符合情况
	能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	锁定 3 分钟，已设置超时 5 分钟自动退出。	
	c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	经核查，数据库服务器未启用 Telnet 服务，采用 SSH 协议进行远程管理，可防止鉴别信息在网络传输过程中被窃听。	符合
访问控制	a)应对登录的用户分配账户和权限；	经核查，数据库服务器已对登录的用户分配账户和权限，已配置超级管理员账户：root、数据库管理员账户：oracle、安全管理员账户：anquan、审计管理员账户：shenji，未禁止 root 账户远程登录，不存在匿名账户。	部分符合
	b)应重命名或删除默认账户，修改默认账户的默认口令；	经核查，系统默认账户 root 不宜重命名，口令已修改为复杂口令。	符合
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在；	经核查，数据库服务器已禁用多余账户，不存在过期账户，不存在共享账户的情况。	符合
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离。	经核查，数据库服务器已配置数据库管理员账户：oracle、安全管理员账户：anquan、审计管理员账户：shenji，账户权限已分离，分别拥有其工作所需的最小权限，root 账户要经过授权审批才能使用，实现管理用户的权限分离。	符合
安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经核查，数据库服务器已开启 rsyslog 系统日志和 auditd 安全审计功能，守护进程运行正常， 审计覆盖到每个用户，可实现对重要的用户行为和重要安全事件的安全审计。	符合
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经核查，数据库服务器审计记录包括 message、audit 等审计记录，message 日志及 secure 日志包括：日期、时间、服务器、进程、详细信息等内容；	符合

控制点	测评项	结果记录	符合情况
		wtmp 日志包括：账户名、登录方式、日期、时间、终端 IP 地址等内容；audit 日志包括：类型、时间戳、事件 ID、进程 ID、用户名、执行命令、是否成功等内容。	
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	经核查，数据库服务器重要日志文件及日志配置文件权限值均未超过 644，仅授权用户可管理，已将数据库服务器纳入日志审计系统的审计范围，现场测评时间为 2023 年 7 月 24 日，日志最早可查询时间为 2023 年 2 月 23 日，日志保存时间不足六个月。	部分符合
入侵防范	a)应遵循最小安装的原则，仅安装需要的组件和应用程序；	经核查，数据库服务器遵循最小安装原则，未安装多余的组件和应用程序。	符合
	b)应关闭不需要的系统服务、默认共享和高危端口；	经核查，数据库服务器操作系统不存在不必要的默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的服务。	符合
	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	经核查，已通过服务器区防火墙限制仅 10.1.15.*、192.168.*.0/27 可远程登录数据库服务器。	符合
	d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于服务器。	不适用
	e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经核查，已部署深信服终端安全管理系统，数据库服务器已安装深信服终端安全管理系统 Agent，漏洞库更新于 2023 年 07 月 22 日，已设置自动扫描任务，每天 0 点对数据库服务器进行一次漏洞扫描，近期扫描记录中未发现安全漏洞，且在本次漏洞扫描中未发现已知的风险漏洞。	符合

控制点	测评项	结果记录	符合情况
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	经核查，已部署深信服终端安全管理系统，数据库服务器已安装深信服终端安全管理系统 Agent，能及时识别入侵和病毒行为，病毒库最近更新时间为 2023 年 07 月 22 日，现场测评时间为 2023 年 7 月 24 日。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	经核查，数据库服务器未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	经核查，数据库服务器在通信过程中采用 ssh 协议传输数据，可保证重要数据在传输过程中的完整性。	符合
数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能；	经核查，管理员每半个月手动创建数据库服务器的快照一次，存在快照记录，未有备份恢复测试记录。	部分符合
	b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	经核查，未利用通信网络将数据库服务器的重要数据定时批量传送至备用场地。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	经核查，数据库服务器为 Linux 操作系统，用户的鉴别信息所在的存储空间由操作系统自动分配，Linux 自身资源回收机制可满足剩余信息保护。	符合
个人信息保护	a)应仅采集和保存业务必需的用户个人信息；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于服务器。	不适用
	b)应禁止未授权访问和非法使用用户个人信息。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于服务器。	不适用

D.4.1.3.2 应用服务器

控制点	测评项	结果记录	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	经核查，应用服务器采用账户名+口令方式进行登录，身份标识唯一，不存在空口令账户；已配置口令复杂度策略，口令须包含数字、大写字母、小写字母，长度不少于 8 位；已配置口令有效期为 90 天。	符合
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	经核查，应用服务器登录失败 5 次锁定 3 分钟，已配置登录连接超时 5 分钟自动退出。	符合
	c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	经核查，应用服务器未启用 Telnet 服务，采用 SSH 协议进行远程管理，可防止鉴别信息在网络传输过程中被窃听。	符合
访问控制	a)应对登录的用户分配账户和权限；	经核查，应用服务器已对登录的用户分配账户和权限，已配置超级管理员账户：root、安全管理员账户：anquan、审计管理员账户：shenji、普通账户：u01，未限制超级管理员账户：root 的远程登录权限，不存在匿名账户。	部分符合
	b)应重命名或删除默认账户，修改默认账户的默认口令；	经核查，系统默认账户 root 不宜重命名，口令已修改为复杂口令。	符合
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在；	经核查，应用服务器已禁用多余账户，不存在过期账户，不存在共享账户的情况。	符合
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离。	经核查，应用服务器已配置数据库管理员账户：oracle、安全管理员账户：anquan、审计管理员账户：shenji、普通账户：u01，账户权限已分离，分别拥有其工作所需的最小权限，root 账号要通过审批授权才能使用，可实现管理用户的权限分离。	符合

控制点	测评项	结果记录	符合情况
安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经核查，应用服务器已开启 rsyslog 系统日志和 auditd 安全审计功能，守护进程运行正常， 审计覆盖到每个用户，可实现对重要的用户行为和重要安全事件的安全审计。	符合
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经核查，应用服务器审计记录包括 message、audit 等审计记录，message 日志及 secure 日志包括：日期、时间、服务器、进程、详细信息等内容；wtmp 日志包括：账户名、登录方式、日期、时间、终端 IP 地址等内容；audit 日志包括：类型、时间戳、事件 ID、进程 ID、用户名、执行命令、是否成功等内容。	符合
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	经核查，应用服务器重要日志文件及日志配置文件权限值均未超过 644，仅授权用户可管理，已将应用服务器纳入日志审计系统的审计范围，现场测评时间为 2023 年 7 月 24 日，日志最早可查询时间为 2023 年 3 月 7 日，日志保存时间不足六个月。	部分符合
入侵防范	a)应遵循最小安装的原则，仅安装需要的组件和应用程序；	经核查，应用服务器遵循最小安装原则，未安装多余的组件和应用程序。	符合
	b)应关闭不需要的系统服务、默认共享和高危端口；	经核查，应用服务器操作系统不存在不必要的默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的服务。	符合
	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	经核查，已通过服务器区防火墙限制仅 10.1.15.*、192.168.*.0/27 可远程登录应用服务器。	符合
	d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于服务器。	不适用

控制点	测评项	结果记录	符合情况
	e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经核查，已部署深信服终端安全管理系统，应用服务器已安装深信服终端安全管理系统 Agent，漏洞库更新于 2023 年 07 月 22 日，已设置自动扫描任务，每天 0 点对应用服务器进行一次漏洞扫描，近期扫描记录中未发现安全漏洞，且在本次漏洞扫描中未发现已知的风险漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	经核查，已部署深信服终端安全管理系统，应用服务器已安装深信服终端安全管理系统 Agent，能及时识别入侵和病毒行为，病毒库最近更新时间为 2023 年 07 月 22 日，现场测评时间为 2023 年 7 月 24 日。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	经核查，应用服务器未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	经核查，应用服务器在通信过程中采用 ssh 协议传输数据，可保证重要数据在传输过程中的完整性。	符合
数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能；	经核查，管理员每半个月手动创建应用服务器的快照一次，存在快照记录，未有备份恢复测试记录。	部分符合
	b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	经核查，未利用通信网络将应用服务器的重要数据定时批量传送至备用场地。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	经核查，应用服务器为 Linux 操作系统，用户的鉴别信息所在的存储空间由操作系统自动分配，Linux 自身资源回收机制可满足剩余信息保护。	符合

控制点	测评项	结果记录	符合情况
个人信息保护	a)应仅采集和保存业务必需的用户个人信息;	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于服务器。	不适用
	b)应禁止未授权访问和非法使用用户个人信息。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于服务器。	不适用

D.4.1.3.3 备份服务器

控制点	测评项	结果记录	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换;	经核查，备份服务器采用账户名+口令方式进行登录，身份标识唯一，不存在空口令账户;已配置口令复杂度策略，口令长度不少于 8 个字符，须同时包含大写字母、小写字母和特殊字符；未配置口令有效期策略。	部分符合
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施;	经核查，备份服务器未配置登录失败处理策略和登录超时自动退出策略。	不符合
	c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	经核查，备份服务器未启用 Telnet 服务，采用 SSH 协议进行远程管理，可防止鉴别信息在网络传输过程中被窃听。	符合
访问控制	a)应对登录的用户分配账户和权限;	经核查，备份服务器已对登录的用户分配账户和权限，已配置超级管理员账户：root、系统管理员账户：sangfor，审计管理员账户：shenji，安全管理员账户：anquan，普通账户：peanut001，未限制默认超级管理员账户：root 的远程登录权限，不存在匿名账户。	部分符合
	b)应重命名或删除默认账户，修改默认账户的默认口令;	经核查，系统默认账户 root 不宜重命名，登录口令已修改为复杂口令。	符合

控制点	测评项	结果记录	符合情况
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在；	经核查，备份服务器已禁用多余账户，不存在过期账户 ，不存在共享账户的情况。	符合
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离。	经核查，备份服务器已配置系统管理员账户：sangfor，审计管理员账户：shenji，安全管理员账户：anquan，普通账户：peanut001，账户权限已分离，分别拥有其工作所需的最小权限，超级管理员账户 root 要经过授权审批才能使用，可实现管理用户的权限分离。	符合
安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经核查，备份服务器已开启 rsyslog 系统日志和 auditd 安全审计功能，审计覆盖到每个用户，可对重要的用户行为和重要安全事件进行审计。	符合
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经核查，备份服务器审计记录包括 message、audit 等审计记录，message 日志及 secure 日志包括：日期、时间、服务器、进程、详细信息等内容；wtmp 日志包括：账户名、登录方式、日期、时间、终端 IP 地址等内容；audit 日志包括：类型、时间戳、事件 ID、进程 ID、用户名、执行命令、是否成功等内容。	符合
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	经核查，备份服务器重要日志文件及日志配置文件权限值均未超过 644，仅授权用户可管理，已纳入日志审计系统的审计范围，可避免日志受到未预期的删除、修改或覆盖等，现场测评时间为 2023 年 7 月 24 日，日志最早可查询时间为 2023 年 1 月 3 日，日志留存时间满足六个月。	符合
入侵防范	a)应遵循最小安装的原则，仅安装需要的组件和应用程序；	经核查，备份服务器遵循最小安装原则，未安装多余的组件和应用程序。	符合
	b)应关闭不需要的系统服务、默认共享和高危端口；	经核查，备份服务器操作系统不存在不必要的默认共享，已关闭不必要的	符合

控制点	测评项	结果记录	符合情况
		端口，仅开启业务所需端口，已禁用不必要的服务。	
	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	经核查，已通过服务器区防火墙限制仅 10.1.15.*、192.168.*.0/27 可远程登录备份服务器。	符合
	d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于服务器。	不适用
	e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经核查，已部署深信服终端安全管理系统，备份服务器已安装深信服终端安全管理系统 Agent，漏洞库更新于 2023 年 07 月 22 日，已设置自动扫描任务，每天 0 点对备份服务器进行一次漏洞扫描，近期扫描记录中未发现安全漏洞，且在本次漏洞扫描中未发现已知的风险漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	经核查，已部署深信服终端安全管理系统，备份服务器已安装深信服终端安全管理系统 Agent，能及时识别入侵和病毒行为，病毒库最近更新时间为 2023 年 07 月 22 日，现场测评时间为 2023 年 7 月 24 日。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	经核查，备份服务器未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	经核查，备份服务器在通信过程中采用 ssh 协议传输数据，可保证重要数据在传输过程中的完整性。	符合
数据备份恢复	a)应提供重要数据的本地	经核查，管理员在备份服务器配置变	部分

控制点	测评项	结果记录	符合情况
	数据备份与恢复功能；	更后将配置文件备份到运维终端，未有备份恢复测试记录。	符合
	b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	经核查，未利用通信网络将备份服务器的重要数据定时批量传送至备用场地。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	经核查，备份服务器为 Linux 操作系统，用户的鉴别信息所在的存储空间由操作系统自动分配，Linux 自身资源回收机制可满足剩余信息保护。	符合
个人信息保护	a)应仅采集和保存业务必需的用户个人信息；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于服务器。	不适用
	b)应禁止未授权访问和非法使用用户个人信息。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于服务器。	不适用

D.4.1.3.4 运维终端

控制点	测评项	结果记录	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	经核查，运维终端采用账户名+口令方式进行登录，身份标识唯一，不存在空口令账户；已启用“密码必须符合复杂性要求”，口令须包含数字、大写字母、小写字母和特殊字符中三类，“密码长度最小值”为 8 个字符，“密码最长使用期限”为 180 天。	符合
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	经核查，运维终端登录失败 5 次锁定 30 分钟，未配置屏幕保护程序。	部分符合
	c)当进行远程管理时，应采取必要措施防止鉴别信息	经核查，运维终端已启用远程桌面，但未配置“远程（RDP）连接要求使	不符合

控制点	测评项	结果记录	符合情况
	在网络传输过程中被窃听。	用指定的安全层”为“SSL”和未配置“设置客户端连接加密级别”为“高级别”。	
访问控制	a)应对登录的用户分配账户和权限;	经核查,运维终端已对登录的用户分配账户和权限,已为登录的用户配置系统管理员账户：admin、mmzy、安全管理员账户：anquan、审计管理员账户：shenji，不存在匿名账户。	符合
	b)应重命名或删除默认账户,修改默认账户的默认口令;	经核查，运维终端不存在默认账户，不存在默认口令。	符合
	c)应及时删除或停用多余的、过期的账户,避免共享账户的存在;	经核查,运维终端不存在多余、过期账户，不存在共享账户的情况。	符合
	d)应授予管理用户所需的最小权限,实现管理用户的权限分离。	经核查,运维终端已为登录的用户配置系统管理员账户:admin/mmzy、安全管理员账户：anquan、审计管理员账户:shenji,账户权限已分离,分别拥有其工作所需的最小权限。	符合
安全审计	a)应启用安全审计功能,审计覆盖到每个用户,对重要的用户行为和重要安全事件进行审计;	经核查，审计服务 Windows Event Log 运行正常,运维终端本地审核策略均已设置为“成功、失败”,审计覆盖每个用户,可对重要的用户行为和安全事件进行审计。	符合
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息;	经核查,运维终端审计记录包含:级别、日期和时间、来源、事件 id、任务类别、关键字等审计相关信息。	符合
	c)应对审计记录进行保护,定期备份,避免受到未预期的删除、修改或覆盖等。	经核查，运维终端仅 Administrators 组具备“管理审核和安全日志”权限，现场测评时间 2023 年 7 月 24 日，日志最早可查看到 2020 年 5 月 27 日,日志留存时间大于六个月;但审计记录仅本地保存，未定期备份。	部分符合
入侵防范	a)应遵循最小安装的原则,	经核查,运维终端未安装不必要的组	符合

控制点	测评项	结果记录	符合情况
	仅安装需要的组件和应用程序；	件，未安装不必要的应用程序。	
	b)应关闭不需要的系统服务、默认共享和高危端口；	经核查，终端不存在不必要的默认共享，已通过系统防火墙严格限制 80、21、23、25、135、139、445 等端口的访问规则，已禁用不必要的服务。	符合
	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	经核查，未限制远程接入运维终端的地址范围。	不符合
	d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于终端。	不适用
	e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经核查，已安装 360 安全卫士，可对运维终端进行漏洞管理，近期漏洞扫描结果未发现已知漏洞，有系统补丁安装记录。在本次漏洞扫描中未发现存在已知的风险漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	经核查，运维终端已安装 360 杀毒，能及时识别和防范病毒行为，已通过互联网自动实时更新病毒库，360 杀毒病毒库版本：5.0.0.8170，更新时间 2023 年 7 月 22 日，现场测评时间：2023 年 7 月 24 日。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	经核查，运维终端未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	经核查，运维终端已启用远程桌面，但未配置“远程（RDP）连接要求使用指定的安全层”为“SSL”和未	不符合

控制点	测评项	结果记录	符合情况
		配置“设置客户端连接加密级别”为“高级别”,不能保证重要数据在传输过程中的完整性。	
数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能;	经核查，运维终端无重要配置数据，出现故障后使用其他后备机或者重装系统，不影响业务系统的使用，故此项不适用。	不适用
	b)应提供异地数据备份功能,利用通信网络将重要数据定时批量传送至备用场地。	经核查，运维终端无重要配置数据，出现故障后使用其他后备机或者重装系统，不影响业务系统的使用，故此项不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	经核查,运维终端已启用“交互式登录：不显示上次登录”和“关机：清除虚拟内存页面文件”,可能保证鉴别数据被释放前得到完全清除。	符合
个人信息保护	a)应仅采集和保存业务必需的用户个人信息;	依据《信息安全技术 网络安全等级保护测评要求》,此项不适用于终端。	不适用
	b)应禁止未授权访问和非法使用用户个人信息。	依据《信息安全技术 网络安全等级保护测评要求》,此项不适用于终端。	不适用

D.4.1.4 其他系统或设备

本次测评不包含本安全层面检测项。

D.4.1.5 系统管理软件/平台

D.4.1.5.1 中间件 1

控制点	测评项	结果记录	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别,身份标识具有唯一性,身份鉴别信息具有复杂度要求并定期更换;	由于中间件 1 未提供独立的登录管理界面,中间件 1 的身份鉴别功能由数据库服务器操作系统实现,故此测评项不适用。	不适用
	b)应具有登录失败处理功能，应配置并启用结束会	由于中间件 1 未提供独立的登录管理界面,中间件 1 的身份鉴别功能由	不适用

控制点	测评项	结果记录	符合情况
	话、限制非法登录次数和当登录连接超时自动退出等相关措施；	数据库服务器操作系统实现，故此测评项不适用。	
	c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	由于中间件 1 未提供独立的登录管理界面，中间件 1 的身份鉴别功能由数据库服务器操作系统实现，故此测评项不适用。	不适用
访问控制	a)应对登录的用户分配账户和权限；	由于中间件 1 未提供独立的登录管理界面，中间件 1 的访问控制功能由数据库服务器操作系统实现，故此测评项不适用。	不适用
	b)应重命名或删除默认账户，修改默认账户的默认口令；	由于中间件 1 未提供独立的登录管理界面，中间件 1 的访问控制功能由数据库服务器操作系统实现，故此测评项不适用。	不适用
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在；	由于中间件 1 未提供独立的登录管理界面，中间件 1 的访问控制功能由数据库服务器操作系统实现，故此测评项不适用。	不适用
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离。	由于中间件 1 未提供独立的登录管理界面，中间件 1 的访问控制功能由数据库服务器操作系统实现，故此测评项不适用。	不适用
安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经核查，中间件 1 已开启安全审计功能，在日志配置中已开启 Cataline 引擎日志、控制台输出日志、manager 应用日志和内部代码丢出的日志，审计覆盖到每个用户，能对重要的用户行为和重要安全事件进行审计。	符合
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经核查，中间件 1 的日志审计结果包含：事件的日期和时间、用户、事件类型、操作 IP、动作、结果等。 中间件 1 所在的服务器的操作系统时间与北京时间一致。	符合
	c)应对审计记录进行保护，	经核查，中间件 1 日志本地存储，日	部分

控制点	测评项	结果记录	符合情况
	定期备份，避免受到未预期的删除、修改或覆盖等。	志文件权限值均为 640，仅授权用户可以访问，测评时间为 2023 年 7 月 24 日，可查询到日志最早时间为 2023 年 4 月 8 日，日志保存时间不足 6 个月。	符合
入侵防范	a)应遵循最小安装的原则，仅安装需要的组件和应用程序；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于中间件。	不适用
	b)应关闭不需要的系统服务、默认共享和高危端口；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于中间件。	不适用
	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于中间件。	不适用
	d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	由于中间件 1 未提供独立的登录管理界面，无对应的人机或通信接口输入功能，故此测评项不适用。	不适用
	e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经核查，已部署深信服终端安全管理系统，中间件 1 所在数据库服务器已安装深信服终端安全管理系统 Agent，已设置自动扫描任务，每天 0 点对数据库服务器进行一次漏洞扫描，近期扫描记录中未发现中间件 1 的安全漏洞，且在本次漏洞扫描中未发现已知的风险漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于中间件。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于中间件。	不适用

控制点	测评项	结果记录	符合情况
	进行报警，并将验证结果形成审计记录送至安全管理中心。		
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	经核查，中间件 1 未提供独立的登录管理界面，中间件 1 数据的传输完整性由数据库服务器操作系统实现，数据库服务器在通信过程中采用 ssh 协议传输数据，可保证重要数据在传输过程中的完整性。	符合
数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能；	经核查，管理员不定期将中间件 1 配置数据备份到本地服务器，具有近期的备份记录，未有备份恢复测试记录。	部分符合
	b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	经核查，中间件 1 的数据仅本地保存，未利用通信网络将重要数据定时传送至备用场地。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	由于中间件 1 未提供独立的登录管理界面，中间件 1 的鉴别信息的剩余信息保护功能由数据库服务器操作系统实现，故此测评项不适用。	不适用
个人信息保护	a)应仅采集和保存业务必需的用户个人信息；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于中间件。	不适用
	b)应禁止未授权访问和非法使用用户个人信息。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于中间件。	不适用

D.4.1.5.2 中间件 2

控制点	测评项	结果记录	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	由于中间件 2 未提供独立的登录管理界面，中间件 2 的身份鉴别功能由应用服务器操作系统实现，故此测评项不适用。	不适用

控制点	测评项	结果记录	符合情况
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	由于中间件 2 未提供独立的登录管理界面，中间件 2 的身份鉴别功能由应用服务器操作系统实现，故此测评项不适用。	不适用
	c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	由于中间件 2 未提供独立的登录管理界面，中间件 2 的身份鉴别功能由应用服务器操作系统实现，故此测评项不适用。	不适用
访问控制	a)应对登录的用户分配账户和权限；	由于中间件 2 未提供独立的登录管理界面，中间件 2 的访问控制功能由应用服务器操作系统实现，故此测评项不适用。	不适用
	b)应重命名或删除默认账户，修改默认账户的默认口令；	由于中间件 2 未提供独立的登录管理界面，中间件 2 的访问控制功能由应用服务器操作系统实现，故此测评项不适用。	不适用
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在；	由于中间件 2 未提供独立的登录管理界面，中间件 2 的访问控制功能由应用服务器操作系统实现，故此测评项不适用。	不适用
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离。	由于中间件 2 未提供独立的登录管理界面，中间件 2 的访问控制功能由应用服务器操作系统实现，故此测评项不适用。	不适用
安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经核查，中间件 2 已开启安全审计功能，在日志配置中已开启 Cataline 引擎日志、控制台输出日志、manager 应用日志和内部代码丢出的日志，审计覆盖到每个用户，能对重要的用户行为和重要安全事件进行审计。	符合
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经核查， 中间件 2 的日志审计结果包含：事件的日期和时间、用户、事件类型、操作 IP、动作、结果等。 中间件 2 所在的服务器的操作系统时间与北京时间一致。	符合

控制点	测评项	结果记录	符合情况
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	经核查，中间件 2 日志手动备份到本地服务器，日志文件权限值均为 640，仅授权用户可以访问，测评时间为 2023 年 7 月 24 日，可查询到日志最早时间为 2023 年 3 月 15 日，日志保存时间不足 6 个月。	部分符合
入侵防范	a)应遵循最小安装的原则，仅安装需要的组件和应用程序；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于中间件。	不适用
	b)应关闭不需要的系统服务、默认共享和高危端口；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于中间件。	不适用
	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于中间件。	不适用
	d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	由于中间件 2 未提供独立的登录管理界面，无对应的人机或通信接口输入功能，故此测评项不适用。	不适用
	e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经核查，已部署深信服终端安全管理系统，中间件 2 所在应用服务器已安装深信服终端安全管理系统 Agent，已设置自动扫描任务，每天 0 点对应用服务器进行一次漏洞扫描，近期扫描记录中未发现中间件 2 的安全漏洞，且在本次漏洞扫描中未发现已知的风险漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于中间件。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于中间件。	不适用

控制点	测评项	结果记录	符合情况
	测到其可信性受到破坏后进行报警,并将验证结果形成审计记录送至安全管理中心。		
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	经核查,中间件 2 未提供独立的登录管理界面,中间件 2 数据的传输完整性由应用服务器操作系统实现,应用服务器在通信过程中采用 ssh 协议传输数据,可保证重要数据在传输过程中的完整性。	符合
数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能;	经核查,管理员不定期将中间件 2 配置数据备份到本地服务器,具有近期的备份记录，未有备份恢复测试记录。	部分符合
	b)应提供异地数据备份功能,利用通信网络将重要数据定时批量传送至备用场地。	经核查，中间件 2 的数据仅本地保存,未利用通信网络将重要数据定时传送至备用场地。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	由于中间件 2 未提供独立的登录管理界面,中间件 2 鉴别信息的剩余信息保护功能由应用服务器操作系统实现，故此测评项不适用。	不适用
个人信息保护	a)应仅采集和保存业务必需的用户个人信息;	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于中间件。	不适用
	b)应禁止未授权访问和非法使用用户个人信息。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于中间件。	不适用

D.4.1.5.3 数据库

控制点	测评项	结果记录	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别,身份标识具有唯一性,身份鉴别信息具	经核查,数据库采用账户名＋口令的方式登录，身份标识具有唯一性，不存在空口令账户;已配置口令复杂度	符合

控制点	测评项	结果记录	符合情况
	有复杂度要求并定期更换；	策略，口令须包含数字、大写字母和小写字母，不少于 8 位；口令有效期为 180 天。	
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	经核查，数据库登录失败 5 次锁定一天，超时退出时间为 10 分钟。	符合
	c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	经核查，数据库已采用 ssl 协议进行远程管理，可防止鉴别信息在网络传输过程中被窃听。	符合
访问控制	a)应对登录的用户分配账户和权限；	经核查，数据库已对登录的用户分配账户和权限，已配置系统管理员账户 SYS、SYSTEM，业务账户 OAUSER、WXUSER、ETL_USER，备份账户：OABACKUP。	符合
	b)应重命名或删除默认账户，修改默认账户的默认口令；	经核查，数据库未重命名默认账户 SYS、SYSTEM、SYSMAN、SCOTT、DBSNMP，但账户 SYSMAN、SCOTT、DBSNMP 已被锁定，账户 SYS、SYSTEM 不宜重命名，口令已修改为复杂口令。	符合
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在；	经核查及访谈，数据库已禁用多余账户，不存在过期账户 ，不存在共享账户的情况。	符合
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离。	经核查，数据库已配置系统管理员账户 SYS、SYSTEM，业务账户 OAUSER、WXUSER、ETL_USER，备份账户：OABACKUP，未设置审计管理、安全管理员账户，未实现管理用户的权限分离。	不符合
安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经核查，数据库已对普通用户开启审计功能，已启用对所有用户的重要行为进行审计，已启用对 SYSDBA 或 SYSOPER 特权连接时直接发出的 SQL 语句进行审计。	符合

控制点	测评项	结果记录	符合情况
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经核查，数据库告警日志记录了 id、日期、时间、用户、操作、事件、结果等信息。	符合
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	经核查，数据库日志仅授权用户可进行访问，管理员不定期手动创建数据库服务器快照，避免审计记录受到未预期的删除、修改或覆盖等；现场测评时间为 2023 年 7 月 24 日，最早可查询到的日志时间为 2023 年 2 月 23 日，日志保存时间不足六个月。	部分符合
入侵防范	a)应遵循最小安装的原则，仅安装需要的组件和应用程序；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于数据库。	不适用
	b)应关闭不需要的系统服务、默认共享和高危端口；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于数据库。	不适用
	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于数据库。	不适用
	d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于数据库。	不适用
	e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经核查，已部署深信服终端安全管理系统，数据库所在数据库服务器已安装深信服终端安全管理系统 Agent，已设置自动扫描任务，每天 0 点对数据库服务器进行一次漏洞扫描，近期扫描记录中未发现数据库的安全漏洞，且在本次漏洞扫描中未发现已知的风险漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于数据库。	不适用

控制点	测评项	结果记录	符合情况
	恶意代码库。		
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于数据库。	不适用
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	经核查，数据库已采用 ssl 协议进行远程管理，可保证重要数据在传输过程中的完整性。	符合
数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能；	经核查，已设置数据库备份计划，每天晚上 11 点 10 分自动全量备份数据库到数据库服务器本地，未有备份恢复测试记录。	部分符合
	b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	经核查，数据库的重要数据仅本地保存，未利用通信网络将重要数据定时传送至备用场地。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	经核查，数据库登出后不记录账号和口令，数据库系统资源释放或清除机制正常且满足要求。	符合
个人信息保护	a)应仅采集和保存业务必需的用户个人信息；	经核查，数据库仅采集和保存必需的用户个人信息，如职工的姓名、部门、岗位、职级、人员类型、人员状态等。	符合
	b)应禁止未授权访问和非法使用用户个人信息。	经核查，系统中保存的个人信息仅授权用户可访问，非授权用户无法访问及使用，已制定相关制度明确个人信息保护的相关管理要求和流程规定。	符合

D.4.1.5.4 UIS 超融合管理平台

控制点	测评项	结果记录	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	经核查，UIS 超融合管理平台采用账户名+口令方式进行登录，身份标识唯一，不存在空口令账户；已配置口令复杂度策略，口令必须由字母、数字和特殊字符组成，长度最少为 8 位；未配置口令有效期。	部分符合
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	经核查，UIS 超融合管理平台登录失败 3 次锁定 1 分钟，操作员闲置 60 分钟自动退出。	符合
	c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	经核查，UIS 超融合管理平台采用 HTTPS 协议进行远程管理，可防止鉴别信息在网络传输过程中被窃听。	符合
访问控制	a)应对登录的用户分配账户和权限；	经核查，UIS 超融合管理平台已对登录的用户分配账户和权限，已配置系统管理员账户 super、安全管理员账户 anquanguanliyuan、审计管理员账户 shenjiguanliyuan。	符合
	b)应重命名或删除默认账户，修改默认账户的默认口令；	经核查，系统不存在默认账户，不存在默认口令。	符合
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在；	经核查及访谈，UIS 超融合管理平台无多余账户，不存在过期账户 ，不存在共享账户的情况。	符合
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离。	经核查，UIS 超融合管理平台设置了系统管理员账户 super、安全管理员账户 anquanguanliyuan、审计管理员账户 shenjiguanliyuan，账户权限已分离，分别拥有其工作所需的最小权限。	符合
安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经核查，UIS 超融合管理平台已开启操作日志和安全审计功能，审计功能运行正常， 审计覆盖到每个用户，可实现对重要的用户行为和重要安全事件的安全审计。	符合

控制点	测评项	结果记录	符合情况
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经核查，UIS 超融合管理平台审计记录包括登录名、操作员名称、完成时间、登录地址、操作分类、操作对象、操作描述、执行结果、失败原因、风险级别和事件类型。	符合
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	经核查，UIS 超融合管理平台审计记录仅授权用户可管理，已手动备份到备份服务器，避免受到未预期的删除、修改或覆盖；现场测评时间为 2023 年 7 月 24 日，日志最早可查询时间为 2023 年 3 月 16 日，日志留存时间不足六个月。	部分符合
入侵防范	a)应遵循最小安装的原则，仅安装需要的组件和应用程序；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于系统管理软件平台。	不适用
	b)应关闭不需要的系统服务、默认共享和高危端口；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于系统管理软件平台。	不适用
	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于系统管理软件平台。	不适用
	d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	经测试，UIS 超融合管理平台在数据输入界面提供有效性校验功能，可对无效或非法数据、字符长度和有效性进行校验。	符合
	e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经核查，UIS 超融合管理平台未定期进行漏洞扫描，在本次漏洞扫描中未发现高、中危安全漏洞。	部分符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于系统管理软件平台。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程	经核查，UIS 超融合管理平台未基于可信根对计算设备的系统引导程序、	不符合

控制点	测评项	结果记录	符合情况
	序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	经核查，UIS 超融合管理平台在通信过程中采用 HTTPS 协议传输数据，可保证重要数据在传输过程中的完整性。	符合
数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能；	经核查，UIS 超融合管理平台每天一次自动将当前的数据和配置文件保存到系统所管理的随机挑选的三台主机上，每台主机上保留最近 7 次的备份文件，未有备份恢复测试记录。	部分符合
	b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	经核查，未利用通信网络将 UIS 超融合管理平台的重要数据定时批量传送至备用场地。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	经核查，UIS 超融合管理平台登出后不保存上次登录信息，资源回收机制可满足剩余信息保护。	符合
个人信息保护	a)应仅采集和保存业务必需的用户个人信息；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于系统管理软件平台。	不适用
	b)应禁止未授权访问和非法使用用户个人信息。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于系统管理软件平台。	不适用

D.4.1.6 业务应用系统/平台

D.4.1.6.1 OA 系统

控制点	测评项	结果记录	符合情况
身份鉴别	a)应对登录的用户进行身	经核查，OA 系统采用用户名+口令+	符合

控制点	测评项	结果记录	符合情况
	份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	验证码后台登录或通过统一身份验证平台登录（账号登录：用户名+口令；动态码登录：用户名+验证码+动态码；微信扫描登录）；APP 端采用用户名+口令+验证码进行身份鉴别，身份标识唯一，不存在同名用户，不存在空口令用户；系统已开启密码安全设置功能，密码强度设置为中，由大写字母，小写字母和字符中的任意两种组成，长度不小于 8 位，口令设置 180 天定期更换。	
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	经核查，OA 系统、AAP 端已开启登录失败处理功能，失败 5 次锁定 3 小时，系统和 AAP 端已有超时自动退出功能，30 分钟超时自动退出。	符合
	c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	经核查，OA 系统、AAP 端在通信过程中采用 https 协议传输数据，用户口令信息加密传输，可防止鉴别信息在网络传输过程中被窃听。	符合
访问控制	a)应对登录的用户分配账户和权限；	经核查，OA 系统已对登录的用户分类账户和权限，系统角色包括系统管理员、安全审计员、单位管理员、普通人员、编外人员等角色，不同角色具备不同的权限，不存在匿名账户。	符合
	b)应重命名或删除默认账户，修改默认账户的默认口令；	经核查，OA 系统用户采用实名登录，不存在默认账户，用户首次登录需要强制修改口令，不存在默认口令。	符合
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在；	经核查，OA 系统用户为学校的教师、领导，已设置 60 天账号不登录自动停用，不存在多余、过期的账户，账户对应到学校教师个人，不存在共享账户。	符合
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离。	经核查，OA 系统已授予管理用户最小权限，包括系统管理员、单位管理员、安全审计员，实现管理用户的权	符合

控制点	测评项	结果记录	符合情况
		限分离。	
安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经核查，OA 系统、APP 端已开启安全审计功能，包括登录日志、应用日志，审计覆盖到每个用户，已对重要的用户行为和事件进行审计。	符合
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经核查，OA 系统的登录日志包括人员、登录名、部门、岗位、登录时间、退出时间、在线时长、IP 地址；应用日志包括操作人员、操作人员登录名、操作类型、操作描述、操作时间、IP 地址、所在单位、操作结果、操作模块；APP 端审计日志包括人员、登录名、部门、岗位、登录时间、退出时间、在线时长、IP 地址。	符合
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	经核查，OA 系统、APP 端已对审计记录进行保护，仅安全审计员和系统管理员能进行查看，已定期每天备份日志到数据库服务器，日志一直保存，测评时间为 2023 年 7 月 24 日，可查看到 2022 年 11 月 8 日之前的日志，保存周期大于 6 个月。	符合
入侵防范	a)应遵循最小安装的原则，仅安装需要的组件和应用程序；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于业务应用系统。	不适用
	b)应关闭不需要的系统服务、默认共享和高危端口；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于业务应用系统。	不适用
	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于业务应用系统。	不适用
	d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	经核查，OA 系统、APP 端已设置上传文件的后缀，对 aps、jsp、jspx、HTML、ascx、ashx、cer 等格式进行限制。输入框禁止*、？ 、 、%等特殊字符的输入。	符合

控制点	测评项	结果记录	符合情况
	e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经核查，OA 系统、APP 端未定期进行漏洞扫描，本次漏洞扫描发现中风险漏洞未修复。	部分符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于业务应用系统。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	依据《信息安全技术 网络安全等级保护测评要求》，此项不适用于业务应用系统。	不适用
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	经核查，OA 系统、APP 端已采用 https 进行通信，能保证重要数据在传输中的完整性。	符合
数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能；	经核查，OA 系统、APP 端所有重要数据每天全量备份到数据库服务器，未有备份恢复测试记录。	部分符合
	b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	经核查，OA 系统、APP 端备份数据仅在本地保存，未利用通信网络将关键数据定时批量传送至备用场地。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	经测试，OA 系统、APP 端登录时不自动保存和显示历史账号和口令，在用户退出后及时清空会话信息，无法通过回退操作访问退出前界面，用户的鉴别信息所在的存储空间被释放或重新分配前能够得到完全清除。	符合
个人信息保护	a)应仅采集和保存业务必需的用户个人信息；	经核查，OA 系统用户输入框有姓名，手机号、性别、所属部门等信息，均为业务必需的个人信息，未发现超范围采集情况，单位具备个人信息保护的相关管理要求和流程。	符合

控制点	测评项	结果记录	符合情况
	b)应禁止未授权访问和非法使用用户个人信息。	经核查，OA 系统保存的个人信息仅授权用户可访问，非授权用户无法访问及使用，且具备个人信息保护的相关管理要求和流程规定。	符合

D.4.1.7 数据资源

D.4.1.7.1 重要业务数据

控制点	测评项	结果记录	符合情况
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	经核查，OA 系统、APP 端已采用 https 进行通信，能保证重要业务数据在传输中的完整性。	符合
数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能；	经核查，OA 系统、APP 端所有重要业务数据每天全量备份到数据库服务器，未有备份恢复测试记录。	部分符合
	b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	经核查，OA 系统、APP 端备份数据仅在本地保存，未利用通信网络将关键业务数据定时批量传送至备用场地。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	根据《信息安全技术 网络安全等级保护测评要求》(GB/T 28448-2019)，该重要业务数据的剩余信息保护无鉴别信息相关判定需求，因此该数据在该要求项不适用。	不适用
个人信息保护	a)应仅采集和保存业务必需的用户个人信息；	经核查，OA 系统业务数据不涉及个人信息，该测评项不适用。	不适用
	b)应禁止未授权访问和非法使用用户个人信息。	经核查，OA 系统业务数据不涉及个人信息，该测评项不适用。	不适用

D.4.1.7.2 重要个人信息

控制点	测评项	结果记录	符合情况
数据完整性	应采用校验技术保证重要	经核查，OA 系统、APP 端已采用	符合

控制点	测评项	结果记录	符合情况
	数据在传输过程中的完整性。	https 进行通信，能保证重要个人信息在传输中的完整性。	
数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能；	经核查，OA 系统、APP 端所有重要个人信息每天全量备份到数据库服务器，未有备份恢复测试记录。	部分符合
	b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	经核查，OA 系统、APP 端备份数据仅在本地备份保存，未利用通信网络将重要个人信息定时批量传送至备用场地。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	根据《信息安全技术 网络安全等级保护测评要求》(GB/T 28448-2019)，该重要个人信息的剩余信息保护无鉴别信息相关判定需求，因此该数据在该要求项不适用。	不适用
个人信息保护	a)应仅采集和保存业务必需的用户个人信息；	经核查，OA 系统用户输入框有姓名，手机号、性别、所属部门等信息，均为业务必需的个人信息，未发现超范围采集情况，单位具备个人信息保护的相关管理要求和流程规定。	符合
	b)应禁止未授权访问和非法使用用户个人信息。	经核查，OA 系统保存的个人信息仅授权用户可访问，非授权用户无法访问及使用，单位具备个人信息保护的相关管理要求和流程规定。	符合

D.4.2 安全扩展要求部分

D.4.2.1 移动互联安全扩展要求

附录 D 表-20 安全计算环境结果记录表（移动互联安全扩展要求）

测评指标	控制点	测评项	结果记录	符合情况
移动互联安全扩展要求	移动应用管控	a)应具有选择应用软件安装、运行的功能；	经核查，OA 系统 APP 采用通用手机，不涉及专用移动终端，此项不适用。	不适用
		b)应只允许可靠证书签	经核查，OA 系统 APP 采用通	不适

测评指标	控制点	测评项	结果记录	符合情况
		名的应用软件安装和运行。	用手机，不涉及专用移动终端，此项不适用。	用

D.5 安全管理中心

D.5.1 安全通用要求部分

控制点	测评项	结果记录	符合情况
系统管理	a)应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；	经核查，安全设备、网络设备、服务器均有建立系统管理员账户，并对系统管理员进行身份鉴别，只允许系统管理员通过特定的命令或操作界面进行系统管理操作，服务器通过堡垒机进行身份鉴别，仅允许系统管理员进行操作和管理，并且各设备已开启安全审计对系统管理员的操作行为进行审计。	符合
	b)应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。	经核查，该单位已配置系统管理员，并且安全设备、网络设备、服务器均由系统管理员负责系统的资源和运行，包括用户身份，系统资源配置、系统加载和启动、系统运行的异常处理，数据和设备的备份恢复。	符合
审计管理	a)应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；	经核查，安全设备、网络设备、服务器均配置审计管理员账户，并对审计管理员账户进行身份鉴别，只允许其通过日志审计系统进行安全审计操作，并且设备已开启安全审计对审计管理员的操作行为进行审计。	符合
	b)应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	经核查，该单位已设置审计管理员岗位并配置相应的人员，并且有部署日志审计系统收集各设备的日志审计记录进行分析、处理。	符合

D.6 安全管理制度

通用扩展	控制点	测评项	结果记录	符合情况
安全通用要求	安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。	经核查，该单位秉承“积极防御，综合防范”的信息安全方针，根据国家信息安全等级保护等有关政策和标准要求，建立“三个体系，一个中心，三重防护”的安全保障体系框架，已在《信息安全总体策略》中阐明机构安全工作的总体目标、范围、原则和安全框架等。	符合
	管理制度	a)应对安全管理活动中的主要管理内容建立安全管理制度；	经核查，该单位已对安全活动中的主要内容建立了管理制度，已制定《数据安全管理规范.》、《网络安全管理规范》、《网络安全管理规范》、《应用安全管理规范》。	符合
		b)应对管理人员或操作人员执行的日常管理操作建立操作规程。	经核查，该单位已建立《设备操作规程》、《 软件操作手册》、《防火墙配置和操作手册》等操作规程，相关文档中包含对网络安全、系统运行维护、系统配置、用户操作等方面的规定。	符合
	制定和发布	a)应指定或授权专门的部门或人员负责安全管理制度的制定；	经核查，该单位《信息安全制度管理规范》已指定信息化办公室负责主持制定茂名职业技术学院信息化技术规范和有关规章制度，安全管理制度由信息化办公室发布。	符合
		b)安全管理制度应通过正式、有效的方式发布，并进行版本控制。	经核查，该单位《信息安全制度管理规范》已规定总体安全管理制度和规定以及安全技术标准和规范须经信息安全领导小组审批确认，方可发布，已通过 OA 系统正式发文通知，制度版本为 V2.0，具备“收发文登记记录”。	符合

通用扩展	控制点	测评项	结果记录	符合情况
	评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	经核查，该单位《信息安全制度管理规范》明确了对信息安全管理制度进行定期的评审与修订，每年或在发生重大变更时，对单位信息安全管理制度进行检查和评审，对发现不足或需要修改的安全管理制度进行修订；每年至少组织一次安全管理制度体系的合理性和适用性审定，由原制定和发布部门组织修订或经其批准实施修订，并由原发布部门对修订进行发布；但未具有管理制度评审记录和修订记录。	部分符合

D.7 安全管理机构

通用扩展	控制点	测评项	结果记录	符合情况
安全通用要求	岗位设置	a)应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；	经核查，该单位《安全组织及职责管理规定》已设立办公室为网络安全管理职能部门，《岗位安排及岗位职责》中已明确了各岗位负责人的职责，包括安全管理员、系统管理员、网络管理员、应用管理员、资料管理员、安全主管等方面的岗位职责。	符合
		b)应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。	经核查，该单位《安全组织及职责管理规定》已进行安全管理岗位的划分，包括网络管理员、系统管理员、安全管理员、安全审计员、数据库管理员、机房管理员等管理岗位，文档中明确了部门及各个工作岗位的职责，详见《岗位安排及岗位职责》。	符合
	人员配备	应配备一定数量的系统管理员、审计管理员和	经核查，该单位《岗位安排及岗位职责》已设置系统管理员	符合

通用扩展	控制点	测评项	结果记录	符合情况
		安全管理员等。	为黄海东、安全审计管理员为麦才赞、安全管理员为龙恒，网络管理员为吴国华、机房管理员为陈思凡、资产管理员为黄健。	
	授权和审批	a)应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；	经核查，该单位《授权和审批管理规定》规定由信息安全领导小组办公室确定审批内容后，报送信息安全领导小组批准。	符合
		b)应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。	经核查，该单位《授权和审批管理规定》明确审批的内容，重大事项应由信息安全领导小组办公室确定后，报送信息安全领导小组批准。重大事项至少包括网络系统、应用系统、数据库管理系统、重要服务器和设备等重要资源的变更、操作、访问和接入等。	符合
	沟通和合作	a)应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；	经核查，该单位《安全组织机构-沟通合作》规定各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通机制，每年组织一次工作会议进行沟通合作，共同协调处理信息安全相关问题，具有“沟通会议记录表”。	符合
		b)应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；	经核查，该单位《安全组织机构-沟通合作》已规定通过聘请信息安全专家和外部顾问成员，指导茂名职业技术学院信息安全建设，规定服务中心有关部门建立沟通、合作机制，定期组织相关单位、部门召开内部协调会议，具备“B005 信息安全会议记录”。	符合
		c)应建立外联单位联系	经核查，该单位已建立“外部	符合

通用扩展	控制点	测评项	结果记录	符合情况
		列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	联系表”，内容包含外联单位名称、合作内容、联系人和联系方式等信息。	
	审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。	经核查，该单位《安全审核与检查管理制度》规定学校部门每月进行一次安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况，详见《安全检查报告 20230321》。	符合

D.8 安全管理人员

通用扩展	控制点	测评项	结果记录	符合情况
安全通用要求	人员录用	a)应指定或授权专门的部门或人员负责人员录用；	经核查，该单位已指定由人力资源保障科负责本学院职工聘用与录用。	符合
		b)应对被录用人员的身份、安全背景、专业资格或资质等进行审查。	经核查，该单位《内部人员信息安全管理规定》规定信息安全相关岗位人员上岗前必须经人力资源保障科进行身份、背景、专业资格和资质的审查和考查，教育信息与网络中心进行技术和业务技能考核，具备“C002 人员信息审查记录”。	符合
	人员离岗	应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。	经核查，该单位规定离职人员职工离职时需要回收涉密资料、账号口令、钥匙、资产等以及其他任何形式的载体，具有人员离岗终止权限、交还软硬件设备的记录。	符合
	安全意识教育和培训	应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。	经核查，该单位《安全教育和培训制度》规定由学院教育信息与网络中心负责人员的安全意识教育和岗位培训，明确考核结果由信息中心进行备案，	符合

通用扩展	控制点	测评项	结果记录	符合情况
			具备“学院信息管理人员培训签到记录”，具备“C014 专业培训考核记录表”。	
	外部人员访问管理	a)应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；	经核查，该单位已制定《外部人员访问管理制度》，已规定外部人员进场前，需要出示盖章申请，由学校项目负责人批准后陪同，并登记个人资料留底。单位已通过 OA 系统保留进出审批记录。	符合
		b)应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；	经核查，该单位《外部接入受控网络访问系统管理规范》要求外部人员接入受控网络前由对接人在 OA 提出申请，教育信息与网络中心负责人批准后由系统管理员开设账户、分配权限，并登记备案，记录外部人员访问的权限、时限、账户等信息的规定，具有相关登记记录。	符合
		c)外部人员离场后应及时清除其所有的访问权限。	经核查，该单位《外部接入受控网络访问系统管理规范》规定在外部人员离场后应及时清除其所有的访问权限，并保留清除记录，具备“C020 离场信息资料交接表”。	符合

D.9 安全建设管理

D.9.1 安全通用要求部分

D.9.1.1 制度或记录类文档

附录 D 表-21 安全建设管理结果记录表（制度或记录类文档）

安全控制点	测评指标	结果记录	符合程度
定级和备案	a)应以书面的形式说明保	经核查，该系统具有“茂名职业技	符合

安全控制点	测评指标	结果记录	符合程度
	护对象的安全保护等级及确定等级的方法和理由；	术学院 OA 系统定级报告”，报告中明确了系统的安全保护等级为第 2 级（S2A2），且描述了安全保护等级确定的方法和理由。	
	b)应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；	经核查，该单位已组织上级部门及相关安全技术专家对系统定级结果的合理性和正确性进行论证评审，具备《OA 系统专家评审意见表》。	符合
	c)应保证定级结果经过相关部门的批准；	经核查，该单位 OA 系统定级结果经过当地公安部门批准，已取得备案证，备案证明编号为：444090243008-00008。	符合
	d)应将备案材料报主管部门和相应公安机关备案。	经核查，该单位已将备案材料报主管部门和相应公安机关备案，具有由公安局出具的备案证明，备案证明编号：44090243008-00008。	符合
安全方案设计	a)应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；	经核查，该系统的建设方案包含有总体安全设计方案，方案中已明确须根据等级保护二级的要求对系统实施安全防护，方案内容包括了：信息系统安全等级定级、信息系统安全风险分析、信息系统安全技术方案、信息安全设备选型等内容。	符合
	b)应根据保护对象的安全保护等级进行安全方案设计；	经核查，该系统根据建设方案中的安全规划设计方案中要求该系统的安全保护等为二级，并且根据二级标准制定了信息系统安全技术方案。	符合
	c)应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。	经核查，该单位未组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，未有相关的方案评审记录。	不符合
产品采购和使用	a)应确保网络安全产品采购和使用符合国家的有关规定；	经核查，该系统相关网络安全产品均采用公开招投标、邀请招标、单一来源等方式开展采购，招投标文	符合

安全控制点	测评指标	结果记录	符合程度
		件、流程符合国家《中华人民共和国招投标法》的有关要求，并且采购的网络安全产品都有提供公安部签署的销售许可证。	
	b)应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。	经核查，该系统未使用密码产品，不适用。	不适用
自行软件开发	a)应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；	经核查，该单位系统为外包软件开发，本项不适用。	不适用
	b)应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。	经核查，该单位系统为外包软件开发，本项不适用。	不适用
外包软件开发	a)应在软件交付前检测其中可能存在的恶意代码；	经核查，该单位《信息系统信息安全管理制度汇编 V2.0》规定系统上线前需要进行恶意代码检测，但未有相关代码检测记录。	部分符合
	b)应保证开发单位提供软件设计文档和使用指南。	经核查，开发单位已提供交付清单，清单包括软件操作手册、系统测试文件及用户手册、需求说明文档、系统设计流程、系统使用指南等文档。	符合
工程实施	a)应指定或授权专门的部门或人员负责工程实施过程的管理；	经核查，该单位《工程管理制度》明确规定由信息中心负责系统建设管理和工程实施管理。	符合
	b)应制定安全工程实施方案控制工程实施过程。	经核查，该单位《建设方案》明确工程的实施过程，包括工程完成时间、进度、质量控制等方面的内容。	符合
测试验收	a)应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；	经核查，该单位《测试及验收方案》明确规定了验收的阶段、过程、人员、部门等内容。但未有相关测试验收报告。	部分符合
	b)应进行上线前的安全性	经核查，该系统未进行上线前的安	不符

安全控制点	测评指标	结果记录	符合程度
	测试，并出具安全测试报告。	全性测试。	合
系统交付	a)应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；	经核查，该单位《系统交付管理》规定了系统建设完成后，需要项目承建方向信息中心交付项目相关清单，详见“系统交付清单”。	符合
	b)应对负责运行维护的技术人员进行相应的技能培训；	经核查，该单位在系统上线前已对负责系统运行维护的技术人员进行技能培训，具有“D009 技能培训记录”。	符合
	c)应提供建设过程文档和运行维护文档。	经核查，该单位具有《OA 系统-需求规格说明书 》、《系统安装配置维护手册》、《用户使用手册（新增功能)》等运行维护文档，《软件需求说明书》等建设过程文档。	符合
等级测评	a)应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；	经核查，该系统每年进行等级测评，本次等级测评时间与上次等级测评时间间隔符合制度规定，已针对上次网络安全等级保护测评结论进行了相应的整改，具备整改报告及整改记录文件。	符合
	b)应在发生重大变更或级别发生变化时进行等级测评；	经核查，该系统在确定该信息系统的安全保护等级后，并未发生较大变更，未调整安全保护级别，且已在《系统变更管理制度》中规定系统发生重大变更或级别发生变化时及时进行等级测评。	符合
	c)应确保测评机构的选择符合国家有关规定。	经核查，该系统于 2022 年由广东南方信息安全研究院进行了等级测评，本年度由广东中科实数科技有限公司负责测评工作，单位已选择符合国家有关规定的测评机构进行等级测评。	符合
服务供应商选择	a)应确保服务供应商的选择符合国家的有关规定；	经核查，该系统由深信服科技有限公司提供安全产品及服务，该服务供应商符合国家的有关规定。	符合

安全控制点	测评指标	结果记录	符合程度
	b)应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。	经核查，该系统与深信服科技有限公司签订《设备采购合同》服务合同，服务合同中明确了甲乙双方的责任和义务。	符合

D.9.2 安全扩展要求部分

D.9.2.1 移动互联安全扩展要求

附录 D 表-22 安全建设管理结果记录表（移动互联安全扩展要求）

测评指标	安全控制点	测评指标	结果记录	符合程度
移动互联安全扩展要求	移动应用软件采购	a)应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名；	j 经核查，该单位 app 可通过应用宝等可靠软件商店下载，具有可靠分发渠道。	符合
		b)应保证移动终端安装、运行的应用软件由可靠的开发者开发。	经核查，单位已与外包开发人员签署有相关保密协议，可保证其可靠。	符合
	移动应用软件开发	a)应对移动业务应用软件开发者进行资格审查；	经核查，单位未对外包开发人员进行资格审查，未有相应的考核记录。	不符合
		b)应保证开发移动业务应用软件的签名证书合法性。	经核查，移动业务应用软件的签名证书由腾讯应用宝颁发，具备合法性。	符合

D.10安全运维管理

D.10.1 安全通用要求部分

D.10.1.1 制度或记录类文档

附录 D 表-23 安全运维管理结果记录表（制度或记录类文档）

安全控制点	测评指标	结果记录	符合程度
环境管理	a)应指定专门的部门或人	经核查，该单位《机房安全管理制	符合

安全控制点	测评指标	结果记录	符合程度
	员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；	度》规定教育信息与网络中心负责机房安全，已指定机房管理员负责对机房进行管理，对机房供配电、UPS 电源、空调、温湿度监控设备等进行管理，具有机房进出登记表、机房值班记录、机房设备维护记录表。	
	b)应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；	经核查，该单位《机房安全管理制度》规定所有进入机房的人员都需要向教育信息与网络中心提交进入机房的申请，说明进入机房的原因、操作内容、及访问时间，并填写《机房进出登记表》，并在操作过程中需要由运维工程师陪同和监督，在进行关键操作之前需请示主管，不可把外部人员单独留在设备旁；机房内应保持清洁，定期消毒、杀菌，保证机房的安全和卫生；机房禁止放置易燃、易爆、腐蚀、强磁性物品，禁止将机房内的电源引出挪做他用，确保机房安全。	符合
	c)应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	经核查，该单位《机房安全管理制度》明确规定不可在重要区域接待来访人员和不随意放置含有敏感信息的移动介质，明确办公桌上不准摆放机要文件，机要文件的草稿纸应立即销毁，不准乱丢，各类记录本不准乱放，一律置于文件柜内或其他固定地方。	符合
资产管理	应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。	经核查，该单位已配置资产管理员定期对资产进行清点核查，具有“资产清单”，清单内容包括部门、重要程度、编号、类型、型号、编码、ip、入库时间、资产使用部门、资产归属部门等。	符合
介质管理	a)应将介质存放在安全的环境中，对各类介质进行	经核查，该单位存储介质由资产管理员统一管理，存储在带锁的介质	符合

安全控制点	测评指标	结果记录	符合程度
	控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；	保存柜中，并定期对介质进行盘点，具有“介质记录清单”。	
	b)应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。	经核查，该单位《介质安全管理规定》明确对涉密介质应实行集中编号登记，责任到人管理，防止失控，处理过涉密信息或者重要数据的存储介质，不得转让或者出借给无关人员使用，不得私自带出境外，不得送往无安全保密保障的机构修理，对需要送出维修或销毁的介质，首先清除其中的敏感数据，防止信息的非法泄漏；对介质归档和查询等过程进行记录，并根据存档介质的目录清单定期盘点；具有“存储介质目录清单”。	符合
设备维护管理	a)应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	经核查，该单位《设备安全管理制度》规定对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定系统管理员定期进行维护管理；系统管理员在日常巡检过程中对设备和线路等进行维护，巡检记录含有相关维护记录。	符合
	b)应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。	经核查，该单位《设备安全管理制度》已规定由教育信息与网络中心负责相关的维护工作，已明确维护责任、维修和服务流程、维修过程的监督控制等内容。	符合
漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。	经核查，该单位《网络安全管理规定》已指定由教育信息与服务中心对网络漏洞进行持续跟踪，制度规定每半年进行一次漏洞扫描，但未有相关漏洞扫描报告和修复记录。	部分符合
网络和系统安全管理	a)应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责	经核查，该单位已设立系统管理员、网络管理员、安全管理员等角色，已在制度和文档中划分各管理	符合

安全控制点	测评指标	结果记录	符合程度
	任和权限；	人员的职责，详见《网络安全管理规定》、“ 岗位安排及岗位职责”。	
	b)应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	经核查，该单位《系统安全管理规定》已指定教育信息与网络中心负责账户管理，创建账户、修改账户权限、删除账户等操作需经过审批后在 OA 系统上填写在审批申请，经过审批后方可执行，OA 系统具有相关审批记录，审批记录中包含审批内容如申请账户、建立账户、删除账户等，审批人，审批时间等。	符合
	c)应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	经核查，该单位《系统安全管理规定》明确对账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定。	符合
	d)应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；	经核查，该单位具有网络安全设备、数据库、服务器操作系统等重要设备的配置操作手册，包含了设备的操作步骤，参数配置等内容。	符合
	e)应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。	经核查，该单位具备系统运维日志记录，具有“机房巡检记录”、“系统维护记录表”等记录文档。	符合
恶意代码防范管理	a)应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	经核查，该单位《恶意代码防范管理制度》已规定须定期组织召开恶意代码宣传培训，并对外来计算机或存储设备接入系统前进行恶意代码检查，具有“E004 防恶意代码意识培训记录”。	符合
	b)应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的	经核查，该单位《恶意代码防范管理制度》规定凡接入单位网络的计算机都必须安装全局统一的恶意代码防范软件，并纳入全局统一的恶	符合

安全控制点	测评指标	结果记录	符合程度
	定期查杀等；	意代码防范管理体系，对外来人员的计算机或存储设备在接入单位网络系统之前应先进行恶意代码检查；安全员要定时检查入侵和恶意代码防范服务器的入侵特征库、恶意代码库、扫描引擎的更新情况，保持入侵特征库、恶意代码库、扫描引擎为最新状态。	
	c)应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。	经核查，该单位《恶意代码防范管理制度》已指定教育信息与网络中心负责对截获的危险恶意代码进行分析处理，定期每月对恶意代码软件病毒库升级更新，未发生过病毒攻击行为，未截获到恶意代码。	符合
配置管理	应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。	经核查，该单位已记录和保存系统的基本配置信息，包括系统名称、型号、版本、VLAN 信息、端口信息、网络结构等内容，详见“网络配置信息表格”。	符合
密码管理	a)应遵循密码相关国家标准和行业标准；	经核查，该单位已在《密码管理制度》中明确信息系统采用密码技术应符合国家标准和行业标准。	符合
	b)应使用国家密码管理主管部门认证核准的密码技术和产品。	经核查，该系统未使用任何密码产品。	不适用
变更管理	应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。	经核查，该单位《变更控制管理制度》明确要求变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施，具有变更审批记录，但未提供变更方案和评审记录。	部分符合
备份与恢复管理	a)应识别需要定期备份的重要业务信息、系统数据及软件系统等；	经核查，该单位《备份与恢复管理制度》已明确备份策略和数据恢复策略，已根据业务重要程度，制定备份清单，具有“数据备份记录表”。	符合

安全控制点	测评指标	结果记录	符合程度
	b)应规定备份信息的备份方式、备份频度、存储介质、保存期等；	经核查，该单位已建立《备份与恢复管理制度》对备份方式、频度、介质、保存期等内容进行了规定。	符合
	c)应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	经核查，该单位已建立《备份与恢复管理制度》规定对重要数据每周全量备份，已制定《E005 应用系统及数据库等重要数据备份和恢复管理办法》作为备份程序和恢复程序。	符合
安全事件处置	a)应及时向安全管理部门报告所发现的安全弱点和可疑事件；	经核查，该单位《网络安全事件报告制度》规定了发生安全事件应向教育信息与网络中心报告，该单位未发生安全事件。	符合
	b)应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；	经核查，该单位已制定《网络安全事件报告制度》，制度中明确了安全事件的报告、处置和响应流程，明确不同安全事件的定义：一般、严重和重大三个事件级别、组织人员职责、安全事件处理流程处置和响应流程：发现事件、应急恢复、事件分析与处理事件记录、上报途径、恢复程序。	符合
	c)应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。	经核查，该单位已制定了安全事件报告模板，要求发生安全事件时，根据报告模板进行填报，安全事件报告包括了发生事件的时间、责任人、影响、影响范围、事件的类型、响应分级、事件描述、事件对业务的负面影响、攻击者的动机、已经采取的应对措施、初步判定事件的发展趋势、计划采取的应对措施、网络安全负责人签名等内容。	符合
应急预案管理	a)应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；	经核查，该单位《校园网络信息安全应急预案》，已明确重要事件的应急预案，包括机房火灾故障、停电事故、设备故障、应用系统故障和网络故障的应急处理流程及系统恢	符合

安全控制点	测评指标	结果记录	符合程度
		复流程等内容。	
	b)应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。	经核查，该单位《校园网络信息安全应急预案》规定每 6 个月对系统相关的人员进行应急预案培训，并进行应急预案的演练；具有《应急预案培训记录》和《应急预案演练记录》。	符合
外包运维管理	a)应确保外包运维服务商的选择符合国家的有关规定；	经核查，该单位目前未涉及任何外包运维服务，不适用。	不适用
	b)应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。	经核查，该单位目前未涉及任何外包运维服务，不适用。	不适用

D.10.2 安全扩展要求部分

D.11其他安全要求

本次测评不包含其他安全要求。

附录E 漏洞扫描结果记录

附录 E 表-1 漏洞扫描主要安全漏洞

序号	安全漏洞名称	关联资产/域名	严重程度
1	允许 Traceroute 探测	10.1.4.27 10.1.4.28 10.1.15.253 10.2.1.2 10.2.1.4 10.2.1.3 172.16.1.1 172.16.1.14 172.16.1.18 172.16.1.50 192.168.10.25 172.16.2.1	低

序号	安全漏洞名称	关联资产/域名	严重程度
		192.168.10.3 10.1.4.16	
2	SSH 版本信息可被获取	10.1.4.27 10.1.4.28 172.16.1.2 172.16.2.1 172.16.1.50	低
3	探测到 SSH 服务器支持的算法	10.1.4.27 10.1.4.28 172.16.2.1 172.16.1.50 172.16.1.2	低
4	OpenSSH CBC 模式信息泄露漏洞(CVE-2008-5161)【原理扫描】	10.1.4.27 10.1.4.28 172.16.1.2 172.16.1.50 172.16.2.1	低
11	服务器允许 SSL 会话恢复【原理扫描】	10.2.1.2 10.2.1.3 172.16.1.18	低
12	SMTP 服务器版本信息可被获取	10.2.1.3 10.2.1.4 172.16.1.1	低
13	可通过 NetBIOS 名字服务端口远程获取系统信息	192.168.10.3	低
14	可通过 HTTP 获取远端 WWW 服务信息	172.16.1.1 172.16.1.14	低
15	获取目标 SSL 证书过期时间【原理扫描】【可验证】	172.16.1.14 10.2.1.2	低
16	探测到服务器支持的 SSL 加密协议【原理扫描】【可验证】	172.16.1.14 10.2.1.2 10.2.1.3	低
17	远端 HSTS 服务运行中	10.2.1.2	低

序号	安全漏洞名称	关联资产/域名	严重程度
18	检测到目标 URL 存在 http host 头攻击漏洞	OA 系统	中
19	检测到目标 X-Content-Type-Options 响应头缺失	OA 系统	低
20	检测到目标 X-XSS-Protection 响应头缺失	OA 系统	低
21	检测到目标 Content-Security-Policy 响应头缺失	OA 系统	低
22	点击劫持：X-Frame-Options 未配置	OA 系统	低

附录F 渗透测试结果记录

F.1 项目实施摘要

F.1.1 测试时间

实施阶段	开始日期	结束日期
渗透测试初测	2023年7月24日	2023年7月24日
渗透测试复测	2023年7月26日	2023年7月26日

表 4.3–II

F.1.2 测试方式

本次测试使用对目标进行远程测试的方式，模拟黑客攻击，使用各种主流测评工具及自主开发的内部测试工具，参照相应安全性能指标标准进行安全检查。被测单位项目组内设立了一个项目配合团队，保证项目有秩序的进行。

F.1.3 测试对象

本次测试按照资产列表（表 4.3－III）的内容中的授权对象作为渗透的对象，进行测试及安全评估，因此本次报告反映了业务系统安全有关的详细安全总结报告。

序号	业务系统名称	域名/IP	备注
01	OA系统	https://oa.mmpt.edu.cn/	现场+远程
02	OA系统APP	-	远程

表 4.3–III

F.1.4 测试工具

测试工具是指为实施测试活动而采用的工具。一切能够满足测试需求、协助测试活动发现问题的工具都是测试工具。在本项目中使用的工具包含但不限于以下工具：

工具名称	工具用途
OKscan	自动化主机扫描、自动化 web 扫描，漏洞探测，精准扫描“操作系统、应用服务、中间件、数据库、web 应用、web 代码”等多种应用漏洞以及弱口令
Nessus	主机发现、高级扫描、基础网络扫描、高级动态扫描等功能
Burp Suite	拦截数据包、修改数据包、重放数据包、暴力破解、解码等功能
Nmap	端口扫描、快速扫描大型的网络、主机发现、版本侦测、操作系统侦测等功能
Sqlmap	自动化的SQL注入，布尔类型的盲注、时间的盲注、报错注入、联合查询注入、堆叠查询注入等方式对数据库进行检测

表 4.3–IV

F.2 渗透测试概述

渗透测试（Penetration Test）,是完全模拟黑客可能使用的攻击技术和漏洞发现技术，对目标系统的安全做深入的探测，发现系统最脆弱的环节。

WEB 网络渗透测试：主要通过对目标系统信息的全面收集、对系统中网路设备的探测、对服务器系统主机的漏洞扫描、对应用平台及数据库系统的安全性扫描及通过应用系统程序的安全性渗透测试等手段来完成对整个 WEB 系统的安全性渗透检测。该渗透测试是一个完整、系统的测试过程，涵盖了网络层面、

主机层面、数据层面以及应用服务层面的安全性测试。

入侵者的攻击入侵需要利用目标网络的安全弱点，渗透测试也是同样的道理。测试人员模拟真正的入侵者入侵攻击方法，以人工渗透为主，辅助以攻击工具的使用，以保证整个渗透测试过程都在可以控制和调整的范围之内，同时确保对网络没有造成破坏性的损害。由于采用可控制的、非破坏性质的渗透测试，因此不会对被评估的客户信息系统造成严重的影响。在渗透测试结束后，客户信息系统将基本保持一致。

对于已经部署了安全防护措施（安全产品、安全服务）或者即将部署安全防护措施的用户而言，明确网络当前的安全现状对下一步的安全建设有重大的指导意义。渗透测试服务用于验证在当前的安全防护措施下网络、系统抵抗黑客攻击的能力。

F.2.1 渗透测试目的

通过模拟黑客的渗透测试，评估目标系统是否存在可以被攻击者真实利用的漏洞以及由此引起的风险大小，为制定相应的安全措施与解决方案提供实际的依据。

分析客户 WEB 应用系统的安全现状，检测 WEB 应用系统的漏洞和安全问题，并验证其他已知的脆弱点。对系统的任何弱点、技术缺陷或漏洞的主动分析，并且以有利于攻击为目的而对漏洞加以利用。从而全面了解和掌握 WEB 应用系统的信息安全威胁和风险，为 WEB 应用系统开展安全调优及加固建设提供依据，并指导客户实施调优及加固工作，具体的目标包括：

- 帮助客户理解应用系统当前的安全状况，发现在系统复杂结构中的最脆

弱链路；

- 通过改进建议，保证 WEB 应用系统和相关基础设施满足标准的安全性基线；
- 降低 WEB 应用系统信息安全事件发生的可能性；
- 保障 WEB 应用系统的安全、可靠、稳定运行。

F.2.2 渗透测试风险管理

相对其他服务而言，渗透测试是一种需要相当技术深度的高端服务，要求渗透测试人员有丰富的经验及新颖的思路。

在渗透测试过程中，虽然我们尽量避免影响正常业务的运行，也会采取适当的风险规避、风险降低的方法，但是由于测试的不确定性，渗透测试服务仍然有可能对网络、系统运行造成一定不同程度的影响，可能造成服务停止，甚至是宕机。

另外，对于安全防护措施严密的网络、系统，在有限的时间内进行渗透测试可能不会获得成功结果。这在一定程度也证明了网络、系统能够在一定程度上抵抗黑客的攻击。

F.2.3 渗透测试收益

从攻击者的角度进行测试将有助于发现并识别出一些隐性存在的安全漏洞和风险点。

从客户收益的角度来说，特别是在进行安全项目之前进行渗透测试，可以对信息系统的安全性得到较深的感性认知，有助于后续的安全建设。

在进行了安全项目之后进行渗透测试,则可以用于验证经过安全保护后的网络是否真实的达到了预定安全目标、遵循了安全策略。

F.2.4 渗透测试流程

本次渗透测试基本流程如下:

1. 选择渗透测试目标,向客户提交渗透测试申请。申请包括渗透测试对象、时间、影响等内容。
2. 在获取客户批准后，进行具体渗透测试工作。
3. 具体渗透操作包括信息收集分析、漏洞发现、权限提升、密码破解等工作。

F.2.5 渗透测试技术方法

渗透测试一般采用工具扫描及人工渗透的技术方法，本项目主要是针对 web 系统开展渗透测试，为保证测试范围覆盖 web 系统的各个组成部分，我方将从如下几个方面开展项目测试工作。

- 信息收集;
- 系统层渗透测试;
- 数据库层渗透测试;
- 网络层渗透测试;
- 应用及中间件层渗透测试。

F.3 测试结果综述

F.3.1 漏洞等级分布

序号	业务系统	URL 地址	高	中	低	小计
1	OA系统	https://oa.mmpt.edu.cn/	0	0	0	0
2	OA系统APP	-	0	0	0	0
合计			0	0	0	0



图表 4.3–I

根据漏洞的影响范围、利用方式、攻击后果等情况，从高到低将其分为三个等级，即高危、中危、低危。漏洞危害等级分布如图表 4.3－I 所示，其中高风险问题 0 个，中风险问题 0 个，低风险问题 0 个。

F.3.2 漏洞信息摘要

本次渗透测试发现应用系统风险漏洞，具体漏洞信息情况如下：

序号	漏洞名称	漏洞位置	危险等级	章节	修复情况
1	反射型xss	https://oa.mmpt.edu.cn/seeyon/content/content.do?method=index&isFullPage=true&hasDealArea=false&moduleId=442336378970786207&moduleType=1&rightId=&contentType=41&viewState=2&openFrom=listSent&canDeleteISigntureHtml=false&isSubFlow=false&isShowMoveMenu=false&isShowDocLockMenu=false&fromIframeName=summary&nodeName=&officecanPrint=true&canEditContent=false&rnd=0.09445067648736138	中	错误！未找到引用源。	已修复

表 4.3–V

F.4 漏洞详情

F.4.1 茂名职业技术学院 OA 系统漏洞详情

F.4.1.1【中】反射型 xss

漏洞名称：反射型 xss

修复结果：已修复

漏洞等级：中

漏洞位置：

https://oa.mmpt.edu.cn/seeyon/content/content.do?method=index&isFullPage=true&hasDealArea=false&moduleId=442336378970786207&moduleType=1&rightId=&con

tentType=41&viewState=2&openFrom=listSent&canDeleteISigntureHtml=false&isSubFlow=false&isShowMoveMenu=false&isShowDocLockMenu=false&fromIframeName=summary&nodeName=&officecanPrint=true&canEditContent=false&rnd=0.09445067648736138

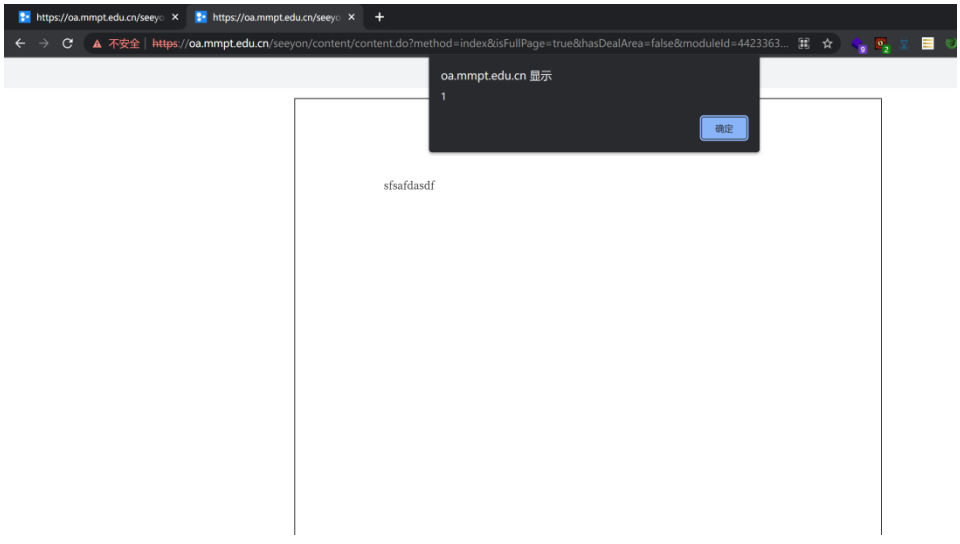
漏洞描述：

跨站点脚本编制，即 XSS 攻击，是一种经常出现在 web 应用中的计算机安全漏洞，它允许恶意 web 用户将代码植入到提供给其它用户使用的页面中。比如这些代码包括 HTML 代码和客户端脚本。攻击者利用 XSS 漏洞旁路掉访问控制——例如同源策略(same origin policy)。这种类型的漏洞由于被黑客用来编写危害性更大的网络钓鱼(Phishing)攻击而变得广为人知

漏洞说明：。

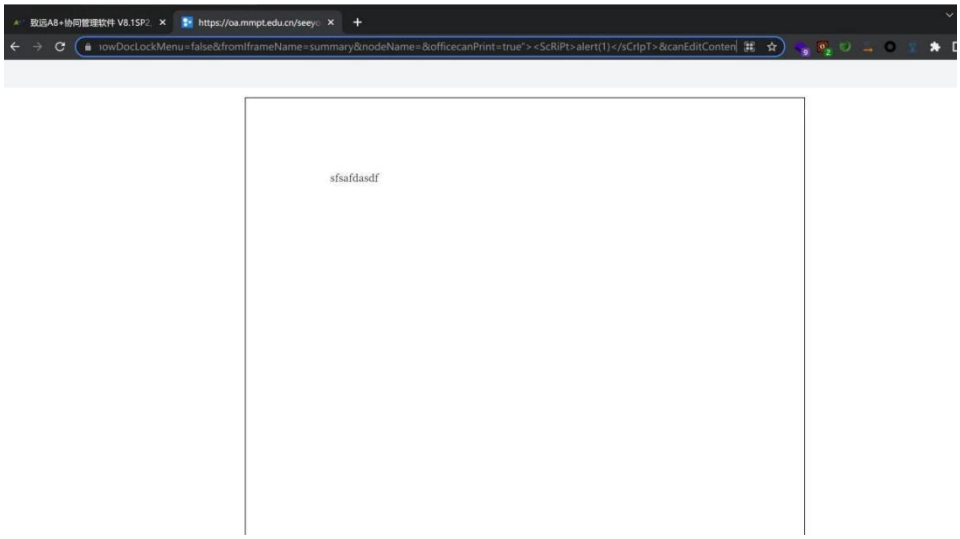
将 payload 放入 officecanPrint 参数当中即可触发 xss 。

Payload:”><ScRiPt>alert(1)</sCrIpT>



漏洞修复证明：

该漏洞经过验证已修复，修复结果：


https://oa.mmpt.edu.cn/seey
iowDocLockMenu=false&fromIframeName=summary&nodeName=&officecanPrint=true"><ScRiPt>alert(1)</sCrIpT>&canEditConten
sfsafdasdf

F.5 整体建议

- 1、定期对系统、服务器进行渗透测试，及时对存在的安全漏洞问题进行修复加固；
- 2、检查各服务器信息系统、应用程序的运行情况，定期做好系统数据、系统日志检查和备份工作；
- 3、定期对网络进行安全评估，随时监控网络的安全状况，并形成文档；
- 4、保持与我司工程师联系，互相沟通信息。

附录G 威胁列表

附录 G 表-1 威胁列表

序号	威胁分（子）类	威胁描述
1	恶意攻击	利用工具和技术对信息系统进行攻击和入侵。
2	软硬件故障	对业务实施或系统运行产生影响的设备硬件故障、通讯链路中断、系统本身或软件缺陷造等问题。
3	管理不到位	由于制度缺失、不完善等原因导致安全管理无法落实或者不到位。
4	无作为或操作失误	应该执行而没有执行相应的操作，或者无意执行了错误的操作。
5	敏感信息泄露	敏感信息泄露给不应了解的他人。
6	物理环境影响	对信息系统正常运行造成影响的物理环境问题和自然灾害。
7	越权或滥用	越权访问本来无权访问的资源，或者滥用自己的权限破坏信息系统。
8	物理攻击	通过物理的接触造成对软件、硬件和数据的破坏。
9	篡改	非法修改信息，破坏信息的完整性使系统的安全性降低或信息不可用。
10	抵赖	否认所做的操作。
11	供应链失效	业务或系统所依赖的供应商、接口等不可用。
12	恶意代码	受到病毒、蠕虫、逻辑炸弹、木马后门等恶意代码的攻击可能造成的影响。
13	物理损害	对业务实施或系统运行产生影响的物理损害。
14	自然灾害	自然界中所发生的异常现象，且对业务开展或者系统运行会造成危害的现象和事件。
15	信息损害	对系统或资产中的信息产生破坏、篡改、丢失、盗取等行为。
16	技术失效	信息系统所依赖的软硬件设备不可用。
17	未授权行为	超出权限设置或授权进行操作或者使用的行为。

序号	威胁分（子）类	威胁描述
18	功能损害	造成业务或系统运行的部分功能不可用或者损害。

报告编号：44090243008-00008-22-0163-01

网络安全等级保护
OA系统等级测评报告

委托单位：茂名职业技术学院

测评单位：广东南方信息安全研究院

报告时间：2022年10月30日

网络安全等级测评基本信息表

被测对象				
被测对象名称	OA系统		安全保护等级	第二级（S2A2）
备案证明编号	44090243008-00008			
被测单位				
单位名称	茂名职业技术学院			
单位地址	广东省茂名市茂南区文明北路232号大院		邮政编码	525000
联系人	姓名	龙恒	职务/职称	教师
	所属部门	教育信息与网络中心	办公电话	0668-2920122
	移动电话	13377766618	电子邮件	372383968@qq.com
测评单位				
单位名称	广东南方信息安全研究院		机构代码	SC202127130010163
单位地址	广州市科学城彩频路9号B座12楼1202		邮政编码	510663
联系人	姓名	谢若雨	职务/职称	助理
	所属部门	办公室	办公电话	020-32290702
	移动电话	18819149895	电子邮件	office@cybersec-gd.cn
审核批准	编制人		编制日期	2022.10.30
	审核人		审核日期	2022.10.30
	批准人		批准日期	2022.10.30

声明

本报告是OA系统的等级测评报告。

本报告测评结论的有效性建立在被测评单位提供相关证据的真实性基础之上。

本报告中给出的测评结论仅对被测对象当时的安全状态有效。当测评工作完成后，由于被测对象发生变更而涉及到的系统构成组件（或子系统）本报告不再适用。

本报告中给出的测评结论不能作为对被测对象内部部署的相关系统构成组件（或产品）的测评结论。

在任何情况下，若需引用本报告中的测评结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。

单位名称：广东南方信息安全研究院

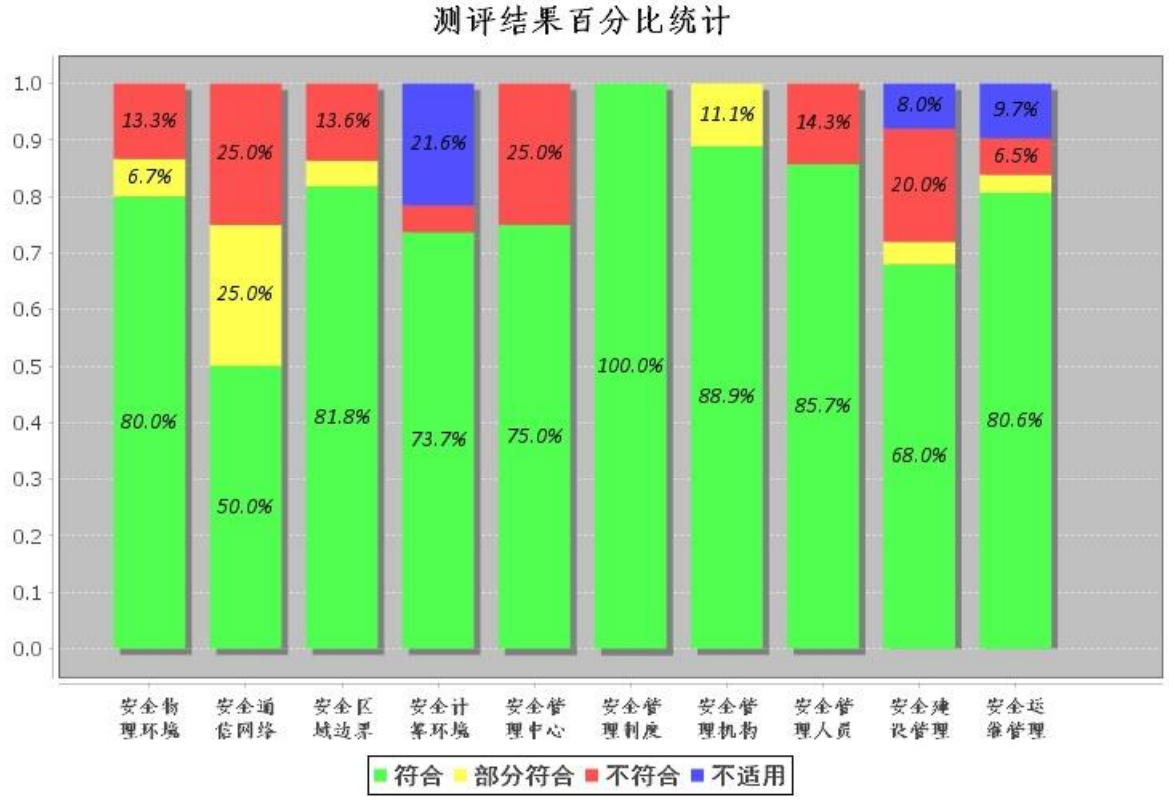
2022年10月30日

等级测评结论

测评结论和综合得分			
被测对象名称	OA系统	安全保护等级	第二级（S2A2）
扩展要求应用情况	□云计算 □移动互联 □物联网 □工业控制系统 □大数据		
被测对象描述	OA系统是由茂名职业技术学院统一组织规划建设，由北京致远互联软件有限公司负责开发，于2018年10月正式投入运行，由教育信息与网络中心负责运行维护。茂名职业技术学院是该信息系统的业务主管部门，茂名职业技术学院为该信息系统定级的责任单位。 OA系统网络主要分为4个区域，分别为外网边界区域、安全管理区域、服务器存储区域、办公网区域，主要由网络设备、安全设备组成，不对互联网提供业务访问。OA系统为B/S结构，主要由Linux平台的操作系统，Oracle平台的数据库系统，及Tomcat中间件系统组成。单位采用自主运维模式，通过部署运维及管理终端提供专用运维环境管理，采用运维安全管理系统实现设备的统一管理，并进行操作运维审计，日志审计系统进行设备日志统一收集存储与分析。 茂名职业技术学院OA系统是学院实现办公流程话的系统，包括了公文管理、会议管理、流程管理、移动管理、全文检索、高级office套件等模块，OA系统实现了学校办文、办会、办事的规范化，实现了规范流程管理、内控合规管理、标准高效管理。		
安全状况描述	OA系统通信传输具备一定的保护措施，安全区域边界较清晰，网络层具备访问控制、安全审计的相应技术措施。各设备在身份鉴别、访问控制、安全审计、入侵防范方面具备控制措施。重要数据在数据完整性、个人信息保护方面具备保护措施。在安全管理制度层面较为完善。在网络架构不够完整，网络层在入侵防范、恶意代码和垃圾邮件防范的技术措施存在不足。重要数据在数据备份恢复方面存在不足。 OA系统在本次测评中总共出现27类问题，其中0类高风险问题,11类中风险问题，16类低风险问题。在本次测评通过扫描及渗透发现6类漏洞问题，其中0类危险程度为高的漏洞，1类危险程度为中的漏洞，5类危险程度为低的漏洞。 OA系统本次等级测评的综合得分为73.85，且不存在高等级安全风险，等级测评结论为中。		
等级测评结论	中	综合得分	73.85

总体评价

通过对信息系统基本安全保护状态的分析，茂名职业技术学院针对OA系统面临的主要安全威胁采取了相应的安全机制，基本达到保护信息系统重要资产的作用。OA系统在本次测评中采用了GB/T 22239-2019，其中安全通用要求135项，不适用5项。



在安全物理环境方面，针对安全通用要求，基础设施在防雷击、电磁防护、防水和防潮、物理位置选择、电力供应、防盗窃和防破坏、温湿度控制等方面较为完善（如：信息化机房）。在物理访问控制、防静电等方面还不够完善（如：信息化机房），机房出入口未配置电子门禁系统，机房内缺乏防静电措施（如防静电地板或铺设防静电地毯）。

在安全通信网络方面,针对安全通用要求,网络环境在通信传输等方面较为完善(如:安全通信网络）。在网络架构等方面还不够完善（如：安全通信网络），关键的应用服务和数据库服务网段未独立进行子网划分的情况。

在安全区域边界方面，针对安全通用要求，网络环境在边界防护、安全审计、访问控制等方面较为完善（如：外网边界区域，安全管理区域，服务器存储区域等）。在入侵防范、恶意代码和垃圾邮件防范等方面还不够完善(如:安全管理区域,办公网区域)，网络层部署防火墙,防火墙未配置对内部发起的攻击行为实现防范功能策略,无法检测、防止或限制从内部发起的网络攻击行为,现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。

在安全计算环境方面，针对安全通用要求，计算环境在个人信息保护、安全审计、数据完整性、访问控制、入侵防范、恶意代码防范、身份鉴别、剩余信息保护等方面较为完善。在主机方面，在可信验证等方面还不够完善（如：业务终端-2，业务终端-1，运维及管理终端-2等），缺乏对计算设备可信验证方面的安全设计要求，现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。在应用方面，在数据备份恢复等方面还不够完善（如：OA系统），未能提供应用软件系统重要数据的异地定时数据备份功能。在网络及安全设备方面，在可信验证等方面还不够完善（如：基线核查系统，上网行为管理系统，WEB应用防火墙等），设备不具备相关可信验证的技术措施。在数据保护方面,在数据备份恢复等方面还不够完善(如:重要个人信息,重要业务数据)，未能提供应用软件系统重要数据的异地定时数据备份功能。

在安全管理中心方面，针对安全通用要求，安全控制措施在审计管理等方面较为完善（如：管理中心）。在系统管理等方面还不够完善（如：管理中心），系统管理的资源、运行及配置管理不够全面。

在安全管理制度方面,针对安全通用要求,管理制度体系在制定和发布、安全策略、管理制度、评审和修订等方面较为完善（如：制度文件、执行/记录文件）。

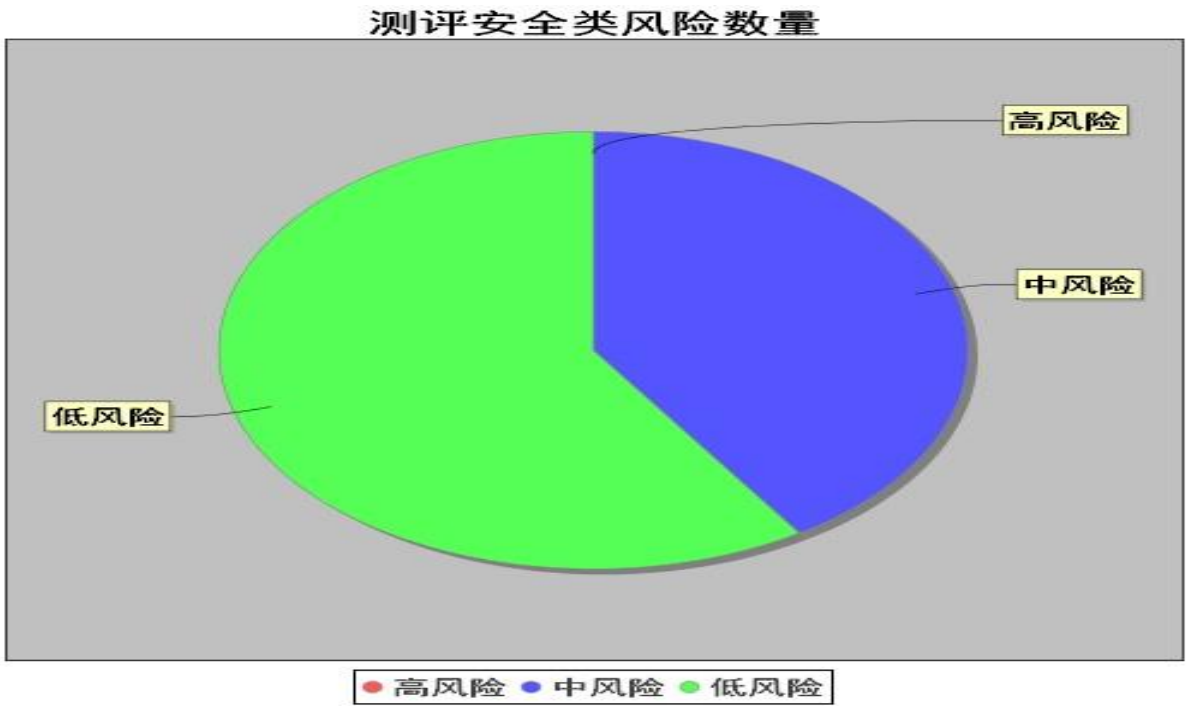
在安全管理机构方面，针对安全通用要求，机构建设在人员配备、沟通和合作、授权和审批、岗位设置等方面较为完善（如：制度文件、执行/记录文件）。在审核和检查等方面还不够完善（如：制度文件、执行/记录文件），单位开展的检查工作不够完善。

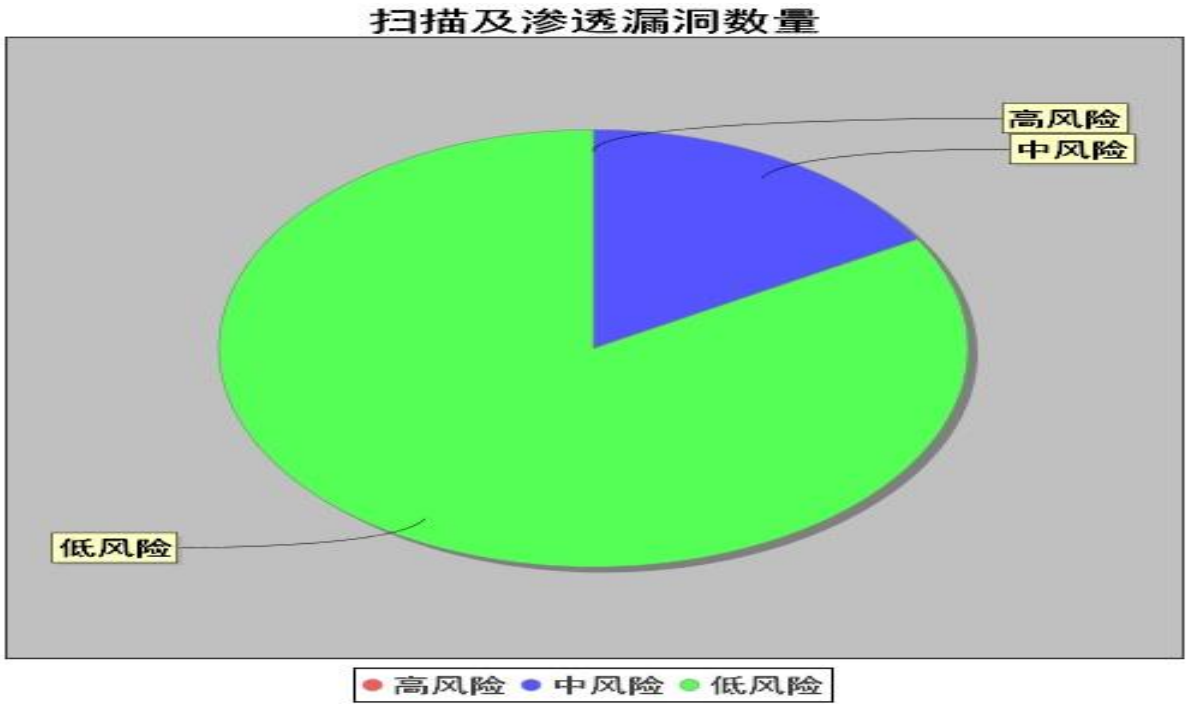
在安全管理人员方面,针对安全通用要求,人员在人员录用、安全意识教育和培训、人员离岗等方面较为完善（如：制度文件、执行/记录文件）。在外部人员访问管理等方面还不够完善（如：制度文件、执行/记录文件），单位未完全按管理规范开展人员离场后的清理工作。

在安全建设管理方面，针对安全通用要求，系统建设在定级和备案、工程实施、等级测评、产品采购和使用、服务供应商选择、系统交付等方面较为完善(如：制度文件、执行/记录文件)。在安全方案设计等方面还不够完善(如：制度文件、执行/记录文件)，单位未具备完整的安全设计方案相关的文档，单位相关方案的设计的内容不够完善。

在安全运维管理方面，针对安全通用要求，系统运维在介质管理、设备维护管理、网络和系统安全管理、备份与恢复管理、资产管理、应急预案管理、环境管理、配置管理、安全事件处置、变更管理等方面较为完善（如：制度文件、执行/记录文件）。在密码管理等方面还不够完善（如：制度文件、执行/记录文件），单位不了解现有密码相关的国家标准和行业标准，单位缺乏密码管理要求的制度文档。

OA系统在本次测评中总共出现27类问题，其中0类高风险问题,11类中风险问题，16类低风险问题。在本次测评通过扫描及渗透发现6类漏洞问题，其中0类危险程度为高的漏洞，1类危险程度为中的漏洞，5类危险程度为低的漏洞。





OA系统本次等级测评的综合得分为73.85，且不存在高等级安全风险，等级测评结论为中。

主要安全问题及整改建议

一、安全物理环境

安全通用要求

(1)中风险 机房出入口未配置电子门禁系统（如：信息化机房）。 上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域,可能对系统的平稳运行造成影响。

建议安排专人7*24小时负责机房出入，对出入的人员进行身份鉴别和登记，且出入有专人陪同或在机房出入口配置电子门禁系统，控制、鉴别和记录进入的人员。

(2)中风险 机房内缺乏防静电措施（如防静电地板或铺设防静电地毯 ）（如：信息化机房）。 存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。

建议采用防静电地板或地面并采用必要的接地防静电措施。

二、安全通信网络

安全通用要求

(1)中风险 关键的应用服务和数据库服务网段未独立进行子网划分的情况（如：安全通信网络）。 上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变得更为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。

建议独立划分出应用服务器网段、数据库服务器网段。

三、安全区域边界

安全通用要求

(1)中风险 网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为（如：办公网区域）。 存在不

能及时发现内部主机作为攻击跳板，或网络攻击行为而造成系统损坏/网络资源浪费的风险。

建议网络层部署的防火墙配置对内部发起的攻击行为实现防范功能策略，实现检测、防止或限制从内部发起的网络攻击行为。

(2)中风险 **现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面（如：办公网区域）。 无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。**

建议现有部署的恶意代码防范措施网络边界覆盖全面，及时对恶意代码及逆行检测和清除。

四、安全计算环境

1、网络设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

2、安全设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

3、服务器和终端

安全通用要求

(1)中风险 **操作系统及数据库存在较多中风险的漏洞。 系统存在风险级别为中的漏洞，存在容易造成系统被入侵的可能性。**

建议对系统服务、中间件、数据库补丁进行分析，尽量及时更新关键的漏洞补丁或更新相应系统版本。

4、系统管理软件/平台

安全通用要求

(1)中风险 未能提供数据库系统重要数据的异地定时数据备份功能（如：应用/数据库服务器-Oracle）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供，使企业的经济利益或声誉受到损害。

建议数据库系统利用通信网络将关键数据定时批量传送至备用场地，实现异地数据异地备份。

5、业务应用系统/平台

安全通用要求

(1)中风险 未能提供应用软件系统重要数据的异地定时数据备份功能（如：OA系统）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。

建议利用通信网络将应用软件系统关键数据定时批量传送至备用场地，实现异地数据异地备份。

6、数据资源

安全通用要求

重要业务数据

(1)中风险 未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要业务数据）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。

建议利用通信网络将应用软件系统关键数据定时批量传送至备用场地，实现异地数据异地备份。

重要个人信息

(1)中风险 未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要个人信息）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。

建议利用通信网络将应用软件系统关键数据定时批量传送至备用场地，实现异地数据异地备份。

7、其他系统或设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

五、安全管理中心

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

六、安全管理制度

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

七、安全管理机构

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

八、安全管理人员

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

九、安全建设管理

安全通用要求

(1)中风险 单位未具备完整的安全设计方案相关的文档。单位相关方案的设计的内容不够完善（如：制度文件、执行/记录文件）。 相关合规的规划配套文件缺失，可能导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。

建议根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件。

十、安全运维管理

安全通用要求

(1)中风险 单位不了解现有密码相关的国家标准和行业标准。单位缺乏密码管理要求的制度文档（如：制度文件、执行/记录文件）。 密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不到位，存在违反国家政策的风险。

建议单位学习现有密码相关的国家标准和行业标准。建立密码管理要求的制度文档。

目录

网络安全等级测评基本信息表 I
声明 II
等级测评结论 III
总体评价 IV
主要安全问题及整改建议 VIII
一、安全物理环境 VIII
安全通用要求 VIII
二、安全通信网络 VIII
安全通用要求 VIII
三、安全区域边界 VIII
安全通用要求 VIII
四、安全计算环境 IX
1、网络设备 IX
安全通用要求 IX
2、安全设备 IX
安全通用要求 IX
3、服务器和终端 IX
安全通用要求 IX
4、系统管理软件/平台 X
安全通用要求 X
5、业务应用系统/平台 X
安全通用要求 X
6、数据资源 X
安全通用要求 X
7、其他系统或设备 XI
安全通用要求 XI
五、安全管理中心 XI
安全通用要求 XI
六、安全管理制度 XI
安全通用要求 XI
七、安全管理机构 XI
安全通用要求 XI
八、安全管理人员 XI
安全通用要求 XI
九、安全建设管理 XI
安全通用要求 XII
十、安全运维管理 XII
安全通用要求 XII

目录.....XIII
1 测评项目概述.....1
1.1 测评目的.....1
1.2 测评依据.....1
1.3 测评过程.....2
1.4 报告分发范围.....5
2 被测对象描述.....5
2.1 被测对象概述.....5
2.1.1 定级结果.....5
2.1.2 业务和采用的技术.....5
2.1.3 网络结构.....5
2.2 测评指标.....7
2.2.1 安全通用要求指标.....7
2.2.2 安全扩展要求指标.....9
2.2.3 其他安全要求指标.....10
2.2.4 不适用安全要求指标.....10
2.3 测评对象.....10
2.3.1 测评对象选择方法.....10
2.3.2 测评对象选择结果.....11
2.3.2.1 物理机房.....12
2.3.2.2 网络设备.....12
2.3.2.3 安全设备.....12
2.3.2.4 服务器.....13
2.3.2.5 终端设备.....13
2.3.2.6 其他系统或设备.....13
2.3.2.7 系统管理软件/平台.....14
2.3.2.8 业务应用软件/平台.....14
2.3.2.9 数据资源.....15
2.3.2.10 安全相关人员.....15
2.3.2.11 安全管理文档.....16
3 单项测评结果分析.....20
3.1 安全物理环境.....21
3.1.1 已有安全控制措施汇总分析.....21
3.1.2 主要安全问题汇总分析.....22
3.2 安全通信网络.....23
3.2.1 已有安全控制措施汇总分析.....23
3.2.2 主要安全问题汇总分析.....23
3.3 安全区域边界.....24
3.3.1 已有安全控制措施汇总分析.....24
3.3.2 主要安全问题汇总分析.....25
3.4 安全计算环境.....26
3.4.1 网络设备.....26

3.4.1.1 已有安全控制措施汇总分析 26
3.4.1.2 主要安全问题汇总分析 28
3.4.2 安全设备 28
3.4.2.1 已有安全控制措施汇总分析 28
3.4.2.2 主要安全问题汇总分析 32
3.4.3 服务器和终端 32
3.4.3.1 已有安全控制措施汇总分析 32
3.4.3.2 主要安全问题汇总分析 36
3.4.4 系统管理软件/平台 37
3.4.4.1 已有安全控制措施汇总分析 37
3.4.4.2 主要安全问题汇总分析 40
3.4.5 业务应用系统/平台 40
3.4.5.1 已有安全控制措施汇总分析 40
3.4.5.2 主要安全问题汇总分析 42
3.4.6 数据资源 42
3.4.6.1 已有安全控制措施汇总分析 42
3.4.6.2 主要安全问题汇总分析 43
3.4.7 其他系统或设备 43
3.4.7.1 已有安全控制措施汇总分析 43
3.4.7.2 主要安全问题汇总分析 44
3.5 安全管理中心 44
3.5.1 已有安全控制措施汇总分析 44
3.5.2 主要安全问题汇总分析 45
3.6 安全管理制度 45
3.6.1 已有安全控制措施汇总分析 45
3.6.2 主要安全问题汇总分析 46
3.7 安全管理机构 46
3.7.1 已有安全控制措施汇总分析 46
3.7.2 主要安全问题汇总分析 48
3.8 安全管理人员 48
3.8.1 已有安全控制措施汇总分析 48
3.8.2 主要安全问题汇总分析 49
3.9 安全建设管理 49
3.9.1 已有安全控制措施汇总分析 49
3.9.2 主要安全问题汇总分析 51
3.10 安全运维管理 52
3.10.1 已有安全控制措施汇总分析 52
3.10.2 主要安全问题汇总分析 56
3.11 其他安全要求指标 57
3.11.1 已有安全控制措施汇总分析 57
3.11.2 主要安全问题汇总分析 57
3.12 验证测试 57
3.12.1 漏洞扫描 57
3.12.1.1 漏洞扫描结果统计 57

3.12.1.2 漏洞扫描问题描述 61
3.12.2 渗透测试 62
3.12.2.1 渗透测试过程说明 62
3.12.2.2 渗透测试问题描述 64
3.13 单项测评小结 64
3.13.1 控制点符合情况汇总 64
3.13.2 安全问题汇总 68
4 整体测评 72
4.1 安全控制点间安全测评 72
4.1.1 安全建设管理 72
4.1.1.1 安全通用要求 72
4.1.2 安全运维管理 73
4.1.2.1 安全通用要求 73
4.2 区域间安全测评 73
4.2.1 安全物理环境 73
4.2.1.1 安全通用要求 73
4.2.2 安全通信网络 74
4.2.2.1 安全通用要求 74
4.2.3 安全区域边界 74
4.2.3.1 安全通用要求 74
4.3 整体测评结果汇总 75
5 安全问题风险分析 76
6 等级测评结论 81
7 安全问题整改建议 83
附录A 被测对象资产 90
A.1 物理机房 90
A.2 网络设备 90
A.3 安全设备 90
A.4 服务器 91
A.5 终端设备 91
A.6 其他系统或设备 91
A.7 系统管理软件/平台 91
A.8 业务应用软件/平台 92
A.9 数据资源 92
A.10 密码产品 93
A.11 安全相关人员 93
A.12 安全管理文档 93
附录B 上次测评问题整改情况说明 98
附录C 单项测评结果汇总 99
C.1 安全物理环境 99

C.2 安全通信网络 99
C.3 安全区域边界 99
C.4 安全计算环境 100
C.4.1 网络设备 100
C.4.2 安全设备 101
C.4.3 服务器和终端 102
C.4.4 系统管理软件/平台 102
C.4.5 业务应用系统/平台 103
C.4.6 数据资源 103
C.4.7 其他系统或设备 104
C.5 安全管理中心 104
C.6 安全管理制度 104
C.7 安全管理机构 104
C.8 安全管理人员 105
C.9 安全建设管理 105
C.10 安全运维管理 105
C.11 其他安全要求指标 106

附录D 单项测评结果记录 107

D.1 安全物理环境 107
D.1.1 安全通用要求 107
D.1.1.1 信息化机房 107
D.2 安全通信网络 109
D.2.1 安全通用要求 109
D.2.1.1 安全通信网络 109
D.3 安全区域边界 109
D.3.1 安全通用要求 109
D.3.1.1 办公网区域 110
D.3.1.2 外网边界区域 112
D.3.1.3 安全管理区域 114
D.3.1.4 服务器存储区域 116
D.4 安全计算环境 119
D.4.1 安全通用要求 119
D.4.1.1 网络设备 119
D.4.1.2 安全设备 126
D.4.1.3 服务器和终端 151
D.4.1.4 系统管理软件/平台 172
D.4.1.5 业务应用系统/平台 180
D.4.1.6 数据资源 183
D.4.1.7 其他系统或设备 191
D.5 安全管理中心 191
D.5.1 安全通用要求 191
D.5.1.1 管理中心 191
D.6 安全管理制度 193
D.6.1 安全通用要求 193

D.6.1.1 制度文件、执行/记录文件 193
D.7 安全管理机构 195
D.7.1 安全通用要求 195
D.7.1.1 制度文件、执行/记录文件 195
D.8 安全管理人员 197
D.8.1 安全通用要求 197
D.8.1.1 制度文件、执行/记录文件 197
D.9 安全建设管理 199
D.9.1 安全通用要求 199
D.9.1.1 制度文件、执行/记录文件 199
D.10 安全运维管理 203
D.10.1 安全通用要求 203
D.10.1.1 制度文件、执行/记录文件 203
D.11 其他安全要求 211
附录E 漏洞扫描结果记录 211
附录F 渗透测试结果记录 212
附录G 威胁列表 214

1 测评项目概述

1.1 测评目的

安全等级测评的目标是通过对目标系统在安全技术及管理方面的测评,对目标系统的安全技术状态及安全管理状况做出初步判断,给出目标系统在安全技术及安全管理方面与其相应安全等级保护要求之间的差距。测评结论作为委托方进一步完善系统安全策略及安全技术防护措施依据。

项目背景是为进一步提高信息系统的保障能力,根据《信息安全等级保护管理办法》（公通字2007【43】号）的精神，茂名职业技术学院委托广东南方信息安全研究院（SC202127130010163）对OA系统实施等级测评，以期发现信息系统和等级保护标准的差距以及存在的安全隐患，为后续的安全整改工作提供参考依据。

1.2 测评依据

测评过程中主要依据的标准:

测评标准

（1）GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》

（2）GB/T 28448-2019 《信息安全技术 网络安全等级保护测评要求》

测评参考标准

（1）GB 17859-1999 《计算机信息系统 安全保护等级划分准则》

（2）GB/T 28449-2018 《信息安全技术 网络安全等级保护测评过程指南》

（3）GB/T 20984-2007 《信息安全技术 信息安全风险评估规范》

（4）GB/T 25058-2019 《信息安全技术 网络安全等级保护实施指南》

测评参考法律法规

（1）《中华人民共和国网络安全法》

（2）《中华人民共和国密码法》

（3）《中华人民共和国数据安全法》

1.3 测评过程

本次等级测评分为四个过程：测评准备活动、方案编制活动、测评实施活动、报告编制活动。具体如图 1-1 所示。其中，各阶段的时间安排如下：

⑴ 测评准备活动

测评准备活动的目标是顺利启动测评项目,收集定级对象相关资料,准备测评所需资料,为编制测评方案打下良好的基础。测评准备活动包括工作启动、信息收集和分析、工具和表单准备三项主要任务。

（2）方案编制活动

方案编制活动的目标是整理测评准备活动中获取的定级对象相关资料,为现场测评活动提供最基本的文档和指导方案。方案编制活动包括测评对象确定、测评指标确定、测评内容确定、工具测试方法确定、测评指导书开发及测评方案编制六项主要任务。

（3）现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调,为现场测评的顺利开展打下良好基础,依据测评方案实施现场测评工作,将测评方案和测评方法等内容具体落实到现场测评活动中。现场测评工作应取得报告编制活动所需的、足够的证据和资料。现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

（4）报告编制活动

在现场测评工作结束后,测评机构应对现场测评获得的测评结果(或称测评证据)进行汇总分析,形成等级测评结论,并编制测评报告。测评人员在初步判定单项测评结果后,还需进行单元测评结果判定、整体测评、系统安全保障评估,经过整体测评后,有的单项

测评结果可能会有所变化,需进一步修订单项测评结果,而后针对安全问题进行风险评估,形成等级测评结论。分析与报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、系统安全保障评估、安全问题风险评估、等级测评结论形成及测评报告编制七项主要任务。

各阶段完成的关键任务：

序号	阶段	任务	对象	开始日期	结束日期
1	测评准备活动	工作启动	项目甲乙双方	2022年8月15日	2022年8月19日
2		信息收集与分析	调研表	2022年8月22日	2022年8月25日
3		工具和表单准备	测评工具、测评授权书、文档交接单	2022年8月25日	2022年8月30日
4	方案编制活动	测评对象确认	测评方案-对象列表	2022年8月31日	2022年8月31日
5		测评指标确认	测评方案-指标列表	2022年8月31日	2022年8月31日
6		测评内容确认	测评方案-内容列表	2022年9月1日	2022年9月1日
7		工具测试方法确认	测评方案-工具测试方法列表	2022年9月1日	2022年9月1日
8		测评指导书开发	测评作业指导书	2022年9月2日	2022年9月2日
9		测评方案编制	测评方案	2022年9月5日	2022年9月5日
10	现场测评活动	现场测评准备	工具、人员、表单准备	2022年9月28日	2022年9月28日
11		现场测评和结果记录	安全管理访谈	2022年9月28日	2022年9月28日
12			安全管理文档检查	2022年9月28日	2022年9月28日
13			安全物理环境测评	2022年9月28日	2022年9月28日
14			安全通信网络	2022年9月28日	2022年9月29日
15			安全区域边界	2022年9月28日	2022年9月29日
16			安全计算环境	2022年9月28日	2022年9月29日
17			工具测试	2022年9月29日	2022年10月9日
18		结果确认和资料归还	检测人员出入场确认单、测评现场服务评价单	2022年10月8日	2022年10月9日
19	报告编制活动	单项测评结果	测评报告	2022年10月9日	2022年10月12日

序号	阶段	任务	对象	开始日期	结束日期
		判定			
20		单元测评结果判定		2022年10月9日	2022年10月17日
21		整体测评		2022年10月9日	2022年10月17日
22		系统安全保障评估		2022年10月9日	2022年10月17日
23		安全问题风险分析		2022年10月9日	2022年10月17日
24		等级测评结论形成		2022年10月17日	2022年10月30日
25		测评报告编制		2022年10月17日	2022年10月30日

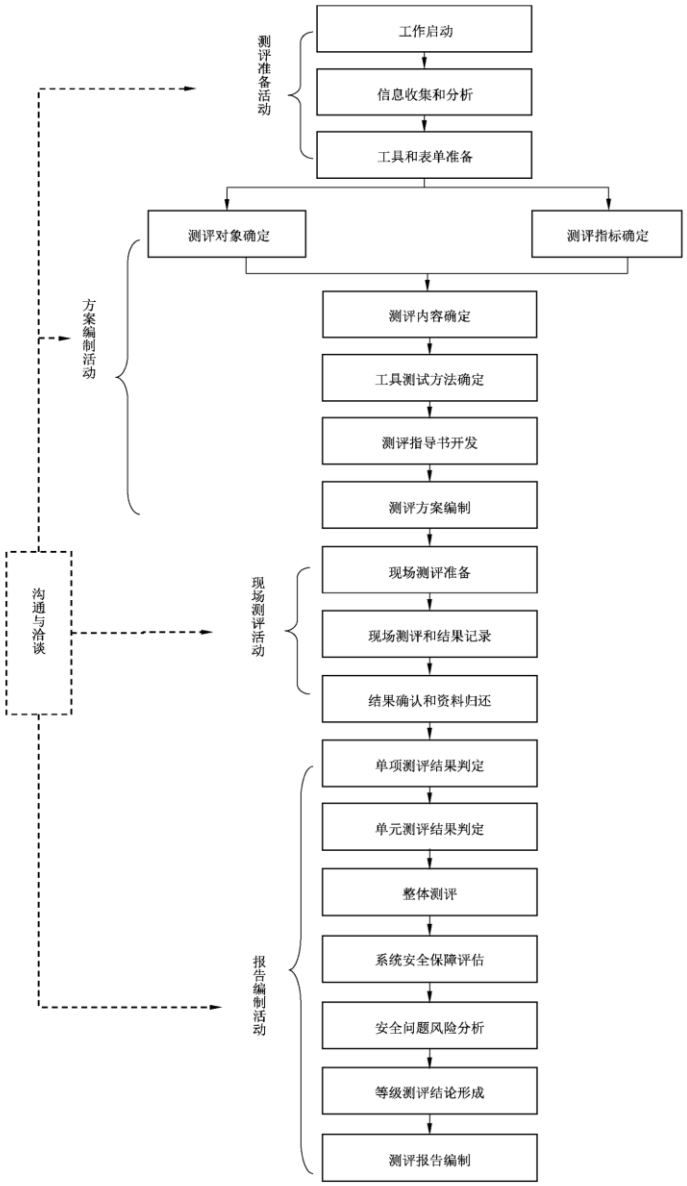


图 1-1 等级保护测评工作流程图

其中，于项目前期召开了项目启动会议，确定了工作方案及项目人员名单；于现场测评完成后召开了项目末次会议，确认了测评发现的问题；于2022年10月30日在对系统的整改情况进行了复核确认后，完成报告编制。

1.4 报告分发范围

等级测评报告正本一式3份，其中茂名职业技术学院1份，广东南方信息安全研究院1份，受理备案的公安机关1份。

2 被测对象描述

2.1 被测对象概述

2.1.1 定级结果

表 2-1定级结果

被测对象名称	安全保护等级	业务信息安全等级	系统服务安全等级
OA系统	2	2	2

2.1.2 业务和采用的技术

茂名职业技术学院OA系统是学院实现办公流程话的系统，包括了公文管理、会议管理、流程管理、移动管理、全文检索、高级office套件等模块，OA系统实现了学校办文、办会、办事的规范化，实现了规范流程管理、内控合规管理、标准高效管理。

被测对象未采用云计算/移动互联/物联网/工业控制/大数据等技术情况。

2.1.3 网络结构

OA系统主要是对内网提供服务，相关设备部署在信息化机房当中,其简要拓扑如下:

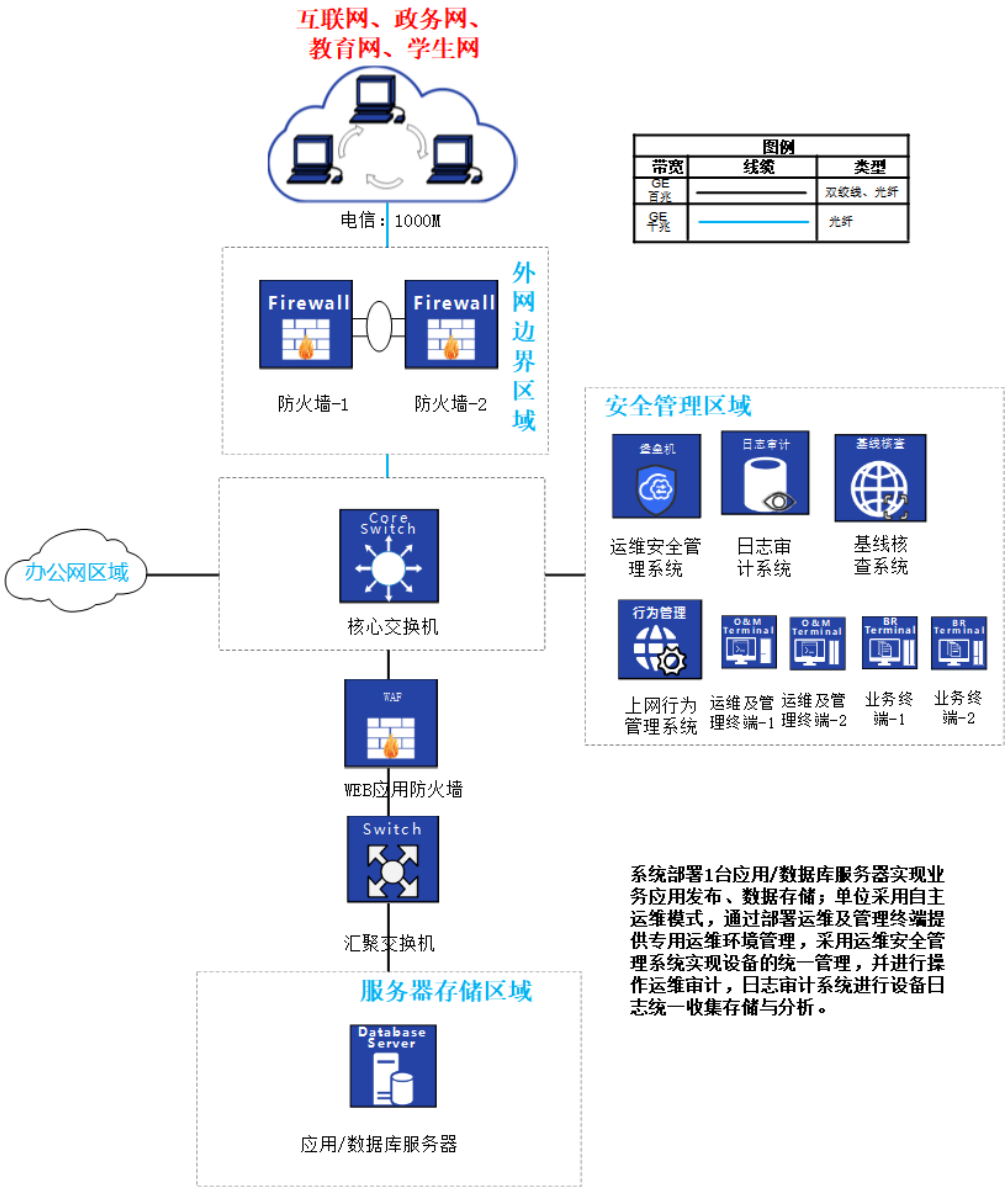


图 2-10A 系统网络拓扑图

如图2-1OA系统网络拓扑图所示，OA系统网络安全域划分为4个，分别为外网边界区域、安全管理区域、服务器存储区域、办公网区域。

1、外网边界区域：

外网边界区域网络主要包括OA系统的业务服务和信息交换应用，是安全管理区域、服务器存储区域、办公网区域的出口边界；其链路接入为光纤线，带宽为1000mb。通过部署核心交换机、防火墙等设备实施网络访问控制，防火墙（入侵防御模块）实现网络入侵攻击行为防御。

2、办公网区域：

办公网区域网络主要包括OA系统与办公区域的信息交换应用，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、防火墙、上网行为管理系统等设备实施网络访问控制、防火墙（入侵防御模块）实现网络入侵攻击行为防御。

3、安全管理区域：

安全管理区域网络主要包括日志审计系统、运维安全管理系统、上网行为管理系统，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、上网行为管理系统等设备实施网络访问控制。

4、服务器存储区域：

服务器存储区域网络主要包括OA系统的应用服务器、数据库服务器，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、上网行为管理系统等设备实现一定的网络访问控制。

5、服务器部署情况：

OA系统由1台应用/数据库服务器实现应用发布、数据处理、存储、维护。

6、灾备及冗余

OA系统无异地备份机房，未实现异地备份数据定时传输功能。系统重要数据根据需求采用每天增量、每月全备到本地信息化机房。

OA系统未实现冗余措施。

2.2 测评指标

2.2.1 安全通用要求指标

表 2-2 安全通用要求指标

安全类	安全控制点	测评项数
安全物理环境	物理位置选择	2
	物理访问控制	1
	防盗窃和防破坏	2
	防雷击	1
	防火	2
	防水和防潮	2
	防静电	1
	温湿度控制	1
	电力供应	2
	电磁防护	1
安全通信网络	网络架构	2
	通信传输	1
	可信验证	1
安全区域边界	边界防护	1
	访问控制	4
	入侵防范	1
	恶意代码和垃圾邮件防范	1
	安全审计	3
	可信验证	1
安全计算环境	身份鉴别	3
	访问控制	4
	安全审计	3
	入侵防范	5
	恶意代码防范	1
	可信验证	1
	数据完整性	1
	数据备份恢复	2
	剩余信息保护	1
	个人信息保护	2
安全管理中心	系统管理	2
	审计管理	2
安全管理制度	安全策略	1
	管理制度	2
	制定和发布	2
	评审和修订	1
安全管理机构	岗位设置	2
	人员配备	1
	授权和审批	2
	沟通和合作	3

安全类	安全控制点	测评项数
	审核和检查	1
安全管理人员	人员录用	2
	人员离岗	1
	安全意识教育和培训	1
	外部人员访问管理	3
安全建设管理	定级和备案	4
	安全方案设计	3
	产品采购和使用	2
	自行软件开发	2
	外包软件开发	2
	工程实施	2
	测试验收	2
	系统交付	3
	等级测评	3
	服务供应商选择	2
安全运维管理	环境管理	3
	资产管理	1
	介质管理	2
	设备维护管理	2
	漏洞和风险管理	1
	网络和系统安全管理	5
	恶意代码防范管理	3
	配置管理	1
	密码管理	2
	变更管理	1
	备份与恢复管理	3
	安全事件处置	3
	应急预案管理	2
	外包运维管理	2
安全通用要求指标数量统计		135

2.2.2 安全扩展要求指标

表 2-3 安全扩展要求指标

扩展类型	安全类	安全控制点	测评项数
本次测评不涉及安全扩展要求指标			

2.2.3 其他安全要求指标

表 2-4 其他安全要求指标

安全类	安全控制点	测评项数
本次测评不涉及其他安全要求指标		

2.2.4 不适用安全要求指标

表 2-5-1 不适用安全要求指标

安全类	安全控制点	不适用项	不适用原因
安全建设管理	自行软件开发	a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。
安全建设管理	自行软件开发	b) 应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。
安全运维管理	密码管理	b) 应使用国家密码管理主管部门认证核准的密码技术和产品。	（1）单位未采购涉及密码技术的产品，不适用。
安全运维管理	外包运维管理	a) 应确保外包运维服务商的选择符合国家的有关规定；	（1）单位目前未涉及任何外包运维服务情况，不适用。
安全运维管理	外包运维管理	b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。	（1）单位目前未涉及任何外包运维服务情况，不适用。

表 2-5-2 其他不适用安全要求指标

安全类	安全控制点	不适用项	不适用原因
本次测评不涉及其他安全要求指标			

2.3 测评对象

2.3.1 测评对象选择方法

OA系统等级测评的测评对象种类上基本覆盖、数量进行抽样，重点抽查主要的设备、设施、人员和文档等。结合OA系统的网络拓扑结构和业务情况，本次等级测评的测评对象在抽样时主要考虑以下几个方面：

（1） 主机房（包括其环境、设备和设施等）和灾备机房；

（2） 存储被测系统重要数据的介质的存放环境；

（3） 办公场地；

（4） 整个系统的网络拓扑结构；

（5） 安全设备，包括防火墙等；

（6） 边界网络设备，包括路由器、楼层交换机等；

（7） 对整个信息系统或其局部的安全性起作用的网络互联设备，如核心交换机、路由器等；

（8） 承载业务处理系统主要业务或数据的服务器（包括其操作系统和数据库）；

（9） 管理终端和主要应用系统终端；

（10） 能够完成系统不同业务使命的业务应用系统；

（11） 业务备份系统；

（12） 信息安全主管人员、各方面的负责人员、具体负责安全管理的当事人、业务负责人；

（13） 涉及到信息系统安全的所有管理制度和记录。

抽样原则：在等级测评时，业务处理系统中配置相同的安全设备、边界网络设备、网络互联设备、服务器、终端以及备份设备，每类至少抽查两台作为测评对象。

2.3.2 测评对象选择结果

2.3.2.1 物理机房

表 2-6 物理机房

序号	机房名称	物理位置	重要程度
1	信息化机房	茂名市茂南区文明北路232号大院大楼	关键

2.3.2.2 网络设备

表 2-7 网络设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度
1	核心交换机	否	H3C version 7.1.070, Release 7585P07	H3C S7500E-X	核心数据交换、访问控制	关键
2	汇聚交换机	否	H3C version 7.1.070, Release 6126P20	H3C S5560X-30C-EI	数据交换	重要

2.3.2.3 安全设备

表 2-8 安全设备

序号	设备名称	是否虚拟设备	系统及版本	品牌型号	用途	重要程度
1	上网行为管理系统	否	深信服AC12.0.26	深信服AC-1000-D600-PT	上网行为管理及终端准入控制	重要
2	WEB应用防火墙	否	深信服AF 8.0.9	深信服WAF-2000-H642	应用防护、入侵防范、病毒防护	重要
3	日志审计系统	否	深信服LAS 3.0.5	深信服AC-1000-D601-PT	日志审计	重要
4	防火墙-2	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键
5	防火墙-1	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键
6	基线核查系统	否	深信服V3.0.3	深信服AC-1000-D602-	漏洞扫描	重要

序号	设备名称	是否虚拟设备	系统及版本	品牌型号	用途	重要程度
				PT		
7	运维安全管理系统	否	深信服V3.0.6	深信服AC-1000-D603-PT	运维审计	重要

2.3.2.4 服务器

表 2-9 服务器

序号	设备名称	所属业务应用系统/平台	是否虚拟设备	操作系统及版本	数据库管理系统及版本	中间件及版本	重要程度
1	应用/数据库服务器	OA系统	否	CentOS 6.8	Oracle 11.2.0.1.0	Tomcat 8.0.37	关键

2.3.2.5 终端设备

表 2-10 终端设备

序号	设备名称	是否虚拟设备	操作系统及版本	用途	重要程度
1	业务终端-1	否	Windows 10 （版本 20H2（内部版本 19044.1889）	业务管理	一般
2	运维及管理终端-1	否	Windows 10 （版本 20H2（内部版本 19044.1889）	运维管理、系统管理	一般
3	运维及管理终端-2	否	Windows 10 （版本 21H2（内部版本 19044.1889）)	运维管理、系统管理	一般
4	业务终端-2	否	Windows 10 （版本 20H2（内部版本 19044.1889）	业务管理	一般

2.3.2.6 其他系统或设备

表 2-11 其他系统或设备

序号	设备名称	是否虚拟设备	系统及版本	用途	重要程度
/	/	/	/	/	/

注释：本次测评对象中不涉及专用移动互联终端等，不开展抽测。

2.3.2.7 系统管理软件/平台

表 2-12 系统管理软件/平台

序号	系统管理软件/平台名称	主要功能	版本	所在设备名称	重要程度
1	应用/数据库服务器-Tomcat	页面发布	8.0.37	应用/数据库服务器	关键
2	应用/数据库服务器-Oracle	数据生产、存储	11.2.0.1.0	应用/数据库服务器	关键

2.3.2.8 业务应用软件/平台

表 2-13 业务应用系统/平台

序号	业务应用软件/平台名称	主要功能	业务应用软件及版本	开发厂商	重要程度
1	OA系统	茂名职业技术学院OA系统是学院实现办公流程话的系统，包括了公文管理、会议管理、流程管理、移动管理、全文检索、高级office套件等模块，OA系统实现了学校办文、办会、办事的规范化，实现了规范流程管理、内控合规管理、标准高效管理。	V6.0	北京致远互联软件股份有限公司	关键

2.3.2.9 数据资源

表 2-14 数据资源

序号	数据类别	所属业务应用	安全防护需求	重要程度
1	重要业务数据	OA系统	完整性、保密性	关键
2	重要个人信息	OA系统	完整性、保密性	关键
3	鉴别数据	OA系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性、保密性	关键
4	重要审计数据	OA系统（安全管理中心）	完整性	重要
5	重要配置数据	OA系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性	关键

注释：网络设备、安全设备、服务器、终端、系统管理软件/平台和业务应用系统等所涉及的鉴别数据和重要配置数据分别在各自测评对象中汇总测评证据后集中体现,包括数据完整性、数据保密性和备份恢复。重要审计数据在安全管理中心进行汇总测评证据，包括数据完整性。重要业务数据和重要个人信息分别在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。

2.3.2.10 安全相关人员

表 2-15 安全相关人员

序号	姓名	岗位/角色	联系方式	所属单位
1	龙恒	数据管理员	13377766618	茂名职业技术学院
2	杨云	资产管理员	0668-2920122	茂名职业技术学院
3	杨云	审计管理员	0668-2920122	茂名职业技术学院
4	龙恒	应用管理员	13377766618	茂名职业技术学院
5	叶永利	安全管理员	0668-2920122	茂名职业技术学院
6	吴国华	系统管理员	0668-2920122	茂名职业技术学院
7	龙恒	网络管理员	13377766618	茂名职业技术学院

序号	姓名	岗位/角色	联系方式	所属单位
8	吴国华	机房管理员	0668-2920122	茂名职业技术学院

2.3.2.11 安全管理文档

表 2-16 安全管理文档

序号	文档名称	主要内容
1	制度类文档-办公环境保密管理	关于单位办公环境管理制度文档
2	制度类文档-信息系统外包运维管理制度	关于单位外包运维工作管理制度文档
3	制度类文档-外部接入受控网络访问系统管理规范	关于单位针对外部人员工作接入规范制度文档
4	制度类文档-授权和审批管理规定	关于单位授权审批、审批流程规范制度文档
5	制度类文档-办公环境管理制度	关于单位办公环境管理制度文档
6	制度类文档-网络与信息系统安全设计规范	关于单位网络与信息化安全设计制度文档
7	制度类文档-安全事件报告和处置	关于单位网络安全事件管理、处置、流程等报告制度文档
8	制度类文档-外部人员访问管理制度	关于单位针对外来人员访问管控制度文档
9	制度类文档-物理安全管理规范	关于加强单位办公区域及电子计算机机房的管理和设备运行安全，规范办公区域及机房建设，使人员办公高效及机房设备安全、稳定运行的制度文档
10	制度类文档-安全管理组织规范	关于单位组织结构管理规范制度文档
11	制度类文档-介质管理制度	关于单位介质安全管理工制度文档
12	制度类文档-系统安全管理制度	关于单位系统安全管理、安全服务管理制度文档
13	制度类文档-信息安全总体策略	关于单位网络安全方针、策略制度文档
14	制度类文档-主机安全管理规范	关于规定单位主机系统安全管理要求规范，指导业务平台主机的安全配置和维护的制度文档
15	制度类文档-信息安全奖惩办法	关于单位人员奖惩制度文档
16	制度类文档-服务供应商选择安全管理制度	关于单位安全服务供应商管理规定制度文档
17	制度类文档-网络安全事件	关于单位网络安全事件应急处理、流程、培训等管理制度文档

序号	文档名称	主要内容
	应急预案	
18	制度类文档-制度制定、发布、评审和修订管理制度	关于单位制度制定、发布、评审和修订等管理文档
19	制度类文档-安全漏洞管理制度	关于单位安全漏洞管理工作制度文档
20	制度类文档-测试及验收方案	关于单位测试验收方案文档
21	制度类文档-组织安全结构和人员职责制度	关于单位安全结构、人员职责
22	制度类文档-信息系统恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
23	制度类文档-网络安全事件报告制度	关于单位网络安全事件管理报告文档
24	制度类文档-应用安全管理规范	关于规定单位应用安全管理要求及规范的制度文档
25	制度类文档-外部服务人员管理规范	关于单位针对外部人员工作管理规范制度文档
26	制度类文档-变更控制管理制度	关于单位变更流程、控制管理制度文档
27	制度类文档-外包开发软件管理规定	关于单位外包项目管理工作制度文档
28	制度类文档-系统交付管理	关于单位交付工作管理制度文档
29	制度类文档-系统及应用数据备份管理规范	关于单位数据备份、恢复管理制度文档
30	制度类文档-安全审查和检查管理规范	关于单位安全检查、审查工作规范制度文档
31	制度类文档-工程测试验收管理	关于单位工程测试工作管理制度文档
32	制度类文档-离岗人员工作交接规范	关于单位离岗交接工作规范制度文档
33	制度类文档-安全教育和培训制度	关于单位安全培训、安全交流工作制度文档
34	制度类文档-数据安全管理规范	关于保障关键数据安全，从数据库本身、数据加密、数据备份恢复三个方面对数据安全进行规范的制度文档
35	制度类文档-设备安全管理制度	关于单位设备安全管理制度文档
36	制度类文档-组织安全结构和人员职责制度	关于单位组织结构、人员安排、人员职责制度文档
37	制度类文档-网络安全管理制度	关于单位网络安全工作管理制度文档
38	制度类文档-工程实施管理制度	关于单位工程实施工作管理制度文档

序号	文档名称	主要内容
39	制度类文档-岗位安排及岗位职责	关于单位岗位职责、岗位安排制度文档
40	制度类文档-应用系统业务用户密码设置规定	关于单位用户密码管理制度文档
41	制度类文档-恶意代码防范管理制度	关于单位恶意代码防范工作制度文档
42	制度类文档-备份与恢复管理制度	关于单位数据备份、恢复管理制度文档
43	制度类文档-机房安全管理制度	关于单位机房安全管理工作制度文档
44	制度类文档-人员管理制度	关于单位人员录用、调岗、离岗管理制度文档
45	制度类文档-恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
46	制度类文档-信息安全漏洞扫描规范	关于单位安全漏洞工作规范制度文档
47	制度类文档-网络安全管理规范	关于保障单位网络系统的安全稳定运行，抵御内部和外部各种形式的网络攻击或威胁制定的管理文档
48	制度类文档-员工考核管理制度	关于单位人员考核工作管理制度文档
49	操作类文档-设备及系统软件配置和操作手册	关于单位安全设备操作、Linux服务器配置手册、主机运维操作手册、软件操作手册、防火墙配置和操作手册、数据库日常运维操作手册等指导文档
50	操作类文档-设备操作规程	关于单位相关设备操作指导文档
51	操作类文档-数据备份策略	关于单位数据备份策略文件
52	操作类文档-软硬件日常维护管理规程	关于单位计算机网络系统使用、管理、信息安全、资源共享有所遵循,规范上网操作流程,提高网络系统安全性的指导文档
53	记录类文档-设备操作维护记录	关于单位设备维护工作记录
54	记录类文档-外部人员访问申请表	关于外来人员访问申请流程工作记录
55	记录类文档-技能培训记录	关于单位系统培训工作、考核工作记录
56	记录类文档-设备维修申请表	关于单位设备维护工作申请记录
57	记录类文档-接入受控网络申请表	关于外来人员接入工作记录
58	记录类文档-网络信息安全事件记录表	关于单位网络安全事件工作记录
59	记录类文档-人员离岗申请表	关于人员离岗申请记录
60	记录类文档-安全建设方案评审纪录	关于单位网络与信息化安全设计方案评审工作记录
61	记录类文档-信息系统存储	关于备份介质存储使用清单

序号	文档名称	主要内容
	介质使用清单	
62	记录类文档-收发文登记记录	关于单位文档签发记录
63	记录类文档-系统交付清单	关于单位交付工作记录
64	记录类文档-备份介质使用记录	关于备份介质使用登记工作记录
65	记录类文档-信息安全检查记录表	关于单位安全检查工作记录
66	记录类文档-评审和修订记录	关于单位变更评审、修订工作记录
67	记录类文档-离职员工物品交回登记表	关于人员离岗工物交接工作记录
68	记录类文档-信息系统存储介质销毁申请表	关于备份介质销毁申请工作记录
69	记录类文档-机房维护日志	关于机房维护工作记录
70	记录类文档-设备出入登记记录表	关于设备进出机房登记工作记录
71	记录类文档-机房巡检记录表	关于单位机房环境巡检记录
72	记录类文档-网络配置信息	关于单位配置信息登记工作记录
73	记录类文档-备份工作汇总表	关于单位数据备份工作总结表
74	记录类文档-数据备份记录表	关于单位数据备份工作记录
75	记录类文档-监理审批表	关于单位监理审核工作记录
76	记录类文档-关键岗位人员考核记录	关于关键岗位考核工作记录
77	记录类文档-应急预案培训记录表	关于单位应急预案培训工作记录
78	记录类文档-离场信息资料交接表	关于人员离岗交接工作记录
79	记录类文档-访问记录表	关于人员访问工作记录
80	记录类文档-人员培训及考核记录表	关于人员培训、考核等工作记录
81	记录类文档-机房出入登记表	关于人员进出机房登记工作记录
82	记录类文档-安全管理制度评审记录	关于单位制度审计记录
83	记录类文档-外部会议文件和记录	关于单位外部联系、交流及会议工作记录
84	记录类文档-软件交付清单	关于单位交付工作记录
85	记录类文档-外部人员访问	关于外来人员访问登记工作记录

序号	文档名称	主要内容
	记录表	
86	记录类文档-漏洞检测报告	关于单位安全漏洞检测报告文档
87	记录类文档-机房设备维修记录表	关于单位机房设备维修工作记录
88	记录类文档-信息管理系统漏洞检查表	关于单位安全漏洞工作检测记录表
89	记录类文档-数据恢复申请表	关于单位数据恢复工作申请表
90	记录类文档-机房设备维护记录表	关于设备维护登记工作记录
91	记录类文档-存储介质目录清单	关于备份介质存储工作清单
92	记录类文档-人员入职考核记录	关于人员录用、考核工作记录
93	记录类文档-重要操作审批表	关于单位审批工作记录
94	记录类文档-通用变更记录表	关于单位变更工作记录
95	记录类文档-信息安全会议记录	关于单位安全培训、安全交流会议记录
96	记录类文档-专家论证记录表	关于单位网络方案论证记录
97	证据类文档-定级备案	关于单位系统定级报告、备案证文件
98	证据类文档-网络安全系统设计方案	关于单位网络与信息化安全设计方案文档
99	证据类文档-网络安全等级保护工作小组名单	关于单位网络安全等级保护工作小组人员名单文件
100	证据类文档-工程项目实施方案	关于单位工程实施方案文档
101	证据类文档-深信服安全采购合同	关于单位与安全厂家服务采购、产品选择合同文件
102	证据类文档-网络安全等级保护测评服务合同	关于单位与安全服务商签定的安全服务合同文件
103	证据类文档-资产清单	关于单位信息系统资产清单统计表
104	证据类文档-信息安全事件分析报告表	关于单位安全事件分析报告
105	证据类文档-外部联系表	关于单位内部联系及外部联系名单
106	证据类文档-安全职位人员	关于单位人员岗位安排名单

3 单项测评结果分析

3.1 安全物理环境

3.1.1 已有安全控制措施汇总分析

安全通用要求

物理位置选择	
a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；	
信息化机房	（1）机房和办公场地场所在建筑物具有建筑验收文档，包含对防震、防风和防雨能力的说明； （2）机房和办公场地未出严重的问题。
b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	
信息化机房	（1）机房未部署在易发生问题的位置； （2）机房对于空调设备的排水管等部位采取密封防漏处理； （3）机房对于楼板进行了防护措施。
防盗窃和防破坏	
a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识；	
信息化机房	（1）机房设备或主要部件都固定在机架上； （2）机房内对主要部件已绑定相应不易除去的标签； （3）重要机柜已进行上锁处理。
b) 应将通信线缆铺设在隐蔽安全处。	
信息化机房	（1）通信线缆铺设在下走线槽隐蔽处中； （2）通信线缆设有明显的源目的标识； （3）通信线缆均铺设整齐、规范。
防雷击	
应将各类机柜、设施和设备等通过接地系统安全接地。	
信息化机房	（1）机房设置专用地线； （2）机房内机柜、设施和设备等进行接地处理； （3）交流电源接地验收检测结果符合要求。
防火	
a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；	
信息化机房	（1）机房采用经消防检测部门检测合格并在有效期内的（如 七氟丙烷）气体自动灭火设备，火灾自动报警类型为烟感+红外； （2）自动消防系统工作状态正常，有定期巡检和维护记录《机房巡检记录表》； （3）建立机房消防的管理制度相关文档《机房安全管理制度》，按管理要求机房无人情况下气体灭火配置为自动模式，进入机房调整为手动模式，机房报警有7*24小时值班人员进行监控。
防水和防潮	
a) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	
信息化机房	（1）机房不存在雨水渗透、破损等不合规情况； （2）机房不位于建筑的顶层、边缘区域。
b) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。	

信息化机房	（1）机房区域范围已部署1台科华品牌（精密）空调，机房内分别配置1组温湿度传感器监控； （2）机房内空调下方已铺设安装好挡水和排水设施； （3）机房墙壁或楼板的管道采取必要的防渗防漏等防水保护措施； （4）机房安装检测设备（如：漏水检测绳）检测地下积水，及时处理机房水蒸气结露和地下积水的转移与渗透； （5）目前防水\防潮检测未发现异常情况，并且有防水防潮的运维记录《机房维护日志》。
温湿度控制	
应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。	
信息化机房	（1）机房范围已部署1组科华品牌精密空调进行温湿度调节； （2）机房范围已部署空调及加湿机进行温湿度调节； (3)温湿度自动调节设施运作正常,有运行和维护记录《机房维护日志》; （4）机房温度能保持在24摄氏度到28摄氏度之间； （5）机房湿度能保持在40%到65%之间。
电力供应	
a) 应在机房供电线路上配置稳压器和过电压防护设备；	
信息化机房	（1）机房配备了稳压器和过电压防护设备； （2）稳压器和过电压防护设备正常工作； （3）机房具备电力供应安全设计，并在其中标明配备稳压器、过电压防护设备等要求。
b) 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。	
信息化机房	（1）机房配备了1组科华品牌UPS； （2）UPS正常工作，可满足主要设备断电情况下的至少1小时正常运行要求； （3）UPS有定期（至少每年）检查和维护，有运行和维护记录《机房巡检记录表》。
电磁防护	
电源线和通信线缆应隔离铺设，避免互相干扰。	
信息化机房	（1）通信线缆铺设采用独立的具有电磁屏蔽作用线槽； （2）电源线缆铺设采用独立的具有电磁屏蔽作用线槽； （3）弱电线缆隔离铺设，没有干扰。

3.1.2 主要安全问题汇总分析

安全通用要求

（1）机房出入口未配置电子门禁系统（如：信息化机房）。上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域,可能对系统的平稳运行造成影响。中风险。

（2）机房建设未完全采用符合耐火等级的建筑材料。机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级（如：信息化机房）。存在发生火情时助燃火灾的风险。 低风险。

（3）机房内缺乏防静电措施（如防静电地板或铺设防静电地毯 ）（如：信息化机房）。存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。 中风险。

3.2 安全通信网络

3.2.1 已有安全控制措施汇总分析

安全通用要求

网络架构	
b) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	
安全通信网络	(1) 网络内重要网段未部署在网络边界处，且未直接连接外部信息系统； （2） 系统通过防火墙对重要网段采取访问控制策略； （3） 各安全域（子网）的出口唯一。
通信传输	
应采用校验技术保证通信过程中数据的完整性。	
安全通信网络	（1）网络系统中未涉及完整性保障设备，但在安全计算环境方面网络设备采用SSH协议、安全设备采用HTTPS协议、操作系统采用SSH协议、应用系统采用HTTPS协议来保证通信过程中数据的完整性。

3.2.2 主要安全问题汇总分析

安全通用要求

（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况（如：安全通信网络）。上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变得更为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。 中风险。

（2）缺乏对通信设备可信验证方面的安全设计要求。现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况（如：安全通信网络）。缺乏对系统可执行程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致计算资源被干扰和破坏造成损失。 低风险。

3.3 安全区域边界

3.3.1 已有安全控制措施汇总分析

安全通用要求

边界防护	
应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络存在受保护的边界； （2）网络边界处部署了可提供访问控制功能的设备； （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。
访问控制	
a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。
b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。
c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。
d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	
办公网区域 外网边界区域	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设

安全管理区域 服务器存储区域	备； （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。
入侵防范	
应在关键网络节点处监视网络攻击行为。	
外网边界区域 服务器存储区域	（1）网络层部署支持对内部发起的攻击行为进行防范的设备； （2）现有的防范措施满足相应防护要求； （3）内部安全防范措施能检测相应攻击行为。
恶意代码和垃圾邮件防范	
应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	
外网边界区域 服务器存储区域	（1）在关键网络节点处部署合规的防恶意代码措施； （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试。
安全审计	
a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； （3）现有的审计措施满足相应的审计要求。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； （3）设备本地时间正常。
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。

3.3.2 主要安全问题汇总分析

安全通用要求

（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为（如：办公网区域）。存在不能及时

发现内部主机作为攻击跳板，或网络攻击行为而造成系统损坏/网络资源浪费的风险。中风险。

（2）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面（如：办公网区域）。无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。 中风险。

（3）缺乏对边界设备可信验证方面的安全设计要求。现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况（如：办公网区域）。缺乏对边界设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4 安全计算环境

3.4.1 网络设备

3.4.1.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
核心交换机 汇聚交换机	（1）设备对各登录模式均启用身份鉴别； （2）设备对登录管理的用户进行身份鉴别； （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的全局密码策略； （6）设备配置加密的super认证。
b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
核心交换机 汇聚交换机	（1）设备配置合规的全局登录失败处理策略； （2）设备配置合规的操作超时退出措施。
c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
核心交换机 汇聚交换机	（1）设备配置合规的远程管理模式。
访问控制	

a) 应对登录的用户分配账户和权限；	
核心交换机 汇聚交换机	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。
b) 应重命名或删除默认账户，修改默认账户的默认口令；	
核心交换机 汇聚交换机	（1）设备不存在默认账户名； （2）设备账户口令设置合规。
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
核心交换机 汇聚交换机	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	
核心交换机 汇聚交换机	（1）设备根据安全策略要求对特权用户进行分离； （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
核心交换机 汇聚交换机	（1）设备开启审计功能，审计进程正常； （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
核心交换机 汇聚交换机	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
核心交换机 汇聚交换机	（1）设备限制审计文件的访问控制权限，普通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效； （5）日志及审计记录保存大于6个月。
入侵防范	
a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	
核心交换机 汇聚交换机	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。
b) 应关闭不需要的系统服务、默认共享和高危端口；	
核心交换机 汇聚交换机	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。
c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
核心交换机 汇聚交换机	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制；

	（2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
核心交换机 汇聚交换机	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
核心交换机 汇聚交换机	鉴别数据、重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； （2）设备对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a）应提供重要数据的本地数据备份与恢复功能；	
核心交换机 汇聚交换机	（1）设备定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。

3.4.1.2 主要安全问题汇总分析

安全通用要求

（1）设备不具备相关可信验证的技术措施（如：核心交换机）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.2 安全设备

3.4.2.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
WEB应用防火墙 上网行为管理系统 基线核查系统	（1）设备对各登录模式均启用身份鉴别； （2）设备对登录管理的用户进行身份鉴别； （3）设备名及登录用户设置的身份标识具有唯一性；

日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。
b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备启用合规登录失败处理策略； （2）设备配置合规的操作超时退出措施。
c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备配置合规的远程管理模式； （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。
访问控制	
a）应对登录的用户分配账户和权限；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。
b）应重命名或删除默认账户，修改默认账户的默认口令；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备不存在默认账户名； （2）设备账户口令设置合规。
c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。

防火墙-1 防火墙-2	
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备根据安全策略要求对特权用户进行分离； (2) 设备不存在多个管理级别高的特权用户； (3) 设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备开启审计功能，审计进程正常； (2)设备的日志审计级别满足要求,审计覆盖所有用户操作审计和记录。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备日期、时间正常； (2) 设备审计记录内容基本完整。
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
WEB应用防火墙 上网行为管理系统 基线核查系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备限制审计文件的访问控制权限，普通用户不可删除及修改； (2) 设备针对日志、审计记录具备充足的存储容量； (3) 对审计记录进行定期存档备份，其备份策略有效； (4) 部署日志审计系统实时对日志进行统一收集存储； (5) 日志及审计记录保存大于6个月。
日志审计系统	(1) 设备限制审计文件的访问控制权限，普通用户不可删除及修改； (2) 设备针对日志、审计记录具备充足的存储容量； (3) 对审计记录进行定期存档备份，其备份策略有效； (4) 日志及审计记录保存大于6个月。
入侵防范	
a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统	(1) 设备在全局模式下禁用部分不必要的服务； (2) 设备在部分接口模式下禁用部分不必要的服务； (3) 漏洞扫描未发现高风险设备固件漏洞。

运维安全管理系统 防火墙-1 防火墙-2	
b) 应关闭不需要的系统服务、默认共享和高危端口；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。
c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 防火墙-1 防火墙-2	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
运维安全管理系统	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制。
d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备管理具备数据有效性检验功能； （2）设备管理的校验接口范围较全面。
e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。
恶意代码防范	
应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	
WEB应用防火墙 防火墙-1 防火墙-2	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。
数据完整性	

应采用校验技术保证重要数据在传输过程中的完整性。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	鉴别数据、重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； （2）设备对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。

3.4.2.2 主要安全问题汇总分析

安全通用要求

（1）设备不具备相关可信验证的技术措施（如：WEB应用防火墙）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.3 服务器和终端

3.4.3.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统对登录系统的用户进行身份鉴别； （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施；

	（5）用户属性策略未勾选“密码永不过期”。
应用/数据库服务器	（1）操作系统对登录系统的用户进行身份鉴别； （2）操作系统不存在空口令用户； （3）操作系统不存在默认信任的登录模式； （4）操作系统为登录用户设置的身份标识具有唯一性； （5）操作系统配置的一定的密码长度且定期更换； （6）操作系统配置一定的密码复杂度策略。
b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统启用登录失败处理策略。 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略。
应用/数据库服务器	（1）操作系统启用pam_tally2模块的合规登录失败处理策略； （2）操作系统配置合规的操作超时锁定； （3）操作系统启用SSH的合规登录超时策略。
c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS的管理。
应用/数据库服务器	（1）操作系统配置合规的远程管理模式； （2）操作系统远程端口使用情况合规； （3）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
访问控制	
a）应对登录的用户分配账户和权限；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。
应用/数据库服务器	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在所有用户均属于root组的情况。
b）应重命名或删除默认账户，修改默认账户的默认口令；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统针对默认账户采用相应的安全策略配置； （2）操作系统账户不存在弱口令或空口令。
应用/数据库服务器	（1）操作系统对多余帐户进行删除、锁定或禁止其登录； （2）操作系统账户口令设置合规。

c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	(1) 操作系统不存在多余或过期账户； (2) 操作系统管理员用户与账户之间一一对应。
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	(1) 操作系统根据安全策略要求对特权用户进行分离； (2) 操作系统不存在特权用户； (3) 操作系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
应用/数据库服务器	(1) 操作系统根据安全策略要求对特权用户进行分离； (2) 操作系统不存在除root外的特权用户； (3) 操作系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	(1) 操作系统开启审计策略，操作系统审计策略基本完整； (2) 审计覆盖所有用户操作审计和记录。
应用/数据库服务器	(1) 操作系统开启审计功能，审计进程正常； (2) 操作系统开启审计范围及策略满足要求，审计覆盖所有用户操作审计和记录。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	(1) 操作系统日期、时间正常； (2) 操作系统审计记录内容基本完整。
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	(1) 操作系统采取对审计记录存储容量如下： 运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； (2) 限制审计文件的访问控制权限，用户不可删除及修改； (3) “管理审核和安全日志”，除审计员、administrators外其他用户无权限； (4) 对审计记录进行定期存档备份，其备份策略有效； (5) 部署日志审计系统实时对日志进行统一收集存储； (6) 日志及审计记录保存6个月。
应用/数据库服务器	(1)操作系统限制审计文件的访问控制权限,普通用户不可删除及修改； (2) 操作系统针对日志、审计记录具备充足的存储容量； (3) 操作系统采取合规的日志文件权限策略； (4) 部署日志审计系统实时对日志进行统一收集存储； (5) 日志及审计记录保存大于6个月。

入侵防范	
a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	
应用/数据库服务器 业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。
b) 应关闭不需要的系统服务、默认共享和高危端口；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统不存在多余的默认共享及其它文件共享； （2）操作系统关闭不必要端口； （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。
应用/数据库服务器	（1）操作系统关闭不必要端口； （2）操作系统禁用不必要服务； （3）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口； （4）漏洞扫描未发现高风险主机端口。
c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
应用/数据库服务器	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。
应用/数据库服务器	（1）操作系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。
恶意代码防范	
应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。
应用/数据库服务器	（1）操作系统安装深信服edr防恶意代码软件；

	（2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	鉴别数据、重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。
应用/数据库服务器	鉴别数据: （1）系统在通信传输过程中对鉴别数据采取完整性保护措施。 重要配置数据: （1）系统在通信传输过程中对重要配置数据采取完整性保护措施。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施: 安全选项“不显示上次的用户名”->启用
应用/数据库服务器	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统不保存过多终端历史记录。

3.4.3.2 主要安全问题汇总分析

安全通用要求

（1）缺乏对计算设备可信验证方面的安全设计要求。现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。现有的计算设备存在对系统运行过程中的可信检验不全面的情况。现有的可信验证存在部分告警、审计及联动措施不全面的情况(如：应用/数据库服务器）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终

运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.4 系统管理软件/平台

3.4.4.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
应用/数据库服务器-Oracle	（1）数据库系统对登录系统的用户进行身份鉴别； （2）数据库系统不存在弱口令用户； （3）数据库系统为登录用户设置的身份标识具有唯一性； （4）数据库系统配置合规的密码长度及复杂度策略； （5）数据库系统配置合规的密码有效周期策略。
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
应用/数据库服务器-Oracle	（1）数据库系统启用合规登录失败处理策略； （2）数据库系统执行合规的锁定策略。
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
应用/数据库服务器-Oracle	（1）数据库系统配置合规的远程管理模式。
访问控制	
a) 应对登录的用户分配账户和权限；	
应用/数据库服务器-Oracle	（1）登录数据库系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （2）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在多用户均与sys、DBA用户权限一致的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。
应用/数据库服务器-Tomcat	（1）对应不同的账户均按需分配不同的用户权限，不存在中间件用户均属于管理级别、高权限的情况； （2）中间件配置可降权启动Tomcat的用户； （3）宿主系统针对中间件用户分别赋予相应的管理操作权限。
b) 应重命名或删除默认账户，修改默认账户的默认口令；	
应用/数据库服务器-Oracle	（1）数据库系统对多余帐户进行删除、锁定或禁止其登录； （2）数据库系统账户口令设置合规。
应用/数据库服务器-Tomcat	（1）中间件不存在除如:Tomcat、admin、manager、role1等默认账户名； （2）中间件账户口令设置合规。
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
应用/数据库服务器-Oracle	（1）数据库系统不存在多余或过期账户；

	（2）数据库系统管理员用户与账户之间一一对应。
应用/数据库服务器-Tomcat	（1）中间件不存在多余或过期账户； （2）中间件管理员用户与账户之间一一对应； （3）中间件启用合规的管理用户名配置。
d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	
应用/数据库服务器-Oracle	（1）数据库系统根据安全策略要求对特权用户进行分离； （2）数据库系统用户权限合理，非管理员未设置过大权限； （3）数据库系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
应用/数据库服务器-Tomcat	（1）中间件根据安全策略要求对特权用户及宿主管理用户进行分离； （2）中间件管理不存在多个管理级别高的特权用户； （3）中间件管理按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
应用/数据库服务器-Oracle	（1）数据库系统开启审计功能，审计进程正常； （2）ORACLE数据库系统启动数据库日志模式和自动归档； （3）审计覆盖所有用户操作审计和记录。
应用/数据库服务器-Tomcat	（1）中间件开启审计功能，审计进程正常； （2）系统的日志审计级别满足要求。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
应用/数据库服务器-Oracle	（1）数据库宿主系统日期、时间正常； （2）数据库系统审计记录内容基本完整。
应用/数据库服务器-Tomcat	（1）中间件日期、时间正常； （2）中间件审计记录开启审核策略且日志级别正常。
c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
应用/数据库服务器-Oracle	（1）数据库系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）数据库系统针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）日志及审计记录保存大于6个月。
应用/数据库服务器-Tomcat	（1）中间件限制审计文件的访问控制权限，普通用户不可删除及修改； （2）宿主系统针对中间件日志、审计记录具备充足的存储容量； （3）对中间件审计记录进行定期存档备份，其备份策略有效； （4）审计记录及日志保存大于6个月。
入侵防范	
c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
应用/数据库服务器-Oracle	（1）网络设备ACL策略有效限制访问本机的IP地址及管理模式。
d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	
应用/数据库服务器-Tomcat	（1）中间件管理具备数据有效性检验功能； （2）中间件管理的校验接口范围较全面。
e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
应用/数据库服务器-Oracle	（1）数据库系统已根据需要不定期地对已发布的安全性补丁进行更新；

	（2）数据库宿主系统不存在启用未加控制的高危端口； （3）MY_SQL分离默认安装的示例数据库； （4）数据库系统进行渗透及扫描未发现存在可造成高风险的漏洞。
应用/数据库服务器-Tomcat	（1）中间件已根据需要不定期地对已发布的版本进行更新； （2）中间件更新安装前进行安全性和兼容性测试； （3）在系统上线或发生重大变更时测试并安装最新的中间件版本或更新补丁； （4）在不影响业务系统正常运行情况下，对发现的中间件漏洞在确保安全的情况下进行修补； （5）中间件进行扫描未发现存在可造成高风险的漏洞。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
应用/数据库服务器-Oracle	鉴别数据、重要配置数据: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。
应用/数据库服务器-Tomcat	鉴别数据、重要配置数据: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a）应提供重要数据的本地数据备份与恢复功能；	
应用/数据库服务器-Oracle	（1）数据库系统定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）数据库系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
应用/数据库服务器-Tomcat	（1）系统定义了相关需要备份的中间件重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）宿主系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）中间件相关数据的备份周期合理：每天增量一次、每月全备一次； （5）中间件开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	
应用/数据库服务器-Oracle	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）数据库系统不保存终端历史记录。
应用/数据库服务器-Tomcat	（1）宿主系统具有清除用户鉴别信息的功能； （2）经测试，宿主系统退出后无法访问先前中间件登录过的页面； （3）经测试，宿主系统关闭后无残留的中间件用户鉴别信息。
个人信息保护	
a）应仅采集和保存业务必需的用户个人信息；	
应用/数据库服务器-Oracle	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）数据库存储的用户个人信息均为业务应用必需的环节。

b) 应禁止未授权访问和非法使用用户个人信息。	
应用/数据库服务器-Oracle	(1) 系统对所有涉及个人信息的环节均有明确的授权同意过程； (2) 数据库具备控制措施禁止未授权访问用户个人信息表单； (3) 数据库具备控制措施禁止非法使用用户个人信息表单。

3.4.4.2 主要安全问题汇总分析

安全通用要求

(1) 未能提供数据库系统重要数据的异地定时数据备份功能（如：应用/数据库服务器-Oracle）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供，使企业的经济利益或声誉受到损害。 中风险。

3.4.5 业务应用系统/平台

3.4.5.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
OA系统	(1) 系统对各登录模式均启用身份鉴别； (2) 系统对登录管理的用户进行身份鉴别； (3) 系统登录用户设置的身份标识具有唯一性； (4) 系统不存在空口令用户； (5) 设备配置合规的密码策略。
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
OA系统	(1) 系统启用合规登录失败处理策略； (2) 系统配置合规的操作超时退出措施。
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
OA系统	(1)应用系统的用户鉴别数据采用SHA-512算法在可控网络环境中传输； (2) 系统配置合规的远程管理模式。
访问控制	
a) 应对登录的用户分配账户和权限；	
OA系统	(1) 可提供系统权限分配表； (2) 登录系统的用户均相应分配不同的账户，不存在使用共用账户的情况； (3) 对应不同的账户均按需分配不同的用户权限，不存在所有用户均属

	于管理级别、高权限的情况。
b) 应重命名或删除默认账户，修改默认账户的默认口令；	
OA系统	（1）系统禁用默认账户名； （2）系统账户口令设置合规。
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
OA系统	（1）系统不存在多余或过期账户； （2）系统管理员用户与账户之间一一对应。
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	
OA系统	（1）系统不存在多个管理级别高的特权用户； （2）系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
OA系统	（1）系统开启审计功能，审计进程正常； (2)系统的日志审计级别满足要求,审计覆盖所有用户操作审计和记录。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
OA系统	（1）系统日期、时间正常； （2）系统审计记录内容基本完整。
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
OA系统	（1）系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）系统针对日志、审计记录具备充足的存储容量； （3）审计记录及日志保存大于6个月。
入侵防范	
c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
OA系统	（1）系统自身设定有效的终端访问策略，通过访问措施进行管理地址的限制。
d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	
OA系统	（1）系统具备数据有效性检验功能； （2）系统的校验接口范围较全面。
e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
OA系统	（1）系统已根据需要不定期地对已发布的版本进行更新； （2）在系统上线或发生重大变更时测试并安装最新的版本或更新补丁； （3）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
OA系统	鉴别数据、重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； （2）系统对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
OA系统	（1）系统定义了相关需要备份重要数据；

	（2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	
OA系统	（1）系统具有清除用户鉴别信息的功能； （2）经测试，系统退出后无法访问先前登录过的页面； （3）经测试，系统关闭后无残留的用户鉴别信息。
个人信息保护	
a) 应仅采集和保存业务必需的用户个人信息；	
OA系统	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息； （3）系统采集的用户个人信息均为业务应用必需的环节。
b) 应禁止未授权访问和非法使用用户个人信息。	
OA系统	（1）系统不采集和保存任何形式的用户个人信息； （2）系统对所有涉及个人信息的环节均有明确的授权同意过程； （3）系统具备控制措施禁止未授权访问用户个人信息； （4）系统具备控制措施禁止非法使用用户个人信息。

3.4.5.2 主要安全问题汇总分析

安全通用要求

（1）未能提供应用软件系统重要数据的异地定时数据备份功能（如：OA系统）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

3.4.6 数据资源

3.4.6.1 已有安全控制措施汇总分析

安全通用要求

数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
重要业务数据 重要个人信息	（1）系统在通信传输过程中对相关数据采取完整性保护措施； （2）系统对重要数据在传输过程中采取必要的完整性保护措施。

数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
重要业务数据 重要个人信息	（1）系统定义了相关需要备份重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
个人信息保护	
a) 应仅采集和保存业务必需的用户个人信息；	
重要个人信息	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息； （3）系统采集的用户个人信息均为业务应用必需的环节。
b) 应禁止未授权访问和非法使用用户个人信息。	
重要个人信息	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； （2）系统具备控制措施禁止未授权访问用户个人信息； （3）系统具备控制措施禁止非法使用用户个人信息。

3.4.6.2 主要安全问题汇总分析

安全通用要求

重要业务数据

（1）未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要业务数据）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

重要个人信息

（1）未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要个人信息）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

3.4.7 其他系统或设备

3.4.7.1 已有安全控制措施汇总分析

安全通用要求

无其他系统或设备，不涉及相关测评

3.4.7.2 主要安全问题汇总分析

安全通用要求

无其他系统或设备，不涉及相关测评

3.5 安全管理中心

3.5.1 已有安全控制措施汇总分析

安全通用要求

系统管理	
a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；	
管理中心	（1）网络中部署运维安全管理系统实现集中的系统管理； （2）系统对登录用户进行身份鉴别； （3）系统用户标识具有唯一性； （4）系统可实现对账户的身份鉴别数据进行保密性和完整性保护； （5）系统管理操作模式具备控制措施； （6）系统具备相应的管理操作审计措施。
审计管理	
a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；	
管理中心	（1）网络中部署运维安全管理系统实现集中安全审计功能； （2）审计系统对审计管理员进行身份鉴别； （3）审计系统用户标识具有唯一性； （4）审计系统管理操作模式具备控制措施； （5）审计系统具备相应的管理操作审计措施。
b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	
管理中心	OA系统: （1）审计管理员定期对审计记录进行分析，对发现的安全可疑事件及时处理； （2）单位具有安全审计策略文件，规范审计记录的存储、管理和查询要求； （3）审计管理员按规范要求对审计记录进行管理。

	重要审计数据: 日志审计系统、运维安全管理系统: （1）设备在通信传输过程中对相关数据采取完整性保护措施; （2）设备对重要数据在传输过程中采取必要的完整性保护措施。

3.5.2 主要安全问题汇总分析

安全通用要求

（1）系统管理的资源、运行及配置管理不够全面（如：管理中心）。系统的资源和运行缺少统一的管理，将导致系统可能无法按规划实现基于资源配置、 系统加载、异常处理、及备份/恢复等的安全控制措施。 低风险。

3.6 安全管理制度

3.6.1 已有安全控制措施汇总分析

安全通用要求

安全策略	
应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。	
制度文件、执行/记录文件	（1）单位具有网络安全工作的总体方针和安全策略文件; （2）制度内容包括明确的单位安全工作要求; （3）管理文件详见《信息安全总体策略》。
管理制度	
a) 应对安全管理活动中的主要管理内容建立安全管理制度;	
制度文件、执行/记录文件	（1）单位有针对安全管理活动中的各类管理内容建立安全管理制度; （2）现有制度已覆盖管理活动的主要的方面; （3）制度详见：《信息安全总体策略》、《网络安全管理规范》、《组织安全结构和人员职责制度》、《人员管理制度》、《员工考核管理制度》。
b) 应对管理人员或操作人员执行的日常管理操作建立操作规程。	
制度文件、执行/记录文件	（1）单位针对相关业务日常管理的操作建立规程类管理制度; （2）现有制度已覆盖重要管理方面的系统维护手册和用户操作规程等; （3）管理文件详见《设备及系统软件配置和操作手册》。
制定和发布	
a) 应指定或授权专门的部门或人员负责安全管理制度的制定;	
制度文件、执行/记录文件	（1）单位针对安全管理制度的制定，指定教育信息与网络中心部主要负责;

	（2）在已制定的相关制度中可查阅到被授权制定管理制度的部门/人员信息； （3）管理文件详见《安全管理组织规范》。
b）安全管理制度应通过正式、有效的方式发布，并进行版本控制。	
制度文件、执行/记录文件	（1）单位针对制度的制定和发布要求，制定管理规范文件； （2）管理规范文件对文件制定及发布定义了规范要求； （3）安全管理制度的收发登记记录有效； （4）管理文件详见《制度制定、发布、评审和修订管理制度》、《收发文登记记录》。
评审和修订	
应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	
制度文件、执行/记录文件	（1）单位针对制度的合理性和适用性需进行论证和审定及修订的要求，制定管理规范文件； （2）管理规范文件对制度的评审及修订定义了规范要求； （3）单位具有安全管理制度的审定或论证的过程记录； （4）单位对做过修订的制度，具备有修订版本的安全管理过程记录； （5）管理文件详见《制度制定、发布、评审和修订管理制度》及 《安全管理制度评审记录》。

3.6.2 主要安全问题汇总分析

安全通用要求

OA系统针对安全管理制度层面的安全通用要求采取的安全措施比较完善，未发现不符合项。

3.7 安全管理机构

3.7.1 已有安全控制措施汇总分析

安全通用要求

岗位设置	
a）应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；	
制度文件、执行/记录文件	（1）单位已明确网络安全管理工作的职能部门，并明确了各岗位职责； （2）单位各部门职责文档已明确网络安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备网络安全岗位划分情况和岗位职责的详细说明；

	（4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。
b）应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。	
制度文件、执行/记录文件	（1）单位已明确系统安全管理工作的职能部门，并明确了各岗位职责； （2）单位各部门职责文档已明确系统安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备系统安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。
人员配备	
应配备一定数量的系统管理员、审计管理员和安全管理员等。	
制度文件、执行/记录文件	（1）单位针对人员配备要求，制定了管理制度； （2）单位按要求配备一定数量的重要岗位管理人员； （3）单位针对各岗位人员，制定并维护人员档案； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。
授权和审批	
a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；	
制度文件、执行/记录文件	（1）单位在制度中用文字描述或在流程图中明确，对关键活动进行审批； （2）单位对审批过程明确审批权限，对各项信息系统的重要操作与变更明确审批部门和批准人； （3）管理文件详见《授权和审批管理规定》。
b）应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。	
制度文件、执行/记录文件	（1）单位针对各项业务操作及变更等建立了审批程序规定； （2）单位针对系统变更、系统接入、物理范围等事项已明确按审批程序执行，记录有批准人签字； （3）管理文件详见《授权和审批管理规定》。
沟通和合作	
a）应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；	
制度文件、执行/记录文件	（1）单位针对机构内部管理人员之间、部门之间的沟通与合作，制定了管理制度； （2）单位的管理制度规范了合作和沟通的方式和周期； （3）单位有组织机构内部人员联系表； （4）单位有定期召开信息安全会议，保存有会议纪要； （5）管理文件详见《安全教育和培训制度》、《技能培训记录》《外部联系表》。
b）应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；	
制度文件、执行/记录文件	（1）单位针对加强与外部单位的合作与沟通，制定了管理制度规定； （2）单位能按要求与相关单位保持沟通合作，并提供相关单位联系方式和交流会议纪要； （3）管理文件详见《安全教育和培训制度》、《技能培训记录》、《外部联系表》。

c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	
制度文件、执行/记录文件	(1) 单位建立了完善的对外联单位的联系列表; (2) 管理文件详见《外部联系表》。

3.7.2 主要安全问题汇总分析

安全通用要求

(1) 单位开展的检查工作不够完善（如：制度文件、执行/记录文件）。检查工作开展不仔细，可能对存在或潜在的安全风险不能被及时发现并进行处理。 低风险。

3.8 安全管理人员

3.8.1 已有安全控制措施汇总分析

安全通用要求

人员录用	
a) 应指定或授权专门的部门或人员负责人员录用;	
制度文件、执行/记录文件	(1) 单位授权专门的部门负责人员录用工作，制定了管理制度规范; (2) 由人力资源保障科负责人员录用工作; (3) 管理文件详见《人员管理制度》。
b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查。	
制度文件、执行/记录文件	(1) 单位针对人员录用过程，制定了明确要求，并形成人员安全管理制度; (2) 单位现有管理制度明确说明录用人员应具备的条件; (3) 单位按规定执行人员录用的相关审查过程; (4) 管理文件详见《人员管理制度》、《人员入职考核记录》。
人员离岗	
应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。	
制度文件、执行/记录文件	(1) 单位针对离岗人员权限终止及取回机构提供的各种设施的要求，制定了管理制度; (2) 单位按规范开展对离岗人员的相关管理工作; (3) 管理文件详见《人员管理度》、《人员离岗申请表》、《离场信息资料交接表》。
安全意识教育和培训	
应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。	
制度文件、执行/记录文件	(1) 单位针对人员安全培训及责任和惩戒措施，制定了管理制度; (2) 单位已开展安全意识教育及岗位技能培训。 (3) 管理文件详见《安全教育和培训制度》。

外部人员访问管理	
a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；	
制度文件、执行/记录文件	（1）单位针对外部人员物理访问，制定了外部人员访问管理文档； （2）单位具备有效的外部人员访问重要区域的书面申请文档； （3）单位具备外部人员访问重要区域的登记记录； （4）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。
b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；	
制度文件、执行/记录文件	（1）单位针对外部接入受控网络访问系统，制定了管理制度； （2）单位具备外部人员接入受控网络前的申请审批流程； （3）单位具备外部人员接入及访问系统的书面申请文档； （4）单位具备外部人员接入及访问系统的登记记录； （5）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。

3.8.2 主要安全问题汇总分析

安全通用要求

（1）单位未完全按管理规范开展人员离场后的清理工作（如：制度文件、执行/记录文件）。人员离场后的清理工作开展不规范，可能导致遗留外部人员访问受控区域的记录，存在被二次非法利用，造成泄密。 低风险。

3.9 安全建设管理

3.9.1 已有安全控制措施汇总分析

安全通用要求

定级和备案	
a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；	
制度文件、执行/记录文件	（1）单位的被测系统于2022年4月已完成备案； （2）系统备案相关文档（定级报告）中明确等级划分方法和理由，SAG三个方面的级别描述清晰； （3）管理文件详见《定级备案》。
b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；	
制度文件、执行/记录文件	(1)单位针对系统定级结果的审批及评审工作等要求,制定了管理制度;

	（2）现有系统的定级已具备合理性和正确性审定； （3）管理文件详见《定级备案》。
c）应保证定级结果经过相关部门的批准；	
制度文件、执行/记录文件	（1）单位针对系统定级结果的上级批准要求，制定了管理制度； （2）现有系统的定级获得了相关部门的批准； （3）管理文件详见《定级备案》。
d）应将备案材料报主管部门和相应公安机关备案。	
制度文件、执行/记录文件	（1）单位对被测系统的等级备案表、定级报告等备案材料已经报相应公安机关备案； （2）单位具备公安机关出具的备案号； （3）管理文件详见《定级备案》。
产品采购和使用	
a）应确保网络安全产品采购和使用符合国家的有关规定；	
制度文件、执行/记录文件	（1）单位已建立安全产品管理的相关管理规定； （2）单位具备安全产品采购流程及相关实施文档； （3）被测系统使用的安全产品具备销售许可资质； （4）安全产品具均为国内产品； （5）管理文件详见《设备安全管理制度》。
b）应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。	
制度文件、执行/记录文件	（1）单位已建立密码产品与服务管理的相关管理制度； （2）系统未使用密码产品； （3）管理文件详见《设备安全管理制度》。
外包软件开发	
b）应保证开发单位提供软件设计文档和使用指南。	
制度文件、执行/记录文件	（1）单位制定软件开发项目验收要求，明确开发单位的提交材料； （2）开发单位提供软件日常维护和使用所需的文档； （3）管理文件详见《外包开发软件管理规定》、《设备及系统软件配置和操作手册》。
工程实施	
a）应指定或授权专门的部门或人员负责工程实施过程的管理；	
制度文件、执行/记录文件	（1）单位针对专门的部门负责工程实施过程的管理要求，制定管理度； （2）单位由专岗负责系统建设的工程实施，且按照实施方案的要求对进度和质量进行控制； （3）管理文件详见《工程实施管理制度》。
b）应制定安全工程实施方案控制工程实施过程。	
制度文件、执行/记录文件	（1）单位制定了详细的工程实施方案； （2）工程实施单位严格按照方案执行，并有过程记录； （3）管理文件详见《测试及验收方案》、《工程项目实施方案》。
系统交付	
a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；	
制度文件、执行/记录文件	（1）单位具备系统交付清单； （2）系统交付清单内容较详细； （3）单位的清点工作较合规； （4）管理文件详见《系统交付管理》、《资产清单》。

b) 应对负责运行维护的技术人员进行相应的技能培训；	
制度文件、执行/记录文件	(1) 单位已对负责系统运行维护的技术人员进行了技能培训； (2) 具备运维人员的培训记录； (3) 管理文件详见《系统交付管理》、《资产清单》、《系统交付清单》、《技能培训记录》。
c) 应提供建设过程文档和运行维护文档。	
制度文件、执行/记录文件	(1) 单位提供了系统建设过程中的文档； (2) 单位提供了指导用户进行系统运维的文档和系统培训手册； (3) 管理文件详见《系统交付管理》、《系统交付清单》、《设备及系统软件配置和操作手册》。
等级测评	
a) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；	
制度文件、执行/记录文件	(1) 单位针对系统等级测评要求，制定管理制度； (2) 系统按要求开展首次测评工作； (3) 管理文件详见《系统安全管理制度》。
b) 应在发生重大变更或级别发生变化时进行等级测评；	
制度文件、执行/记录文件	(1) 管理制度中已规定在系统发生变更时及时对系统进行等级测评； (2) 系统未发生过重大变更，系统等级未发生变化； (3) 管理文件详见《系统安全管理制度》。
c) 应确保测评机构的选择符合国家有关规定。	
制度文件、执行/记录文件	(1) 已选择在“全国等级保护测评机构推荐目录”中的测评单位进行等级测评； (2) 管理文件详见《系统安全管理制度》、《网络安全等级保护测评服务合同》。
服务供应商选择	
a) 应确保服务供应商的选择符合国家的有关规定；	
制度文件、执行/记录文件	(1) 单位在管理制度内明确提出安全服务供应商选择的要求； (2) 单位选择的安全服务商符合国家的有关规定，具备相应的安全服务资质； (3) 管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。
b) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。	
制度文件、执行/记录文件	(1) 单位的管理制度中已规定，需与安全服务商签订安全相关的协议并明确整个服务供应链各方需履行的网络安全相关义务； (2) 单位已按规定与选定的安全服务商签订合规的协议； (3) 管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。

3.9.2 主要安全问题汇总分析

安全通用要求

（1）单位未具备适用于被测系统的安全规划设计方案（如：制度文件、执行/记录文件）。规划设计需求不全面，可能导致安全方案设计不完善，信息系统存在安全缺陷。低风险。

（2）单位未具备完整的安全设计方案相关的文档。单位相关方案的设计的内容不够完善（如：制度文件、执行/记录文件）。相关合规的规划配套文件缺失，可能导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。 中风险。

（3）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定。单位未对相关论证过程及内容进行完整的记录（如：制度文件、执行/记录文件）。未开展规范的审批过程，可能存在安全整体规划缺乏合理性和可行性，导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。 低风险。

（4）单位未在软件开发过程中对所有软件安全性进行测试。单位未在软件安装之前按要求对所有软件开展恶意代码检测（如：制度文件、执行/记录文件）。软件交付前恶意代码检测不规范，可能在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。 低风险。

（5）单位未完全根据测试验收方案组织相关部门和人员开展验收工作（如：制度文件、执行/记录文件）。可能由于验收测试不严谨，造成测试过程缺乏计划性及操作性，无法保证经过测试验收的系统达到既定的安全性等目标。 低风险。

(6)针对系统上线前的安全性测试工作存在问题(如:制度文件、执行/记录文件)。未按规定开展上线前测试，安全隐患可能在系统上线运行前未被发现并作出相应处理。低风险。

3.10 安全运维管理

3.10.1 已有安全控制措施汇总分析

安全通用要求

环境管理	
a) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；	
制度文件、执行/记录文件	（1）单位建立机房安全方面的管理制度，对有关运维方面的管理作出规定； （2）单位具备完整的机房出入登记记录； （3）单位具备完整的机房基础设施的维护记录； （4）管理文件详见《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。
b) 应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；	
制度文件、执行/记录文件	（1）单位建立机房安全方面的管理制度； （2）单位现有机房管理记录与制度相符； （3）制度详见：《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。
c) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	
制度文件、执行/记录文件	（1）单位机房安全管理制度已明确来访人员的接待区域的要求； （2）单位按规范要求开展人员来访接待； （3）单位办公环境未发现有随意放置含有敏感信息介质的情况； （4）制度详见：《机房安全管理制度》、《物理安全管理规范》、《办公环境保密管理》。
资产管理	
应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。	
制度文件、执行/记录文件	（1）单位已建立有效的资产清单； （2）单位现有资产清单内容较全面； （3）制度详见：《设备安全管理制度》、《资产清单》。
介质管理	
a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；	
制度文件、执行/记录文件	（1）介质按管理要求放置于受控的环境中（如：机房）； （2）介质管理具备较全面的记录； （3）制度详见：《设备安全管理制度》、《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。
b) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。	
制度文件、执行/记录文件	（1）介质管理制度中对介质安全传输有明确规定； （2）存储重要信息的介质在物理传输过程，具备严格的环节控制，无重大环节疏漏； （3）对介质的归档和查询均具备记录；

	（4）制度详见：《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。
设备维护管理	
a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	
制度文件、执行/记录文件	（1）单位人员岗位职责相关文档已明确设备维护管理的责任部门； （2）单位对各类设施、设备进行定期维护； （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。
b）应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。	
制度文件、执行/记录文件	（1）单位建立了配套设施、软硬件维护管理方面的管理制度； （2）单位开展相关工作与制度相符，且保留记录； （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。
网络和系统安全管理	
a）应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；	
制度文件、执行/记录文件	（1）单位建立系统安全管理文档，对系统管理员的管理制定了要求； （2）单位对各类关键角色建立了相应的工作职责文档； （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。
b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	
制度文件、执行/记录文件	（1）单位制定管理制度，对系统账号进行管理； （2）单位按管理规范开展账号管理工作； （3）账户管理记录内容较完整； （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。
c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	
制度文件、执行/记录文件	（1）单位建立了网络和系统安全管理制度； （2）网络和系统安全管理制度内容较全面； （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。
d）应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；	
制度文件、执行/记录文件	（1）单位对重要设备、系统的配置和操作建立配置手册； （2）现有操作配置手册已明确操作步骤、参数配置； （3）制度详见：《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。
e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。	
制度文件、执行/记录文件	（1）单位制定日常运维管理的相关制度规范； （2）单位按制度规范开展日常运维管理工作； （3）单位具备合规的运维记录； （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》、《设备及系统软件配置和操作手册》、《软硬件日

	常维护管理规程》。
恶意代码防范管理	
a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	
制度文件、执行/记录文件	（1）单位制定恶意代码防范管理制度，明确对外来计算机或存储设备接入系统前进行恶意代码检查； （2）单位按外来计算机接入恶意代码检查规范开展工作； （3）单位制定培训管理制度，明确需通过培训提升员工的防恶意代码意识； （4）单位按培训管理要求开展工作； （5）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申请表》、《信息管理系统漏洞检查表》。
b) 应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；	
制度文件、执行/记录文件	（1）建立恶意代码防范管理文档； （2）管理制度中覆盖防恶意代码软件的授权使用、恶意代码库升级、定期查杀等内容； （3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》。
配置管理	
应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。	
制度文件、执行/记录文件	（1）单位制定了基本配置信息管理的制度要求； （2）管理文件详见：《主机安全管理规范》、《网络安全管理规范》、《应用安全管理规范》、《网络配置信息》。
变更管理	
应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。	
制度文件、执行/记录文件	（1）单位建立了关于系统变更管理的制度文件； （2）现有变更管理制度覆盖了变更管理的各方面要求； （3）制度详见：《变更控制管理制度》、《通用变更记录表》。
备份与恢复管理	
a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；	
制度文件、执行/记录文件	（1）单位根据业务重要程度，制定了需要定期备份的重要业务信息列表或清单。清单内需要定期备份的重要数据已经过用户方确认； （2）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。
b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等；	
制度文件、执行/记录文件	（1）单位建立了备份与恢复管理相关的安全管理制度； （2）备份与恢复管理的相关要求比较明确； （3）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。
c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	
制度文件、执行/记录文件	（1）单位现有管理制度，明确了数据备份策略和数据恢复策略，以及备份程序和恢复程序； （2）单位可按策略要求实现重要数据的定期备份与恢复性测试；

	(3)单位现有的备份的数据均经过恢复性测试,可确保备份的数据可用; (4) 制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。
安全事件处置	
a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件;	
制度文件、执行/记录文件	(1)单位已在安全培训及宣传过程中告知用户在发现安全弱点和可疑事件时及时向安全管理部门报告; (2)单位在系统运维过程中对发现的安全弱点和可疑事件均编制了对应的报告或相关文档; (3) 单位现有安全弱点和可疑事件报告文档内容较详实; (4) 制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。
b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等;	
制度文件、执行/记录文件	(1) 单位制定了安全事件报告和处置管理制度; (2) 现有安全事件管理制度内容较完整; (3) 制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。
c) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。	
制度文件、执行/记录文件	(1) 单位具备对安全事件的分析、处理、总结、防范等的报告／过程文档; (2) 单位提供的安全事件报告和响应处置记录内容较完整; (3) 制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。
应急预案管理	
a) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容;	
制度文件、执行/记录文件	(1) 单位制定重要事件的应急预案; (2) 单位现有应急预案涉及的类型范围较全面; (3) 单位现有应急预案的内容较完整; (4) 制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。
b) 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。	
制度文件、执行/记录文件	(1) 单位定期对相关人员进行应急预案培训; (2) 单位根据不同的应急预案，按要求进行应急演练; (3) 单位具备近期应急预案工作开展的相关记录; (4) 单位提供的应急预案培训记录比较完整; (5) 单位提供的应急预案演练记录比较完整; (6) 经检查单位目前一旦出现应急事件，可参照预案合理有序的进行应急事件处置过程; (7) 制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。

3.10.2 主要安全问题汇总分析

安全通用要求

（1）单位未严格按规范开展漏洞及安全隐患检测工作（如：制度文件、执行/记录文件）。漏洞检测、修补工作不到位，可能存在未授权人员利用漏洞攻击信息系统的风险。 低风险。

（2）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作（如：制度文件、执行/记录文件）。可能导致系统恶意代码检测管理不到位，存在信息系统感染恶意代码，从而导致严重的信息安全风险。 低风险。

（3）单位不了解现有密码相关的国家标准和行业标准。单位缺乏密码管理要求的制度文档（如：制度文件、执行/记录文件）。密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不到位，存在违反国家政策的风险。 中风险。

3.11 其他安全要求指标

3.11.1 已有安全控制措施汇总分析

本次测评未涉及其他安全要求指标。

3.11.2 主要安全问题汇总分析

本次测评未涉及其他安全要求指标。

3.12 验证测试

验证测试包括漏洞扫描，渗透测试等，验证测试发现的安全问题对应到相应的测评项的结果记录中。详细验证测试报告见报告附录。

3.12.1 漏洞扫描

3.12.1.1 漏洞扫描结果统计

本次测评主要使用了[绿盟远程安全评估系统]对系统的设备进行了安全扫描，其所涉及的系统版本为：[V6.0R04F01SP06]，规则库版本为：[V6.0R02F01.2900]。扫描结果如下：

经分析统计，共发现各接入点存在5类漏洞，其中0类危险程度为高的漏洞，1类危害程度为中的漏洞，4类危害程度为低的漏洞。

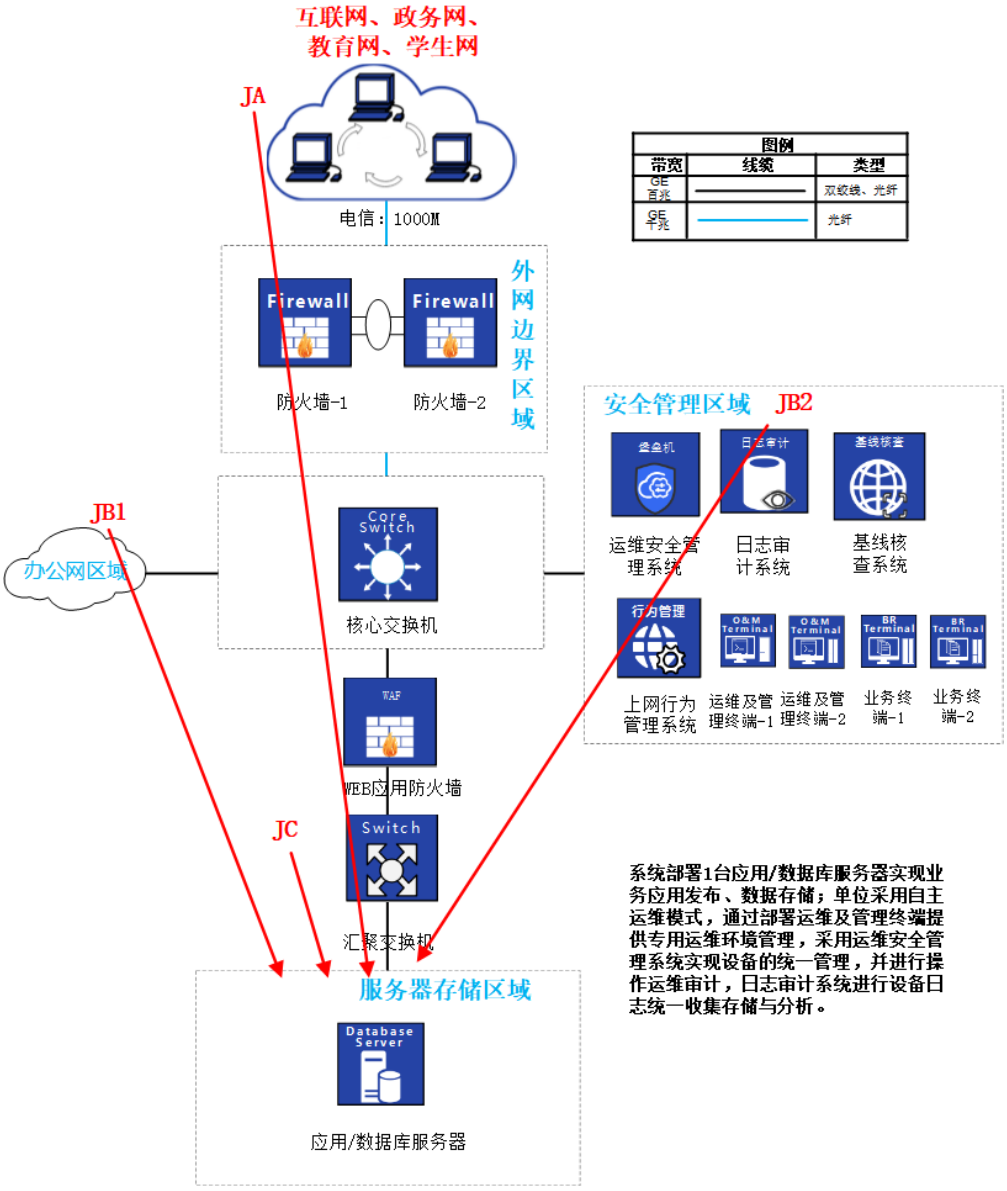


图 3-1 漏洞扫描工具接入测试示意图

接入点JA：在防火墙外侧接入，开展扫描/渗透主要目的是，探测对外服务功能区上各服务器、应用系统对外部网络边界暴露的安全漏洞情况，并根据漏洞扫描的结果接入渗透测试工具集，试图利用服务器、应用的安全漏洞入侵网络的行为。

接入点JB：在办公网区域VLAN段、安全管理区域VLAN段接入，开展扫描/渗透主要目的是，模拟外联单位/内部恶意用户发现操作系统、数据库、Web应用、第三方产

品等安全漏洞的过程，并尝试利用以上漏洞实施诸如获取系统控制权（GetShell）、获得大量敏感信息（DragLibrary）等模拟攻击行为。

接入点JC：在系统所在VLAN的交换机接入，开展扫描/渗透主要目的是，直接测试对服务功能区上各服务器在最小化防御的基础上，对网络暴露的安全漏洞情况。

（1）接入点A漏洞扫描结果统计

根据在接入点A对14台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-1 接入点 A 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.3.10/应用/数据库服务器	(服务器存储设备)CentOS 6.8	0	0	0	0
2	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	0	0	0	0
3	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	0	0	0	0
4	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	0	0	0	0
5	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	0	0	0	0
6	172.16.1.14/上网行为管理系统	(安全设备)深信服 AC12.0.26	0	0	0	0
7	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	0	0	0	0
8	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	0	0	0	0
9	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	0	0	0	0
10	192.168.33.11/业务终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
11	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
12	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
13	192.168.33.10/业务终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
14	https://oa.mmpt.edu.cn/OA系统	(业务应用软件平台) V6.0	0	0	0	0

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
安全漏洞数量小计			0	0	0	0

（2）接入点B漏洞扫描结果统计

根据在接入点B对14台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-2 接入点 B 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.3.10/应用/数据库服务器	(服务器存储设备)CentOS 6.8	3	1	0	4
2	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	1	0	0	1
3	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	1	0	0	1
4	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	1	0	0	1
5	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	2	0	0	2
6	172.16.1.14/上网行为管理系统	(安全设备)深信服AC12.0.26	1	0	0	1
7	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	1	0	0	1
8	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	1	0	0	1
9	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	1	0	0	1
10	192.168.33.11/业务终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
11	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
12	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
13	192.168.33.10/业务终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
14	https://oa.mmpt.edu.cn/OA系统	(业务应用软件平台) V6.0	0	0	0	0
安全漏洞数量小计			12	1	0	13

（3）接入点C漏洞扫描结果统计

根据在接入点C对14台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-3 接入点 C 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.3.10/应用/数据库服务器	(服务器存储设备)CentOS 6.8	3	1	0	4
2	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	1	0	0	1
3	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	1	0	0	1
4	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	1	0	0	1
5	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	2	0	0	2
6	172.16.1.14/上网行为管理系统	(安全设备)深信服 AC12.0.26	1	0	0	1
7	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	1	0	0	1
8	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	1	0	0	1
9	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	1	0	0	1
10	192.168.33.11/业务终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
11	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
12	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
13	192.168.33.10/业务终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
14	https://oa.mmpt.edu.cn/OA系统	(业务应用软件平台) V6.0	0	0	0	0
安全漏洞数量小计			12	1	0	13

3.12.1.2 漏洞扫描问题描述

通过对漏洞扫描结果进行分析，OA系统存在的主要安全漏洞汇总如下表所示

表 3-4 主要安全漏洞汇总表

序号	安全漏洞名称	关联资产/域名	严重程度
1	SSH 服务支持弱加密算法【原理扫描】 此类漏洞涉及服务器存储设备。	10.2.3.10/应用/数据库服务器	中
2	允许Traceroute探测 此类漏洞涉及安全设备、网络设备。	10.2.1.4/运维安全管理系统 10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/上网行为管理系统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/汇聚交换机 172.16.1.2/核心交换机	低
3	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161) 此类漏洞涉及服务器存储设备、网络设备。	10.2.3.10/应用/数据库服务器 172.16.1.2/核心交换机	低
4	OpenSSH 信息泄露漏洞(CVE-2011-4327) 此类漏洞涉及服务器存储设备。	10.2.3.10/应用/数据库服务器	低
5	OpenSSH 本地信息泄露漏洞(CVE-2016-10011) 此类漏洞涉及服务器存储设备。	10.2.3.10/应用/数据库服务器	低

3.12.2 渗透测试

经分析统计，共发现各接入点存在1类漏洞，其中0类危险程度为高的漏洞，0类危害程度为中的漏洞，1类危害程度为低的漏洞。

3.12.2.1 渗透测试过程说明

方案制定：

在得到委托单位的书面授权许可后，才进行渗透测试的实施。并且将实施范围、方法、时间、人员等具体的方案委托单位进行交流，并得到委托单位的认同。在测试实施

之前，会做到让委托单位对渗透测试过程和风险的知晓，使随后的正式测试流程都在委托单位的管控下。

信息收集：

此阶段中，渗透测试人员对目标信息系统进行必要的信息收集，如操作系统类型、开放的端口和服务、中间件信息、后台数据库类型、web开发语言等，即收集有利于漏洞挖掘的相关信息，为渗透测试做准备。

漏洞挖掘方法：

此阶段中，渗透测试人员对目标信息系统开始进行渗透测试，利用已知信息和现有条件及技术进行漏洞挖掘，尽可能发现目标信息系统中存在的所有安全风险，并进行记录。

漏洞利用：

此阶段中，渗透测试人员对目标信息系统对上一阶段漏洞挖掘中发现的漏洞进行必要的利用以证明其危害性，再对渗透测试过程所产生的测试数据进行清除。

输出报告：

此阶段中，渗透测试人员把渗透测试记录、截图等相关信息进行整理，然后撰写渗透测试报告，最终提交给委托单位。

漏洞修复：

此阶段中，委托单位依据收到的渗透测试报告对其中所提出的漏洞进行整改，可参考报告中所提出的修复建议，整改完成后联系本单位相关人员准备回归测试。

回归测试：

此阶段中，渗透测试人员对整改后的目标信息系统进行复测，以确定报告中提出的漏洞是否已被修复，若已被修复，则进入下一阶段；否则，返回上一阶段。

测试工具：

序号	工具	工具用途
1	Burpsuite Pro	用于攻击Web应用程序的集成软件
2	Sqlmap	开源的自动化SQL注入工具
3	Nmap	开源的网络发现和安全审计工具
4	OWASP ZAP	自动化Web应用漏洞扫描工具
5	其他测试工具	根据信息系统的类别选择不同的工具（如自写脚本、目录扫描器、木马扫描器、其它开源工具等）

3.12.2.2 渗透测试问题描述

通过渗透测试发现，OA系统存在的安全问题汇总如下表所示。

表 3-5 渗透测试结果汇总表

序号	安全问题	关联资产/域名	严重程度
1	缺少“X-Content-Type-Options”响应头 此类漏洞涉及业务应用软件平台。	https://oa.mmpt.edu.cn/OA 系统	低

3.13 单项测评小结

3.13.1 控制点符合情况汇总

根据单项测评结果汇总控制点符合情况如下表所示。(表格以不同颜色对测评结果进行区分，不符合的安全控制点采用红色标识，部分符合的采用黄色标识，不适用的采用蓝色标识且不做勾选。)

表 3-6 控制点符合情况汇总表

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
1	安全通用要求	安全物理环境	物理位置选择	√		
2			物理访问控制		√	
3			防盗窃和防破坏	√		

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
4			防雷击	√		
5			防火		√	
6			防水和防潮	√		
7			防静电			√
8			温湿度控制	√		
9			电力供应	√		
10			电磁防护	√		
11	安全通用要求	安全通信网络	网络架构		√	
12			通信传输	√		
13			可信验证			√
14	安全通用要求	安全区域边界	边界防护	√		
15			访问控制	√		
16			入侵防范		√	
17			恶意代码和垃圾邮件防范		√	
18			安全审计	√		
19			可信验证			√
20	安全通用要求	安全计算环境	身份鉴别	√		
21			访问控制	√		
22			安全审计	√		
23			入侵防范	√		

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
24			恶意代码防范	√		
25			可信验证			√
26			数据完整性	√		
27			数据备份恢复		√	
28			剩余信息保护	√		
29			个人信息保护	√		
30	安全通用要求	安全管理中心	系统管理		√	
31			审计管理	√		
32	安全通用要求	安全管理制度	安全策略	√		
33			管理制度	√		
34			制定和发布	√		
35			评审和修订	√		
36	安全通用要求	安全管理机构	岗位设置	√		
37			人员配备	√		
38			授权和审批	√		
39			沟通和合作	√		
40			审核和检查		√	
41	安全通用要求	安全管理人员	人员录用	√		
42			人员离岗	√		
43			安全意识教育和培训	√		

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
44			外部人员访问管理		√	
45	安全通用要求	安全建设管理	定级和备案	√		
46			安全方案设计			√
47			产品采购和使用	√		
48			自行软件开发			
49			外包软件开发		√	
50			工程实施	√		
51			测试验收		√	
52			系统交付	√		
53			等级测评	√		
54			服务供应商选择	√		
55	安全通用要求	安全运维管理	环境管理	√		
56			资产管理	√		
57			介质管理	√		
58			设备维护管理	√		
59			漏洞和风险管理			√
60			网络和系统安全管理	√		
61			恶意代码防范管理		√	
62			配置管理	√		
63			密码管理			√

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
64			变更管理	√		
65			备份与恢复管理	√		
66			安全事件处置	√		
67			应急预案管理	√		
68			外包运维管理			
安全通用要求控制点符合情况数量统计				47	12	7
控制点符合情况数量统计				47	12	7

3.13.2 安全问题汇总

针对单项测评结果中存在的部分符合和不符合项进行汇总，形成了安全问题如下表所示。

表 3-7 安全问题汇总表

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T1	（1）机房出入口未配置电子门禁系统。	信息化机房	安全通用要求	安全物理环境	物理访问控制	机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。
T2	（1）机房建设未完全采用符合耐火等级的建筑材料； （2）机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级。	信息化机房	安全通用要求	安全物理环境	防火	b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。
T3	（1）机房内缺乏防静电措施（如防静电地板或铺设防静电地毯）。	信息化机房	安全通用要求	安全物理环境	防静电	应采用防静电地板或地面并采用必要的接地防静电措施。
T4	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	安全通用要求	安全通信网络	网络架构	a）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
T5	（1）缺乏对通信设备可信	安全通信网络	安全通	安全通信	可信验证	可基于可信根对通信设

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
	验证方面的安全设计要求； （2）现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况。		用要求	网络		备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T6	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	安全通用要求	安全区域边界	入侵防范	应在关键网络节点处监视网络攻击行为。
T7	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	安全通用要求	安全区域边界	恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。
T8	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	办公网区域 外网边界区域 安全管理区域 服务器存储区域	安全通用要求	安全区域边界	可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T9	（1）设备不具备相关可信验证的技术措施。	WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2	安全通用要求	安全计算环境	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T10	（1）缺乏对计算设备可信验证方面的安全设计要	业务终端-1 业务终端-2	安全通用要求	安全计算环境	可信验证	可基于可信根对计算设备的系统引导程序、系

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
	求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。	运维及管理终端-1 运维及管理终端-2				统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T11	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况； （3）现有的计算设备存在对系统运行过程中的可信检验不全面的情况； （4）现有的可信验证存在部分告警、审计及联动措施不全面的情况。	应用/数据库服务器	安全通用要求	安全计算环境	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T12	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	OA系统	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T13	（1）未能提供数据库系统重要数据的异地定时数据备份功能。	应用/数据库服务器-Oracle	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T14	（1）未能提供中间件重要数据的异地定时数据备份功能。	应用/数据库服务器-Tomcat	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T15	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	重要业务数据 重要个人信息	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T16	（1）系统管理的资源、运行及配置管理不够全面。	管理中心	安全通用要求	安全管理中心	系统管理	b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
						理、数据和设备的备份与恢复等。
T17	（1）单位开展的检查工作不够完善。	制度文件、执行/记录文件	安全通用要求	安全管理机构	审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。
T18	（1）单位未完全按管理规范开展人员离场后的清理工作。	制度文件、执行/记录文件	安全通用要求	安全管理人员	外部人员访问管理	c）外部人员离场后应及时清除其所有的访问权限。
T19	（1）单位未具备适用于被测系统的安全规划设计方案。	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
T20	（1）单位未具备完整的安全设计方案相关的文档； （2）单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	b）应根据保护对象的安全保护等级进行安全方案设计；
T21	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； （2）单位未对相关论证过程及内容进行完整的记录。	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	c）应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。
T22	（1）单位未在软件开发过程中对所有软件安全性进行测试； （2）单位未在软件安装之前按要求对所有软件开展恶意代码检测。	制度文件、执行/记录文件	安全通用要求	安全建设管理	外包软件开发	a）应在软件交付前检测其中可能存在的恶意代码；
T23	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	安全通用要求	安全建设管理	测试验收	a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；
T24	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	安全通用要求	安全建设管理	测试验收	b）应进行上线前的安全性测试，并出具安全测试报告。
T25	（1）单位未严格按规范开展漏洞及安全隐患检测工作。	制度文件、执行/记录文件	安全通用要求	安全运维管理	漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T26	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	安全通用要求	安全运维管理	恶意代码防范管理	c）应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。
T27	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	制度文件、执行/记录文件	安全通用要求	安全运维管理	密码管理	a）应遵循密码相关国家标准和行业标准；

4 整体测评

从安全控制间、区域间和验证测试等方面对单元测评的结果进行验证、分析和整体评价。

具体内容参见《GB/T 28448-2019信息安全技术 网络安全等级保护测评要求》。

4.1 安全控制点间安全测评

安全控制间的安全测评主要考虑同一区域内、同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用。安全功能上的增强和补充可以使两个不同强度、不同等级的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。

4.1.1 安全建设管理

4.1.1.1 安全通用要求

（T23）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。

单位未具备适用于被测系统的安全规划设计方案。安全方案设计不完善，导致规划设计需求不全面，信息系统存在安全缺陷。可升高单位未完全根据测试验收方案组织相

关部门和人员开展验收工作的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

（T24）针对系统上线前的安全性测试工作存在问题。

单位未在软件交付之前按要求对所有软件开展恶意代码检测,导致在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。可升高针对系统上线前的安全性测试工作存在问题的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

4.1.2 安全运维管理

4.1.2.1 安全通用要求

（T26）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。

单位未严格按规范开展漏洞及安全隐患检测工作，漏洞检测工作不到位，导致存在未授权人员利用漏洞攻击信息系统的风险。可升高单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

4.2 区域间安全测评

区域间的安全测评主要考虑互连互通（包括物理上和逻辑上的互连互通等）的不同区域之间存在的安全功能增强、补充和削弱等关联作用，特别是有数据交换的两个不同区域。

4.2.1 安全物理环境

4.2.1.1 安全通用要求

（T1）机房出入口未配置电子门禁系统。

机房所在位置处于内部受控区域，非授权人员无法随意通过现有控制措施（如机械锁）进出机房，且具备相对完善的机房出入管理要求（具备《机房安全管理制度》），并实际执行措施效果良好（具备《机房出入登记表》），可降低机房出入口访问控制措施缺失的问题严重程度（如信息化机房）。根据整体测评分析，问题严重程度变化为降低。

4.2.2 安全通信网络

4.2.2.1 安全通用要求

（T4）关键的应用服务和数据库服务网段未独立进行子网划分的情况。

单位有完整的IP地址规范，对IP地址的使用、回收均有记录《资产清单》，且系统具备相对完善的设备自身访问控制策略管理要求（具备《网络安全管理规范》、《设备及系统软件配置和操作手册》），措施效果良好，有助于部分补充未划分子网的安全功能不足（如安全通信网络）。根据整体测评分析，问题严重程度变化为降低。

4.2.3 安全区域边界

4.2.3.1 安全通用要求

（T6）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。

网络环境划分了相应的安全区域，区域间具备有效的访问控制措施，区域内各主机设备部署深信服EDR单机版，策略库、规则库更新及时，能够对攻击行为进行检测、阻断或限制，实际措施效果良好，且系统具备相对完善的策略库、规则库更新/校准管理要求，管理措施效果良好且及时检查更新有效性（具备《漏洞检测报告》、《主机安全管理规范》），可降低外部网络攻击防御措施缺失的问题严重程度（如办公网区域、安全管理区域）。根据整体测评分析，问题严重程度变化为降低。

（T7）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。

系统部署于可控的网络环境内（具备有效的访问控制、入侵防护措施）限制相关主机对象访问非受控网络，操作系统层面配置防御策略（具备本地防火墙策略、核心交换机地址限制策略、部署深信服EDR单机版），恶意代码入侵的可能性相对较低，可降低恶意代码防范措施缺失的问题严重程度（如办公网区域、安全管理区域）。根据整体测评分析，问题严重程度变化为降低。

4.3 整体测评结果汇总

经整体测评后安全问题严重程度变化情况如下表所示

表 4-1 整体测评结果汇总表

问题编号	安全问题描述	测评对象	整体测评描述	严重程度变化
T1	（1）机房出入口未配置电子门禁系统。	信息化机房	（1）机房所在位置处于内部受控区域，非授权人员无法随意通过现有控制措施（如机械锁）进出机房，且具备相对完善的机房出入管理要求（具备《机房安全管理制度》），并实际执行措施效果良好（具备《机房出入登记表》），可降低机房出入口访问控制措施缺失的问题严重程度。	□升高 ☑降低
T4	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	（1）单位有完整的IP地址规范，对IP地址的使用、回收均有记录《资产清单》，且系统具备相对完善的设备自身访问控制策略管理要求（具备《网络安全管理规范》、《设备及系统软件配置和操作手册》），措施效果良好，有助于部分补充未划分子网的安全功能不足。	□升高 ☑降低
T6	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	（1）网络环境划分了相应的安全区域，区域间具备有效的访问控制措施，区域内各主机设备部署深信服EDR单机版，策略库、规则库更新及时，能够对攻击行为进行检测、阻断或限制，实际措施效果良好，	□升高 ☑降低

问题编号	安全问题描述	测评对象	整体测评描述	严重程度变化
			且系统具备相对完善的策略库、规则库更新/校准管理要求，管理措施效果良好且及时检查更新有效性（具备《漏洞检测报告》、《主机安全管理规范》），可降低外部网络攻击防御措施缺失的问题严重程度。	
T7	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域安全管理区域	（1）系统部署于可控的网络环境内（具备有效的访问控制、入侵防护措施）限制相关主机对象访问非受控网络，操作系统层面配置防御策略（具备本地防火墙策略、核心交换机地址限制策略、部署深信服EDR单机版），恶意代码入侵的可能性相对较低，可降低恶意代码防范措施缺失的问题严重程度。	□升高 ☑降低
T23	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	（1）单位未具备适用于被测系统的安全规划设计方案。安全方案设计不完善，导致规划设计需求不全面，信息系统存在安全缺陷。可升高单位未完全根据测试验收方案组织相关部门和人员开展验收工作的问题严重程度。	☑升高 □降低
T24	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	（1）单位未在软件交付之前按要求对所有软件开展恶意代码检测，导致在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。可升高针对系统上线前的安全性测试工作存在问题的问题严重程度。	☑升高 □降低
T26	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	（1）单位未严格按规范开展漏洞及安全隐患检测工作，漏洞检测工作不到位，导致存在未授权人员利用漏洞攻击信息系统的风险。可升高单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作的问题严重程度。	☑升高 □降低

5 安全问题风险分析

针对等级测评结果中存在的所有安全问题,结合关联资产和威胁分别分析安全问题可能产生的危害结果,找出可能对系统、单位、社会及国家造成的最大安全危害(损失),并根据最大安全危害(损失)的严重程度进一步确定安全问题的风险等级,结果为“高”、“中”或“低”。最大安全危害（损失）结果应结合安全问题所影响业务的重要程度、相关系统组件的重要程度、安全问题严重程度以及安全事件影响范围等进行综合分析。

表 5-1 安全问题风险分析

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
1	安全物理环境	（1）机房出入口未配置电子门禁系统。	信息化机房	物理攻击	（1）上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域，可能对系统的平稳运行造成影响。	中风险
2	安全物理环境	（1）机房建设未完全采用符合耐火等级的建筑材料; （2）机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级。	信息化机房	物理环境影响	（1）存在发生火情时助燃火灾的风险。	低风险
3	安全物理环境	（1）机房内缺乏防静电措施(如防静电地板或铺设防静电地毯 ）。	信息化机房	软硬件故障	（1）存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。	中风险
4	安全通信网络	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	恶意攻击	（1）上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变得更为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。	中风险
5	安全通信网络	（1）缺乏对通信设备可信验证方面的安全设计要求; （2）现有的通信设备存	安全通信网络	恶意攻击	（1）缺乏对系统可执行程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将	低风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
		在对系统运行过程中的可信检验完全缺失的情况。			导致计算资源被干扰和破坏造成损失。	
6	安全区域边界	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	恶意攻击	（1）存在不能及时发现内部主机作为攻击跳板，或网络攻击行为而造成系统损坏/网络资源浪费的风险。	中风险
7	安全区域边界	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	恶意攻击	（1）无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。	中风险
8	安全区域边界	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	办公网区域 外网边界区域 安全管理区域 服务器存储区域	恶意攻击	（1）缺乏对边界设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险
9	安全计算环境	（1）设备不具备相关可信验证的技术措施。	WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2	恶意攻击	（1）缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险
10	安全计算环境	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。	业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	恶意攻击	（1）缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险
11	安全计算环境	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存	应用/数据库服务器	恶意攻击	（1）缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程	低风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
		在对系统运行过程中的可信检验完全缺失的情况； （3）现有的计算设备存在对系统运行过程中的可信检验不全面的情况； （4）现有的可信验证存在部分告警、审计及联动措施不全面的情况。			序将导致边界防护措施被干扰和破坏造成风险。	
12	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	OA系统	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。	中风险
13	安全计算环境	（1）未能提供数据库系统重要数据的异地定时数据备份功能。	应用/数据库服务器-Oracle	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供，使企业的经济利益或声誉受到损害。	中风险
14	安全计算环境	（1）未能提供中间件重要数据的异地定时数据备份功能。	应用/数据库服务器-Tomcat	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。	中风险
15	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	重要业务数据 重要个人信息	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。	中风险
16	安全管理中心	（1）系统管理的资源、运行及配置管理不够全面。	管理中心	恶意攻击	（1）系统的资源和运行缺少统一的管理，将导致系统可能无法按规划实现基于资源配置、 系统加载、异常处理、及备份/恢复等的安全控制措施。	低风险
17	安全管理机构	（1）单位开展的检查工作不够完善。	制度文件、执行/记录文件	管理不到位	（1）检查工作开展不仔细，可能对存在或潜在的安全风险不能被及时发现并进行处理。	低风险
18	安全管理	（1）单位未完全按管理	制度文件、执行/	管理	（1）人员离场后的清理工	低风

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
	人员	规范开展人员离场后的清理工作。	记录文件	不到位	作开展不规范，可能导致遗留外部人员访问受控区域的记录，存在被二次非法利用，造成泄密。	险
19	安全建设管理	（1）单位未具备适用于被测系统的安全规划设计方案。	制度文件、执行/记录文件	管理不到位	（1）规划设计需求不全面，可能导致安全方案设计不完善，信息系统存在安全缺陷。	低风险
20	安全建设管理	（1）单位未具备完整的安全设计方案相关的文档； （2）单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	管理不到位	（1）相关合规的规划配套文件缺失，可能导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。	中风险
21	安全建设管理	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； （2）单位未对相关论证过程及内容进行完整的记录。	制度文件、执行/记录文件	管理不到位	（1）未开展规范的审批过程，可能存在安全整体规划缺乏合理性和可行性，导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。	低风险
22	安全建设管理	（1）单位未在软件开发过程中对所有软件安全性进行测试； （2）单位未在软件安装之前按要求对所有软件开展恶意代码检测。	制度文件、执行/记录文件	管理不到位	（1）软件交付前恶意代码检测不规范，可能在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。	低风险
23	安全建设管理	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	管理不到位	（1）可能由于验收测试不严谨，造成测试过程缺乏计划性及操作性，无法保证经过测试验收的系统达到既定的安全性等目标。	低风险
24	安全建设管理	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	管理不到位	（1）未按规定开展上线前测试，安全隐患可能在系统上线运行前未被发现并作出相应处理。	低风险
25	安全运维管理	（1）单位未严格按规范开展漏洞及安全隐患检测工作。	制度文件、执行/记录文件	管理不到位	（1）漏洞检测、修补工作不到位，可能存在未授权人员利用漏洞攻击信息系统的风险。	低风险
26	安全运维管理	（1）单位未严格按规范要求，针对防范恶意代码	制度文件、执行/记录文件	管理不到	（1）可能导致系统恶意代码检测管理不到位，存在	低风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
		攻击的技术措施的有效性验证，开展工作。		位	信息系统感染恶意代码，从而导致严重的信息安全风险。	
27	安全运维管理	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	制度文件、执行/记录文件	管理不到位	（1）密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不到位，存在违反国家政策的风险。	中风险

6 等级测评结论

等级测评结论由安全问题风险分析结果和综合得分共同确定,判定依据如下表所示。

表 6-1 等级测评结论判别依据

测评结论	判别依据
优	被测对象中存在安全问题，但不会导致被测对象面临中、高等级安全风险，且系统综合得分 90 分以上（含90 分）。
良	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分 80分以上（含 80分）。
中	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分 70分以上（含 70分）
差	被测对象中存在安全问题，而且会导致被测对象面临高等级安全风险，或被测对象综合得分低于 70 分。

综合得分计算方法如下:

设M为被测对象的综合得分，$M = V_t + V_m$，V_t和V_m根据下列公式计算。

$$V_t = \begin{cases} 100 \cdot y - \sum_{k=1}^{t} f(\omega_k) \cdot (1 - x_k) \cdot S, & V_t > 0 \\ 0, & V_t \leq 0 \end{cases}$$

$$V_m = \begin{cases} 100 \cdot (1-y) - \sum_{k=1}^{m} f(\omega_k) \cdot (1-x_k) \cdot S, & V_m > 0 \\ 0, & V_m \le 0 \end{cases}$$

$$0 \le x_k \le 1,\ S = 100 \cdot \frac{1}{n},\ f(\omega_k) = \begin{cases} 1, & \omega_k = \text{一般} \\ 2, & \omega_k = \text{重要} \\ 3, & \omega_k = \text{关键} \end{cases}$$

其中，y为关注系数，取值在0至1之间，由等级保护工作管理部门给出，默认值为0.5。n为被测对象涉及的总测评项数（不含不适用项，下同），t为技术方面对应的总测评项数，V_t为技术方面的得分，m为管理方面对应的总测评项数，V_m为管理方面的得分，ω_k为测评项k的重要程度（分为一般、重要和关键），x_k为测评项k的得分，如果测评项k涉及多测评项对象，则x_k取值为多测评对象得分的算术平均值。

x_k的得分计算如下：

测评项k涉及对象 / 测评项k定性判定	只涉及单个对象	涉及多个对象
符合	1	1
部分符合	0.5	计算测评对象平均分，取值在0至1之间
不符合	0	0

注：当测评项k涉及多个对象时，针对每个对象的得分取值为1、0.5和0。

根据第5章安全问题风险分析结果统计高、中、低风险安全问题的数量，利用综合得分计算公式计算出被测对象的综合得分，并将相关结果填入下表。

表 6-2 安全问题统计和综合得分

被测对象名称	安全问题数量			综合得分
	高风险	中风险	低风险	
OA系统	0	11	16	73.85

依据 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》和GB/T 28448—2019《信息安全技术 网络安全等级保护测评要求》的第二级要求，经对OA系统的安全保护状况进行综合分析评价，等级测评结论如下：

OA系统本次等级测评的综合得分为73.85，且不存在高等级安全风险，等级测评结论为中。

7 安全问题整改建议

表 7-1 安全问题整改建议

序号	安全类	安全问题	关联资产	整改建议
1	安全物理环境	(1)机房出入口未配置电子门禁系统。	信息化机房	(1) 采用电子门禁系统严格控制机房其他出入口的进出，或安排专人值守； (2) 采用电子门禁系统，对机房所有人员出入进行登记记录，并保存。
2	安全物理环境	(1)机房建设未完全采用符合耐火等级的建筑材料； (2)机房建设不具备防火设计/验收文档,或机房验收文档未明确相关建筑材料的耐火等级。	信息化机房	(1) 机房及相关的工作房间和辅助房采用具有耐火等级的建筑材料； (2) 机房建设采用符合相关耐火等级（二级）的建筑材料。（内外墙壁均应采用具有防火涂料、隔热板、铝板、钢板等阻燃或不燃的材料）； (3) 机房耐火等级建筑材料有相关合格证，并留存机房验收文档。
3	安全物理环境	(1)机房内缺乏防静电措施（如防静电地板或铺设防静电地毯）。	信息化机房	(1) 机房铺设防静电地板或铺设防静电地毯； (2) 机房房静电设计可依据GB50174-2008和GB50314-2006相关规定进行机房设计和验收。
4	安全通信网络	(1)关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	(1) 建议独立划分出应用服务器网段、数据库服务器网段。
5	安全通信网络	(1)缺乏对通信设备可信验证方面的安全设计要求；	安全通信网络	(1) 建议在管理规范文档内对通信设备可信验证方面的安全设计提出要求；

序号	安全类	安全问题	关联资产	整改建议
		(2)现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况。		（2）建议系统实现对所有可执行环节进行可信验证，包括： 运行过程中的可信检验： ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■通信应用连接过程。
6	安全区域边界	(1)网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	（1）建议网络层部署的防火墙配置对内部发起的攻击行为实现防范功能策略，实现检测、防止或限制从内部发起的网络攻击行为； （2）内部安全防范措施能检测以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、碎片攻击、网络蠕虫攻击、应用漏洞攻击。
7	安全区域边界	(1)现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	（1）建议现有部署的恶意代码防范措施网络边界覆盖全面，及时对恶意代码及逆行检测和清除。
8	安全区域边界	(1)缺乏对边界设备可信验证方面的安全设计要求； (2)现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）建议对边界设备系统程序的可信验证设计并保存设计文件； （2）建议系统实现对所有可执行环节进行可信验证。
9	安全计算环境	(1)设备不具备相关可信验证的技术措施。	WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2	（1）建议通过设备的启动过程和运行过程中对预装软件（包括系统引导程序、系统程序、相关应用程序和重要配置参数）的完整性验证或检测，确保对系统引导程序、系统程序、重要配置参数和关键应用程序可信根验证； （2）建议设备启用在检测到其可信性受到破坏后进行报警的相关功能。
10	安全计算环境	(1)缺乏对计算设备可信验证方面的安全设计要求； (2)现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。	业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终	（1）建议对计算设备系统程序的可信验证设计并保存设计文件； （2）建议系统实现对所有可执行环节进行可信验证。

序号	安全类	安全问题	关联资产	整改建议
			端-2	
11	安全计算环境	(1)缺乏对计算设备可信验证方面的安全设计要求; (2)现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况; (3)现有的计算设备存在对系统运行过程中的可信检验不全面的情况; (4)现有的可信验证存在部分告警、审计及联动措施不全面的情况。	应用/数据库服务器	(1) 建议对计算设备系统程序的可信验证设计并保存设计文件; (2) 建议系统实现对所有可执行环节进行可信验证。
12	安全计算环境	(1)未能提供应用软件系统重要数据的异地定时数据备份功能。	OA系统	(1) 建议设置异地灾备机房，并利用通信网络将应用软件系统重要数据定时备份至备份场地; (2) 异地备份的应用软件系统数据范围（不限于）包括系统的：配置数据、重要日志数据，业务数据。
13	安全计算环境	(1)未能提供数据库系统重要数据的异地定时数据备份功能。	应用/数据库服务器-Oracle	(1) 建议设置异地灾备机房，并利用通信网络将重要数据定时备份至备份场地; (2) 异地备份的数据范围（不限于）包括系统的: ■配置数据 ■重要业务数据。
14	安全计算环境	(1)未能提供中间件重要数据的异地定时数据备份功能。	应用/数据库服务器-Tomcat	(1) 建议设置异地灾备机房，并利用通信网络将中间件重要数据定时备份至备份场地; (2) 异地备份的中间件数据范围（不限于）包括系统的: ■配置数据 ■重要日志数据。
15	安全计算环境	(1)未能提供应用软件系统重要数据的异地定时数据备份功能。	重要业务数据 重要个人信息	(1) 建议设置异地灾备机房，并利用通信网络将应用软件系统重要数据定时备份至备份场地。
16	安全管理中心	(1) 系统管理的资源、运行及配置管理不够全面。	管理中心	(1) 需实现系统包括对可信证书管理、可信基准库的管理。
17	安全管理机构	(1)单位开展的检查工作不够完善。	制度文件、执行/记录文件	(1) 建议单位按要求提供安全检查报告。
18	安全管理人员	(1)单位未完全按管理规范开展人员离场后的清理工	制度文件、执行/记录文件	(1) 建议单位按管理规范开展人员离场后的清理工作。至少包括：保留清理

序号	安全类	安全问题	关联资产	整改建议
		作。		记录、及时清除离场后的所有访问权限、记录访问权限清除时间。
19	安全建设管理	(1)单位未具备适用于被测系统的安全规划设计方案。	制度文件、执行/记录文件	(1) 建议单位根据等保要求进行过全面的自查或对比，根据系统的安全级别选择基本安全措施； (2) 建议规划方案需根据风险分析结果对系统安全措施进行补充和整，并在系统建设\\整改方案中有详细描述。
20	安全建设管理	(1)单位未具备完整的安全设计方案相关的文档； (2)单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	(1) 建议单位根据信息系统的等级划分情况，准备安全设计方案、安全管理策略、安全建设规划文档等； (2) 建议相关文档内容应完善，包括统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、密码技术要求、总体建设规划和详细设计方案，并形成一致性的配套文件。
21	安全建设管理	(1) 单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； (2)单位未对相关论证过程及内容进行完整的记录。	制度文件、执行/记录文件	(1) 建议单位组织相关部门和安全技术专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定； (2) 保存论证和审定记录，记录包括批准时间、批准人员签字； (3) 文件经过批准后，才能正式实施。
22	安全建设管理	(1)单位未在软件开发过程中对所有软件安全性进行测试； (2)单位未在软件安装之前按要求对所有软件开展恶意代码检测。	制度文件、执行/记录文件	(1) 建议开发商提供软件源代码，软件安装前检测软件中的恶意代码； (2) 输出检测报告（或提供第三方检测报告），内容包括测试时间、测试地点、测试对象、测试结论、测试人员。
23	安全建设管理	(1)单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	(1) 建议根据测试验收过程记录与结果，形成测试验收报告。
24	安全建设管理	(1)针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	(1) 建议系统建设完成后，委托第三方测试单位对系统进行安全性测试，并出具安全性测试报告； (2) 测试报告内容至少包括测试时间、测试地点、测试人、测试对象、测试方法、测试过程、测试发现的安全问题、整改建议、测试结论，并有第三方测试机构的签字盖章。
25	安全运维管理	(1)单位未严格按规范开展漏洞及安全隐患检测工作。	制度文件、执行/记录文件	(1) 建议单位定期开展漏洞扫描，对发现的安全漏洞和隐患进行及时修补

序号	安全类	安全问题	关联资产	整改建议
				评估； （2）对必需修补的安全漏洞和隐患进行加固测试，测试无误后，备份系统数据，再从生产环境进行修补； （3）对于剩余安全漏洞和隐患进行残余风险分析，明确安全风险整改原则。
26	安全运维管理	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	（1）建议单位按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。包括;定期对相关产品的恶意代码库进行升级；对相关设备升级情况进行记录；对各类防病毒产品上截获的恶意代码进行分析并汇总上报； （2）单位需保留完整的恶意代码检测/升级的记录。至少具备：执行人、升级结果/检测结果、处理方式、负责人签字 。
27	安全运维管理	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	制度文件、执行/记录文件	（1）建议单位学习现有密码相关的国家标准和行业标准。建立密码管理要求的制度文档。

漏洞安全问题整改建议

序号	安全类	安全问题	关联资产	整改建议
1	安全计算环境	SSH 服务支持弱加密算法【原理扫描】 此类漏洞涉及服务器存储设备。	10.2.3.10/应用/数据库服务器	解决方法：* 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。https://tools.ietf.org/html/rfc4253#section-6.3 方案一：修改 SSH 配置文件，添加加密算法： vi /etc/ssh/sshd_config 最后添加一下内容（去掉 arcfour、arcfour128、arcfour256 等弱加密算法）Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc 保存文件后重启 SSH 服务：service sshd restart 方案二：升级 openssh 版本为最新版本 官网有说明，OpenSSH 7.0 以后的版本默认禁用了一些较低版本的密钥算法。 SSH Weak

序号	安全类	安全问题	关联资产	整改建议
				MAC Algorithms Enabled 漏洞修复使用同样的方式，添加以下行： MACs hmac-sha1,umac-64,hmac-sha2-256,hmac-sha2-512,hmac-ripemd160 参考链接：https://linux.uits.uconn.edu/2014/06/25/ssh-weak-ciphers-and-mac-algorithms/#
2	安全计算环境	允许Traceroute探测 此类漏洞涉及安全设备、网络设备。	10.2.1.4/运维安全管理系统 10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/ 上网行为管理系统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/ 汇聚交换机 172.16.1.2/核心交换机	在防火墙出站规则中禁用echo-reply（type 0）、time-exceeded（type 11）、destination-unreachable（type 3）类型的ICMP包。
3	安全计算环境	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161) 此类漏洞涉及服务器存储设备、网络设备。	10.2.3.10/应用/数据库服务器 172.16.1.2/核心交换机	临时解决方法：* 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://downloads.ssh.com/ 对于具体Linux发行版中使用的版本，可以参考如下链接,确认系统是否受该漏洞影响: Redhat ------- https://rhn.redhat.com/errata/RHSA-2009-1287.html Suse ------- http://support.novell.com/security/cve/CVE-2008-5161.html Ubuntu ------- http://people.canonical.com/~ubuntu-security/cve/2008/CVE-2008-5161.html
4	安全计算环境	OpenSSH 信息泄露漏洞(CVE-2011-4327) 此类漏洞涉及服务器存储设	10.2.3.10/应用/数据库服务器	厂商补丁： OpenSSH ------- 目前厂商已经发布升级版本修复此安全问题，建议升级OpenSSH至最新版本，请到厂商

序号	安全类	安全问题	关联资产	整改建议
		备。		的官方页面下载升级版本：http://www.openssh.com/openbsd.html http://www.openssh.com/
5	安全计算环境	OpenSSH 本地信息泄露漏洞(CVE-2016-10011) 此类漏洞涉及服务器存储设备。	10.2.3.10/应用/数据库服务器	厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://www.openssh.com/txt/release-7.4 http://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/authfile.c.diff?r1=1.121&r2=1.122
6	安全计算环境	缺少“X-Content-Type-Options”响应头 此类漏洞涉及业务应用软件平台。	https://oa.mmpt.edu.cn/OA 系统	在服务器中配置 X-Content-Type-Options 响应头为“nosniff”。

【正文结束】

附录A 被测对象资产

A.1 物理机房

附录A 表- 1物理机房

序号	机房名称	物理位置	重要程度
1	信息化机房	茂名市茂南区文明北路232号大院大楼	关键

A.2 网络设备

附录A 表- 2网络设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度	备注
1	核心交换机	否	H3C version 7.1.070, Release 7585P07	H3C S7500E-X	核心数据交换、访问控制	关键	
2	汇聚交换机	否	H3C version 7.1.070, Release 6126P20	H3C S5560X-30C-EI	数据交换	重要	

A.3 安全设备

附录A 表- 3安全设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度	备注
1	上网行为管理系统	否	深信服AC12.0.26	深信服AC-1000-D600-PT	上网行为管理及终端准入控制	重要	
2	WEB应用防火墙	否	深信服AF 8.0.9	深信服WAF-2000-H642	应用防护、入侵防范、病毒防护	重要	
3	日志审计系统	否	深信服LAS 3.0.5	深信服AC-1000-D601-PT	日志审计	重要	
4	防火墙-2	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键	
5	防火墙-1	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键	
6	基线核查系统	否	深信服V3.0.3	深信服AC-1000-D602-PT	漏洞扫描	重要	
7	运维安全管理系统	否	深信服V3.0.6	深信服AC-1000-D603-PT	运维审计	重要	

A.4 服务器

附录A 表-4服务器

序号	设备名称	所属业务应用系统/平台名称	是否虚拟设备	操作系统及版本	数据库管理系统及版本	中间件及版本	重要程度	备注
1	应用/数据库服务器	OA系统	否	CentOS 6.8	Oracle 11.2.0.1.0	Tomcat 8.0.37	关键	

A.5 终端设备

附录A 表-5终端设备

序号	设备名称	是否虚拟设备	操作系统/控制软件及版本	用途	重要程度	备注
1	业务终端-1	否	Windows 10（版本20H2（内部版本19044.1889）	业务管理	一般	
2	运维及管理终端-1	否	Windows 10（版本20H2（内部版本19044.1889）	运维管理、系统管理	一般	
3	运维及管理终端-2	否	Windows 10（版本21H2（内部版本19044.1889））	运维管理、系统管理	一般	
4	业务终端-2	否	Windows 10（版本20H2（内部版本19044.1889）	业务管理	一般	

A.6 其他系统或设备

附录A 表-6其他系统或设备

序号	设备名称	是否虚拟设备	操作系统/控制软件及版本	用途	重要程度	备注
/	/	/	/	/	/	/

注释：本次测评对象中不涉及专用移动互联终端等，不开展抽测。

A.7 系统管理软件/平台

附录A 表-7系统管理软件/平台

序号	系统管理软件/平台名称	所在设备名称	版本	主要功能	重要程度	备注
1	应用/数据库服务器-Tomcat	应用/数据库服务器	8.0.37	页面发布	关键	

序号	系统管理软件/平台名称	所在设备名称	版本	主要功能	重要程度	备注
2	应用/数据库服务器-Oracle	应用/数据库服务器	11.2.0.1.0	数据生产、存储	关键	

A.8 业务应用软件/平台

附录A 表- 8业务应用系统/平台

序号	业务应用系统/平台名称	主要功能	业务应用软件及版本	开发厂商	重要程度
1	OA系统	茂名职业技术学院OA系统是学院实现办公流程话的系统，包括了公文管理、会议管理、流程管理、移动管理、全文检索、高级office套件等模块，OA系统实现了学校办文、办会、办事的规范化，实现了规范流程管理、内控合规管理、标准高效管理。	V6.0	北京致远互联软件股份有限公司	关键

A.9 数据资源

附录A 表- 9数据资源

序号	数据类别	所属业务应用	安全防护需求	重要程度
1	重要业务数据	OA系统	完整性、保密性	关键
2	重要个人信息	OA系统	完整性、保密性	关键
3	鉴别数据	OA系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性、保密性	关键
4	重要审计数据	OA系统（安全管理中心）	完整性	重要
5	重要配置数据	OA系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性	关键

注释：网络设备、安全设备、服务器、终端、系统管理软件/平台和业务应用系统等所涉及的鉴别数据和重要配置数据分别在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。重要审计数据在安全管理中心进行汇总测评证据，

包括数据完整性。重要业务数据和重要个人信息分别在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。

A.10 密码产品

附录A 表-10密码产品

序号	产品/模块名称	生成厂商	商密型号	密码算法	用途	重要程度
/	/	/	/	/	/	/

注释：本次测评不存在加密机等密码产品。

A.11 安全相关人员

附录A 表-11安全相关人员

序号	姓名	岗位/角色	联系方式	所属单位
1	龙恒	数据管理员	13377766618	茂名职业技术学院
2	杨云	资产管理员	0668-2920122	茂名职业技术学院
3	杨云	审计管理员	0668-2920122	茂名职业技术学院
4	龙恒	应用管理员	13377766618	茂名职业技术学院
5	叶永利	安全管理员	0668-2920122	茂名职业技术学院
6	吴国华	系统管理员	0668-2920122	茂名职业技术学院
7	龙恒	网络管理员	13377766618	茂名职业技术学院
8	吴国华	机房管理员	0668-2920122	茂名职业技术学院

A.12 安全管理文档

附录A 表-12安全管理文档

序号	文档名称	主要内容
1	制度类文档-办公环境保密管理	关于单位办公环境管理制度文档
2	制度类文档-信息系统外包运维管理制度	关于单位外包运维工作管理制度文档
3	制度类文档-外部接入受控网络访问系统管理规范	关于单位针对外部人员工作接入规范制度文档
4	制度类文档-授权和审	关于单位授权审批、审批流程规范制度文档

序号	文档名称	主要内容
	批管理规定	
5	制度类文档-办公环境管理制度	关于单位办公环境管理制度文档
6	制度类文档-网络与信息系统安全设计规范	关于单位网络与信息化安全设计制度文档
7	制度类文档-安全事件报告和处置	关于单位网络安全事件管理、处置、流程等报告制度文档
8	制度类文档-外部人员访问管理制度	关于单位针对外来人员访问管控制度文档
9	制度类文档-物理安全管理规范	关于加强单位办公区域及电子计算机机房的管理和设备运行安全，规范办公区域及机房建设，使人员办公高效及机房设备安全、稳定运行的制度文档
10	制度类文档-安全管理组织规范	关于单位组织结构管理规范制度文档
11	制度类文档-介质管理制度	关于单位介质安全管理工制度文档
12	制度类文档-系统安全管理制度	关于单位系统安全管理、安全服务管理制度文档
13	制度类文档-信息安全总体策略	关于单位网络安全方针、策略制度文档
14	制度类文档-主机安全管理规范	关于规定单位主机系统安全管理要求规范，指导业务平台主机的安全配置和维护的制度文档
15	制度类文档-信息安全奖惩办法	关于单位人员奖惩制度文档
16	制度类文档-服务供应商选择安全管理制度	关于单位安全服务供应商管理规定制度文档
17	制度类文档-网络安全事件应急预案	关于单位网络安全事件应急处理、流程、培训等管理制度文档
18	制度类文档-制度制定、发布、评审和修订管理制度	关于单位制度制定、发布、评审和修订等管理文档
19	制度类文档-安全漏洞管理制度	关于单位安全漏洞管理工作制度文档
20	制度类文档-测试及验收方案	关于单位测试验收方案文档
21	制度类文档-组织安全结构和人员职责制度	关于单位安全结构、人员职责
22	制度类文档-信息系统恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
23	制度类文档-网络安全事件报告制度	关于单位网络安全事件管理报告文档
24	制度类文档-应用安全	关于规定单位应用安全管理要求及规范的制度文档

序号	文档名称	主要内容
	管理规范	
25	制度类文档-外部服务人员管理规范	关于单位针对外部人员工作管理规范制度文档
26	制度类文档-变更控制管理制度	关于单位变更流程、控制管理制度文档
27	制度类文档-外包开发软件管理规定	关于单位外包项目管理工作制度文档
28	制度类文档-系统交付管理	关于单位交付工作管理制度文档
29	制度类文档-系统及应用数据备份管理规范	关于单位数据备份、恢复管理制度文档
30	制度类文档-安全审查和检查管理规范	关于单位安全检查、审查工作规范制度文档
31	制度类文档-工程测试验收管理	关于单位工程测试工作管理制度文档
32	制度类文档-离岗人员工作交接规范	关于单位离岗交接工作规范制度文档
33	制度类文档-安全教育和培训制度	关于单位安全培训、安全交流工作制度文档
34	制度类文档-数据安全管理规范	关于保障关键数据安全，从数据库本身、数据加密、数据备份恢复三个方面对数据安全进行规范的制度文档
35	制度类文档-设备安全管理制度	关于单位设备安全管理制度文档
36	制度类文档-组织安全结构和人员职责制度	关于单位组织结构、人员安排、人员职责制度文档
37	制度类文档-网络安全管理制度	关于单位网络安全工作管理制度文档
38	制度类文档-工程实施管理制度	关于单位工程实施工作管理制度文档
39	制度类文档-岗位安排及岗位职责	关于单位岗位职责、岗位安排制度文档
40	制度类文档-应用系统业务用户密码设置规定	关于单位用户密码管理制度文档
41	制度类文档-恶意代码防范管理制度	关于单位恶意代码防范工作制度文档
42	制度类文档-备份与恢复管理制度	关于单位数据备份、恢复管理制度文档
43	制度类文档-机房安全管理制度	关于单位机房安全管理工作制度文档
44	制度类文档-人员管理制度	关于单位人员录用、调岗、离岗管理制度文档
45	制度类文档-恶意代码	关于单位恶意代码工作管理制度文档

序号	文档名称	主要内容
	防范管理制度	
46	制度类文档-信息安全漏洞扫描规范	关于单位安全漏洞工作规范制度文档
47	制度类文档-网络安全管理规范	关于保障单位网络系统的安全稳定运行，抵御内部和外部各种形式的网络攻击或威胁制定的管理文档
48	制度类文档-员工考核管理制度	关于单位人员考核工作管理制度文档
49	操作类文档-设备及系统软件配置和操作手册	关于单位安全设备操作、Linux服务器配置手册、主机运维操作手册、软件操作手册、防火墙配置和操作手册、数据库日常运维操作手册等指导文档
50	操作类文档-设备操作规程	关于单位相关设备操作指导文档
51	操作类文档-数据备份策略	关于单位数据备份策略文件
52	操作类文档-软硬件日常维护管理规程	关于单位计算机网络系统使用、管理、信息安全、资源共享有所遵循,规范上网操作流程,提高网络系统安全性的指导文档
53	记录类文档-设备操作维护记录	关于单位设备维护工作记录
54	记录类文档-外部人员访问申请表	关于外来人员访问申请流程工作记录
55	记录类文档-技能培训记录	关于单位系统培训工作、考核工作记录
56	记录类文档-设备维修申请表	关于单位设备维护工作申请记录
57	记录类文档-接入受控网络申请表	关于外来人员接入工作记录
58	记录类文档-网络信息安全事件记录表	关于单位网络安全事件工作记录
59	记录类文档-人员离岗申请表	关于人员离岗申请记录
60	记录类文档-安全建设方案评审纪录	关于单位网络与信息化安全设计方案评审工作记录
61	记录类文档-信息系统存储介质使用清单	关于备份介质存储使用清单
62	记录类文档-收发文登记记录	关于单位文档签发记录
63	记录类文档-系统交付清单	关于单位交付工作记录
64	记录类文档-备份介质使用记录	关于备份介质使用登记工作记录
65	记录类文档-信息安全检查记录表	关于单位安全检查工作记录
66	记录类文档-评审和修	关于单位变更评审、修订工作记录

序号	文档名称	主要内容
	订记录	
67	记录类文档-离职员工物品交回登记表	关于人员离岗工物交接工作记录
68	记录类文档-信息系统存储介质销毁申请表	关于备份介质销毁申请工作记录
69	记录类文档-机房维护日志	关于机房维护工作记录
70	记录类文档-设备出入登记记录表	关于设备进出机房登记工作记录
71	记录类文档-机房巡检记录表	关于单位机房环境巡检记录
72	记录类文档-网络配置信息	关于单位配置信息登记工作记录
73	记录类文档-备份工作汇总表	关于单位数据备份工作总结表
74	记录类文档-数据备份记录表	关于单位数据备份工作记录
75	记录类文档-监理审批表	关于单位监理审核工作记录
76	记录类文档-关键岗位人员考核记录	关于关键岗位考核工作记录
77	记录类文档-应急预案培训记录表	关于单位应急预案培训工作记录
78	记录类文档-离场信息资料交接表	关于人员离岗交接工作记录
79	记录类文档-访问记录表	关于人员访问工作记录
80	记录类文档-人员培训及考核记录表	关于人员培训、考核等工作记录
81	记录类文档-机房出入登记表	关于人员进出机房登记工作记录
82	记录类文档-安全管理制度评审记录	关于单位制度审计记录
83	记录类文档-外部会议文件和记录	关于单位外部联系、交流及会议工作记录
84	记录类文档-软件交付清单	关于单位交付工作记录
85	记录类文档-外部人员访问记录表	关于外来人员访问登记工作记录
86	记录类文档-漏洞检测报告	关于单位安全漏洞检测报告文档
87	记录类文档-机房设备维修记录表	关于单位机房设备维修工作记录

序号	文档名称	主要内容
88	记录类文档-信息管理系统漏洞检查表	关于单位安全漏洞工作检测记录表
89	记录类文档-数据恢复申请表	关于单位数据恢复工作申请表
90	记录类文档-机房设备维护记录表	关于设备维护登记工作记录
91	记录类文档-存储介质目录清单	关于备份介质存储工作清单
92	记录类文档-人员入职考核记录	关于人员录用、考核工作记录
93	记录类文档-重要操作审批表	关于单位审批工作记录
94	记录类文档-通用变更记录表	关于单位变更工作记录
95	记录类文档-信息安全会议记录	关于单位安全培训、安全交流会议记录
96	记录类文档-专家论证记录表	关于单位网络方案论证记录
97	证据类文档-定级备案	关于单位系统定级报告、备案证文件
98	证据类文档-网络安全系统设计方案	关于单位网络与信息化安全设计方案文档
99	证据类文档-网络安全等级保护工作小组名单	关于单位网络安全等级保护工作小组人员名单文件
100	证据类文档-工程项目实施方案	关于单位工程实施方案文档
101	证据类文档-深信服安全采购合同	关于单位与安全厂家服务采购、产品选择合同文件
102	证据类文档-网络安全等级保护测评服务合同	关于单位与安全服务商签定的安全服务合同文件
103	证据类文档-资产清单	关于单位信息系统资产清单统计表
104	证据类文档-信息安全事件分析报告表	关于单位安全事件分析报告
105	证据类文档-外部联系表	关于单位内部联系及外部联系名单
106	证据类文档-安全职位人员	关于单位人员岗位安排名单

附录B 上次测评问题整改情况说明

此次为OA系统初次等级测评，之前未实施过等级保护测评工作。

附录B 表- 1上次测评问题整改情况

序号	主要安全问题	整改情况	情况说明
/	/	□已整改 □未整改	/

附录C 单项测评结果汇总

C.1 安全物理环境

附录 C 表-1 安全物理环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			物理位置选择	物理访问控制	防盗窃和防破坏	防雷击	防火	防水和防潮	防静电	温湿度控制	电力供应	电磁防护
1	信息化机房	符合	2	0	2	1	1	2	0	1	2	1
		部分符合	0	1	0	0	0	0	0	0	0	0
		不符合	0	0	0	0	1	0	1	0	0	0
		不适用	0	0	0	0	0	0	0	0	0	0

附录 C 表-2 安全物理环境单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.2 安全通信网络

附录 C 表-3 安全通信网络单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求		
			网络架构	通信传输	可信验证
1	安全通信网络	符合	1	1	0
		部分符合	1	0	0
		不符合	0	0	1
		不适用	0	0	0

附录 C 表-4 安全通信网络单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.3 安全区域边界

附录 C 表-5 安全区域边界单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求					
			边界防护	访问控制	入侵防范	恶意代码和垃圾邮件防范	安全审计	可信验证
1	外网边界区域	符合	1	4	1	1	3	0
		部分符合	0	0	0	0	0	0
		不符合	0	0	0	0	0	1
		不适用	0	0	0	0	0	0
2	安全管理区域	符合	1	4	0	0	3	0
		部分符合	0	0	0	1	0	0
		不符合	0	0	1	0	0	1
		不适用	0	0	0	0	0	0
3	服务器存储区域	符合	1	4	1	1	3	0
		部分符合	0	0	0	0	0	0
		不符合	0	0	0	0	0	1
		不适用	0	0	0	0	0	0
4	办公网区域	符合	1	4	0	0	3	0
		部分符合	0	0	0	1	0	0
		不符合	0	0	1	0	0	1
		不适用	0	0	0	0	0	0

附录 C 表-6 安全区域边界单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.4 安全计算环境

C.4.1 网络设备

附录 C 表-7 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	汇聚交换机	符合	3	4	3	4	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	1	0	0	1	1	--
2	核心交换机	符合	3	4	3	4	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
		不适用	0	0	0	1	1	0	0	1	1	--

C.4.2 安全设备

附录 C 表-8 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	基线核查系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
2	上网行为管理系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
3	WEB应用防火墙	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
4	防火墙-1	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
5	防火墙-2	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
6	日志审计系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
7	运维安全	符合	3	4	3	5	0	0	1	1	0	--
		部分符	0	0	0	0	0	0	0	0	0	--

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
	管理系统	合										
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--

C.4.3 服务器和终端

附录 C 表-9 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	应用/数据库服务器	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
2	业务终端-2	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
3	业务终端-1	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
4	运维及管理终端-2	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
5	运维及管理终端-1	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--

C.4.4 系统管理软件/平台

附录 C 表-10 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	应用/数据库服务器-Tomcat	符合	0	4	3	2	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	3	0	0	3	1	1	0	0	0	--
2	应用/数据库服务器-Oracle	符合	3	4	3	2	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	0	0	0	3	1	1	0	0	0	--

C.4.5 业务应用系统/平台

附录 C 表-11 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	OA系统	符合	3	4	3	3	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	0	0	0	2	1	1	0	0	0	--

C.4.6 数据资源

附录 C 表-12 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	重要个人信息	符合	--	--	--	--	--	--	1	1	0	2
		部分符合	--	--	--	--	--	--	0	0	0	0
		不符合	--	--	--	--	--	--	0	1	0	0
		不适用	--	--	--	--	--	--	0	0	1	0
2	重要业务数据	符合	--	--	--	--	--	--	1	1	0	0
		部分符合	--	--	--	--	--	--	0	0	0	0
		不符合	--	--	--	--	--	--	0	1	0	0

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
		不适用	--	--	--	--	--	--	0	0	1	2

C.4.7 其他系统或设备

附录 C 表-13 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	--	符合	--	--	--	--	--	--	--	--	--	--
		部分符合	--	--	--	--	--	--	--	--	--	--
		不符合	--	--	--	--	--	--	--	--	--	--
		不适用	--	--	--	--	--	--	--	--	--	--

C.5 安全管理中心

附录 C 表-14 安全管理中心单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求	
			系统管理	审计管理
1	管理中心	符合	1	2
		部分符合	0	0
		不符合	1	0
		不适用	0	0

附录 C 表-15 安全管理中心单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.6 安全管理制度

附录 C 表-16 安全管理制度单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求			
			安全策略	管理制度	制定和发布	评审和修订
1	制度文件、执行/记录文件	符合	1	2	2	1
		部分符合	0	0	0	0
		不符合	0	0	0	0
		不适用	0	0	0	0

C.7 安全管理机构

附录 C 表-17 安全管理机构单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求				
			岗位设置	人员配备	授权和审批	沟通和合作	审核和检查
1	制度文件、执行/记录文件	符合	2	1	2	3	0
		部分符合	0	0	0	0	1
		不符合	0	0	0	0	0
		不适用	0	0	0	0	0

C.8 安全管理人员

附录 C 表-18 安全管理人员单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求			
			人员录用	人员离岗	安全意识教育和培训	外部人员访问管理
1	制度文件、执行/记录文件	符合	2	1	1	2
		部分符合	0	0	0	0
		不符合	0	0	0	1
		不适用	0	0	0	0

C.9 安全建设管理

附录 C 表-19 安全建设管理单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			定级和备案	安全方案设计	产品采购和使用	自行软件开发	外包软件开发	工程实施	测试验收	系统交付	等级测评	服务供应商选择
1	制度文件、执行/记录文件	符合	4	0	2	0	1	2	0	3	3	2
		部分符合	0	0	0	0	0	0	1	0	0	0
		不符合	0	3	0	0	1	0	1	0	0	0
		不适用	0	0	0	2	0	0	0	0	0	0

附录 C 表-20 安全建设管理单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.10 安全运维管理

附录 C 表-21 安全运维管理单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求												
			环境管理	资产管理	介质管理	设备维护管理	漏洞和风险管理	网络和系统安全管理	恶意代码防范管理	配置管理	密码管理	变更管理	备份与恢复管理	安全事件处置	应急预案管理	外包运维管理
1	制度文件、执行/记录文件	符合	3	1	2	2	0	5	2	1	0	1	3	3	2	0
		部分符合	0	0	0	0	0	0	1	0	0	0	0	0	0	0
		不符合	0	0	0	0	1	0	0	0	1	0	0	0	0	0
		不适用	0	0	0	0	0	0	0	0	1	0	0	0	0	2

附录 C 表-22 安全运维管理单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.11 其他安全要求指标

附录 C 表-23 其他指标单项测评结果汇总表

序号	测评对象	符合情况
本报告不涉及		

附录D 单项测评结果记录

D.1 安全物理环境

D.1.1 安全通用要求

D.1.1.1 信息化机房

安全控制点	测评指标	结果结论	符合程度
物理位置选择	a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；	（1）机房和办公场地场所在建筑物具有建筑验收文档，包含对防震、防风和防雨能力的说明； ■机房建设地址为：茂名市茂南区文明北路232号大院大楼 （2）机房和办公场地未出严重的问题。 ■无雨水渗透痕迹 ■无因风导致的较严重尘土 ■无屋顶、墙体、地面等破损开裂	符合
	b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	（1）机房未部署在易发生问题的位置； （2）机房对于空调设备的排水管等部位采取密封防漏处理； （3）机房对于楼板进行了防护措施。	符合
物理访问控制	机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。	（1）制定了《机房安全管理制度》，内容包含机房出入方面的管理规定； （2）对未配置电子门禁系统的出入口指定专人7*24小时负责机房出入，对出入的人员进行身份鉴别和登记，可查出入记录，且出入有专人陪同； （3）机房存在未配置门禁系统的开放出入口。	部分符合
防盗窃和防破坏	a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识；	（1）机房设备或主要部件都固定在机架上； （2）机房内对主要部件已绑定相应不易除去的标签； ■包括网络设备 ■包括安全设备 ■包括服务器 ■包括网络线缆 （3）重要机柜已进行上锁处理。	符合
	b) 应将通信线缆铺设在隐蔽安全处。	（1）通信线缆铺设在下走线槽隐蔽处中； （2）通信线缆设有明显的源目的标识； （3）通信线缆均铺设整齐、规范。	符合
防雷击	应将各类机柜、设施和设备等通过接地系统安全接地。	（1）机房设置专用地线； （2）机房内机柜、设施和设备等进行接地处理； （3）交流电源接地验收检测结果符合要求。	符合
防火	a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭	（1）机房采用经消防检测部门检测合格并在有效期内的（如 七氟丙烷）气体自动灭火设备，火灾自动报警类型为烟感+红外；	符合

安全控制点	测评指标	结果结论	符合程度
	火；	（2）自动消防系统工作状态正常，有定期巡检和维护记录《机房巡检记录表》； （3）建立机房消防的管理制度相关文档《机房安全管理制度》，按管理要求机房无人情况下气体灭火配置为自动模式，进入机房调整为手动模式，机房报警有7*24小时值班人员进行监控。	
	b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。	（1）机房及相关的工作房间和辅助房没有采用具有耐火等级的建筑材料； （2）缺乏机房防火设计文档； （3）缺乏机房防火验收文档。	不符合
防水和防潮	a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	（1）机房不存在雨水渗透、破损等不合规情况； （2）机房不位于建筑的顶层、边缘区域。	符合
	b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。	（1）机房区域范围已部署1台科华品牌（精密）空调，机房内分别配置1组温湿度传感器监控； （2）机房内空调下方已铺设安装好挡水和排水设施； （3）机房墙壁或楼板的管道采取必要的防渗防漏等防水保护措施； （4）机房安装检测设备（如：漏水检测绳）检测地下积水，及时处理机房水蒸气结露和地下积水的转移与渗透； （5）目前防水\防潮检测未发现异常情况，并且有防水防潮的运维记录《机房维护日志》。	符合
防静电	应采用防静电地板或地面并采用必要的接地防静电措施。	（1）对机房内设备（可导电金属线槽）采用了接地静电泄放措施； （2）机房未采用防静电地板或铺设防静电地毯。	不符合
温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。	（1）机房范围已部署1组科华品牌精密空调进行温湿度调节； （2）机房范围已部署空调及加湿机进行温湿度调节； （3）温湿度自动调节设施运作正常，有运行和维护记录《机房维护日志》； （4）机房温度能保持在24摄氏度到28摄氏度之间； （5）机房湿度能保持在40%到65%之间。	符合
电力供应	a）应在机房供电线路上配置稳压器和过电压防护设备；	（1）机房配备了稳压器和过电压防护设备； （2）稳压器和过电压防护设备正常工作； （3）机房具备电力供应安全设计，并在其中标明配备稳压器、过电压防护设备等要求。	符合
	b）应提供短期的备用电力	（1）机房配备了1组科华品牌UPS；	符合

安全控制点	测评指标	结果结论	符合程度
	供应，至少满足设备在断电情况下的正常运行要求。	（2）UPS正常工作，可满足主要设备断电情况下的至少1小时正常运行要求； （3）UPS有定期（至少每年）检查和维护，有运行和维护记录《机房巡检记录表》。	
电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。	（1）通信线缆铺设采用独立的具有电磁屏蔽作用线槽； （2）电源线缆铺设采用独立的具有电磁屏蔽作用线槽； （3）弱电线缆隔离铺设，没有干扰。	符合

D.2 安全通信网络

D.2.1 安全通用要求

D.2.1.1 安全通信网络

安全控制点	测评指标	结果结论	符合程度
网络架构	a）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；	（1）已对网络地址划分，且便于管理和控制； （2）网络地址划分采用核心交换机实现外网边界区域、服务器存储区域等的划分； （3）重要核心网络区域与非重要网络在同一网段； （4）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	部分符合
	b）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	（1）网络内重要网段未部署在网络边界处，且未直接连接外部信息系统； （2）系统通过防火墙对重要网段采取访问控制策略； （3）各安全域（子网）的出口唯一。	符合
通信传输	应采用校验技术保证通信过程中数据的完整性。	（1）网络系统中未涉及完整性保障设备，但在安全计算环境方面网络设备采用SSH协议、安全设备采用HTTPS协议、操作系统采用SSH协议、应用系统采用HTTPS协议来保证通信过程中数据的完整性。	符合
可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对通信设备可信验证方面的安全设计要求； （2）现有的通信设备存在未能实现操作系统到上层应用的信任链的情况，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■通信应用连接过程	不符合

D.3 安全区域边界

D.3.1 安全通用要求

D.3.1.1 办公网区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■办公网区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	符合
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问	符合

安全控制点	测评指标	结果结论	符合程度
		的能力。	
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略,无法检测、防止或限制从内部发起的网络攻击行为。	不符合
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试； （4）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	部分符合
安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备	（1）缺乏对边界设备可信验证方面的安全设	不符合

安全控制点	测评指标	结果结论	符合程度
	的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	

D.3.1.2 外网边界区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■外网边界区域 （2）网络边界处部署了可提供访问控制功能的设备； ■防火墙 ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	符合
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■防火墙 ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址	符合

安全控制点	测评指标	结果结论	符合程度
		■源端口 ■目的端口 ■协议	
	d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制,能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署支持对内部发起的攻击行为进行防范的设备； ■防火墙(带入侵防御模块) ■WEB应用防火墙 （2）现有的防范措施满足相应防护要求； ■所有关键网络边界均有检测措施 ■设备的规则库及时更新 ■检测(模块)符合国家相关产品检测要求 ■其安全策略有效 (3)内部安全防范措施能检测相应攻击行为。 ■端口扫描 ■强力攻击 ■木马后门攻击 ■拒绝服务攻击 ■缓冲区溢出攻击 ■碎片攻击 ■网络蠕虫攻击 ■应用漏洞攻击	符合
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试。	符合
安全审计	a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块)	符合

安全控制点	测评指标	结果结论	符合程度
		■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.3.1.3 安全管理区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■安全管理区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设	符合

安全控制点	测评指标	结果结论	符合程度
		备通过非法无线热点接入内部网络。	
访问控制	a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	不符合
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容	部分符合

安全控制点	测评指标	结果结论	符合程度
		性进行测试； （4）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	
安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.3.1.4 服务器存储区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和	（1）网络存在受保护的边界；	符合

安全控制点	测评指标	结果结论	符合程度
	数据流通过边界设备提供的受控接口进行通信。	■服务器存储区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■WEB应用防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视	（1）网络层部署支持对内部发起的攻击行为	符合

安全控制点	测评指标	结果结论	符合程度
	网络攻击行为。	进行防范的设备； ■WEB应用防火墙 （2）现有的防范措施满足相应防护要求； ■所有关键网络边界均有检测措施 ■设备的规则库及时更新 ■检测(模块)符合国家相关产品检测要求 ■其安全策略有效 （3）内部安全防范措施能检测相应攻击行为。 ■端口扫描 ■强力攻击 ■木马后门攻击 ■拒绝服务攻击 ■缓冲区溢出攻击 ■碎片攻击 ■网络蠕虫攻击 ■应用漏洞攻击	
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■WEB应用防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试。	符合
安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■WEB应用防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c）应对审计记录进行保	（1）网络层部署日志审计系统，统一接收及	符合

安全控制点	测评指标	结果结论	符合程度
	护，定期备份，避免受到未预期的删除、修改或覆盖等。	保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.4 安全计算环境

D.4.1 安全通用要求

D.4.1.1 网络设备

D.4.1.1.1 核心交换机

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括VTY认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的全局密码策略； ■Password control:Enabled ■Password aging:Enabled (180 days) ■Password length:Enabled (8 characters) ■Password composition:Enabled (4 types, 1 characters per type) （6）设备配置加密的super认证。	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备配置合规的全局登录失败处理策略； ■Password control: Enabled ■Maximum login attempts: 5 ■Action for exceeding login attempts: Lock user for 5 minutes	符合

安全控制点	测评指标	结果结论	符合程度
		（2）设备配置合规的操作超时退出措施。 ■VTY配置idle-timeout 15 0	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式。 ■未启用TELNET ■启用SSH	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； ■Information Center: Enabled ■Console: Enabled ■Monitor: Enabled ■Log host: Enabled 10.2.1.2 ■Security log file: Enabled （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间	符合

安全控制点	测评指标	结果结论	符合程度
		■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制； ■对ssh 登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）网络层相关设备不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的交换功能，不具备恶意代码防范模块，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配	（1）网络层设备不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	前得到完全清除。		
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.1.2 汇聚交换机

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括VTY认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的全局密码策略； ■Password control:Enabled ■Password aging:Enabled (180 days) ■Password length:Enabled (8 characters) ■Password composition:Enabled (4 types, 1 characters per type) （6）设备配置加密的super认证。	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备配置合规的全局登录失败处理策略； ■Password control: Enabled ■Maximum login attempts: 5 ■Action for exceeding login attempts: Lock user for 5 minutes （2）设备配置合规的操作超时退出措施。 ■VTY配置idle-timeout 15 0	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式。 ■未启用TELNET ■启用SSH	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令	符合

安全控制点	测评指标	结果结论	符合程度
		■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； ■Information Center: Enabled ■Console: Enabled ■Monitor: Enabled ■Log host: Enabled 10.2.1.2 ■Security log file: Enabled （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效；	符合

安全控制点	测评指标	结果结论	符合程度
		（5）日志及审计记录保存大于6个月。	
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制； ■对ssh 登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）网络层相关设备不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的交换功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要	符合

安全控制点	测评指标	结果结论	符合程度
		的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2 安全设备

D.4.1.2.1 WEB应用防火墙

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有	符合

安全控制点	测评指标	结果结论	符合程度
		唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，	（1）设备开启审计功能，审计进程正常；	符合

安全控制点	测评指标	结果结论	符合程度
	审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请	符合

安全控制点	测评指标	结果结论	符合程度
		表》。	
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.2 上网行为管理系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合

安全控制点	测评指标	结果结论	符合程度
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要	符合

安全控制点	测评指标	结果结论	符合程度
		的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.3 基线核查系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性；	符合

安全控制点	测评指标	结果结论	符合程度
		（4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆	符合

安全控制点	测评指标	结果结论	符合程度
	重要的用户行为和重要安全事件进行审计；	盖所有用户操作审计和记录。	
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成	符合

安全控制点	测评指标	结果结论	符合程度
		高风险的漏洞。	
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的基线核查功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要	不适用

安全控制点	测评指标	结果结论	符合程度
	数据定时批量传送至备用场地。	求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.4 日志审计系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合

安全控制点	测评指标	结果结论	符合程度
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 (2)设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合

安全控制点	测评指标	结果结论	符合程度
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施；	符合

安全控制点	测评指标	结果结论	符合程度
		■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.5 运维安全管理系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合

安全控制点	测评指标	结果结论	符合程度
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； (2)登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 (2)设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期	符合

安全控制点	测评指标	结果结论	符合程度
	他与审计相关的信息；	■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制。 ■对Web登录配置管理地址，限制登录范围	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备	（1）设备不具备相关可信验证的技术措施；	不符合

安全控制点	测评指标	结果结论	符合程度
	的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.6 防火墙-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合

安全控制点	测评指标	结果结论	符合程度
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方	（1）设备通过核心交换机的访问控制策略，	符合

安全控制点	测评指标	结果结论	符合程度
	式或网络地址范围对通过网络进行管理的管理终端进行限制；	通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要	符合

安全控制点	测评指标	结果结论	符合程度
		的完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.7 防火墙-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会	（1）设备启用合规登录失败处理策略； ■启用登录失败策略	符合

安全控制点	测评指标	结果结论	符合程度
	话、限制非法登录次数和当登录连接超时自动退出等相关措施；	■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型	符合

安全控制点	测评指标	结果结论	符合程度
		■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合

安全控制点	测评指标	结果结论	符合程度
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配	（1）网络层设备不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	前得到完全清除。		
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.3 服务器和终端

D.4.1.3.1 应用/数据库服务器

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）操作系统不存在空口令用户； ■etc/passwd文件中各用户的第二字段处不为空 ■/etc/shadow文件中各用户密码字段处不为空 （3）操作系统不存在默认信任的登录模式； （4）操作系统为登录用户设置的身份标识具有唯一性； ■UID具有唯一性 ■UID=0只能root用户 （5）操作系统配置的一定的密码长度且定期更换； ■PASS_MAX_DAYS 180 ■PASS_MIN_DAYS 1 ■PASS_MIN_LEN 8 ■PASS_WARN_AGE 28 （6）操作系统配置一定的密码复杂度策略。 ■minlen=8 ■ucredit=-2 ■lcredit=-1 ■dcredit=-4 ■ocredit=-1	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用pam_tally2模块的合规登录失败处理策略； auth required /lib/security/pam_tally.so onerr=fail no_magic_root和 account required /lib/security/pam_tally.so deny=10 no_magic_root reset （2）操作系统配置合规的操作超时锁定； ■配置具备以下措施：	符合

安全控制点	测评指标	结果结论	符合程度
		/etc/profile设置TMOUT=300 （3）操作系统启用SSH的合规登录超时策略。 ■配置具备以下措施： /sshd_config设置 ClientAliveInterval 60 ClientAliveCountMax 3	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）操作系统配置合规的远程管理模式； ■启用SSH （2）操作系统远程端口使用情况合规； ■21（FTP）未启用 ■23（Telnet）未启用 （3）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在所有用户均属于root组的情况。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统对多余帐户进行删除、锁定或禁止其登录； （2）操作系统账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； （2）操作系统不存在除root外的特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计功能，审计进程正常； ■rsyslog：loaded ■auditctl：enabled=1 （2）操作系统开启审计范围及策略满足要求，审计覆盖所有用户操作审计和记录。 ■rsyslog： *.info;mail.none;news.none;authpriv.none;cron.none /var/log/messages	符合

安全控制点	测评指标	结果结论	符合程度
		■auditctl： 关键目录、文件的审计行为采用 perm=rwxa	
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）操作系统针对日志、审计记录具备充足的存储容量； （3）操作系统采取合规的日志文件权限策略； ■/var/log/messages：640 ■/var/log/secure：640 ■/var/log/audit/audit.log：640 对审计记录进行定期存档备份，其备份策略有效 （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统关闭不必要端口； （2）操作系统禁用不必要服务； （3）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口； （4）漏洞扫描未发现高风险主机端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服edr防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证； ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序 （3）现有的可信验证缺乏以下措施。 ■对可信性破坏报警 ■将可信性验证结果形成审计记录 ■对可信性审计的动态关联感知	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对鉴别数据采取完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）系统在通信传输过程中对重要配置数据采取完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确	符合

安全控制点	测评指标	结果结论	符合程度
		的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为服务器设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统不保存过多终端历史记录。 ■通过echo $HISTSIZE查看history保留数目为30	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）本设备不存在此部分的控制需求，故此项不适用	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）本设备不存在此部分的控制需求，故此项不适用	不适用

D.4.1.3.2 业务终端-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟	符合

安全控制点	测评指标	结果结论	符合程度
	等相关措施；	■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败	符合

安全控制点	测评指标	结果结论	符合程度
		■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下：运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略	符合

安全控制点	测评指标	结果结论	符合程度
	进行限制；	要求下，统一集中管理远程登录地址。	
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据	符合

安全控制点	测评指标	结果结论	符合程度
		（2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.3 业务终端-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用	符合

安全控制点	测评指标	结果结论	符合程度
		户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户	（1）操作系统根据安全策略要求对特权用户进行分离；	符合

安全控制点	测评指标	结果结论	符合程度
	的权限分离。	■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1)操作系统采取对审计记录存储容量如下:运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用	符合

安全控制点	测评指标	结果结论	符合程度
		必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整	鉴别数据: （1）系统在通信传输过程中对相关数据采取	符合

安全控制点	测评指标	结果结论	符合程度
	性。	完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必	（1）操作系统不存在此部分的控制需求，不	不适用

安全控制点	测评指标	结果结论	符合程度
	需的用户个人信息；	适用。	
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.4 运维及管理终端-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 (5)用户属性策略未勾选“密码永不过期”。	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户	符合

安全控制点	测评指标	结果结论	符合程度
		权限分配表，系统现状与权限分配表情况一致。	
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到	(1)操作系统采取对审计记录存储容量如下:运维审计和日志记录 应用日志 1G、安全日	符合

安全控制点	测评指标	结果结论	符合程度
	未预期的删除、修改或覆盖等。	志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备；	符合

安全控制点	测评指标	结果结论	符合程度
		（5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施： 安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.5 运维及管理终端-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超	符合

安全控制点	测评指标	结果结论	符合程度
		时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败	符合

安全控制点	测评指标	结果结论	符合程度
		■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下：运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入	（1）操作系统不存在此部分的控制需求，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	的内容符合系统设定要求；		
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能	符合

安全控制点	测评指标	结果结论	符合程度
		发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.4 系统管理软件/平台

D.4.1.4.1 应用/数据库服务器-Oracle

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）数据库系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）数据库系统不存在弱口令用户； ■ORACLE数据库已修改默认口令 ■ORACLE数据库不存在空口令用户 （3）数据库系统为登录用户设置的身份标识具有唯一性； （4）数据库系统配置合规的密码长度及复杂	符合

安全控制点	测评指标	结果结论	符合程度
		度策略； ■PASSWORD_VERIFY_FUNCTION ，LIMIT=VERIFY_FUNCTION ■IF LENGTH(password) 值为8 ■PASSWORD_REUSE_MAX值为5 （5）数据库系统配置合规的密码有效周期策略。 ■PASSWORD_LIFE_TIME值为 180	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）数据库系统启用合规登录失败处理策略； ■ORACLE 数据库系统FAILED_LOGIN_ATTEMPTS= 10 （2）数据库系统执行合规的锁定策略。 ■PASSWORD_LOCK_TIME=1	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）数据库系统配置合规的远程管理模式。 ■ORACLE 数据库系统sqlnet.encryption为true ■ORACLE 数据库系统采用sqlplus连接数据库，客户端与服务器端之间通信是加密的	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）登录数据库系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （2）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在多用户均与sys、DBA用户权限一致的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）数据库系统对多余帐户进行删除、锁定或禁止其登录； ■数据库系统账户禁用不常用的默认用户 （2）数据库系统账户口令设置合规。 ■数据库系统各用户未使用空口令 ■数据库系统未使用弱口令或默认与用户名相同的口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）数据库系统不存在多余或过期账户； （2）数据库系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）数据库系统根据安全策略要求对特权用户进行分离； ■配置系统管理员 ■配置安全审计员 ■配置系统操作员 （2）数据库系统用户权限合理，非管理员未设置过大权限；	符合

安全控制点	测评指标	结果结论	符合程度
		■具备DBA角色的用户仅为 SYS、SYSTEM （3）数据库系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）数据库系统开启审计功能，审计进程正常； ■ORACLE 数据库系统audit_sys_operations=TRUE ■ORACLE 数据库系统audit_trail=DB （2）ORACLE数据库系统启动数据库日志模式和自动归档； ■Automatic archival=Enabled （3）审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）数据库宿主系统日期、时间正常； （2）数据库系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括重要用户行为 ■包括系统资源的异常使用情况 ■包括重要系统命令的使用 ■包括重要的安全相关事件	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）数据库系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）数据库系统针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）日志及审计记录保存大于6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）网络设备ACL策略有效限制访问本机的IP地址及管理模式。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）数据库系统不存在此部分的控制需求，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）数据库系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）数据库宿主系统不存在启用未加控制的高危端口； （3）MY_SQL分离默认安装的示例数据库； （4）数据库系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■SQLNET.ENCRYPTION_SERVER = REQUIRED ■SQLNET.ENCRYPTION_TYPES_SERVER = RC4_256 ■SQLNET.CRYPTO_CHECKSUM_SERVER = REQUIRED 重要配置数据: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■SQLNET.ENCRYPTION_SERVER = REQUIRED ■SQLNET.ENCRYPTION_TYPES_SERVER = RC4_256 ■SQLNET.CRYPTO_CHECKSUM_SERVER = REQUIRED	符合

安全控制点	测评指标	结果结论	符合程度
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）数据库系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）数据库系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）数据库系统未能提供异地数据备份功能。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）数据库系统不保存终端历史记录。	符合
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）数据库存储的用户个人信息均为业务应用必需的环节。	符合
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； ■包括信息采集 ■包括信息保存 ■包括信息访问 ■包括信息使用 （2）数据库具备控制措施禁止未授权访问用户个人信息表单； （3）数据库具备控制措施禁止非法使用用户个人信息表单。	符合

D.4.1.4.2 应用/数据库服务器-Tomcat

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）Tomcat中间件关闭web管理控制台，其身份鉴别功能由宿主操作系统实现，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）Tomcat中间件关闭web管理控制台，其身份鉴别功能由宿主操作系统实现，不适用。	不适用
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）Tomcat中间件关闭web管理控制台，其身份鉴别功能由宿主操作系统实现，不适用。	不适用
访问控制	a) 应对登录的用户分配账户和权限；	（1）对应不同的账户均按需分配不同的用户权限，不存在中间件用户均属于管理级别、高权限的情况； （2）中间件配置可降权启动Tomcat的用户； （3）宿主系统针对中间件用户分别赋予相应的管理操作权限。 ■包括审计权限 ■包括操作权限	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）中间件不存在除如:Tomcat、admin、manager、role1等默认账户名； （2）中间件账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）中间件不存在多余或过期账户； (2)中间件管理员用户与账户之间一一对应； （3）中间件启用合规的管理用户名配置。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）中间件根据安全策略要求对特权用户及宿主管理用户进行分离； （2）中间件管理不存在多个管理级别高的特权用户； （3）中间件管理按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）中间件开启审计功能，审计进程正常； ■开启Cataline引擎的日志文件 catalina.org.apache.juli.FileHandler.level = FINE ■开启内部代码丢出的日志 localhost.org.apache.juli.FileHandler.level = FINE ■开启manager应用日志 manager.org.apache.juli.FileHandler.level = FINE ■开启控制台输出的日志	符合

安全控制点	测评指标	结果结论	符合程度
		java.util.logging.ConsoleHandler.level = FINE ■开启Access访问日志。 server.xml文件配置正常，未被注释标记<!-- -->； （2）系统的日志审计级别满足要求。	
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）中间件日期、时间正常； （2）中间件审计记录开启审核策略且日志级别正常。 ■日志级别不低于“FINE” ■日志配置pattern值设为common ■日志配置pattern值为自定义格式，至少包含：%h %l %u %t %s	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）中间件限制审计文件的访问控制权限，普通用户不可删除及修改； ■localhost.log 644 ■catalina.log 644 ■host-manager.log 644 ■manager.log 644 （2）宿主系统针对中间件日志、审计记录具备充足的存储容量； ■日志存储在/log/tomcat/目录下 ■日志创建计划为每天/每周/每月 ■不限制最大日志文件大小 （3）对中间件审计记录进行定期存档备份，其备份策略有效； （4）审计记录及日志保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）中间件系统不存在此部分的安装控制需求，不适用。	不适用
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）Tomcat中间件的管理地址限制功能由宿主操作系统实现，故该项不适用。	不适用
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）中间件管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）中间件管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）中间件已根据需要不定期地对已发布的版本进行更新； （2）中间件更新安装前进行安全性和兼容性	符合

安全控制点	测评指标	结果结论	符合程度
		测试； （3）在系统上线或发生重大变更时测试并安装最新的中间件版本或更新补丁； （4）在不影响业务系统正常运行情况下，对发现的中间件漏洞在确保安全的情况下进行修补； （5）中间件进行扫描未发现存在可造成高风险的漏洞。	
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输 重要配置数据: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份的中间件重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）宿主系统定期完全依照备份策略，采用正确的配置进行本地备份；	符合

安全控制点	测评指标	结果结论	符合程度
		（4）中间件相关数据的备份周期合理：每天增量一次、每月全备一次； （5）中间件开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）宿主系统具有清除用户鉴别信息的功能； （2）经测试，宿主系统退出后无法访问先前中间件登录过的页面； （3）经测试，宿主系统关闭后无残留的中间件用户鉴别信息。	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用

D.4.1.5 业务应用系统/平台

D.4.1.5.1 OA系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）系统对各登录模式均启用身份鉴别； ■包括管理后台认证 （2）系统对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）系统登录用户设置的身份标识具有唯一性； （4）系统不存在空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）系统启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）系统配置合规的操作超时退出措施。 ■管理后台配置超时15分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃	（1）应用系统的用户鉴别数据采用SHA-512算法在可控网络环境中传输； （2）系统配置合规的远程管理模式。	符合

安全控制点	测评指标	结果结论	符合程度
	听。	■启用HTTPS	
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供系统权限分配表； （2）登录系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需分配不同的用户权限，不存在所有用户均属于管理级别、高权限的情况。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）系统禁用默认账户名； （2）系统账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）系统不存在多余或过期账户； （2）系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）系统不存在多个管理级别高的特权用户； （2）系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）系统开启审计功能，审计进程正常； （2）系统的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）系统日期、时间正常； （2）系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）系统针对日志、审计记录具备充足的存储容量； （3）审计记录及日志保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）应用软件系统不存在此部分的安装控制需求，不适用。	不适用
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）应用软件系统不存在此部分的控制需求，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）系统自身设定有效的终端访问策略，通过访问措施进行管理地址的限制。 ■系统管理页面仅能内网登录	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）系统具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）系统的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）系统已根据需要不定期地对已发布的版本进行更新； （2）在系统上线或发生重大变更时测试并安装最新的版本或更新补丁； （3）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）应用软件系统不存在此部分的控制需求，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）应用软件系统不存在此部分的控制需求，不适用。	不适用
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输	符合

安全控制点	测评指标	结果结论	符合程度
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）系统具有清除用户鉴别信息的功能； （2）经测试，系统退出后无法访问先前登录过的页面； （3）经测试，系统关闭后无残留的用户鉴别信息。	符合
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息； （3）系统采集的用户个人信息均为业务应用必需的环节。	符合
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）系统不采集和保存任何形式的用户个人信息； （2）系统对所有涉及个人信息的环节均有明确的授权同意过程； ■包括信息采集 ■包括信息保存 ■包括信息访问 ■包括信息使用 （3）系统具备控制措施禁止未授权访问用户个人信息； （4）系统具备控制措施禁止非法使用用户个人信息。	符合

D.4.1.6 数据资源

D.4.1.6.1 重要业务数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	（1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要业务数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份重要数据； ■包括重要业务数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）该测评项测评对象鉴别数据，已在安全计算环境层面其他对象判定，此项不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）该测评项测评对象为重要个人信息的内容，已在安全计算环境层面其他对象判定，该项不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）该测评项测评对象为重要个人信息的内容，已在安全计算环境层面其他对象判定，该项不适用。	不适用

D.4.1.6.2 重要个人信息

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	（1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要个人信息 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份重要数据； ■包括重要个人信息 （2）单位具备合理的重要数据的备份策略规范；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）该测评项测评对象鉴别数据，已在安全计算环境层面其他对象判定，此项不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息； （3）系统采集的用户个人信息均为业务应用必需的环节。	符合
	b）应禁止未授权访问和非法使用用户个人信息。	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； ■包括信息采集 ■包括信息保存 ■包括信息访问 ■包括信息使用 （2）系统具备控制措施禁止未授权访问用户个人信息； （3）系统具备控制措施禁止非法使用用户个人信息。	符合

D.4.1.6.3 鉴别数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	应用/数据库服务器-Oracle: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■SQLNET.ENCRYPTION_SERVER = REQUIRED ■SQLNET.ENCRYPTION_TYPES_SERVER	符合

安全控制点	测评指标	结果结论	符合程度
		= RC4_256 ■SQLNET.CRYPTO_CHECKSUM_SERVER = REQUIRED 应用/数据库服务器-Tomcat: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输 业务终端-1、业务终端-2、运维及管理终端-1、运维及管理终端-2: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 OA系统: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输 应用/数据库服务器: （1）系统在通信传输过程中对鉴别数据采取完整性保护措施。 ■使用SSH加密协议进行传输	

安全控制点	测评指标	结果结论	符合程度
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	该测评项在各系统及设备已做判定,数据资源针对鉴别数据不做判定	不适用
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	该测评项在各系统及设备已做判定,数据资源针对鉴别数据不做判定，不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	应用/数据库服务器-Tomcat: （1）宿主系统具有清除用户鉴别信息的功能； （2）经测试，宿主系统退出后无法访问先前中间件登录过的页面； （3）经测试，宿主系统关闭后无残留的中间件用户鉴别信息。 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）网络层设备不适用。 OA系统: （1）系统具有清除用户鉴别信息的功能； （2）经测试，系统退出后无法访问先前登录过的页面； （3）经测试，系统关闭后无残留的用户鉴别信息。 业务终端-1、业务终端-2、运维及管理终端-1、运维及管理终端-2: （1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施： 安全选项“不显示上次的用户名”->启用 应用/数据库服务器: （1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统不保存过多终端历史记录。 ■通过echo $HISTSIZE查看history保留数目为30 应用/数据库服务器-Oracle: （1）身份鉴别信息释放或清除机制正常且满足要求； （2）数据库系统不保存终端历史记录。	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	鉴别数据不存在此部分的控制需求,故此项不适用	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	鉴别数据不存在此部分的控制需求,故此项不适用	不适用

D.4.1.6.4 重要配置数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	OA系统: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输 应用/数据库服务器-Oracle: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■SQLNET.ENCRYPTION_SERVER = REQUIRED ■SQLNET.ENCRYPTION_TYPES_SERVER = RC4_256 ■SQLNET.CRYPTO_CHECKSUM_SERVER = REQUIRED 应用/数据库服务器-Tomcat: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 业务终端-1、业务终端-2、运维及管理终端-1、运维及管理终端-2: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必	符合

安全控制点	测评指标	结果结论	符合程度
		要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 应用/数据库服务器: （1）系统在通信传输过程中对重要配置数据采取完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）设备定义了相关重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 应用/数据库服务器-Tomcat: （1）系统定义了相关需要备份的中间件重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）宿主系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）中间件相关数据的备份周期合理：每天增量一次、每月全备一次； （5）中间件开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 业务终端-1、业务终端-2、应用/数据库服务器、运维及管理终端-1、运维及管理终端-2: （1）操作系统定义了相关重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 OA系统: （1）系统定义了相关需要备份重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 应用/数据库服务器-Oracle: （1）数据库系统定义了相关重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）数据库系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、运维安全管理系统、防火墙-1、防火墙-2: （1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 应用/数据库服务器-Oracle: （1）数据库系统未能提供异地数据备份功能。 OA系统、应用/数据库服务器-Tomcat: （1）单位未能提供异地数据备份措施。	不符合

安全控制点	测评指标	结果结论	符合程度
		业务终端-1、业务终端-2、运维及管理终端-1、运维及管理终端-2: （1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 应用/数据库服务器: （1）设备为服务器设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 核心交换机、汇聚交换机: （1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	重要配置数据不存在此部分的控制需求,故此项不适用	不适用
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	重要配置数据不存在此部分的控制需求,故此项不适用	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	重要配置数据不存在此部分的控制需求,故此项不适用	不适用

D.4.1.7 其他系统或设备

无

D.5 安全管理中心

D.5.1 安全通用要求

D.5.1.1 管理中心

安全控制点	测评指标	结果结论	符合程度
系统管理	a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；	（1）网络中部署运维安全管理系统实现集中的系统管理； （2）系统对登录用户进行身份鉴别； ■包括合规的用户名 ■包括合规的口令策略 （3）系统用户标识具有唯一性； ■不存在多人共享 ■增加、删除用户或权限变更需经过审批 （4）系统可实现对账户的身份鉴别数据进行	符合

安全控制点	测评指标	结果结论	符合程度
		保密性和完整性保护； （5）系统管理操作模式具备控制措施； ■只允许系统管理员登录 ■具备特定的登录命令 ■具备特定的登录操作界面 （6）系统具备相应的管理操作审计措施。 ■可实现对系统管理操作进行审计 ■审计范围覆盖所有用户 ■操作审计不可被删除	
	b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。	（1）系统管理员对系统的资源和运行进行配置、控制和管理； ■包括用户身份管理 ■包括资源配置管理 ■包括系统加载和启动管理 ■包括系统运行的异常处理管理 ■包括数据和设备的备份与恢复管理 （2）系统的资源、运行及配置管理不够全面。 ■缺乏可信证书管理 ■缺乏可信基准库管理	不符合
审计管理	a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；	（1）网络中部署运维安全管理系统实现集中安全审计功能； （2）审计系统对审计管理员进行身份鉴别； ■包括合规的用户名 ■包括合规的口令策略 （3）审计系统用户标识具有唯一性； ■不存在多人共享 ■增加、删除用户或权限变更需经过审批 （4）审计系统管理操作模式具备控制措施； ■只允许审计管理员登录 ■具备特定的登录命令 ■具备特定的登录操作界面 （5）审计系统具备相应的管理操作审计措施。 ■可实现对安全审计操作进行审计 ■审计范围覆盖所有审计管理用户 ■操作审计不可被删除	符合
	b）应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	OA系统： （1）审计管理员定期对审计记录进行分析，对发现的安全可疑事件及时处理； （2）单位具有安全审计策略文件，规范审计记录的存储、管理和查询要求； （3）审计管理员按规范要求对审计记录进行管理。 ■审计记录不可随意删除/修改	符合

安全控制点	测评指标	结果结论	符合程度
		■定期备份、存储审计记录 ■审计记录存储周期满足6个月要求 重要审计数据: 日志审计系统、运维安全管理系统: （1）设备在通信传输过程中对相关数据采取完整性保护措施; ■包括重要审计数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■网络设备、安全设备使用rsyslog协议进行传输 ■Linux操作系统使用rsyslog协议进行传输 ■Windows操作系统使用插件+SSL协议进行传输	

D.6 安全管理制度

D.6.1 安全通用要求

D.6.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。	（1）单位具有网络安全工作的总体方针和安全策略文件; ■具备独立的网络安全总体方针文件 ■具备涵盖网络安全总体方针策略要求的相关管理文件 ■具备安全策略文件 (2)制度内容包括明确的单位安全工作要求; ■安全目标 ■安全范围 ■安全原则 ■安全框架 ■各类安全策略 （3）管理文件详见《信息安全总体策略》。	符合
管理制度	a) 应对安全管理活动中的主要管理内容建立安全管理制度;	（1）单位有针对安全管理活动中的各类管理内容建立安全管理制度; (2)现有制度已覆盖管理活动的主要的方面; ■具备文件控制管理 ■具备安全检查管理 ■具备人力资源及培训 ■具备设备管理 ■具备软件开发/外包开发项目管理 ■具备机房安全管理 ■具备信息分类及管理	符合

安全控制点	测评指标	结果结论	符合程度
		■具备网络安全管理 ■具备系统安全管理 ■具备恶意代码管理 ■具备变更控制 ■具备备份及介质管理 ■具备事件管理 ■具备应急预案 （3）制度详见：《信息安全总体策略》、《网络安全管理规范》、《组织安全结构和人员职责制度》、《人员管理制度》、《员工考核管理制度》。	
	b）应对管理人员或操作人员执行的日常管理操作建立操作规程。	（1）单位针对相关业务日常管理的操作建立规程类管理制度； （2）现有制度已覆盖重要管理方面的系统维护手册和用户操作规程等； ■具备网络/安全管理 ■具备服务器管理 ■具备数据库管理 ■具备机房硬件设施管理 ■具备业务应用管理 （3）管理文件详见《设备及系统软件配置和操作手册》。	符合
制定和发布	a）应指定或授权专门的部门或人员负责安全管理制度的制定；	（1）单位针对安全管理制度的制定，指定教育信息与网络中心部主要负责； （2）在已制定的相关制度中可查阅到被授权制定管理制度的部门/人员信息； （3）管理文件详见《安全管理组织规范》。	符合
	b）安全管理制度应通过正式、有效的方式发布，并进行版本控制。	（1）单位针对制度的制定和发布要求，制定管理规范文件； （2）管理规范文件对文件制定及发布定义了规范要求； ■包括安全管理制度的制定和发布程序 ■包括格式要求 ■包括版本编号要求 （3）安全管理制度的收发登记记录有效； ■具备通过正式、有效的方式收发 ■具备正式发文 ■具备领导签署、单位盖章等 （4）管理文件详见《制度制定、发布、评审和修订管理制度》、《收发文登记记录》。	符合
评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需	（1）单位针对制度的合理性和适用性需进行论证和审定及修订的要求，制定管理规范文件；	符合

安全控制点	测评指标	结果结论	符合程度
	要改进的安全管理制度进行修订。	（2）管理规范文件对制度的评审及修订定义了规范要求； （3）单位具有安全管理制度的审定或论证的过程记录； （4）单位对做过修订的制度，具备有修订版本的安全管理过程记录； （5）管理文件详见《制度制定、发布、评审和修订管理制度》及 《安全管理制度评审记录》。	

D.7 安全管理机构

D.7.1 安全通用要求

D.7.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
岗位设置	a) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；	（1）单位已明确网络安全管理工作的职能部门，并明确了各岗位职责； ■已设置机房管理员 ■已设置网络管理员 ■已设置安全管理员 （2）单位各部门职责文档已明确网络安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备网络安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	符合
	b) 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。	（1）单位已明确系统安全管理工作的职能部门，并明确了各岗位职责； ■已设置系统管理员 ■已设置数据管理员 ■已设置审计管理员 ■已设置应用管理员 （2）单位各部门职责文档已明确系统安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备系统安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	符合
人员配备	应配备一定数量的系统管理员、审计管理员和安全管理员等。	（1）单位针对人员配备要求，制定了管理制度； （2）单位按要求配备一定数量的重要岗位管理人员； （3）单位针对各岗位人员，制定并维护人员档案；	符合

安全控制点	测评指标	结果结论	符合程度
		(4) 管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	
授权和审批	a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等;	(1) 单位在制度中用文字描述或在流程图中明确，对关键活动进行审批; ■具备部门职责文档明确各部门审批事项 ■具备岗位职责文档明确各岗位审批事项 (2) 单位对审批过程明确审批权限，对各项信息系统的重要操作与变更明确审批部门和批准人; (3) 管理文件详见《授权和审批管理规定》。	符合
	b) 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。	(1) 单位针对各项业务操作及变更等建立了审批程序规定; ■包括系统变更 ■包括重要操作 ■包括物理访问 ■包括系统接入 (2) 单位针对系统变更、系统接入、物理范围等事项已明确按审批程序执行,记录有批准人签字; (3) 管理文件详见《授权和审批管理规定》。	符合
沟通和合作	a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题;	(1) 单位针对机构内部管理人员之间、部门之间的沟通与合作，制定了管理制度; (2) 单位的管理制度规范了合作和沟通的方式和周期; (3) 单位有组织机构内部人员联系表; (4) 单位有定期召开信息安全会议，保存有会议纪要; (5) 管理文件详见《安全教育和培训制度》、《技能培训记录》《外部联系表》。	符合
	b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通;	(1)单位针对加强与外部单位的合作与沟通，制定了管理制度规定; ■包括公安机关 ■包括网络安全职能部门 ■包括职能监管机构 ■包括各类供应商 ■包括业界专家 ■包括安全组织 (2)单位能按要求与相关单位保持沟通合作，并提供相关单位联系方式和交流会议纪要; (3) 管理文件详见《安全教育和培训制度》、《技能培训记录》、《外部联系表》。	符合
	c) 应建立外联单位联系列表，包括外联单位名称、	(1) 单位建立了完善的对外联单位的联系列表;	符合

安全控制点	测评指标	结果结论	符合程度
	合作内容、联系人和联系方式等信息。	■记录单位名称 ■记录合作内容 ■记录联系人 ■记录联系方式 （2）管理文件详见《外部联系表》。	
审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。	（1）单位针对定期开展常规安全检查，制定了管理制度； （2）单位对检查工作的范围、过程、要求等管理的比较完善； ■系统日常运行 ■系统漏洞 ■数据备份 ■包括敏感系统检查人员 （3）单位已按要求由安全管理员定期检查，检查内容需覆盖系统运行相关的管理活动，并能提供安全检查报告； （4）管理文件详见《安全审查和检查管理规范》； （5）单位开展的检查工作不够完善。 ■未定期检查	部分符合

D.8 安全管理人员

D.8.1 安全通用要求

D.8.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
人员录用	a) 应指定或授权专门的部门或人员负责人员录用；	（1）单位授权专门的部门负责人员录用工作，制定了管理制度规范； （2）由人力资源保障科负责人员录用工作； （3）管理文件详见《人员管理制度》。	符合
	b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查。	（1）单位针对人员录用过程，制定了明确要求，并形成人员安全管理制度； （2）单位现有管理制度明确说明录用人员应具备的条件； ■包括学历/学位要求 ■包括技术人员的专业技术要求 ■包括管理人员的安全管理要求 （3）单位按规定执行人员录用的相关审查过程； ■包括录用人身份 ■包括安全背景 ■包括专业资格 ■包括资质 （4）管理文件详见《人员管理制度》、《人	符合

安全控制点	测评指标	结果结论	符合程度
		员入职考核记录》。	
人员离岗	应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。	（1）单位针对离岗人员权限终止及取回机构提供的各种设施的要求，制定了管理制度； （2）单位按规范开展对离岗人员的相关管理工作； ■明确负责部门 ■及时终止其访问权限 ■交还身份证件 ■交还软硬件设备 （3）管理文件详见《人员管理度》、《人员离岗申请表》、《离场信息资料交接表》。	符合
安全意识教育和培训	应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。	（1）单位针对人员安全培训及责任和惩戒措施，制定了管理制度； （2）单位已开展安全意识教育及岗位技能培训 ■具备明确培训周期 ■具备有效的培训方式 ■具备清晰的培训内容 ■具备考核要求 （3）管理文件详见《安全教育和培训制度》。	符合
外部人员访问管理	a）应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；	（1）单位针对外部人员物理访问，制定了外部人员访问管理文档； ■明确允许外部人员访问的范围 ■明确外部人员进入的条件 ■明确外部人员进入的访问控制措施 （2）单位具备有效的外部人员访问重要区域的书面申请文档； ■具有申请人 ■具有申请原因 ■具有范围 ■具有日期 ■具有批准人签字 （3）单位具备外部人员访问重要区域的登记记录； ■记录进入时间、 ■记录离开时间 ■记录访问区域 ■记录陪同人信息 （4)管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。	符合
	b）应在外部人员接入受控	（1）单位针对外部接入受控网络访问系统，	符合

安全控制点	测评指标	结果结论	符合程度
	网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；	制定了管理制度； （2）单位具备外部人员接入受控网络前的申请审批流程； （3）单位具备外部人员接入及访问系统的书面申请文档； ■具有申请人 ■具有申请原因 ■具有访问权限 ■具有日期 ■具有批准人签字 （4）单位具备外部人员接入及访问系统的登记记录； ■记录访问权限 ■记录访问时限 ■记录账户 （5）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。	
	c）外部人员离场后应及时清除其所有的访问权限。	（1）单位针对人员离场后的清理工作，制定了管理制度； （2）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》； （3）单位未完全按管理规范开展人员离场后的清理工作。 ■缺乏清理记录 ■未及时清除离场后的所有访问权限 ■未记录访问权限清除时间	不符合

D.9 安全建设管理

D.9.1 安全通用要求

D.9.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
定级和备案	a）应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；	（1）单位的被测系统于2022年4月已完成备案； （2）系统备案相关文档（定级报告）中明确等级划分方法和理由，SAG三个方面的级别描述清晰； （3）管理文件详见《定级备案》。	符合
	b）应组织相关部门和有关安全技术专家对定级结果	（1）单位针对系统定级结果的审批及评审工作等要求，制定了管理制度；	符合

安全控制点	测评指标	结果结论	符合程度
	的合理性和正确性进行论证和审定；	（2）现有系统的定级已具备合理性和正确性审定； ■具备单位部门审定 （3）管理文件详见《定级备案》。	
	c）应保证定级结果经过相关部门的批准；	（1）单位针对系统定级结果的上级批准要求，制定了管理制度； （2）现有系统的定级获得了相关部门的批准； （3）管理文件详见《定级备案》。	符合
	d）应将备案材料报主管部门和相应公安机关备案。	（1）单位对被测系统的等级备案表、定级报告等备案材料已经报相应公安机关备案； （2）单位具备公安机关出具的备案号； （3）管理文件详见《定级备案》。	符合
安全方案设计	a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；	（1）单位未具备适用于被测系统的安全规划设计方案； （2）现有方案文档未能完全按照规范要求选择安全措施。 ■缺乏安全保护等级的要求 ■缺乏风险分析结果的要求 ■缺乏实际安全需求	不符合
	b）应根据保护对象的安全保护等级进行安全方案设计；	（1）单位未具备完整的安全设计方案相关的文档。 ■缺乏总体规划 ■缺乏安全设计方案 ■缺乏相关配套文件 ■缺乏保护对象的安全保护等级要求	不符合
	c）应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； ■缺乏安全整体规划 ■缺乏安全设计方案 ■缺乏安全配套文件 （2）单位未对相关论证过程及内容进行完整的记录。	不符合
产品采购和使用	a）应确保网络安全产品采购和使用符合国家的有关规定；	（1）单位已建立安全产品管理的相关管理规定； ■包括采购要求 ■包括使用要求 （2）单位具备安全产品采购流程及相关实施文档； （3）被测系统使用的安全产品具备销售许可资质； （4）安全产品具均为国内产品； （5）管理文件详见《设备安全管理制度》。	符合
	b）应确保密码产品与服务	（1）单位已建立密码产品与服务管理的相关	符合

安全控制点	测评指标	结果结论	符合程度
	的采购和使用符合国家密码管理主管部门的要求。	管理制度； ■包括采购要求 ■包括使用要求 （2）系统未使用密码产品； （3）管理文件详见《设备安全管理制度》。	
自行软件开发	a）应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。	不适用
	b）应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。	不适用
外包软件开发	a）应在软件交付前检测其中可能存在的恶意代码；	（1）单位针对软件交付前测试恶意代码的要求，制定了管理制度； （2）管理文件详见《外包开发软件管理规定》； （3）单位未在软件交付之前按要求对所有软件开展恶意代码检测。 ■缺乏恶意代码检测报告	不符合
	b）应保证开发单位提供软件设计文档和使用指南。	（1）单位制定软件开发项目验收要求，明确开发单位的提交材料； （2）开发单位提供软件日常维护和使用所需的文档； ■包括需求分析说明书 ■包括软件设计说明书 ■包括软件操作手册 （3）管理文件详见《外包开发软件管理规定》、《设备及系统软件配置和操作手册》。	符合
工程实施	a）应指定或授权专门的部门或人员负责工程实施过程的管理；	（1）单位针对专门的部门负责工程实施过程的管理要求，制定管理度； （2）单位由专岗负责系统建设的工程实施，且按照实施方案的要求对进度和质量进行控制； （3）管理文件详见《工程实施管理制度》。	符合
	b）应制定安全工程实施方案控制工程实施过程。	（1）单位制定了详细的工程实施方案； ■包括工程时间限制 ■包括进度控制 ■包括质量控制 （2）工程实施单位严格按照方案执行，并有过程记录； （3）管理文件详见《测试及验收方案》、《工程项目实施方案》。	符合
测试验收	a）应制订测试验收方案，并依据测试验收方案实施	（1）单位可提供被测系统的合规测试验收方案；	部分符合

安全控制点	测评指标	结果结论	符合程度
	测试验收，形成测试验收报告；	■包括测试人员 ■包括测试验收内容 ■包括现场操作过程 （2）管理文件详见《测试及验收方案》、《工程项目实施方案》； （3）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。 ■缺乏验收报告 ■缺乏报告审定意见	
	b）应进行上线前的安全性测试，并出具安全测试报告。	（1）单位对系统上线前需开展安全性测试的要求，制定管理制度； (2)管理文件详见《外包开发软件管理规定》、《系统交付管理》； （3）针对系统上线前的安全性测试工作存在问题。 ■缺乏测试报告	不符合
系统交付	a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；	（1）单位具备系统交付清单； （2）系统交付清单内容较详细； ■包括设备 ■包括软件 ■包括文档 （3）单位的清点工作较合规； ■已依据交付清单开展清点工作 （4）管理文件详见《系统交付管理》、《资产清单》。	符合
	b）应对负责运行维护的技术人员进行相应的技能培训；	（1）单位已对负责系统运行维护的技术人员进行了技能培训； （2）具备运维人员的培训记录； ■包括培训时间 ■包括培训地点 ■包括培训对象 ■包括培训内容 ■包括培训参与人员签字 （3）管理文件详见《系统交付管理》、《资产清单》、《系统交付清单》、《技能培训记录》。	符合
	c）应提供建设过程文档和运行维护文档。	（1）单位提供了系统建设过程中的文档； （2）单位提供了指导用户进行系统运维的文档和系统培训手册； （3）管理文件详见《系统交付管理》、《系统交付清单》、《设备及系统软件配置和操作手册》。	符合
等级测评	a）应定期进行等级测评，	（1）单位针对系统等级测评要求，制定管理	符合

安全控制点	测评指标	结果结论	符合程度
	发现不符合相应等级保护标准要求的及时整改；	制度； （2）系统按要求开展首次测评工作； （3）管理文件详见《系统安全管理制度》。	
	b）应在发生重大变更或级别发生变化时进行等级测评；	（1）管理制度中已规定在系统发生变更时及时对系统进行等级测评； （2）系统未发生过重大变更，系统等级未发生变化； （3）管理文件详见《系统安全管理制度》。	符合
	c）应确保测评机构的选择符合国家有关规定。	（1）已选择在“全国等级保护测评机构推荐目录”中的测评单位进行等级测评； （2）管理文件详见《系统安全管理制度》、《网络安全等级保护测评服务合同》。	符合
服务供应商选择	a）应确保服务供应商的选择符合国家的有关规定；	（1）单位在管理制度内明确提出安全服务供应商选择的要求； （2）单位选择的安全服务商符合国家的有关规定，具备相应的安全服务资质； （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。	符合
	b）应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。	（1）单位的管理制度中已规定，需与安全服务商签订安全相关的协议并明确整个服务供应链各方需履行的网络安全相关义务； （2）单位已按规定与选定的安全服务商签订合规的协议； ■明确整个服务供应链各方需履行的网络安全相关义务 ■包括保密范围 ■包括安全责任 ■包括违约责任 ■包括协议的有效期限 ■包括责任人签字 （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。	符合

D.10 安全运维管理

D.10.1 安全通用要求

D.10.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
环境管理	a）应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维	（1）单位建立机房安全方面的管理制度，对有关运维方面的管理作出规定； ■指定教育信息与网络中心部门负责管理 ■包括出入管理要求 ■包括定期维护要求	符合

安全控制点	测评指标	结果结论	符合程度
	护管理；	■包括空调要求 ■包括供配电设备要求 ■包括消防设施要求 ■包括温湿度控制要求 （2）单位具备完整的机房出入登记记录； ■记录来访人员 ■记录来访时间 ■记录离开时间 ■记录携带物品 （3）单位具备完整的机房基础设施的维护记录； ■记录维护日期 ■记录维护人 ■记录维护设备 ■记录故障原因 ■记录维护结果 （4）管理文件详见《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。	
	b）应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；	（1）单位建立机房安全方面的管理制度； ■包括物理访问管理 ■包括物品进出管理 ■包括环境安全管理 （2）单位现有机房管理记录与制度相符； ■具备物理访问记录 ■具备物品进出记录 ■具备环境安全相关记录 （3）制度详见：《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。	符合
	c）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	（1）单位机房安全管理制度已明确来访人员的接待区域的要求； （2）单位按规范要求开展人员来访接待； ■划分来访人员的接待区域 ■记录来访人员的情况 （3）单位办公环境未发现有随意放置含有敏感信息介质的情况； ■无纸档文件 ■无移动介质 （4）制度详见：《机房安全管理制度》、《物理安全管理规范》、《办公环境保密管理》。	符合

安全控制点	测评指标	结果结论	符合程度
资产管理	应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。	（1）单位已建立有效的资产清单； （2）单位现有资产清单内容较全面； ■包括设备设施类别 ■包括软件类别 ■包括文档类别 ■包括资产责任人 ■包括所属级别 ■包括所处位置 ■包括所处部门 （3）制度详见：《设备安全管理制度》、《资产清单》。	符合
介质管理	a）应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；	（1）介质按管理要求放置于受控的环境中（如：机房）； （2）介质管理具备较全面的记录； ■包括介质归档 ■包括使用情况 ■包括定期盘点记录 （3）制度详见：《设备安全管理制度》、《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。	符合
	b）应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。	（1）介质管理制度中对介质安全传输有明确规定； ■包括人员选择 ■包括打包要求 ■包括交付要求 （2）存储重要信息的介质在物理传输过程，具备严格的环节控制，无重大环节疏漏； （3）对介质的归档和查询均具备记录； （4）制度详见：《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。	符合
设备维护管理	a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	（1）单位人员岗位职责相关文档已明确设备维护管理的责任部门； （2）单位对各类设施、设备进行定期维护； （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。	符合
	b）应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过	（1）单位建立了配套设施、软硬件维护管理方面的管理制度； ■包括维护人员的责任 ■包括维修和服务的审批	符合

安全控制点	测评指标	结果结论	符合程度
	程的监督控制等。	■包括维修过程的监督控制 （2）单位开展相关工作与制度相符，且保留记录； ■包括维修和服务审批 ■包括维修过程记录 （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。	
漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。	（1）单位制定管理制度，规范对安全漏洞和隐患的检测、识别及评估修补要求； （2）制度详见：《恶意代码防范管理制度》； （3）单位未严格按规范开展漏洞及安全隐患检测工作。 ■未定期开展漏洞扫描	不符合
网络和系统安全管理	a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；	（1）单位建立系统安全管理文档，对系统管理员的管理制定了要求； ■包括角色划分 ■包括角色的责任 ■包括角色权限 （2）单位对各类关键角色建立了相应的工作职责文档； ■包括安全管理员 ■包括网络管理员 ■包括系统管理员 ■包括数据管理员 ■包括审计管理员 （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	符合
	b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	（1）单位制定管理制度，对系统账号进行管理； ■指定专人 ■包括申请账户管理 ■包括建立账户管理 ■包括删除账户管理 （2）单位按管理规范开展账号管理工作； ■具备相关审批流程 ■具备相关审批记录 ■具备管理登记记录 （3）账户管理记录内容较完整； ■包括变更日期 ■包括变更时间 ■包括变更人 ■包括变更设备/系统	符合

安全控制点	测评指标	结果结论	符合程度
		■包括变更结果 （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	
	c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	（1）单位建立了网络和系统安全管理制度； （2）网络和系统安全管理制度内容较全面； ■包括安全策略要求 ■包括账户管理 ■包括配置文件的生成及备份 ■包括变更审批管理 ■包括授权访问 ■包括最小服务控制 ■包括升级与打补丁管理 ■包括审计日志管理 ■包括口令管理 （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	符合
	d）应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；	（1）单位对重要设备、系统的配置和操作建立配置手册； ■包括操作系统 ■包括数据库 ■包括网络设备 ■包括安全设备 ■包括应用和组件 （2）现有操作配置手册已明确操作步骤、参数配置； （3）制度详见：《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。	符合
	e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。	（1）单位制定日常运维管理的相关制度规范； （2）单位按制度规范开展日常运维管理工作； （3）单位具备合规的运维记录； ■包括日常巡检记录 ■包括运行维护记录 ■包括参数的设置记录 ■包括参数的修改记录 （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》、《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。	符合
恶意代码防范管理	a）应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	（1）单位制定恶意代码防范管理制度，明确对外来计算机或存储设备接入系统前进行恶意代码检查； （2）单位按外来计算机接入恶意代码检查规范开展工作；	符合

安全控制点	测评指标	结果结论	符合程度
		■对外来计算机接入进行恶意代码检查 ■具备合规的检测记录 （3）单位制定培训管理制度，明确需通过培训提升员工的防恶意代码意识； （4）单位按培训管理要求开展工作； ■定期对员工开展防恶意代码意识培训 ■具备合规的培训记录 （5）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申请表》、《信息管理系统漏洞检查表》。	
	b）应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；	（1）建立恶意代码防范管理文档； （2）管理制度中覆盖防恶意代码软件的授权使用、恶意代码库升级、定期查杀等内容； （3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》。	符合
	c）应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。	（1）单位指定专门的部门负责定期验证防范恶意代码攻击的技术措施的有效性； （2）单位近期未发生过严重的恶意代码攻击事件； （3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申请表》、《信息管理系统漏洞检查表》； （4）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。 ■未定期对相关产品的恶意代码库进行升级 ■未对所有防病毒产品上截获的恶意代码进行分析并汇总上报	部分符合
配置管理	应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。	（1）单位制定了基本配置信息管理的制度要求； ■包括网络拓扑结构 ■包括设备安装的软件组件 ■包括软件组件的版本 （2）管理文件详见：《主机安全管理规范》、《网络安全管理规范》、《应用安全管理规范》、《网络配置信息》。	符合
密码管理	a）应遵循密码相关国家标准和行业标准；	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	不符合
	b）应使用国家密码管理主管部门认证核准的密码技术和产品。	（1）单位未采购涉及密码技术的产品，不适用。	不适用
变更管理	应明确变更需求，变更前	（1）单位建立了关于系统变更管理的制度文	符合

安全控制点	测评指标	结果结论	符合程度
	根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。	件； （2）现有变更管理制度覆盖了变更管理的各方面要求； ■包括变更管理要求 ■包括整体变更管理流程 ■包括变更内容分析与论证 ■包括变更方案审批流程 ■包括变更后通报 （3）制度详见：《变更控制管理制度》、《通用变更记录表》。	
备份与恢复管理	a）应识别需要定期备份的重要业务信息、系统数据及软件系统等；	（1）单位根据业务重要程度，制定了需要定期备份的重要业务信息列表或清单。清单内需要定期备份的重要数据已经过用户方确认； （2）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。	符合
	b）应规定备份信息的备份方式、备份频度、存储介质、保存期等；	（1）单位建立了备份与恢复管理相关的安全管理制度； （2）备份与恢复管理的相关要求比较明确； ■规定备份方式 ■规定备份频度 ■规定存储介质 ■规定保存期 （3）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。	符合
	c）应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	（1）单位现有管理制度，明确了数据备份策略和数据恢复策略，以及备份程序和恢复程序； （2）单位可按策略要求实现重要数据的定期备份与恢复性测试； （3）单位现有的备份的数据均经过恢复性测试，可确保备份的数据可用； （4）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。	符合
安全事件处置	a）应及时向安全管理部门报告所发现的安全弱点和可疑事件；	（1）单位已在安全培训及宣传过程中告知用户在发现安全弱点和可疑事件时及时向安全管理部门报告； （2）单位在系统运维过程中对发现的安全弱	符合

安全控制点	测评指标	结果结论	符合程度
		点和可疑事件均编制了对应的报告或相关文档； （3）单位现有安全弱点和可疑事件报告文档内容较详实； （4）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	
	b）应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；	（1）单位制定了安全事件报告和处置管理制度； （2）现有安全事件管理制度内容较完整； ■包括安全事件类型分类 ■包括安全事件有关的工作职责 ■包括安全事件的报告 ■包括安全事件的处置 ■包括安全事件的响应流程 （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	符合
	c）应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。	（1）单位具备对安全事件的分析、处理、总结、防范等的报告／过程文档； （2）单位提供的安全事件报告和响应处置记录内容较完整； ■记录引发安全事件的原因 ■记录事件的证据 ■记录处置过程 ■包括经验教训 ■提出补救措施 （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	符合
应急预案管理	a）应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；	（1）单位制定重要事件的应急预案； （2）单位现有应急预案涉及的类型范围较全面； ■包括针对机房的预案 ■包括针对网络传输的预案 ■包括针对网络设备的预案 ■包括针对操作系统的预案 ■包括针对数据库的预案 ■包括针对安全漏洞攻击的预案 ■包括针对恶意代码的预案 ■包括针对数据泄露的预案 （3）单位现有应急预案的内容较完整； ■明确重要事件的应急处理流程 ■明确系统恢复流程等内容 （4）制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。	符合

安全控制点	测评指标	结果结论	符合程度
	b) 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。	(1)单位定期对相关人员进行应急预案培训； (2) 单位根据不同的应急预案，按要求进行应急演练； (3) 单位具备近期应急预案工作开展的相关记录； ■具备培训记录 ■具备演练记录 (4)单位提供的应急预案培训记录比较完整； ■明确培训对象 ■明确培训内容 ■明确培训结果 (5)单位提供的应急预案演练记录比较完整； ■记录演练时间 ■记录主要操作内容 ■记录演练结果 (6) 经检查单位目前一旦出现应急事件，可参照预案合理有序的进行应急事件处置过程； (7) 制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。	符合
外包运维管理	a) 应确保外包运维服务商的选择符合国家的有关规定；	(1)单位目前未涉及任何外包运维服务情况，不适用。	不适用
	b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。	(1)单位目前未涉及任何外包运维服务情况，不适用。	不适用

D.11 其他安全要求

本次测评不涉及其他安全要求指标。

附录E 漏洞扫描结果记录

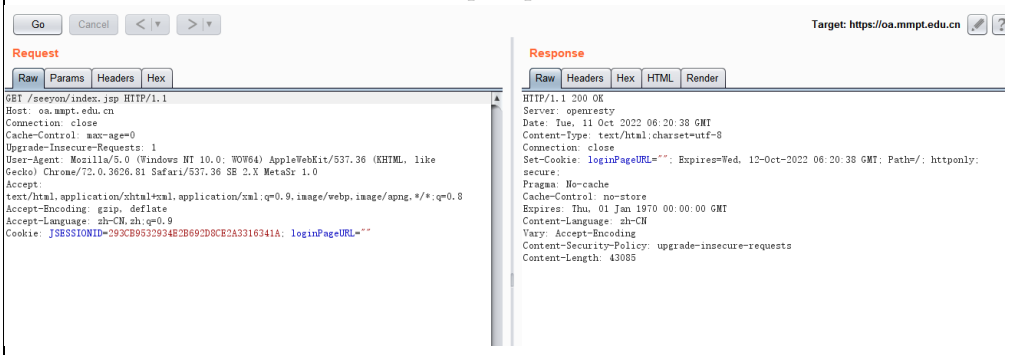
附录E表-1漏洞扫描主要安全漏洞

序号	危险程度	漏洞名称	影响IP
1	中	SSH 服务支持弱加密算法【原理扫描】 此类漏洞涉及服务器存储设备。	10.2.3.10/应用/数据库服务器
2	低	允许Traceroute探测 此类漏洞涉及安全设备、网络设备。	10.2.1.4/运维安全管理系统 10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/上网行为管理系统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/汇聚交换机 172.16.1.2/核心交换机
3	低	OpenSSH CBC模式信息泄露漏洞	10.2.3.10/应用/数据库服务器

序号	危险程度	漏洞名称	影响IP
		(CVE-2008-5161) 此类漏洞涉及服务器存储设备、网络设备。	172.16.1.2/核心交换机
4	低	OpenSSH 信息泄露漏洞(CVE-2011-4327) 此类漏洞涉及服务器存储设备。	10.2.3.10/应用/数据库服务器
5	低	OpenSSH 本地信息泄露漏洞 (CVE-2016-10011) 此类漏洞涉及服务器存储设备。	10.2.3.10/应用/数据库服务器

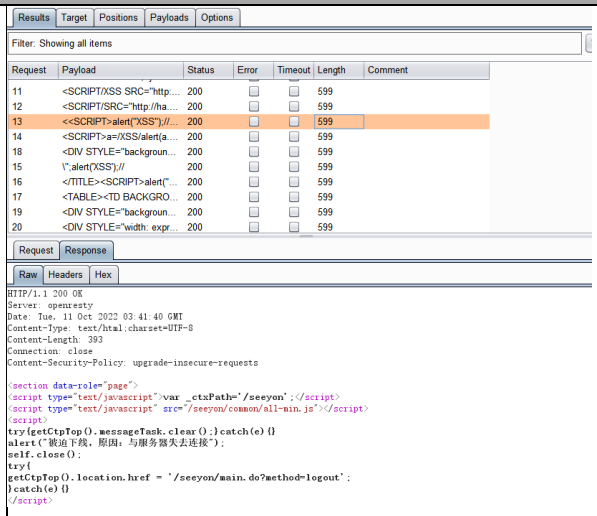
附录F 渗透测试结果记录

F.1 业务应用软件平台 缺少“X-Content-Type-Options”响应头

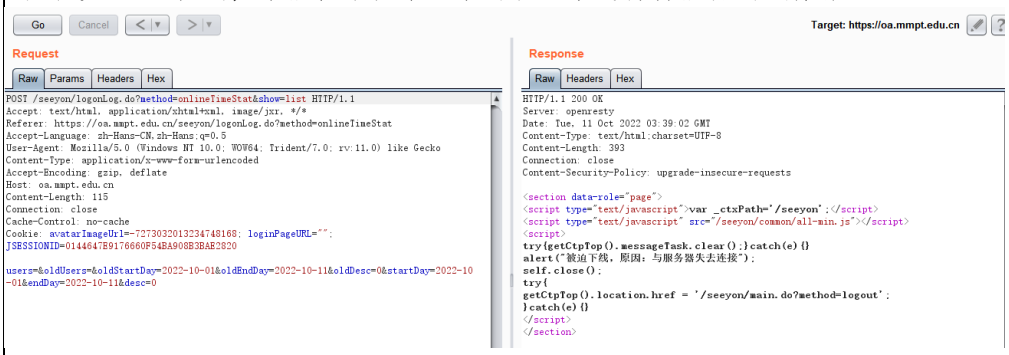
缺少“X-Content-Type-Options”响应头	
危险程度	低
渗透位置	JB,JC
影响URL实体	https://oa.mmpt.edu.cn/seeyon/index.jsp
渗透详情	渗透方法：BurpSuite抓包检测 采用的工具：BurpSuite 测试过程：响应包中没有X-Content-Type-Options响应头，如下图：  	

F.2 业务应用软件平台 XSS跨站脚本攻击

XSS跨站脚本攻击	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：测试是否对客户端输入的HTML代码、客户端脚本进行过滤或限制。 采用的工具：Burpsuite 测试过程：经检测，已对客户端输入的HTML代码、客户端脚本进行过滤或限制，暂未发现该漏洞。

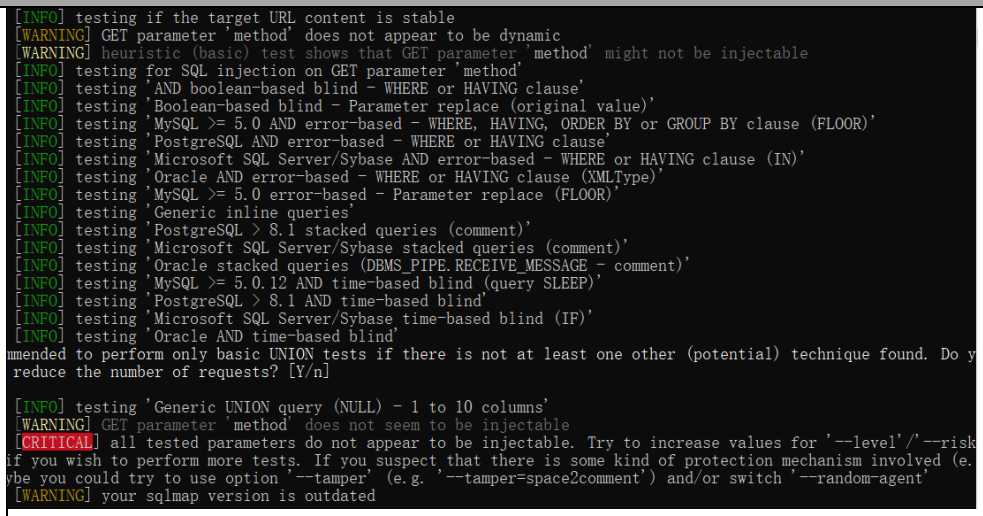
XSS跨站脚本攻击	
	

F.3 业务应用软件平台 未授权访问

未授权访问	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：测试能否在系统未登录的状态下进行登录后功能访问或操作。 采用的工具：Burpsuite 测试过程：已检测，不能在系统未登录的状态下进行功能访问或操作。 

F.4 业务应用软件平台 SQL注入漏洞

SQL注入漏洞	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：通过手工或工具检测系统在执行SQL语句时是否存在注入。 采用的工具：Sqlmap 测试过程：已检测，系统在执行SQL语句时不存在注入，暂未发现该漏洞。

SQL注入漏洞	
	

附录G 威胁列表

附录G 表- 1威胁列表

序号	威胁列表	描述
1	恶意攻击	利用工具和技术对信息系统进行攻击和入侵。威胁行为包括：恶意代码、邮件勒索、网络攻击等。
2	软硬件故障	对业务实施或系统运行产生影响的设备硬件故障、通讯链路中断、系统本身或软件缺陷造等问题。威胁行为包括：设备故障、软件故障等。
3	管理不到位	由于制度缺失、不完善等原因导致安全管理无法落实或者不到位。威胁行为包括：管理不到位、媒体负面报道等。
4	无作为或操作失误	应该执行而没有执行相应的操作，或者无意执行了错误的操作。威胁行为包括：操作失误、维护错误等。
5	敏感信息泄漏	敏感信息泄露给不应了解的他人。威胁行为包括：内部信息泄露、外部信息泄露等。
6	物理环境影响	对信息系统正常运行造成影响的物理环境问题和自然灾害。威胁行为包括：物理损害等。
7	越权或滥用	越权访问本来无权访问的资源，或者滥用自己的权限破坏信息系统。威胁行为包括：未授权的设备使用、权限滥用、权限伪造等。
8	物理攻击	通过物理的接触造成对软件、硬件和数据的破坏。威胁行为包括：设备失效等。
9	篡改	非法修改信息，破坏信息的完整性使系统的安全性降低或信息不可用。威胁行为包括：硬件篡改、数据篡改等。
10	抵赖	否认所做的操作。威胁行为包括：行为否认（抵赖）、媒体负面报道等。

报告编号：44090243008-00003-22-0163-01

网络安全等级保护
财务管理系统等级测评报告

委托单位：茂名职业技术学院

测评单位：广东南方信息安全研究院

报告时间：2022年10月30日

网络安全等级测评基本信息表

被测对象				
被测对象名称	财务管理系统		安全保护等级	第二级（S2A2）
备案证明编号	44090243008-00003			
被测单位				
单位名称	茂名职业技术学院			
单位地址	广东省茂名市茂南区文明北路232号大院		邮政编码	525000
联系人	姓名	龙恒	职务/职称	教师
	所属部门	教育信息与网络中心	办公电话	0668-2920122
	移动电话	13377766618	电子邮件	372383968@qq.com
测评单位				
单位名称	广东南方信息安全研究院		机构代码	SC202127130010163
单位地址	广州市科学城彩频路9号B座12楼1202		邮政编码	510663
联系人	姓名	谢若雨	职务/职称	助理
	所属部门	办公室	办公电话	020-32290702
	移动电话	18819149895	电子邮件	office@cybersec-gd.cn
审核批准	编制人	林炳康	编制日期	2022.10.30
	审核人	李华	审核日期	2022.10.30
	批准人	陈林	批准日期	2022.10.30

声明

本报告是财务管理系统的等级测评报告。

本报告测评结论的有效性建立在被测评单位提供相关证据的真实性基础之上。

本报告中给出的测评结论仅对被测对象当时的安全状态有效。当测评工作完成后，由于被测对象发生变更而涉及到的系统构成组件（或子系统）本报告不再适用。

本报告中给出的测评结论不能作为对被测对象内部部署的相关系统构成组件（或产品）的测评结论。

在任何情况下，若需引用本报告中的测评结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。

单位名称：广东南方信息安全研究院

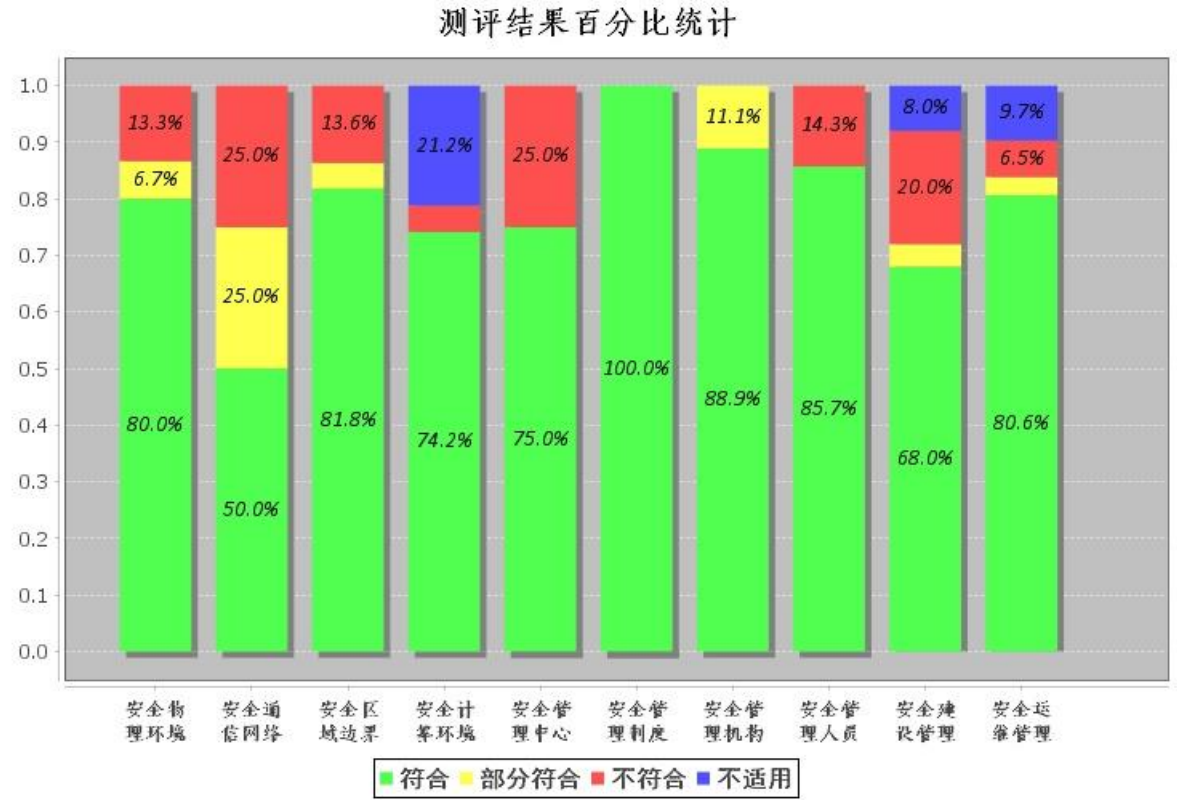
2022年10月30日

等级测评结论

测评结论和综合得分			
被测对象名称	财务管理系统	安全保护等级	第二级（S2A2）
扩展要求应用情况	□云计算 □移动互联 □物联网 □工业控制系统 □大数据		
被测对象描述	财务管理系统是由茂名职业技术学院统一组织规划建设，由天津神州浩天科技有限公司负责开发，于2019年1月正式投入运行，由教育信息与网络中心负责运行维护。茂名职业技术学院是该信息系统的业务主管部门，茂名职业技术学院为该信息系统定级的责任单位。 财务管理系统网络主要分为4个区域，分别为外网边界区域、安全管理区域、服务器存储区域、办公网区域，主要由网络设备、安全设备组成，对互联网提供业务访问。财务管理系统为B/S结构，主要由Windows平台的操作系统，MySQL、Oracle平台的数据库系统，及Tomcat中间件系统组成。单位采用自主运维模式，通过部署运维及管理终端提供专用运维环境管理，采用运维安全管理系统实现设备的统一管理，并进行操作运维审计，日志审计系统进行设备日志统一收集存储与分析。 财务管理系统包含财务核算、学生收费、预算管理、结算、工资管理功能模块，年终结转该系统通过专网与财政系统进行联通通信，涵盖学生收费、奖贷学金发放、预算管理、工资管理、工资结算等业务，是学校财务流转的核心业务系统。		
安全状况描述	财务管理系统通信传输具备一定的保护措施，安全区域边界较清晰，网络层具备访问控制、安全审计的相应技术措施。各设备在身份鉴别、访问控制、安全审计、入侵防范方面具备控制措施。重要数据在数据完整性、个人信息保护方面具备保护措施。在安全管理制度层面较为完善。在网络架构不够完整，网络层在入侵防范、恶意代码和垃圾邮件防范的技术措施存在不足。重要数据在数据备份恢复方面存在不足。 财务管理系统在本次测评中总共出现26类问题，其中0类高风险问题,11类中风险问题，15类低风险问题。在本次测评通过扫描及渗透发现3类漏洞问题，其中0类危险程度为高的漏洞，0类危险程度为中的漏洞，3类危险程度为低的漏洞。 财务管理系统本次等级测评的综合得分为73.85，且不存在高等级安全风险，等级测评结论为中。		
等级测评结论	中	综合得分	73.85

总体评价

通过对信息系统基本安全保护状态的分析，茂名职业技术学院针对财务管理系统面临的主要安全威胁采取了相应的安全机制，基本达到保护信息系统重要资产的作用。财务管理系统在本次测评中采用了GB/T 22239-2019，其中安全通用要求135项，不适用5项。



在安全物理环境方面，针对安全通用要求，基础设施在防雷击、电磁防护、防水和防潮、物理位置选择、电力供应、防盗窃和防破坏、温湿度控制等方面较为完善（如：信息化机房）。在物理访问控制、防静电等方面还不够完善（如：信息化机房），机房出入口未配置电子门禁系统，机房内缺乏防静电措施（如防静电地板或铺设防静电地毯）。

在安全通信网络方面,针对安全通用要求,网络环境在通信传输等方面较为完善(如:安全通信网络)。在网络架构等方面还不够完善（如：安全通信网络），关键的应用服务和数据库服务网段未独立进行子网划分的情况。

在安全区域边界方面，针对安全通用要求，网络环境在边界防护、安全审计、访问控制等方面较为完善（如：外网边界区域，安全管理区域，服务器存储区域等）。在入侵防范、恶意代码和垃圾邮件防范等方面还不够完善(如:安全管理区域,办公网区域)，网络层部署防火墙,防火墙未配置对内部发起的攻击行为实现防范功能策略,无法检测、防止或限制从内部发起的网络攻击行为,现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。

在安全计算环境方面，针对安全通用要求，计算环境在个人信息保护、安全审计、数据完整性、访问控制、入侵防范、恶意代码防范、身份鉴别、剩余信息保护等方面较为完善。在主机方面，在可信验证等方面还不够完善（如：数据库服务器-1，业务终端-2，业务终端-1等），缺乏对计算设备可信验证方面的安全设计要求，现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。在应用方面，在数据备份恢复等方面还不够完善（如：数据库服务器-1-MSSQL，数据库服务器-2-Oracle），未能提供数据库系统重要数据的异地定时数据备份功能。在网络及安全设备方面，在可信验证等方面还不够完善（如：基线核查系统，上网行为管理系统，WEB应用防火墙等），设备不具备相关可信验证的技术措施。在数据保护方面,在数据备份恢复等方面还不够完善(如:重要个人信息，重要业务数据），未能提供应用软件系统重要数据的异地定时数据备份功能。

在安全管理中心方面，针对安全通用要求，安全控制措施在审计管理等方面较为完善（如：管理中心）。在系统管理等方面还不够完善（如：管理中心），系统管理的资源、运行及配置管理不够全面。

在安全管理制度方面，针对安全通用要求，管理制度体系在制定和发布、安全策略、管理制度、评审和修订等方面较为完善（如：制度文件、执行/记录文件）。

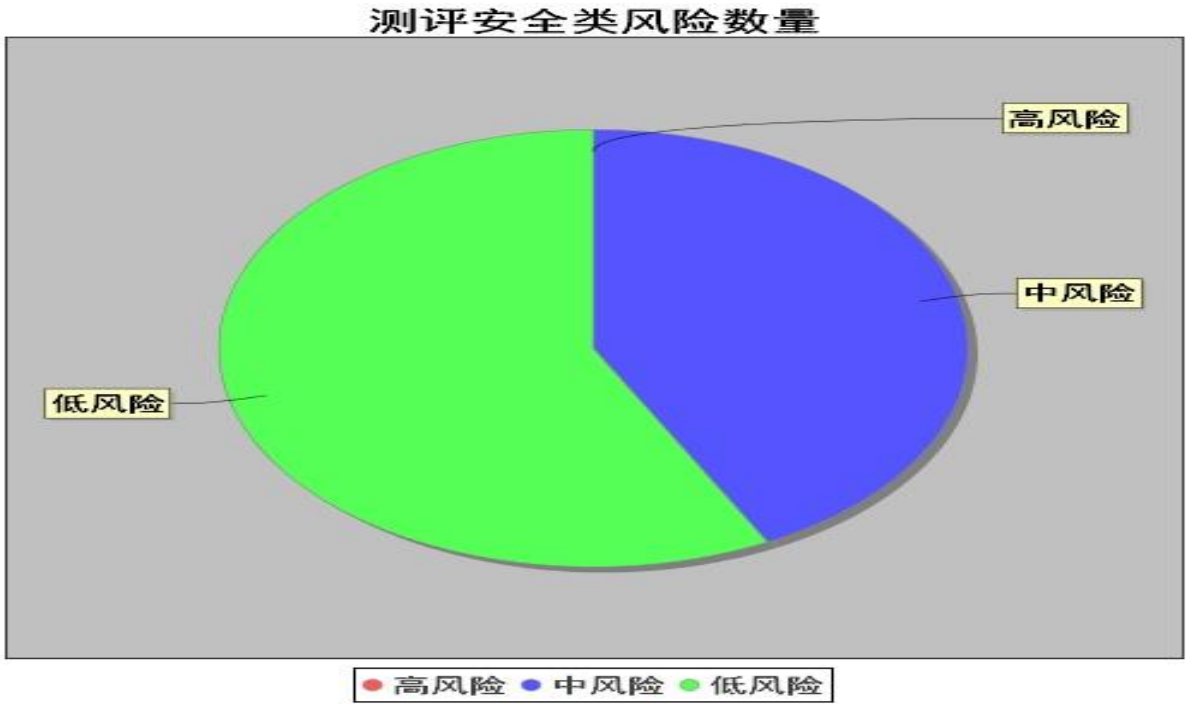
在安全管理机构方面，针对安全通用要求，机构建设在人员配备、沟通和合作、授权和审批、岗位设置等方面较为完善（如：制度文件、执行/记录文件）。在审核和检查等方面还不够完善（如：制度文件、执行/记录文件），单位开展的检查工作不够完善。

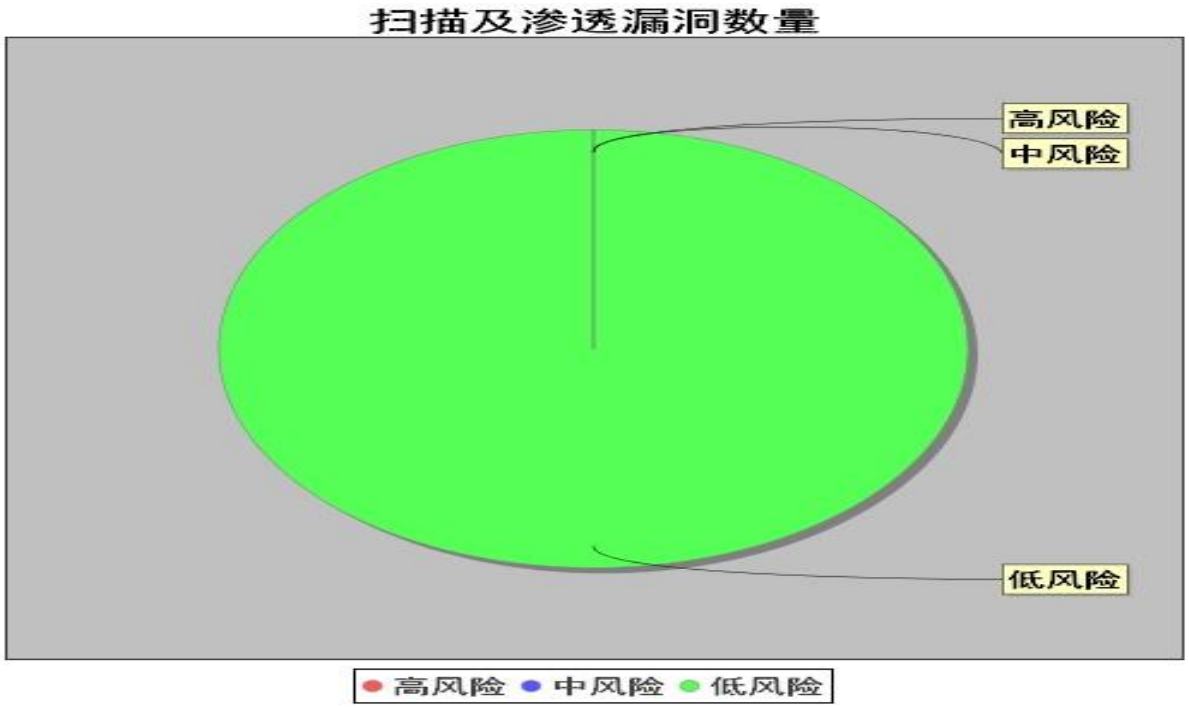
在安全管理人员方面，针对安全通用要求，人员在人员录用、安全意识教育和培训、人员离岗等方面较为完善（如：制度文件、执行/记录文件）。在外部人员访问管理等方面还不够完善（如：制度文件、执行/记录文件），单位未完全按管理规范开展人员离场后的清理工作。

在安全建设管理方面，针对安全通用要求，系统建设在定级和备案、工程实施、等级测评、产品采购和使用、服务供应商选择、系统交付等方面较为完善（如：制度文件、执行/记录文件）。在安全方案设计等方面还不够完善（如：制度文件、执行/记录文件），单位未具备完整的安全设计方案相关的文档，单位相关方案的设计的内容不够完善。

在安全运维管理方面，针对安全通用要求，系统运维在介质管理、设备维护管理、网络和系统安全管理、备份与恢复管理、资产管理、应急预案管理、环境管理、配置管理、安全事件处置、变更管理等方面较为完善（如：制度文件、执行/记录文件）。在密码管理等方面还不够完善（如：制度文件、执行/记录文件），单位不了解现有密码相关的国家标准和行业标准，单位缺乏密码管理要求的制度文档。

财务管理系统在本次测评中总共出现26类问题，其中0类高风险问题,11类中风险问题，15类低风险问题。在本次测评通过扫描及渗透发现3类漏洞问题，其中0类危险程度为高的漏洞，0类危险程度为中的漏洞，3类危险程度为低的漏洞。





财务管理系统本次等级测评的综合得分为73.85，且不存在高等级安全风险，等级测评结论为中。

主要安全问题及整改建议

一、安全物理环境

安全通用要求

(1)中风险 机房出入口未配置电子门禁系统（如：信息化机房）。 上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域,可能对系统的平稳运行造成影响。

建议安排专人7*24小时负责机房出入，对出入的人员进行身份鉴别和登记，且出入有专人陪同或在机房出入口配置电子门禁系统，控制、鉴别和记录进入的人员。

(2)中风险 机房内缺乏防静电措施（如防静电地板或铺设防静电地毯 ）（如：信息化机房）。 存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。

建议采用防静电地板或地面并采用必要的接地防静电措施。

二、安全通信网络

安全通用要求

(1)中风险 关键的应用服务和数据库服务网段未独立进行子网划分的情况（如：安全通信网络）。 上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变得更为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。

建议独立划分出应用服务器网段、数据库服务器网段。

三、安全区域边界

安全通用要求

(1)中风险 网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为（如：办公网区域）。 存在不

能及时发现内部主机作为攻击跳板，或网络攻击行为而造成系统损坏/网络资源浪费的风险。

建议网络层部署的防火墙配置对内部发起的攻击行为实现防范功能策略，实现检测、防止或限制从内部发起的网络攻击行为。

(2)中风险 现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面（如：办公网区域）。 无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。

建议现有部署的恶意代码防范措施网络边界覆盖全面，及时对恶意代码及逆行检测和清除。

四、安全计算环境

1、网络设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

2、安全设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

3、服务器和终端

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

4、系统管理软件/平台

安全通用要求

(1)中风险 未能提供中间件重要数据的异地定时数据备份功能（如：应用服务器

-Tomcat）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。

建议利用通信网络将中间件关键数据定时批量传送至备用场地，实现异地数据异地备份。

5、业务应用系统/平台

安全通用要求

(1)中风险 未能提供应用软件系统重要数据的异地定时数据备份功能（如：财务管理系统）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。

建议利用通信网络将应用软件系统关键数据定时批量传送至备用场地，实现异地数据异地备份。

6、数据资源

安全通用要求

重要业务数据

(1)中风险 未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要业务数据）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。

建议利用通信网络将应用软件系统关键数据定时批量传送至备用场地，实现异地数据异地备份。

重要个人信息

(1)中风险 未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要个人信息）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会

影响到业务服务的持续提供。

建议利用通信网络将应用软件系统关键数据定时批量传送至备用场地，实现异地数据异地备份。

7、其他系统或设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

五、安全管理中心

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

六、安全管理制度

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

七、安全管理机构

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

八、安全管理人员

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

九、安全建设管理

安全通用要求

(1)中风险 单位未具备完整的安全设计方案相关的文档。单位相关方案的设计的内容不够完善（如：制度文件、执行/记录文件）。 相关合规的规划配套文件缺失，可能导

致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。

建议根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件。

十、安全运维管理

安全通用要求

(1)中风险 **单位不了解现有密码相关的国家标准和行业标准。单位缺乏密码管理要求的制度文档（如：制度文件、执行/记录文件）。 密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不到位，存在违反国家政策的风险。**

建议单位学习现有密码相关的国家标准和行业标准。建立密码管理要求的制度文档。

目录

网络安全等级测评基本信息表 I
声明 II
等级测评结论 III
总体评价 IV
主要安全问题及整改建议 VIII
一、安全物理环境 VIII
安全通用要求 VIII
二、安全通信网络 VIII
安全通用要求 VIII
三、安全区域边界 VIII
安全通用要求 VIII
四、安全计算环境 IX
1、网络设备 IX
安全通用要求 IX
2、安全设备 IX
安全通用要求 IX
3、服务器和终端 IX
安全通用要求 IX
4、系统管理软件/平台 IX
安全通用要求 IX
5、业务应用系统/平台 X
安全通用要求 X
6、数据资源 X
安全通用要求 X
7、其他系统或设备 XI
安全通用要求 XI
五、安全管理中心 XI
安全通用要求 XI
六、安全管理制度 XI
安全通用要求 XI
七、安全管理机构 XI
安全通用要求 XI
八、安全管理人员 XI
安全通用要求 XI
九、安全建设管理 XI
安全通用要求 XI
十、安全运维管理 XII
安全通用要求 XII

目录.....XIII
1 测评项目概述.....1
1.1 测评目的.....1
1.2 测评依据.....1
1.3 测评过程.....2
1.4 报告分发范围.....5
2 被测对象描述.....5
2.1 被测对象概述.....5
2.1.1 定级结果.....5
2.1.2 业务和采用的技术.....5
2.1.3 网络结构.....5
2.2 测评指标.....7
2.2.1 安全通用要求指标.....7
2.2.2 安全扩展要求指标.....9
2.2.3 其他安全要求指标.....10
2.2.4 不适用安全要求指标.....10
2.3 测评对象.....10
2.3.1 测评对象选择方法.....10
2.3.2 测评对象选择结果.....11
2.3.2.1 物理机房.....12
2.3.2.2 网络设备.....12
2.3.2.3 安全设备.....12
2.3.2.4 服务器.....13
2.3.2.5 终端设备.....13
2.3.2.6 其他系统或设备.....13
2.3.2.7 系统管理软件/平台.....14
2.3.2.8 业务应用软件/平台.....14
2.3.2.9 数据资源.....15
2.3.2.10 安全相关人员.....15
2.3.2.11 安全管理文档.....16
3 单项测评结果分析.....21
3.1 安全物理环境.....21
3.1.1 已有安全控制措施汇总分析.....21
3.1.2 主要安全问题汇总分析.....22
3.2 安全通信网络.....23
3.2.1 已有安全控制措施汇总分析.....23
3.2.2 主要安全问题汇总分析.....23
3.3 安全区域边界.....24
3.3.1 已有安全控制措施汇总分析.....24
3.3.2 主要安全问题汇总分析.....25
3.4 安全计算环境.....26
3.4.1 网络设备.....26

3.4.1.1 已有安全控制措施汇总分析 26
3.4.1.2 主要安全问题汇总分析 28
3.4.2 安全设备 28
3.4.2.1 已有安全控制措施汇总分析 28
3.4.2.2 主要安全问题汇总分析 32
3.4.3 服务器和终端 32
3.4.3.1 已有安全控制措施汇总分析 32
3.4.3.2 主要安全问题汇总分析 36
3.4.4 系统管理软件/平台 36
3.4.4.1 已有安全控制措施汇总分析 36
3.4.4.2 主要安全问题汇总分析 40
3.4.5 业务应用系统/平台 41
3.4.5.1 已有安全控制措施汇总分析 41
3.4.5.2 主要安全问题汇总分析 43
3.4.6 数据资源 43
3.4.6.1 已有安全控制措施汇总分析 43
3.4.6.2 主要安全问题汇总分析 44
3.4.7 其他系统或设备 44
3.4.7.1 已有安全控制措施汇总分析 44
3.4.7.2 主要安全问题汇总分析 44
3.5 安全管理中心 45
3.5.1 已有安全控制措施汇总分析 45
3.5.2 主要安全问题汇总分析 45
3.6 安全管理制度 46
3.6.1 已有安全控制措施汇总分析 46
3.6.2 主要安全问题汇总分析 47
3.7 安全管理机构 47
3.7.1 已有安全控制措施汇总分析 47
3.7.2 主要安全问题汇总分析 48
3.8 安全管理人员 49
3.8.1 已有安全控制措施汇总分析 49
3.8.2 主要安全问题汇总分析 50
3.9 安全建设管理 50
3.9.1 已有安全控制措施汇总分析 50
3.9.2 主要安全问题汇总分析 52
3.10 安全运维管理 53
3.10.1 已有安全控制措施汇总分析 53
3.10.2 主要安全问题汇总分析 57
3.11 其他安全要求指标 58
3.11.1 已有安全控制措施汇总分析 58
3.11.2 主要安全问题汇总分析 58
3.12 验证测试 58
3.12.1 漏洞扫描 58
3.12.1.1 漏洞扫描结果统计 58

3.12.1.2 漏洞扫描问题描述 63
3.12.2 渗透测试 63
3.12.2.1 渗透测试过程说明 63
3.12.2.2 渗透测试问题描述 65
3.13 单项测评小结 65
3.13.1 控制点符合情况汇总 65
3.13.2 安全问题汇总 69
4 整体测评 73
4.1 安全控制点间安全测评 73
4.1.1 安全建设管理 73
4.1.1.1 安全通用要求 73
4.1.2 安全运维管理 74
4.1.2.1 安全通用要求 74
4.2 区域间安全测评 74
4.2.1 安全物理环境 74
4.2.1.1 安全通用要求 74
4.2.2 安全通信网络 75
4.2.2.1 安全通用要求 75
4.2.3 安全区域边界 75
4.2.3.1 安全通用要求 75
4.3 整体测评结果汇总 76
5 安全问题风险分析 77
6 等级测评结论 81
7 安全问题整改建议 83
附录A 被测对象资产 90
A.1 物理机房 90
A.2 网络设备 90
A.3 安全设备 90
A.4 服务器 91
A.5 终端设备 91
A.6 其他系统或设备 91
A.7 系统管理软件/平台 91
A.8 业务应用软件/平台 92
A.9 数据资源 92
A.10 密码产品 93
A.11 安全相关人员 93
A.12 安全管理文档 93
附录B 上次测评问题整改情况说明 99
附录C 单项测评结果汇总 99
C.1 安全物理环境 99

C.2 安全通信网络 99
C.3 安全区域边界 100
C.4 安全计算环境 100
C.4.1 网络设备 100
C.4.2 安全设备 101
C.4.3 服务器和终端 102
C.4.4 系统管理软件/平台 103
C.4.5 业务应用系统/平台 103
C.4.6 数据资源 104
C.4.7 其他系统或设备 104
C.5 安全管理中心 104
C.6 安全管理制度 105
C.7 安全管理机构 105
C.8 安全管理人员 105
C.9 安全建设管理 106
C.10 安全运维管理 106
C.11 其他安全要求指标 107
附录D 单项测评结果记录 107
D.1 安全物理环境 107
D.1.1 安全通用要求 107
D.1.1.1 信息化机房 107
D.2 安全通信网络 109
D.2.1 安全通用要求 109
D.2.1.1 安全通信网络 109
D.3 安全区域边界 110
D.3.1 安全通用要求 110
D.3.1.1 办公网区域 110
D.3.1.2 外网边界区域 112
D.3.1.3 安全管理区域 115
D.3.1.4 服务器存储区域 117
D.4 安全计算环境 119
D.4.1 安全通用要求 119
D.4.1.1 网络设备 119
D.4.1.2 安全设备 127
D.4.1.3 服务器和终端 151
D.4.1.4 系统管理软件/平台 181
D.4.1.5 业务应用系统/平台 193
D.4.1.6 数据资源 197
D.4.1.7 其他系统或设备 205
D.5 安全管理中心 205
D.5.1 安全通用要求 205
D.5.1.1 管理中心 205
D.6 安全管理制度 206
D.6.1 安全通用要求 206

D.6.1.1 制度文件、执行/记录文件 206
D.7 安全管理机构 208
D.7.1 安全通用要求 208
D.7.1.1 制度文件、执行/记录文件 208
D.8 安全管理人员 211
D.8.1 安全通用要求 211
D.8.1.1 制度文件、执行/记录文件 211
D.9 安全建设管理 213
D.9.1 安全通用要求 213
D.9.1.1 制度文件、执行/记录文件 213
D.10 安全运维管理 217
D.10.1 安全通用要求 217
D.10.1.1 制度文件、执行/记录文件 217
D.11 其他安全要求 225
附录E 漏洞扫描结果记录 225
附录F 渗透测试结果记录 225
附录G 威胁列表 227

1 测评项目概述

1.1 测评目的

安全等级测评的目标是通过对目标系统在安全技术及管理方面的测评,对目标系统的安全技术状态及安全管理状况做出初步判断,给出目标系统在安全技术及安全管理方面与其相应安全等级保护要求之间的差距。测评结论作为委托方进一步完善系统安全策略及安全技术防护措施依据。

项目背景是为进一步提高信息系统的保障能力,根据《信息安全等级保护管理办法》（公通字2007【43】号）的精神，茂名职业技术学院委托广东南方信息安全研究院（SC202127130010163）对财务管理系统实施等级测评，以期发现信息系统和等级保护标准的差距以及存在的安全隐患，为后续的安全整改工作提供参考依据。

1.2 测评依据

测评过程中主要依据的标准:

测评标准

（1）GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》

（2）GB/T 28448-2019 《信息安全技术 网络安全等级保护测评要求》

测评参考标准

（1）GB 17859-1999 《计算机信息系统 安全保护等级划分准则》

（2）GB/T 28449-2018 《信息安全技术 网络安全等级保护测评过程指南》

（3）GB/T 20984-2007 《信息安全技术 信息安全风险评估规范》

（4）GB/T 25058-2019 《信息安全技术 网络安全等级保护实施指南》

测评参考法律法规

（1）《中华人民共和国网络安全法》

（2）《中华人民共和国密码法》

（3）《中华人民共和国数据安全法》

1.3 测评过程

本次等级测评分为四个过程：测评准备活动、方案编制活动、测评实施活动、报告编制活动。具体如图 1-1 所示。其中，各阶段的时间安排如下：

⑴ 测评准备活动

测评准备活动的目标是顺利启动测评项目,收集定级对象相关资料,准备测评所需资料,为编制测评方案打下良好的基础。测评准备活动包括工作启动、信息收集和分析、工具和表单准备三项主要任务。

（2）方案编制活动

方案编制活动的目标是整理测评准备活动中获取的定级对象相关资料,为现场测评活动提供最基本的文档和指导方案。方案编制活动包括测评对象确定、测评指标确定、测评内容确定、工具测试方法确定、测评指导书开发及测评方案编制六项主要任务。

（3）现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调,为现场测评的顺利开展打下良好基础,依据测评方案实施现场测评工作,将测评方案和测评方法等内容具体落实到现场测评活动中。现场测评工作应取得报告编制活动所需的、足够的证据和资料。现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

（4）报告编制活动

在现场测评工作结束后,测评机构应对现场测评获得的测评结果(或称测评证据)进行汇总分析,形成等级测评结论,并编制测评报告。测评人员在初步判定单项测评结果后,还需进行单元测评结果判定、整体测评、系统安全保障评估,经过整体测评后,有的单项

测评结果可能会有所变化,需进一步修订单项测评结果,而后针对安全问题进行风险评估,形成等级测评结论。分析与报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、系统安全保障评估、安全问题风险评估、等级测评结论形成及测评报告编制七项主要任务。

各阶段完成的关键任务：

序号	阶段	任务	对象	开始日期	结束日期
1	测评准备活动	工作启动	项目甲乙双方	2022年8月15日	2022年8月19日
2		信息收集与分析	调研表	2022年8月22日	2022年8月25日
3		工具和表单准备	测评工具、测评授权书、文档交接单	2022年8月25日	2022年8月30日
4	方案编制活动	测评对象确认	测评方案-对象列表	2022年8月31日	2022年8月31日
5		测评指标确认	测评方案-指标列表	2022年8月31日	2022年8月31日
6		测评内容确认	测评方案-内容列表	2022年9月1日	2022年9月1日
7		工具测试方法确认	测评方案-工具测试方法列表	2022年9月1日	2022年9月1日
8		测评指导书开发	测评作业指导书	2022年9月2日	2022年9月2日
9		测评方案编制	测评方案	2022年9月5日	2022年9月5日
10	现场测评活动	现场测评准备	工具、人员、表单准备	2022年9月28日	2022年9月28日
11		现场测评和结果记录	安全管理访谈	2022年9月28日	2022年9月28日
12			安全管理文档检查	2022年9月28日	2022年9月28日
13			安全物理环境测评	2022年9月28日	2022年9月28日
14			安全通信网络	2022年9月28日	2022年9月29日
15			安全区域边界	2022年9月28日	2022年9月29日
16			安全计算环境	2022年9月28日	2022年9月29日
17			工具测试	2022年9月29日	2022年10月9日
18		结果确认和资料归还	检测人员出入场确认单、测评现场服务评价单	2022年10月8日	2022年10月9日
19	报告编制活动	单项测评结果	测评报告	2022年10月9日	2022年10月12日

序号	阶段	任务	对象	开始日期	结束日期
		判定			
20		单元测评结果判定		2022年10月9日	2022年10月17日
21		整体测评		2022年10月9日	2022年10月17日
22		系统安全保障评估		2022年10月9日	2022年10月17日
23		安全问题风险分析		2022年10月9日	2022年10月17日
24		等级测评结论形成		2022年10月17日	2022年10月30日
25		测评报告编制		2022年10月17日	2022年10月30日

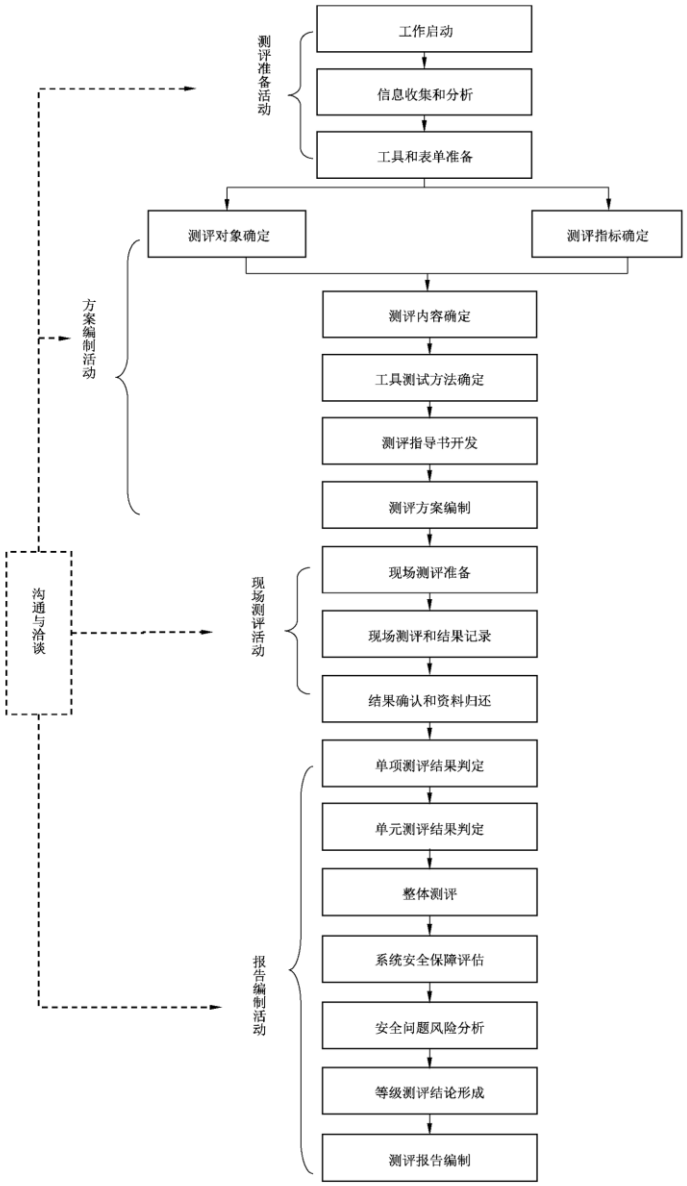


图 1-1 等级保护测评工作流程图

其中，于项目前期召开了项目启动会议，确定了工作方案及项目人员名单；于现场测评完成后召开了项目末次会议，确认了测评发现的问题；于2022年10月30日在对系统的整改情况进行了复核确认后，完成报告编制。

1.4 报告分发范围

等级测评报告正本一式3份，其中茂名职业技术学院1份，广东南方信息安全研究院1份，受理备案的公安机关1份。

2 被测对象描述

2.1 被测对象概述

2.1.1 定级结果

表 2-1定级结果

被测对象名称	安全保护等级	业务信息安全等级	系统服务安全等级
财务管理系统	2	2	2

2.1.2 业务和采用的技术

财务管理系统包含财务核算、学生收费、预算管理、结算、工资管理功能模块，年终结转该系统通过专网与财政系统进行联通通信，涵盖学生收费、奖贷学金发放、预算管理、工资管理、工资结算等业务，是学校财务流转的核心业务系统。

被测对象未采用云计算/移动互联/物联网/工业控制/大数据等技术情况。

2.1.3 网络结构

财务管理系统主要是对互联网提供服务，相关设备部署在信息化机房当中,其简要拓扑如下:

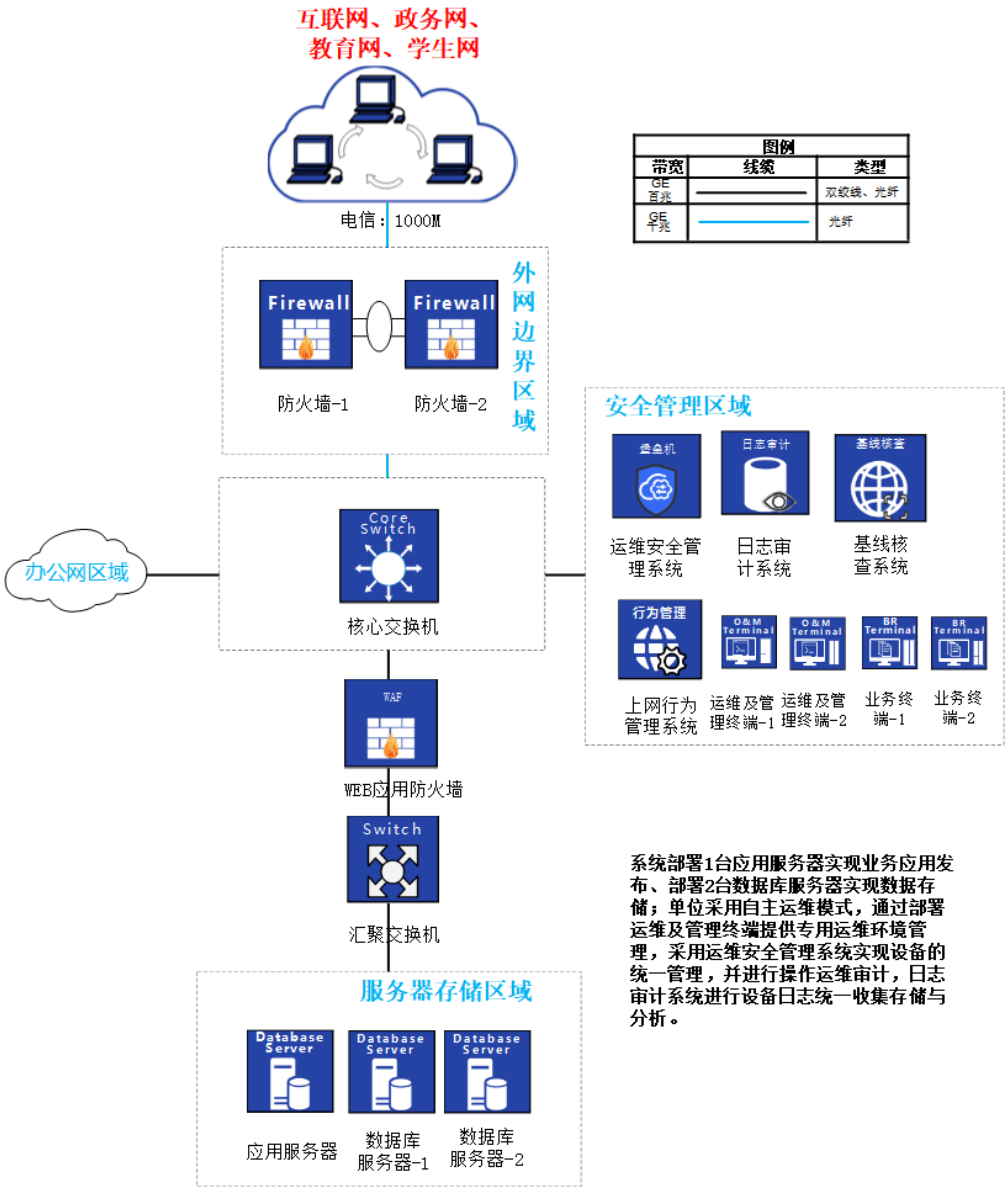


图 2-1 财务管理系统网络拓扑图

如图2-1财务管理系统网络拓扑图所示，财务管理系统网络安全域划分为4个，分别为外网边界区域、安全管理区域、服务器存储区域、办公网区域。

1、外网边界区域：

外网边界区域网络主要包括财务管理系统的业务服务和信息交换应用，是安全管理区域、服务器存储区域、办公网区域的出口边界；其链路接入为光纤线，带宽为1000mb。通过部署核心交换机、防火墙等设备实施网络访问控制，防火墙（入侵防御模块）实现网络入侵攻击行为防御。

2、办公网区域：

办公网区域网络主要包括财务管理系统与办公区域的信息交换应用，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、防火墙、上网行为管理系统等设备实施网络访问控制、防火墙（入侵防御模块）实现网络入侵攻击行为防御。

3、安全管理区域：

安全管理区域网络主要包括日志审计系统、运维安全管理系统、上网行为管理系统，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、上网行为管理系统等设备实施网络访问控制。

4、服务器存储区域：

服务器存储区域网络主要包括财务管理系统的应用服务器、数据库服务器，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、上网行为管理系统等设备实现一定的网络访问控制。

5、服务器部署情况：

财务管理系统由1台应用服务器实现应用发布；2台数据库服务器实现数据处理、存储、维护。

6、灾备及冗余

财务管理系统无异地备份机房，未实现异地备份数据定时传输功能。系统重要数据根据需求采用每天增量、每月全备到本地信息化机房。

财务管理系统未实现冗余措施。

2.2 测评指标

2.2.1 安全通用要求指标

表 2-2 安全通用要求指标

安全类	安全控制点	测评项数
安全物理环境	物理位置选择	2
	物理访问控制	1
	防盗窃和防破坏	2
	防雷击	1
	防火	2
	防水和防潮	2
	防静电	1
	温湿度控制	1
	电力供应	2
	电磁防护	1
安全通信网络	网络架构	2
	通信传输	1
	可信验证	1
安全区域边界	边界防护	1
	访问控制	4
	入侵防范	1
	恶意代码和垃圾邮件防范	1
	安全审计	3
	可信验证	1
安全计算环境	身份鉴别	3
	访问控制	4
	安全审计	3
	入侵防范	5
	恶意代码防范	1
	可信验证	1
	数据完整性	1
	数据备份恢复	2
	剩余信息保护	1
	个人信息保护	2
安全管理中心	系统管理	2
	审计管理	2
安全管理制度	安全策略	1
	管理制度	2
	制定和发布	2
	评审和修订	1
安全管理机构	岗位设置	2
	人员配备	1
	授权和审批	2
	沟通和合作	3

安全类	安全控制点	测评项数
	审核和检查	1
安全管理人员	人员录用	2
	人员离岗	1
	安全意识教育和培训	1
	外部人员访问管理	3
安全建设管理	定级和备案	4
	安全方案设计	3
	产品采购和使用	2
	自行软件开发	2
	外包软件开发	2
	工程实施	2
	测试验收	2
	系统交付	3
	等级测评	3
	服务供应商选择	2
安全运维管理	环境管理	3
	资产管理	1
	介质管理	2
	设备维护管理	2
	漏洞和风险管理	1
	网络和系统安全管理	5
	恶意代码防范管理	3
	配置管理	1
	密码管理	2
	变更管理	1
	备份与恢复管理	3
	安全事件处置	3
	应急预案管理	2
	外包运维管理	2
安全通用要求指标数量统计		135

2.2.2 安全扩展要求指标

表 2-3 安全扩展要求指标

扩展类型	安全类	安全控制点	测评项数
本次测评不涉及安全扩展要求指标			

2.2.3 其他安全要求指标

表 2-4 其他安全要求指标

安全类	安全控制点	测评项数
本次测评不涉及其他安全要求指标		

2.2.4 不适用安全要求指标

表 2-5-1 不适用安全要求指标

安全类	安全控制点	不适用项	不适用原因
安全建设管理	自行软件开发	a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。
安全建设管理	自行软件开发	b) 应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。
安全运维管理	密码管理	b) 应使用国家密码管理主管部门认证核准的密码技术和产品。	（1）单位未采购涉及密码技术的产品，不适用。
安全运维管理	外包运维管理	a) 应确保外包运维服务商的选择符合国家的有关规定；	（1）单位目前未涉及任何外包运维服务情况，不适用。
安全运维管理	外包运维管理	b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。	（1）单位目前未涉及任何外包运维服务情况，不适用。

表 2-5-2 其他不适用安全要求指标

安全类	安全控制点	不适用项	不适用原因
本次测评不涉及其他安全要求指标			

2.3 测评对象

2.3.1 测评对象选择方法

财务管理系统等级测评的测评对象种类上基本覆盖、数量进行抽样，重点抽查主要的设备、设施、人员和文档等。结合财务管理系统的网络拓扑结构和业务情况，本次等级测评的测评对象在抽样时主要考虑以下几个方面：

（1） 主机房（包括其环境、设备和设施等）和灾备机房；

（2） 存储被测系统重要数据的介质的存放环境；

（3） 办公场地；

（4） 整个系统的网络拓扑结构；

（5） 安全设备，包括防火墙等；

（6） 边界网络设备，包括路由器、楼层交换机等；

（7） 对整个信息系统或其局部的安全性起作用的网络互联设备，如核心交换机、路由器等；

（8） 承载业务处理系统主要业务或数据的服务器（包括其操作系统和数据库）；

（9） 管理终端和主要应用系统终端；

（10） 能够完成系统不同业务使命的业务应用系统；

（11） 业务备份系统；

（12） 信息安全主管人员、各方面的负责人员、具体负责安全管理的当事人、业务负责人；

（13） 涉及到信息系统安全的所有管理制度和记录。

抽样原则：在等级测评时，业务处理系统中配置相同的安全设备、边界网络设备、网络互联设备、服务器、终端以及备份设备，每类至少抽查两台作为测评对象。

2.3.2 测评对象选择结果

2.3.2.1 物理机房

表 2-6 物理机房

序号	机房名称	物理位置	重要程度
1	信息化机房	茂名市茂南区文明北路232号大院大楼	关键

2.3.2.2 网络设备

表 2-7 网络设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度
1	核心交换机	否	H3C version 7.1.070, Release 7585P07	H3C S7500E-X	核心数据交换、访问控制	关键
2	汇聚交换机	否	H3C version 7.1.070, Release 6126P20	H3C S5560X-30C-EI	数据交换	重要

2.3.2.3 安全设备

表 2-8 安全设备

序号	设备名称	是否虚拟设备	系统及版本	品牌型号	用途	重要程度
1	防火墙-1	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键
2	WEB应用防火墙	否	深信服AF 8.0.9	深信服WAF-2000-H642	应用防护、入侵防范、病毒防护	重要
3	运维安全管理系统	否	深信服V3.0.6	深信服AC-1000-D603-PT	运维审计	重要
4	基线核查系统	否	深信服V3.0.3	深信服AC-1000-D602-PT	漏洞扫描	重要
5	日志审计系统	否	深信服LAS 3.0.5	深信服AC-1000-D601-PT	日志审计	重要
6	上网行为管理系	否	深信服AC12.0.26	深信服	上网行为管理及终	重要

序号	设备名称	是否虚拟设备	系统及版本	品牌型号	用途	重要程度
	统			AC-1000-D600-PT	端准入控制	
7	防火墙-2	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键

2.3.2.4 服务器

表 2-9 服务器

序号	设备名称	所属业务应用系统/平台	是否虚拟设备	操作系统及版本	数据库管理系统及版本	中间件及版本	重要程度
1	应用服务器	财务管理系统	否	Windows Server 2016 R2	/	Tomcat 9.0.13	关键
2	数据库服务器-1	财务管理系统	否	Windows Server 2016 R2	MSSQL 2014 R2	/	关键
3	数据库服务器-2	财务管理系统	否	Windows Server 2016 R2	Oracle 11.2.0.1.0	/	关键

2.3.2.5 终端设备

表 2-10 终端设备

序号	设备名称	是否虚拟设备	操作系统及版本	用途	重要程度
1	业务终端-2	否	Windows 10 （版本 20H2（内部版本 19044.1889）	业务管理	一般
2	运维及管理终端-2	否	Windows 10 （版本 21H2（内部版本 19044.1889））	运维管理、系统管理	一般
3	运维及管理终端-1	否	Windows 10 （版本 20H2（内部版本 19044.1889）	运维管理、系统管理	一般
4	业务终端-1	否	Windows 10 （版本 20H2（内部版本 19044.1889）	业务管理	一般

2.3.2.6 其他系统或设备

表 2-11 其他系统或设备

序号	设备名称	是否虚拟设备	系统及版本	用途	重要程度
/	/	/	/	/	/

注释：本次测评对象中不涉及专用移动互联终端等，不开展抽测。

2.3.2.7 系统管理软件/平台

表 2-12 系统管理软件/平台

序号	系统管理软件/平台名称	主要功能	版本	所在设备名称	重要程度
1	数据库服务器-2-Oracle	数据生产、存储	11.2.0.1.0	应用/数据库服务器	关键
2	应用服务器-Tomcat	页面发布	9.0.13	应用/数据库服务器	关键
3	数据库服务器-1-MSSQL	数据生产、存储	2014 R2	应用/数据库服务器	关键

2.3.2.8 业务应用软件/平台

表 2-13 业务应用系统/平台

序号	业务应用软件/平台名称	主要功能	业务应用软件及版本	开发厂商	重要程度
1	财务管理系统	财务管理系统包含财务核算、学生收费、预算管理、结算、工资管理功能模块，年终结转该系统通过专网与财政系统进行联通通信，涵盖学生收费、奖贷学金发放、预算管理、工资管理、工资结算等业务，是学校财务流转的核心业务系统。	V3.0	天津神州浩天科技有限公司	关键

2.3.2.9 数据资源

表 2-14 数据资源

序号	数据类别	所属业务应用	安全防护需求	重要程度
1	重要业务数据	财务管理系统	完整性、保密性	关键
2	重要个人信息	财务管理系统	完整性、保密性	关键
3	鉴别数据	财务管理系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性、保密性	关键
4	重要审计数据	财务管理系统（安全管理中心）	完整性	重要
5	重要配置数据	财务管理系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性	关键

注释：网络设备、安全设备、服务器、终端、系统管理软件/平台和业务应用系统等所涉及的鉴别数据和重要配置数据分别在各自测评对象中汇总测评证据后集中体现,包括数据完整性、数据保密性和备份恢复。重要审计数据在安全管理中心进行汇总测评证据，包括数据完整性。重要业务数据和重要个人信息分别在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。

2.3.2.10 安全相关人员

表 2-15 安全相关人员

序号	姓名	岗位/角色	联系方式	所属单位
1	叶永利	安全管理员	0668-2920122	茂名职业技术学院
2	杨云	审计管理员	0668-2920122	茂名职业技术学院
3	杨云	资产管理员	0668-2920122	茂名职业技术学院
4	吴国华	系统管理员	0668-2920122	茂名职业技术学院
5	吴国华	机房管理员	0668-2920122	茂名职业技术学院

序号	姓名	岗位/角色	联系方式	所属单位
6	龙恒	数据管理员	13377766618	茂名职业技术学院
7	龙恒	应用管理员	13377766618	茂名职业技术学院
8	龙恒	网络管理员	13377766618	茂名职业技术学院

2.3.2.11 安全管理文档

表 2-16 安全管理文档

序号	文档名称	主要内容
1	制度类文档-恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
2	制度类文档-测试及验收方案	关于单位测试验收方案文档
3	制度类文档-变更控制管理制度	关于单位变更流程、控制管理制度文档
4	制度类文档-信息安全总体策略	关于单位网络安全方针、策略制度文档
5	制度类文档-授权和审批管理规定	关于单位授权审批、审批流程规范制度文档
6	制度类文档-工程实施管理制度	关于单位工程实施工作管理制度文档
7	制度类文档-安全审查和检查管理规范	关于单位安全检查、审查工作规范制度文档
8	制度类文档-信息系统外包运维管理制度	关于单位外包运维工作管理制度文档
9	制度类文档-系统安全管理制度	关于单位系统安全管理、安全服务管理制度文档
10	制度类文档-介质管理制度	关于单位介质安全管理工制度文档
11	制度类文档-信息系统恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
12	制度类文档-人员管理制度	关于单位人员录用、调岗、离岗管理制度文档
13	制度类文档-备份与恢复管理制度	关于单位数据备份、恢复管理制度文档
14	制度类文档-设备安全管理制度	关于单位设备安全管理制度文档
15	制度类文档-工程测试验收管理	关于单位工程测试工作管理制度文档
16	制度类文档-外部服务人员	关于单位针对外部人员工作管理规范制度文档

序号	文档名称	主要内容
	管理规范	
17	制度类文档-安全管理组织规范	关于单位组织结构管理规范制度文档
18	制度类文档-网络安全管理制度	关于单位网络安全工作管理制度文档
19	制度类文档-网络安全事件应急预案	关于单位网络安全事件应急处理、流程、培训等管理制度文档
20	制度类文档-应用系统业务用户密码设置规定	关于单位用户密码管理制度文档
21	制度类文档-岗位安排及岗位职责	关于单位岗位职责、岗位安排制度文档
22	制度类文档-系统及应用数据备份管理规范	关于单位数据备份、恢复管理制度文档
23	制度类文档-办公环境保密管理	关于单位办公环境管理制度文档
24	制度类文档-制度制定、发布、评审和修订管理制度	关于单位制度制定、发布、评审和修订等管理文档
25	制度类文档-安全漏洞管理制度	关于单位安全漏洞管理工作制度文档
26	制度类文档-服务供应商选择安全管理制度	关于单位安全服务供应商管理规定制度文档
27	制度类文档-信息安全奖惩办法	关于单位人员奖惩制度文档
28	制度类文档-数据安全管理规范	关于保障关键数据安全，从数据库本身、数据加密、数据备份恢复三个方面对数据安全进行规范的制度文档
29	制度类文档-离岗人员工作交接规范	关于单位离岗交接工作规范制度文档
30	制度类文档-外部接入受控网络访问系统管理规范	关于单位针对外部人员工作接入规范制度文档
31	制度类文档-信息安全漏洞扫描规范	关于单位安全漏洞工作规范制度文档
32	制度类文档-安全事件报告和处置	关于单位网络安全事件管理、处置、流程等报告制度文档
33	制度类文档-物理安全管理规范	关于加强单位办公区域及电子计算机机房的管理和设备运行安全，规范办公区域及机房建设，使人员办公高效及机房设备安全、稳定运行的制度文档
34	制度类文档-组织安全结构和人员职责制度	关于单位安全结构、人员职责
35	制度类文档-组织安全结构和人员职责制度	关于单位组织结构、人员安排、人员职责制度文档
36	制度类文档-网络与信息系统安全设计规范	关于单位网络与信息化安全设计制度文档

序号	文档名称	主要内容
37	制度类文档-网络安全管理规范	关于保障单位网络系统的安全稳定运行，抵御内部和外部各种形式的网络攻击或威胁制定的管理文档
38	制度类文档-外包开发软件管理规定	关于单位外包项目管理工作制度文档
39	制度类文档-办公环境管理制度	关于单位办公环境管理制度文档
40	制度类文档-员工考核管理制度	关于单位人员考核工作管理制度文档
41	制度类文档-恶意代码防范管理制度	关于单位恶意代码防范工作制度文档
42	制度类文档-网络安全事件报告制度	关于单位网络安全事件管理报告文档
43	制度类文档-外部人员访问管理制度	关于单位针对外来人员访问管控制度文档
44	制度类文档-机房安全管理制度	关于单位机房安全管理工作制度文档
45	制度类文档-主机安全管理规范	关于规定单位主机系统安全管理要求规范，指导业务平台主机的安全配置和维护的制度文档
46	制度类文档-系统交付管理	关于单位交付工作管理制度文档
47	制度类文档-安全教育和培训制度	关于单位安全培训、安全交流工作制度文档
48	制度类文档-应用安全管理规范	关于规定单位应用安全管理要求及规范的制度文档
49	操作类文档-设备及系统软件配置和操作手册	关于单位安全设备操作、Linux服务器配置手册、主机运维操作手册、软件操作手册、防火墙配置和操作手册、数据库日常运维操作手册等指导文档
50	操作类文档-软硬件日常维护管理规程	关于单位计算机网络系统使用、管理、信息安全、资源共享有所遵循,规范上网操作流程,提高网络系统安全性的指导文档
51	操作类文档-设备操作规程	关于单位相关设备操作指导文档
52	操作类文档-数据备份策略	关于单位数据备份策略文件
53	记录类文档-存储介质目录清单	关于备份介质存储工作清单
54	记录类文档-通用变更记录表	关于单位变更工作记录
55	记录类文档-软件交付清单	关于单位交付工作记录
56	记录类文档-机房维护日志	关于机房维护工作记录
57	记录类文档-机房巡检记录表	关于单位机房环境巡检记录
58	记录类文档-技能培训记录	关于单位系统培训工作、考核工作记录
59	记录类文档-离职员工物品交回登记表	关于人员离岗工物交接工作记录
60	记录类文档-系统交付清单	关于单位交付工作记录

序号	文档名称	主要内容
61	记录类文档-评审和修订记录	关于单位变更评审、修订工作记录
62	记录类文档-应急预案培训记录表	关于单位应急预案培训工作记录
63	记录类文档-收发文登记记录	关于单位文档签发记录
64	记录类文档-设备维修申请表	关于单位设备维护工作申请记录
65	记录类文档-外部会议文件和记录	关于单位外部联系、交流及会议工作记录
66	记录类文档-信息安全检查记录表	关于单位安全检查工作记录
67	记录类文档-专家论证记录表	关于单位网络方案论证记录
68	记录类文档-备份介质使用记录	关于备份介质使用登记工作记录
69	记录类文档-网络配置信息	关于单位配置信息登记工作记录
70	记录类文档-网络信息安全事件记录表	关于单位网络安全事件工作记录
71	记录类文档-信息系统存储介质使用清单	关于备份介质存储使用清单
72	记录类文档-人员培训及考核记录表	关于人员培训、考核等工作记录
73	记录类文档-监理审批表	关于单位监理审核工作记录
74	记录类文档-设备操作维护记录	关于单位设备维护工作记录
75	记录类文档-外部人员访问记录表	关于外来人员访问登记工作记录
76	记录类文档-重要操作审批表	关于单位审批工作记录
77	记录类文档-机房设备维护记录表	关于设备维护登记工作记录
78	记录类文档-漏洞检测报告	关于单位安全漏洞检测报告文档
79	记录类文档-机房设备维修记录表	关于单位机房设备维修工作记录
80	记录类文档-信息管理系统漏洞检查表	关于单位安全漏洞工作检测记录表
81	记录类文档-外部人员访问申请表	关于外来人员访问申请流程工作记录
82	记录类文档-数据恢复申请表	关于单位数据恢复工作申请表
83	记录类文档-机房出入登记	关于人员进出机房登记工作记录

序号	文档名称	主要内容
	表	
84	记录类文档-人员离岗申请表	关于人员离岗申请记录
85	记录类文档-数据备份记录表	关于单位数据备份工作记录
86	记录类文档-设备出入登记记录表	关于设备进出机房登记工作记录
87	记录类文档-信息安全会议记录	关于单位安全培训、安全交流会议记录
88	记录类文档-安全建设方案评审纪录	关于单位网络与信息化安全设计方案评审工作记录
89	记录类文档-接入受控网络申请表	关于外来人员接入工作记录
90	记录类文档-信息系统存储介质销毁申请表	关于备份介质销毁申请工作记录
91	记录类文档-人员入职考核记录	关于人员录用、考核工作记录
92	记录类文档-关键岗位人员考核记录	关于关键岗位考核工作记录
93	记录类文档-访问记录表	关于人员访问工作记录
94	记录类文档-安全管理制度评审记录	关于单位制度审计记录
95	记录类文档-离场信息资料交接表	关于人员离岗交接工作记录
96	记录类文档-备份工作汇总表	关于单位数据备份工作总结表
97	证据类文档-信息安全事件分析报告表	关于单位安全事件分析报告
98	证据类文档-定级备案	关于单位系统定级报告、备案证文件
99	证据类文档-外部联系表	关于单位内部联系及外部联系名单
100	证据类文档-网络安全等级保护测评服务合同	关于单位与安全服务商签定的安全服务合同文件
101	证据类文档-网络安全等级保护工作小组名单	关于单位网络安全等级保护工作小组人员名单文件
102	证据类文档-工程项目实施方案	关于单位工程实施方案文档
103	证据类文档-深信服安全采购合同	关于单位与安全厂家服务采购、产品选择合同文件
104	证据类文档-安全职位人员	关于单位人员岗位安排名单
105	证据类文档-网络安全系统设计方案	关于单位网络与信息化安全设计方案文档
106	证据类文档-资产清单	关于单位信息系统资产清单统计表

3 单项测评结果分析

3.1 安全物理环境

3.1.1 已有安全控制措施汇总分析

安全通用要求

物理位置选择	
a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；	
信息化机房	（1）机房和办公场地场所在建筑物具有建筑验收文档，包含对防震、防风和防雨能力的说明； （2）机房和办公场地未出严重的问题。
b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	
信息化机房	（1）机房未部署在易发生问题的位置； （2）机房对于空调设备的排水管等部位采取密封防漏处理； （3）机房对于楼板进行了防护措施。
防盗窃和防破坏	
a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识；	
信息化机房	（1）机房设备或主要部件都固定在机架上； （2）机房内对主要部件已绑定相应不易除去的标签； （3）重要机柜已进行上锁处理。
b) 应将通信线缆铺设在隐蔽安全处。	
信息化机房	（1）通信线缆铺设在下走线槽隐蔽处中； （2）通信线缆设有明显的源目的标识； （3）通信线缆均铺设整齐、规范。
防雷击	
应将各类机柜、设施和设备等通过接地系统安全接地。	
信息化机房	（1）机房设置专用地线； （2）机房内机柜、设施和设备等进行接地处理； （3）交流电源接地验收检测结果符合要求。
防火	
a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；	
信息化机房	（1）机房采用经消防检测部门检测合格并在有效期内的（如 七氟丙烷）气体自动灭火设备，火灾自动报警类型为烟感+红外； （2）自动消防系统工作状态正常，有定期巡检和维护记录《机房巡检记录表》； （3）建立机房消防的管理制度相关文档《机房安全管理制度》，按管理要求机房无人情况下气体灭火配置为自动模式，进入机房调整为手动模式，机房报警有7*24小时值班人员进行监控。
防水和防潮	

a) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	
信息化机房	（1）机房不存在雨水渗透、破损等不合规情况； （2）机房不位于建筑的顶层、边缘区域。
b) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。	
信息化机房	（1）机房区域范围已部署1台科华品牌（精密）空调，机房内分别配置1组温湿度传感器监控； （2）机房内空调下方已铺设安装好挡水和排水设施； （3）机房墙壁或楼板的管道采取必要的防渗防漏等防水保护措施； （4）机房安装检测设备（如：漏水检测绳）检测地下积水，及时处理机房水蒸气结露和地下积水的转移与渗透； （5）目前防水\防潮检测未发现异常情况，并且有防水防潮的运维记录《机房维护日志》。
温湿度控制	
应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。	
信息化机房	（1）机房范围已部署1组科华品牌精密空调进行温湿度调节； （2）机房范围已部署空调及加湿机进行温湿度调节； (3)温湿度自动调节设施运作正常,有运行和维护记录《机房维护日志》; （4）机房温度能保持在24摄氏度到28摄氏度之间； （5）机房湿度能保持在40%到65%之间。
电力供应	
a) 应在机房供电线路上配置稳压器和过电压防护设备；	
信息化机房	（1）机房配备了稳压器和过电压防护设备； （2）稳压器和过电压防护设备正常工作； （3）机房具备电力供应安全设计，并在其中标明配备稳压器、过电压防护设备等要求。
b) 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。	
信息化机房	（1）机房配备了1组科华品牌UPS； （2）UPS正常工作，可满足主要设备断电情况下的至少1小时正常运行要求； （3）UPS有定期（至少每年）检查和维护，有运行和维护记录《机房巡检记录表》。
电磁防护	
电源线和通信线缆应隔离铺设，避免互相干扰。	
信息化机房	（1）通信线缆铺设采用独立的具有电磁屏蔽作用线槽； （2）电源线缆铺设采用独立的具有电磁屏蔽作用线槽； （3）弱电线缆隔离铺设，没有干扰。

3.1.2 主要安全问题汇总分析

安全通用要求

（1）机房出入口未配置电子门禁系统（如：信息化机房）。上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域,可能对系统的平稳运行造成影响。中风险。

（2）机房建设未完全采用符合耐火等级的建筑材料。机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级（如：信息化机房）。存在发生火情时助燃火灾的风险。 低风险。

（3）机房内缺乏防静电措施（如防静电地板或铺设防静电地毯 ）（如：信息化机房）。存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。 中风险。

3.2 安全通信网络

3.2.1 已有安全控制措施汇总分析

安全通用要求

网络架构	
b) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	
安全通信网络	(1)网络内重要网段未部署在网络边界处,且未直接连接外部信息系统; (2) 系统通过防火墙对重要网段采取访问控制策略; (3) 各安全域（子网）的出口唯一。
通信传输	
应采用校验技术保证通信过程中数据的完整性。	
安全通信网络	(1) 网络系统中未涉及完整性保障设备，但在安全计算环境方面网络设备采用SSH协议、安全设备采用HTTPS协议、操作系统采用SSH协议、应用系统采用HTTPS协议来保证通信过程中数据的完整性。

3.2.2 主要安全问题汇总分析

安全通用要求

（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况（如：安全通信网络）。上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变得更

为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。 中风险。

（2）缺乏对通信设备可信验证方面的安全设计要求。现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况（如：安全通信网络）。缺乏对系统可执行程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致计算资源被干扰和破坏造成损失。 低风险。

3.3 安全区域边界

3.3.1 已有安全控制措施汇总分析

安全通用要求

边界防护	
应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络存在受保护的边界； （2）网络边界处部署了可提供访问控制功能的设备； （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。
访问控制	
a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。
b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。
c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	
办公网区域 外网边界区域 安全管理区域	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数

服务器存储区域	据包是被接收还是拒绝通过特定指示条件来决定。
d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	(1) 网络内支持状态检测和会话机制检测的区域及边界； (2) 网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； (3) 访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。
入侵防范	
应在关键网络节点处监视网络攻击行为。	
外网边界区域 服务器存储区域	(1) 网络层部署支持对内部发起的攻击行为进行防范的设备； (2) 现有的防范措施满足相应防护要求； (3) 内部安全防范措施能检测相应攻击行为。
恶意代码和垃圾邮件防范	
应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	
外网边界区域 服务器存储区域	(1) 在关键网络节点处部署合规的防恶意代码措施； (2) 恶意代码防护机制的代码库运作正常，定期更新恶意代码库； (3) 有对恶意代码库更新前的安全性及兼容性进行测试。
安全审计	
a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	(1) 网络层相关设备均开启本地审计功能； (2) 网络内部署审计措施对网络边界、重要网络节点进行安全审计； (3) 现有的审计措施满足相应的审计要求。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	(1) 设备均开启日志记录功能； (2) 现有环境内日志信息较全面； (3) 设备本地时间正常。
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	(1) 网络层部署日志审计系统，统一接收及保存相关设备的审计记录； (2) 相关网络及安全设备的本地日志文件不可删除修改； (3) 审计记录的备份机制符合信息安全管理要求； (4) 日志及审计记录的保存能力可超过6个月； (5) 定期收集日志记录并定期备份。

3.3.2 主要安全问题汇总分析

安全通用要求

(1)网络层部署防火墙,防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为（如：办公网区域）。存在不能及时发现内部主机作为攻击跳板，或网络攻击行为而造成系统损坏/网络资源浪费的风险。中风险。

(2)现有部署的恶意代码防范措施存在不合规的问题,网络边界覆盖不全面(如：办公网区域）。无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。 中风险。

(3) 缺乏对边界设备可信验证方面的安全设计要求。现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况（如：办公网区域）。缺乏对边界设备的相关程序的可信性验证,无法保证系统始终运行于可信环境中,运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4 安全计算环境

3.4.1 网络设备

3.4.1.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
核心交换机 汇聚交换机	(1) 设备对各登录模式均启用身份鉴别； (2) 设备对登录管理的用户进行身份鉴别； (3) 设备名及登录用户设置的身份标识具有唯一性； (4) 设备不存在明文或空口令用户； (5) 设备配置合规的全局密码策略； (6) 设备配置加密的super认证。
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
核心交换机 汇聚交换机	(1) 设备配置合规的全局登录失败处理策略； (2) 设备配置合规的操作超时退出措施。

c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
核心交换机 汇聚交换机	（1）设备配置合规的远程管理模式。
访问控制	
a) 应对登录的用户分配账户和权限；	
核心交换机 汇聚交换机	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。
b) 应重命名或删除默认账户，修改默认账户的默认口令；	
核心交换机 汇聚交换机	（1）设备不存在默认账户名； （2）设备账户口令设置合规。
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
核心交换机 汇聚交换机	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	
核心交换机 汇聚交换机	（1）设备根据安全策略要求对特权用户进行分离； （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
核心交换机 汇聚交换机	（1）设备开启审计功能，审计进程正常； （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
核心交换机 汇聚交换机	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
核心交换机 汇聚交换机	（1）设备限制审计文件的访问控制权限，普通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效； （5）日志及审计记录保存大于6个月。
入侵防范	
a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	
核心交换机 汇聚交换机	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。
b) 应关闭不需要的系统服务、默认共享和高危端口；	
核心交换机	（1）设备采用安全策略限制部分高危端口；

汇聚交换机	（2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。
c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
核心交换机 汇聚交换机	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
核心交换机 汇聚交换机	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
核心交换机 汇聚交换机	鉴别数据、重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； （2）设备对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a）应提供重要数据的本地数据备份与恢复功能；	
核心交换机 汇聚交换机	（1）设备定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。

3.4.1.2 主要安全问题汇总分析

安全通用要求

（1）设备不具备相关可信验证的技术措施（如：核心交换机）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.2 安全设备

3.4.2.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别

a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备对各登录模式均启用身份鉴别； （2）设备对登录管理的用户进行身份鉴别； （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备启用合规登录失败处理策略； （2）设备配置合规的操作超时退出措施。
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备配置合规的远程管理模式； （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。
访问控制	
a) 应对登录的用户分配账户和权限；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。
b) 应重命名或删除默认账户，修改默认账户的默认口令；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备不存在默认账户名； （2）设备账户口令设置合规。
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	

WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备不存在多余或过期账户； (2) 设备管理员用户与账户之间一一对应。
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备根据安全策略要求对特权用户进行分离； (2) 设备不存在多个管理级别高的特权用户； (3) 设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备开启审计功能，审计进程正常； (2)设备的日志审计级别满足要求,审计覆盖所有用户操作审计和记录。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备日期、时间正常； (2) 设备审计记录内容基本完整。
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
WEB应用防火墙 上网行为管理系统 基线核查系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备限制审计文件的访问控制权限，普通用户不可删除及修改； (2) 设备针对日志、审计记录具备充足的存储容量； (3) 对审计记录进行定期存档备份，其备份策略有效； (4) 部署日志审计系统实时对日志进行统一收集存储； (5) 日志及审计记录保存大于6个月。
日志审计系统	(1) 设备限制审计文件的访问控制权限，普通用户不可删除及修改； (2) 设备针对日志、审计记录具备充足的存储容量； (3) 对审计记录进行定期存档备份，其备份策略有效； (4) 日志及审计记录保存大于6个月。
入侵防范	

a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。
b) 应关闭不需要的系统服务、默认共享和高危端口；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。
c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 防火墙-1 防火墙-2	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
运维安全管理系统	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制。
d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备管理具备数据有效性检验功能； （2）设备管理的校验接口范围较全面。
e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。
恶意代码防范	
应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	

WEB应用防火墙 防火墙-1 防火墙-2	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	鉴别数据、重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； （2）设备对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a）应提供重要数据的本地数据备份与恢复功能；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。

3.4.2.2 主要安全问题汇总分析

安全通用要求

（1）设备不具备相关可信验证的技术措施（如：WEB应用防火墙）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.3 服务器和终端

3.4.3.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别
a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

业务终端-1 业务终端-2 应用服务器 数据库服务器-1 数据库服务器-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统对登录系统的用户进行身份鉴别； （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； （5）用户属性策略未勾选“密码永不过期”。
b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
业务终端-1 业务终端-2 应用服务器 数据库服务器-1 数据库服务器-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统启用登录失败处理策略。 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略。
c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS的管理。
应用服务器 数据库服务器-1 数据库服务器-2	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用‘RDP安全层’参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS的管理。
访问控制	
a）应对登录的用户分配账户和权限；	
业务终端-1 业务终端-2 应用服务器 数据库服务器-1 数据库服务器-2 运维及管理终端-1 运维及管理终端-2	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。
b）应重命名或删除默认账户，修改默认账户的默认口令；	
业务终端-1 业务终端-2 应用服务器 数据库服务器-1 数据库服务器-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统针对默认账户采用相应的安全策略配置； （2）操作系统账户不存在弱口令或空口令。
c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
业务终端-1	（1）操作系统不存在多余或过期账户；

业务终端-2 应用服务器 数据库服务器-1 数据库服务器-2 运维及管理终端-1 运维及管理终端-2	（2）操作系统管理员用户与账户之间一一对应。
d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	
业务终端-1 业务终端-2 应用服务器 数据库服务器-1 数据库服务器-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统根据安全策略要求对特权用户进行分离； （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
业务终端-1 业务终端-2 应用服务器 数据库服务器-1 数据库服务器-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统开启审计策略，操作系统审计策略基本完整； （2）审计覆盖所有用户操作审计和记录。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
业务终端-1 业务终端-2 应用服务器 数据库服务器-1 数据库服务器-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。
c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
业务终端-1 业务终端-2 应用服务器 数据库服务器-1 数据库服务器-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统采取对审计记录存储容量如下： 运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。
入侵防范	
a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	
业务终端-1 业务终端-2	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序；

应用服务器 数据库服务器-1 数据库服务器-2 运维及管理终端-1 运维及管理终端-2	（3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。
b）应关闭不需要的系统服务、默认共享和高危端口；	
业务终端-1 业务终端-2 应用服务器 数据库服务器-1 数据库服务器-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统不存在多余的默认共享及其它文件共享； （2）操作系统关闭不必要端口； （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。
c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
业务终端-1 业务终端-2 应用服务器 数据库服务器-1 数据库服务器-2 运维及管理终端-1 运维及管理终端-2	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
业务终端-1 业务终端-2 应用服务器 数据库服务器-1 数据库服务器-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。
恶意代码防范	
应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	
业务终端-1 业务终端-2 应用服务器 数据库服务器-1 数据库服务器-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
业务终端-1 业务终端-2 应用服务器 数据库服务器-1	鉴别数据、重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处

数据库服务器-2 运维及管理终端-1 运维及管理终端-2	理。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
业务终端-1 业务终端-2 应用服务器 数据库服务器-1 数据库服务器-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	
业务终端-1 业务终端-2 应用服务器 数据库服务器-1 数据库服务器-2 运维及管理终端-1 运维及管理终端-2	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施： 安全选项“不显示上次的用户名”->启用

3.4.3.2 主要安全问题汇总分析

安全通用要求

（1）缺乏对计算设备可信验证方面的安全设计要求。现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况（如：业务终端-1）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.4 系统管理软件/平台

3.4.4.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定

期更换；	
数据库服务器-1-MSSQL	（1）数据库系统对登录系统的用户进行身份鉴别； （2）数据库系统不存在弱口令用户； （3）数据库系统不存在默认信任的登录模式； （4）数据库系统为登录用户设置的身份标识具有唯一性； （5）数据库系统配置合规的密码长度及复杂度策略； （6）数据库系统配置合规的密码有效周期策略。
数据库服务器-2-Oracle	（1）数据库系统对登录系统的用户进行身份鉴别； （2）数据库系统不存在弱口令用户； （3）数据库系统为登录用户设置的身份标识具有唯一性； （4）数据库系统配置合规的密码长度及复杂度策略； （5）数据库系统配置合规的密码有效周期策略。
b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
数据库服务器-1-MSSQL	（1）数据库系统启用合规登录失败处理策略； （2）数据库系统执行合规的锁定策略； （3）数据库系统配置合规的操作超时锁定。
数据库服务器-2-Oracle	（1）数据库系统启用合规登录失败处理策略； （2）数据库系统执行合规的锁定策略。
c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
数据库服务器-1-MSSQL	（1）宿主操作系统配置合规的远程管理模式； （2）使用运维安全管理系统统一管理操作系统远程登录，运维安全管理系统采用了HTTPS 的管理。
数据库服务器-2-Oracle	（1）数据库系统配置合规的远程管理模式。
访问控制	
a）应对登录的用户分配账户和权限；	
应用服务器-Tomcat	（1）对应不同的账户均按需分配不同的用户权限，不存在中间件用户均属于管理级别、高权限的情况； （2）中间件配置可降权启动Tomcat的用户； （3）宿主系统针对中间件用户分别赋予相应的管理操作权限。
数据库服务器-1-MSSQL	（1）可提供数据库系统权限表； （2）登录数据库系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在所有用户均属于sysadmin的情况； （4）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。
数据库服务器-2-Oracle	（1）登录数据库系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （2）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在多用户均与sys、DBA用户权限一致的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。
b）应重命名或删除默认账户，修改默认账户的默认口令；	

应用服务器-Tomcat	（1）中间件不存在除如:Tomcat、admin、manager、role1等默认账户名； （2）中间件账户口令设置合规。
数据库服务器-1-MSSQL 数据库服务器-2-Oracle	（1）数据库系统对多余帐户进行删除、锁定或禁止其登录； （2）数据库系统账户口令设置合规。
c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
应用服务器-Tomcat	（1）中间件不存在多余或过期账户； （2）中间件管理员用户与账户之间一一对应； （3）中间件启用合规的管理用户名配置。
数据库服务器-1-MSSQL 数据库服务器-2-Oracle	（1）数据库系统不存在多余或过期账户； （2）数据库系统管理员用户与账户之间一一对应。
d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	
应用服务器-Tomcat	（1）中间件根据安全策略要求对特权用户及宿主管理用户进行分离； （2）中间件管理不存在多个管理级别高的特权用户； （3）中间件管理按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
数据库服务器-1-MSSQL	（1）数据库系统根据安全策略要求对特权用户进行分离； （2）数据库系统不存除sa外的特权用户； （3）数据库系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
数据库服务器-2-Oracle	（1）数据库系统根据安全策略要求对特权用户进行分离； （2）数据库系统用户权限合理，非管理员未设置过大权限； （3）数据库系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
应用服务器-Tomcat	（1）中间件开启审计功能，审计进程正常； （2）系统的日志审计级别满足要求。
数据库服务器-1-MSSQL	（1）数据库系统开启审计功能，审计进程正常； （2）审计覆盖所有用户操作审计和记录。
数据库服务器-2-Oracle	（1）数据库系统开启审计功能，审计进程正常； （2）ORACLE数据库系统启动数据库日志模式和自动归档； （3）审计覆盖所有用户操作审计和记录。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
应用服务器-Tomcat	（1）中间件日期、时间正常； （2）中间件审计记录开启审核策略且日志级别正常。
数据库服务器-1-MSSQL 数据库服务器-2-Oracle	（1）数据库宿主系统日期、时间正常； （2）数据库系统审计记录内容基本完整。
c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
应用服务器-Tomcat	（1）中间件限制审计文件的访问控制权限，普通用户不可删除及修改； （2）宿主系统针对中间件日志、审计记录具备充足的存储容量； （3）对中间件审计记录进行定期存档备份，其备份策略有效； （4）审计记录及日志保存大于6个月。
数据库服务器-1-MSSQL	（1）数据库系统限制审计文件的访问控制权限，普通用户不可删除及修改；

	（2）数据库系统针对日志、审计记录具备充足的存储容量； （3）MS_SQL数据库系统日志文件安装路径下的log文件（\SQL Server\MSSQLMSSQLSERVER\MSSQL\Log\ERRORLOG）everyone用户没有写权限； （4）日志及审计记录保存大于6个月。
数据库服务器-2-Oracle	（1）数据库系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）数据库系统针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）日志及审计记录保存大于6个月。
入侵防范	
c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
数据库服务器-1-MSSQL	（1）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
数据库服务器-2-Oracle	（1）网络设备ACL策略有效限制访问本机的IP地址及管理模式。
d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	
应用服务器-Tomcat	（1）中间件管理具备数据有效性检验功能； （2）中间件管理的校验接口范围较全面。
e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
应用服务器-Tomcat	（1）中间件已根据需要不定期地对已发布的版本进行更新； （2）中间件更新安装前进行安全性和兼容性测试； （3）在系统上线或发生重大变更时测试并安装最新的中间件版本或更新补丁； （4）在不影响业务系统正常运行情况下，对发现的中间件漏洞在确保安全的情况下进行修补； （5）中间件进行扫描未发现存在可造成高风险的漏洞。
数据库服务器-1-MSSQL	（1）数据库系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）补丁安装前进行安全性和兼容性测试； （3）在系统上线或发生重大变更时测试并安装数据库安全补丁； （4）MS_SQL分离默认安装的示例数据库； （5）数据库系统进行渗透及扫描未发现存在可造成高风险的漏洞。
数据库服务器-2-Oracle	（1）数据库系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）数据库宿主系统不存在启用未加控制的高危端口； （3）MY_SQL分离默认安装的示例数据库； （4）数据库系统进行渗透及扫描未发现存在可造成高风险的漏洞。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
应用服务器-Tomcat	鉴别数据、重要配置数据： （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。
数据库服务器-1-MSSQL 数据库服务器-2-Oracle	鉴别数据、重要配置数据： （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。

数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
应用服务器-Tomcat	（1）系统定义了相关需要备份的中间件重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）宿主系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）中间件相关数据的备份周期合理：每天增量一次、每月全备一次； （5）中间件开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
数据库服务器-1-MSSQL 数据库服务器-2-Oracle	（1）数据库系统定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）数据库系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	
应用服务器-Tomcat	（1）宿主系统具有清除用户鉴别信息的功能； （2）经测试，宿主系统退出后无法访问先前中间件登录过的页面； （3）经测试，宿主系统关闭后无残留的中间件用户鉴别信息。
数据库服务器-1-MSSQL	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）数据库系统不保存终端历史记录； （3）MS_SQL引用产品测试结果，信息删除后可法保证完全清除。
数据库服务器-2-Oracle	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）数据库系统不保存终端历史记录。
个人信息保护	
a) 应仅采集和保存业务必需的用户个人信息；	
数据库服务器-1-MSSQL 数据库服务器-2-Oracle	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）数据库存储的用户个人信息均为业务应用必需的环节。
b) 应禁止未授权访问和非法使用用户个人信息。	
数据库服务器-1-MSSQL 数据库服务器-2-Oracle	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； （2）数据库具备控制措施禁止未授权访问用户个人信息表单； （3）数据库具备控制措施禁止非法使用用户个人信息表单。

3.4.4.2 主要安全问题汇总分析

安全通用要求

(1)未能提供中间件重要数据的异地定时数据备份功能(如:应用服务器-Tomcat)。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

3.4.5 业务应用系统/平台

3.4.5.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
财务管理系统	(1) 系统对各登录模式均启用身份鉴别； (2) 系统对登录管理的用户进行身份鉴别； (3) 系统登录用户设置的身份标识具有唯一性； (4) 系统不存在空口令用户； (5) 设备配置合规的密码策略。
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
财务管理系统	(1) 系统启用合规登录失败处理策略； (2) 系统配置合规的操作超时退出措施。
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
财务管理系统	(1)应用系统的用户鉴别数据采用SHA-512算法在可控网络环境中传输； (2) 系统配置合规的远程管理模式。
访问控制	
a) 应对登录的用户分配账户和权限；	
财务管理系统	(1) 可提供系统权限分配表； (2) 登录系统的用户均相应分配不同的账户，不存在使用共用账户的情况； (3) 对应不同的账户均按需分配不同的用户权限，不存在所有用户均属于管理级别、高权限的情况。
b) 应重命名或删除默认账户，修改默认账户的默认口令；	
财务管理系统	(1) 系统禁用默认账户名； (2) 系统账户口令设置合规。
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
财务管理系统	(1) 系统不存在多余或过期账户； (2) 系统管理员用户与账户之间一一对应。
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	
财务管理系统	(1) 系统不存在多个管理级别高的特权用户； (2) 系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用

	户不必要的操作权限。
安全审计	
a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
财务管理系统	（1）系统开启审计功能，审计进程正常； (2)系统的日志审计级别满足要求,审计覆盖所有用户操作审计和记录。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
财务管理系统	（1）系统日期、时间正常； （2）系统审计记录内容基本完整。
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
财务管理系统	（1）系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）系统针对日志、审计记录具备充足的存储容量； （3）审计记录及日志保存大于6个月。
入侵防范	
c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
财务管理系统	（1）系统自身设定有效的终端访问策略，通过访问措施进行管理地址的限制。
d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	
财务管理系统	（1）系统具备数据有效性检验功能； （2）系统的校验接口范围较全面。
e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
财务管理系统	（1）系统已根据需要不定期地对已发布的版本进行更新； （2）在系统上线或发生重大变更时测试并安装最新的版本或更新补丁； （3）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
财务管理系统	鉴别数据、重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； （2）系统对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
财务管理系统	（1）系统定义了相关需要备份重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	
财务管理系统	（1）系统具有清除用户鉴别信息的功能； （2）经测试，系统退出后无法访问先前登录过的页面； （3）经测试，系统关闭后无残留的用户鉴别信息。

个人信息保护	
a) 应仅采集和保存业务必需的用户个人信息；	
财务管理系统	(1) 单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； (2) 系统按管理规范，仅最小化采集必需的用户个人信息； (3) 系统采集的用户个人信息均为业务应用必需的环节。
b) 应禁止未授权访问和非法使用用户个人信息。	
财务管理系统	(1) 系统不采集和保存任何形式的用户个人信息； (2) 系统对所有涉及个人信息的环节均有明确的授权同意过程； (3) 系统具备控制措施禁止未授权访问用户个人信息； (4) 系统具备控制措施禁止非法使用用户个人信息。

3.4.5.2 主要安全问题汇总分析

安全通用要求

(1) 未能提供应用软件系统重要数据的异地定时数据备份功能（如：财务管理系统）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

3.4.6 数据资源

3.4.6.1 已有安全控制措施汇总分析

安全通用要求

数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
重要业务数据 重要个人信息	(1) 系统在通信传输过程中对相关数据采取完整性保护措施； (2) 系统对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
重要业务数据 重要个人信息	(1) 系统定义了相关需要备份重要数据； (2) 单位具备合理的重要数据的备份策略规范； (3) 系统定期完全依照备份策略，采用正确的配置进行本地备份； (4) 系统的备份周期合理：每天增量一次、每月全备一次； (5) 系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
个人信息保护	
a) 应仅采集和保存业务必需的用户个人信息；	

重要个人信息	(1) 单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； (2) 系统按管理规范，仅最小化采集必需的用户个人信息； (3) 系统采集的用户个人信息均为业务应用必需的环节。
b) 应禁止未授权访问和非法使用用户个人信息。	
重要个人信息	(1) 系统对所有涉及个人信息的环节均有明确的授权同意过程； (2) 系统具备控制措施禁止未授权访问用户个人信息； (3) 系统具备控制措施禁止非法使用用户个人信息。

3.4.6.2 主要安全问题汇总分析

安全通用要求

重要业务数据

(1) 未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要业务数据）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

重要个人信息

(1) 未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要个人信息）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

3.4.7 其他系统或设备

3.4.7.1 已有安全控制措施汇总分析

安全通用要求

无其他系统或设备，不涉及相关测评

3.4.7.2 主要安全问题汇总分析

安全通用要求

无其他系统或设备，不涉及相关测评

3.5 安全管理中心

3.5.1 已有安全控制措施汇总分析

安全通用要求

系统管理	
a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；	
管理中心	（1）网络中部署运维安全管理系统实现集中的系统管理； （2）系统对登录用户进行身份鉴别； （3）系统用户标识具有唯一性； （4）系统可实现对账户的身份鉴别数据进行保密性和完整性保护； （5）系统管理操作模式具备控制措施； （6）系统具备相应的管理操作审计措施。
审计管理	
a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；	
管理中心	（1）网络中部署运维安全管理系统实现集中安全审计功能； （2）审计系统对审计管理员进行身份鉴别； （3）审计系统用户标识具有唯一性； （4）审计系统管理操作模式具备控制措施； （5）审计系统具备相应的管理操作审计措施。
b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	
管理中心	财务管理系统: （1）审计管理员定期对审计记录进行分析，对发现的安全可疑事件及时处理； （2）单位具有安全审计策略文件，规范审计记录的存储、管理和查询要求； （3）审计管理员按规范要求对审计记录进行管理。 重要审计数据: 日志审计系统、运维安全管理系统: （1）设备在通信传输过程中对相关数据采取完整性保护措施； （2）设备对重要数据在传输过程中采取必要的完整性保护措施。

3.5.2 主要安全问题汇总分析

安全通用要求

（1）系统管理的资源、运行及配置管理不够全面（如：管理中心）。系统的资源和运行缺少统一的管理，将导致系统可能无法按规划实现基于资源配置、 系统加载、异常处理、及备份/恢复等的安全控制措施。 低风险。

3.6 安全管理制度

3.6.1 已有安全控制措施汇总分析

安全通用要求

安全策略	
应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。	
制度文件、执行/记录文件	（1）单位具有网络安全工作的总体方针和安全策略文件； （2）制度内容包括明确的单位安全工作要求； （3）管理文件详见《信息安全总体策略》。
管理制度	
a) 应对安全管理活动中的主要管理内容建立安全管理制度；	
制度文件、执行/记录文件	（1）单位有针对安全管理活动中的各类管理内容建立安全管理制度； （2）现有制度已覆盖管理活动的主要的方面； （3）制度详见：《信息安全总体策略》、《网络安全管理规范》、《组织安全结构和人员职责制度》、《人员管理制度》、《员工考核管理制度》。
b) 应对管理人员或操作人员执行的日常管理操作建立操作规程。	
制度文件、执行/记录文件	（1）单位针对相关业务日常管理的操作建立规程类管理制度； （2）现有制度已覆盖重要管理方面的系统维护手册和用户操作规程等； （3）管理文件详见《设备及系统软件配置和操作手册》。
制定和发布	
a) 应指定或授权专门的部门或人员负责安全管理制度的制定；	
制度文件、执行/记录文件	（1）单位针对安全管理制度的制定，指定教育信息与网络中心部主要负责； （2）在已制定的相关制度中可查阅到被授权制定管理制度的部门/人员信息； （3）管理文件详见《安全管理组织规范》。
b) 安全管理制度应通过正式、有效的方式发布，并进行版本控制。	
制度文件、执行/记录文件	（1）单位针对制度的制定和发布要求，制定管理规范文件； （2）管理规范文件对文件制定及发布定义了规范要求； （3）安全管理制度的收发登记记录有效； （4）管理文件详见《制度制定、发布、评审和修订管理制度》、《收发文登记记录》。
评审和修订	

应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	
制度文件、执行/记录文件	（1）单位针对制度的合理性和适用性需进行论证和审定及修订的要求，制定管理规范文件； （2）管理规范文件对制度的评审及修订定义了规范要求； （3）单位具有安全管理制度的审定或论证的过程记录； （4）单位对做过修订的制度，具备有修订版本的安全管理过程记录； （5）管理文件详见《制度制定、发布、评审和修订管理制度》及 《安全管理制度评审记录》。

3.6.2 主要安全问题汇总分析

安全通用要求

财务管理系统针对安全管理制度层面的安全通用要求采取的安全措施比较完善，未发现不符合项。

3.7 安全管理机构

3.7.1 已有安全控制措施汇总分析

安全通用要求

岗位设置	
a) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；	
制度文件、执行/记录文件	（1）单位已明确网络安全管理工作的职能部门，并明确了各岗位职责； （2）单位各部门职责文档已明确网络安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备网络安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。
b) 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。	
制度文件、执行/记录文件	（1）单位已明确系统安全管理工作的职能部门，并明确了各岗位职责； （2）单位各部门职责文档已明确系统安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备系统安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。

人员配备	
应配备一定数量的系统管理员、审计管理员和安全管理员等。	
制度文件、执行/记录文件	（1）单位针对人员配备要求，制定了管理制度； （2）单位按要求配备一定数量的重要岗位管理人员； （3）单位针对各岗位人员，制定并维护人员档案； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。
授权和审批	
a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；	
制度文件、执行/记录文件	（1）单位在制度中用文字描述或在流程图中明确，对关键活动进行审批； （2）单位对审批过程明确审批权限，对各项信息系统的重要操作与变更明确审批部门和批准人； （3）管理文件详见《授权和审批管理规定》。
b) 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。	
制度文件、执行/记录文件	（1）单位针对各项业务操作及变更等建立了审批程序规定； （2）单位针对系统变更、系统接入、物理范围等事项已明确按审批程序执行，记录有批准人签字； （3）管理文件详见《授权和审批管理规定》。
沟通和合作	
a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；	
制度文件、执行/记录文件	（1）单位针对机构内部管理人员之间、部门之间的沟通与合作，制定了管理制度； （2）单位的管理制度规范了合作和沟通的方式和周期； （3）单位有组织机构内部人员联系表； （4）单位有定期召开信息安全会议，保存有会议纪要； （5）管理文件详见《安全教育和培训制度》、《技能培训记录》《外部联系表》。
b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；	
制度文件、执行/记录文件	（1）单位针对加强与外部单位的合作与沟通，制定了管理制度规定； （2）单位能按要求与相关单位保持沟通合作，并提供相关单位联系方式和交流会议纪要； （3）管理文件详见《安全教育和培训制度》、《技能培训记录》、《外部联系表》。
c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	
制度文件、执行/记录文件	（1）单位建立了完善的对外联单位的联系列表； （2）管理文件详见《外部联系表》。

3.7.2 主要安全问题汇总分析

安全通用要求

（1）单位开展的检查工作不够完善（如：制度文件、执行/记录文件）。检查工作开展不仔细，可能对存在或潜在的安全风险不能被及时发现并进行处理。 低风险。

3.8 安全管理人员

3.8.1 已有安全控制措施汇总分析

安全通用要求

人员录用	
a) 应指定或授权专门的部门或人员负责人员录用；	
制度文件、执行/记录文件	（1）单位授权专门的部门负责人员录用工作，制定了管理制度规范； （2）由人力资源保障科负责人员录用工作； （3）管理文件详见《人员管理制度》。
b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查。	
制度文件、执行/记录文件	（1）单位针对人员录用过程，制定了明确要求，并形成人员安全管理制度； （2）单位现有管理制度明确说明录用人员应具备的条件； （3）单位按规定执行人员录用的相关审查过程； （4）管理文件详见《人员管理制度》、《人员入职考核记录》。
人员离岗	
应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。	
制度文件、执行/记录文件	（1）单位针对离岗人员权限终止及取回机构提供的各种设施的要求，制定了管理制度； （2）单位按规范开展对离岗人员的相关管理工作； （3）管理文件详见《人员管理度》、《人员离岗申请表》、《离场信息资料交接表》。
安全意识教育和培训	
应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。	
制度文件、执行/记录文件	（1）单位针对人员安全培训及责任和惩戒措施，制定了管理制度； （2）单位已开展安全意识教育及岗位技能培训。 （3）管理文件详见《安全教育和培训制度》。
外部人员访问管理	
a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；	
制度文件、执行/记录文件	（1）单位针对外部人员物理访问，制定了外部人员访问管理文档； （2）单位具备有效的外部人员访问重要区域的书面申请文档； （3）单位具备外部人员访问重要区域的登记记录； （4）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。
b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并	

登记备案；	
制度文件、执行/记录文件	（1）单位针对外部接入受控网络访问系统，制定了管理制度； （2）单位具备外部人员接入受控网络前的申请审批流程； （3）单位具备外部人员接入及访问系统的书面申请文档； （4）单位具备外部人员接入及访问系统的登记记录； （5）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。

3.8.2 主要安全问题汇总分析

安全通用要求

（1）单位未完全按管理规范开展人员离场后的清理工作（如：制度文件、执行/记录文件）。人员离场后的清理工作开展不规范，可能导致遗留外部人员访问受控区域的记录，存在被二次非法利用，造成泄密。 低风险。

3.9 安全建设管理

3.9.1 已有安全控制措施汇总分析

安全通用要求

定级和备案	
a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；	
制度文件、执行/记录文件	（1）单位的被测系统于2022年4月已完成备案； （2）系统备案相关文档（定级报告）中明确等级划分方法和理由，SAG三个方面的级别描述清晰； （3）管理文件详见《定级备案》。
b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；	
制度文件、执行/记录文件	(1)单位针对系统定级结果的审批及评审工作等要求,制定了管理制度; （2）现有系统的定级已具备合理性和正确性审定； （3）管理文件详见《定级备案》。
c) 应保证定级结果经过相关部门的批准；	
制度文件、执行/记录文件	（1）单位针对系统定级结果的上级批准要求，制定了管理制度； （2）现有系统的定级获得了相关部门的批准； （3）管理文件详见《定级备案》。
d) 应将备案材料报主管部门和相应公安机关备案。	
制度文件、执行/记录文件	（1）单位对被测系统的等级备案表、定级报告等备案材料已经报相应公安机关备案；

	（2）单位具备公安机关出具的备案号； （3）管理文件详见《定级备案》。
产品采购和使用	
a）应确保网络安全产品采购和使用符合国家的有关规定；	
制度文件、执行/记录文件	（1）单位已建立安全产品管理的相关管理规定； （2）单位具备安全产品采购流程及相关实施文档； （3）被测系统使用的安全产品具备销售许可资质； （4）安全产品具均为国内产品； （5）管理文件详见《设备安全管理制度》。
b）应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。	
制度文件、执行/记录文件	（1）单位已建立密码产品与服务管理的相关管理制度； （2）系统未使用密码产品； （3）管理文件详见《设备安全管理制度》。
外包软件开发	
b）应保证开发单位提供软件设计文档和使用指南。	
制度文件、执行/记录文件	（1）单位制定软件开发项目验收要求，明确开发单位的提交材料； （2）开发单位提供软件日常维护和使用所需的文档； （3）管理文件详见《外包开发软件管理规定》、《设备及系统软件配置和操作手册》。
工程实施	
a）应指定或授权专门的部门或人员负责工程实施过程的管理；	
制度文件、执行/记录文件	（1）单位针对专门的部门负责工程实施过程的管理要求，制定管理度； （2）单位由专岗负责系统建设的工程实施，且按照实施方案的要求对进度和质量进行控制； （3）管理文件详见《工程实施管理制度》。
b）应制定安全工程实施方案控制工程实施过程。	
制度文件、执行/记录文件	（1）单位制定了详细的工程实施方案； （2）工程实施单位严格按照方案执行，并有过程记录； （3）管理文件详见《测试及验收方案》、《工程项目实施方案》。
系统交付	
a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；	
制度文件、执行/记录文件	（1）单位具备系统交付清单； （2）系统交付清单内容较详细； （3）单位的清点工作较合规； （4）管理文件详见《系统交付管理》、《资产清单》。
b）应对负责运行维护的技术人员进行相应的技能培训；	
制度文件、执行/记录文件	（1）单位已对负责系统运行维护的技术人员进行了技能培训； （2）具备运维人员的培训记录； （3）管理文件详见《系统交付管理》、《资产清单》、《系统交付清单》、《技能培训记录》。
c）应提供建设过程文档和运行维护文档。	
制度文件、执行/记录文件	（1）单位提供了系统建设过程中的文档； （2）单位提供了指导用户进行系统运维的文档和系统培训手册； （3）管理文件详见《系统交付管理》、《系统交付清单》、《设备及系

	统软件配置和操作手册》。
等级测评	
a) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；	
制度文件、执行/记录文件	（1）单位针对系统等级测评要求，制定管理制度； （2）系统按要求开展首次测评工作； （3）管理文件详见《系统安全管理制度》。
b) 应在发生重大变更或级别发生变化时进行等级测评；	
制度文件、执行/记录文件	（1）管理制度中已规定在系统发生变更时及时对系统进行等级测评； （2）系统未发生过重大变更，系统等级未发生变化； （3）管理文件详见《系统安全管理制度》。
c) 应确保测评机构的选择符合国家有关规定。	
制度文件、执行/记录文件	（1）已选择在“全国等级保护测评机构推荐目录”中的测评单位进行等级测评； （2）管理文件详见《系统安全管理制度》、《网络安全等级保护测评服务合同》。
服务供应商选择	
a) 应确保服务供应商的选择符合国家的有关规定；	
制度文件、执行/记录文件	（1）单位在管理制度内明确提出安全服务供应商选择的要求； （2）单位选择的安全服务商符合国家的有关规定，具备相应的安全服务资质； （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。
b) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。	
制度文件、执行/记录文件	（1）单位的管理制度中已规定，需与安全服务商签订安全相关的协议并明确整个服务供应链各方需履行的网络安全相关义务； （2）单位已按规定与选定的安全服务商签订合规的协议； （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。

3.9.2 主要安全问题汇总分析

安全通用要求

（1）单位未具备适用于被测系统的安全规划设计方案（如：制度文件、执行/记录文件）。规划设计需求不全面，可能导致安全方案设计不完善，信息系统存在安全缺陷。低风险。

（2）单位未具备完整的安全设计方案相关的文档。单位相关方案的设计的内容不够完善（如：制度文件、执行/记录文件）。相关合规的规划配套文件缺失，可能导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。 中风险。

（3）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定。单位未对相关论证过程及内容进行完整的记录（如：制度文件、执行/记录文件）。未开展规范的审批过程，可能存在安全整体规划缺乏合理性和可行性，导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。 低风险。

（4）单位未在软件开发过程中对所有软件安全性进行测试。单位未在软件安装之前按要求对所有软件开展恶意代码检测（如：制度文件、执行/记录文件）。软件交付前恶意代码检测不规范，可能在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。 低风险。

（5）单位未完全根据测试验收方案组织相关部门和人员开展验收工作（如：制度文件、执行/记录文件）。可能由于验收测试不严谨，造成测试过程缺乏计划性及操作性，无法保证经过测试验收的系统达到既定的安全性等目标。 低风险。

(6)针对系统上线前的安全性测试工作存在问题(如:制度文件、执行/记录文件)。未按规定开展上线前测试，安全隐患可能在系统上线运行前未被发现并作出相应处理。低风险。

3.10 安全运维管理

3.10.1 已有安全控制措施汇总分析

安全通用要求

环境管理
a) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；

制度文件、执行/记录文件	（1）单位建立机房安全方面的管理制度，对有关运维方面的管理作出规定； （2）单位具备完整的机房出入登记记录； （3）单位具备完整的机房基础设施的维护记录； （4）管理文件详见《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。
b）应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；	
制度文件、执行/记录文件	（1）单位建立机房安全方面的管理制度； （2）单位现有机房管理记录与制度相符； （3）制度详见：《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。
c）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	
制度文件、执行/记录文件	（1）单位机房安全管理制度已明确来访人员的接待区域的要求； （2）单位按规范要求开展人员来访接待； （3）单位办公环境未发现有随意放置含有敏感信息介质的情况； （4）制度详见：《机房安全管理制度》、《物理安全管理规范》、《办公环境保密管理》。
资产管理	
应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。	
制度文件、执行/记录文件	（1）单位已建立有效的资产清单； （2）单位现有资产清单内容较全面； （3）制度详见：《设备安全管理制度》、《资产清单》。
介质管理	
a）应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；	
制度文件、执行/记录文件	（1）介质按管理要求放置于受控的环境中（如：机房）； （2）介质管理具备较全面的记录； （3）制度详见：《设备安全管理制度》、《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。
b）应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。	
制度文件、执行/记录文件	（1）介质管理制度中对介质安全传输有明确规定； （2）存储重要信息的介质在物理传输过程，具备严格的环节控制，无重大环节疏漏； （3）对介质的归档和查询均具备记录； （4）制度详见：《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。
设备维护管理	
a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	
制度文件、执行/记录文件	（1）单位人员岗位职责相关文档已明确设备维护管理的责任部门；

	（2）单位对各类设施、设备进行定期维护； （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。
b）应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。	
制度文件、执行/记录文件	（1）单位建立了配套设施、软硬件维护管理方面的管理制度； （2）单位开展相关工作与制度相符，且保留记录； （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。
网络和系统安全管理	
a）应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；	
制度文件、执行/记录文件	（1）单位建立系统安全管理文档，对系统管理员的管理制定了要求； （2）单位对各类关键角色建立了相应的工作职责文档； （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。
b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	
制度文件、执行/记录文件	（1）单位制定管理制度，对系统账号进行管理； （2）单位按管理规范开展账号管理工作； （3）账户管理记录内容较完整； （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。
c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	
制度文件、执行/记录文件	（1）单位建立了网络和系统安全管理制度； （2）网络和系统安全管理制度内容较全面； （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。
d）应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；	
制度文件、执行/记录文件	（1）单位对重要设备、系统的配置和操作建立配置手册； （2）现有操作配置手册已明确操作步骤、参数配置； （3）制度详见：《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。
e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。	
制度文件、执行/记录文件	（1）单位制定日常运维管理的相关制度规范； （2）单位按制度规范开展日常运维管理工作； （3）单位具备合规的运维记录； （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》、《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。
恶意代码防范管理	
a）应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	
制度文件、执行/记录文件	（1）单位制定恶意代码防范管理制度，明确对外来计算机或存储设备接入系统前进行恶意代码检查； （2）单位按外来计算机接入恶意代码检查规范开展工作；

	（3）单位制定培训管理制度，明确需通过培训提升员工的防恶意代码意识； （4）单位按培训管理要求开展工作； （5）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申请表》、《信息管理系统漏洞检查表》。
b）应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；	
制度文件、执行/记录文件	（1）建立恶意代码防范管理文档； （2）管理制度中覆盖防恶意代码软件的授权使用、恶意代码库升级、定期查杀等内容； （3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》。
配置管理	
应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。	
制度文件、执行/记录文件	（1）单位制定了基本配置信息管理的制度要求； （2）管理文件详见：《主机安全管理规范》、《网络安全管理规范》、《应用安全管理规范》、《网络配置信息》。
变更管理	
应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。	
制度文件、执行/记录文件	（1）单位建立了关于系统变更管理的制度文件； （2）现有变更管理制度覆盖了变更管理的各方面要求； （3）制度详见：《变更控制管理制度》、《通用变更记录表》。
备份与恢复管理	
a）应识别需要定期备份的重要业务信息、系统数据及软件系统等；	
制度文件、执行/记录文件	（1）单位根据业务重要程度，制定了需要定期备份的重要业务信息列表或清单。清单内需要定期备份的重要数据已经过用户方确认； （2）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。
b）应规定备份信息的备份方式、备份频度、存储介质、保存期等；	
制度文件、执行/记录文件	（1）单位建立了备份与恢复管理相关的安全管理制度； （2）备份与恢复管理的相关要求比较明确； （3）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。
c）应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	
制度文件、执行/记录文件	（1）单位现有管理制度，明确了数据备份策略和数据恢复策略，以及备份程序和恢复程序； （2）单位可按策略要求实现重要数据的定期备份与恢复性测试； （3）单位现有的备份的数据均经过恢复性测试，可确保备份的数据可用； （4）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。
安全事件处置	
a）应及时向安全管理部门报告所发现的安全弱点和可疑事件；	
制度文件、执行/记录文件	（1）单位已在安全培训及宣传过程中告知用户在发现安全弱点和可疑事

	件时及时向安全管理部门报告； （2）单位在系统运维过程中对发现的安全弱点和可疑事件均编制了对应的报告或相关文档； （3）单位现有安全弱点和可疑事件报告文档内容较详实； （4）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。
b）应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；	
制度文件、执行/记录文件	（1）单位制定了安全事件报告和处置管理制度； （2）现有安全事件管理制度内容较完整； （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。
c）应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。	
制度文件、执行/记录文件	（1）单位具备对安全事件的分析、处理、总结、防范等的报告／过程文档； （2）单位提供的安全事件报告和响应处置记录内容较完整； （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。
应急预案管理	
a）应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；	
制度文件、执行/记录文件	（1）单位制定重要事件的应急预案； （2）单位现有应急预案涉及的类型范围较全面； （3）单位现有应急预案的内容较完整； （4）制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。
b）应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。	
制度文件、执行/记录文件	（1）单位定期对相关人员进行应急预案培训； （2）单位根据不同的应急预案，按要求进行应急演练； （3）单位具备近期应急预案工作开展的相关记录； （4）单位提供的应急预案培训记录比较完整； （5）单位提供的应急预案演练记录比较完整； （6）经检查单位目前一旦出现应急事件，可参照预案合理有序的进行应急事件处置过程； （7）制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。

3.10.2 主要安全问题汇总分析

安全通用要求

（1）单位未严格按规范开展漏洞及安全隐患检测工作（如：制度文件、执行/记录文件）。漏洞检测、修补工作不到位，可能存在未授权人员利用漏洞攻击信息系统的风险。 低风险。

（2）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作（如：制度文件、执行/记录文件）。可能导致系统恶意代码检测管理不到位，存在信息系统感染恶意代码，从而导致严重的信息安全风险。 低风险。

（3）单位不了解现有密码相关的国家标准和行业标准。单位缺乏密码管理要求的制度文档（如：制度文件、执行/记录文件）。密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不到位，存在违反国家政策的风险。 中风险。

3.11 其他安全要求指标

3.11.1 已有安全控制措施汇总分析

本次测评未涉及其他安全要求指标。

3.11.2 主要安全问题汇总分析

本次测评未涉及其他安全要求指标。

3.12 验证测试

验证测试包括漏洞扫描，渗透测试等，验证测试发现的安全问题对应到相应的测评项的结果记录中。详细验证测试报告见报告附录。

3.12.1 漏洞扫描

3.12.1.1 漏洞扫描结果统计

本次测评主要使用了[绿盟远程安全评估系统]对系统的设备进行了安全扫描，其所涉及的系统版本为：[V6.0R04F01SP06]，规则库版本为：[V6.0R02F01.2900]。扫描结果如下：

经分析统计，共发现各接入点存在2类漏洞，其中0类危险程度为高的漏洞，0类危害程度为中的漏洞，2类危害程度为低的漏洞。

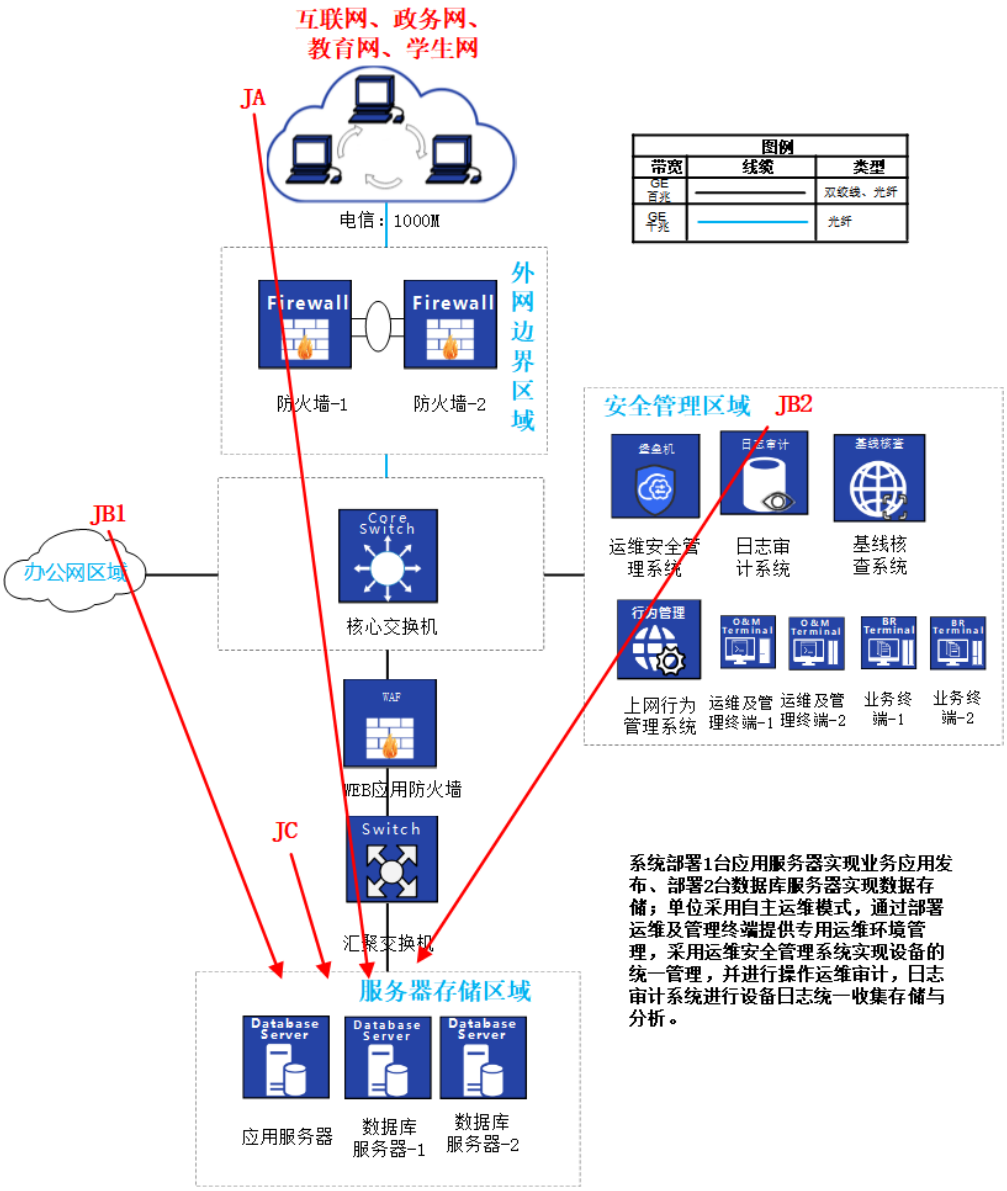


图 3-1 漏洞扫描工具接入测试示意图

接入点JA：在防火墙外侧接入，开展扫描/渗透主要目的是，探测对外服务功能区上各服务器、应用系统对外部网络边界暴露的安全漏洞情况，并根据漏洞扫描的结果接入渗透测试工具集，试图利用服务器、应用的安全漏洞入侵网络的行为。

接入点JB：在办公网区域VLAN段、安全管理区域VLAN段接入，开展扫描/渗透主要目的是，模拟外联单位/内部恶意用户发现操作系统、数据库、Web应用、第三方产品等安全漏洞的过程，并尝试利用以上漏洞实施诸如获取系统控制权（GetShell）、获得大量敏感信息（DragLibrary）等模拟攻击行为。

接入点JC：在系统所在VLAN的交换机接入，开展扫描/渗透主要目的是，直接测试对服务功能区上各服务器在最小化防御的基础上，对网络暴露的安全漏洞情况。

（1）接入点A漏洞扫描结果统计

根据在接入点A对16台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-1 接入点 A 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	0	0	0	0
2	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	0	0	0	0
3	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	0	0	0	0
4	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	0	0	0	0
5	172.16.1.14/上网行为管理系统	(安全设备)深信服 AC12.0.26	0	0	0	0
6	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	0	0	0	0
7	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	0	0	0	0
8	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	0	0	0	0
9	192.168.33.11/业务终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
10	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
11	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
12	192.168.33.10/业务终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
13	10.2.4.14/数据库服务器-2	(服务器存储设备)Windows Server 2016 R2	0	0	0	0
14	10.2.4.12/数据库服务器-1	(服务器存储设备)Windows Server 2016 R2	0	0	0	0
15	10.2.4.13/应用服务器	(服务器存储设备)Windows Server 2016 R2	0	0	0	0
16	https://s.mmpt.edu.cn/财务管理系统	(业务应用软件平台) V3.0	0	0	0	0

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
安全漏洞数量小计			0	0	0	0

（2）接入点B漏洞扫描结果统计

根据在接入点B对16台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-2 接入点 B 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	1	0	0	1
2	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	1	0	0	1
3	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	1	0	0	1
4	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	2	0	0	2
5	172.16.1.14/上网行为管理系统	(安全设备)深信服AC12.0.26	1	0	0	1
6	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	1	0	0	1
7	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	1	0	0	1
8	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	1	0	0	1
9	192.168.33.11/业务终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
10	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
11	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
12	192.168.33.10/业务终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
13	10.2.4.14/数据库服务器-2	(服务器存储设备)Windows Server 2016 R2	1	0	0	1
14	10.2.4.12/数据库服务器-1	(服务器存储设备)Windows Server 2016 R2	1	0	0	1
15	10.2.4.13/应用服务器	(服务器存储设备)Windows Server 2016 R2	1	0	0	1

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
16	https://s.mmpt.edu.cn/财务管理系统	(业务应用软件平台) V3.0	0	0	0	0
安全漏洞数量小计			12	0	0	12

（3）接入点C漏洞扫描结果统计

根据在接入点C对16台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-3 接入点 C 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	1	0	0	1
2	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	1	0	0	1
3	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	1	0	0	1
4	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	2	0	0	2
5	172.16.1.14/上网行为管理系统	(安全设备)深信服AC12.0.26	1	0	0	1
6	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	1	0	0	1
7	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	1	0	0	1
8	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	1	0	0	1
9	192.168.33.11/业务终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
10	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
11	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
12	192.168.33.10/业务终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
13	10.2.4.14/数据库服务器-2	(服务器存储设备)Windows Server 2016 R2	1	0	0	1
14	10.2.4.12/数据库服务器-1	(服务器存储设备)Windows Server 2016 R2	1	0	0	1

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
15	10.2.4.13/应用服务器	(服务器存储设备)Windows Server 2016 R2	1	0	0	1
16	https://s.mmpt.edu.cn/财务管理系统	(业务应用软件平台) V3.0	0	0	0	0
安全漏洞数量小计			12	0	0	12

3.12.1.2 漏洞扫描问题描述

通过对漏洞扫描结果进行分析,财务管理系统存在的主要安全漏洞汇总如下表所示

表 3-4 主要安全漏洞汇总表

序号	安全漏洞名称	关联资产/域名	严重程度
1	允许Traceroute探测 此类漏洞涉及网络设备、安全设备、服务器存储设备。	10.2.4.14/数据库服务器-2 10.2.4.12/数据库服务器-1 10.2.4.13/应用服务器 10.2.1.4/运维安全管理系统 10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/上网行为管理系统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/汇聚交换机 172.16.1.2/核心交换机	低
2	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161) 此类漏洞涉及网络设备。	172.16.1.2/核心交换机	低

3.12.2 渗透测试

经分析统计，共发现各接入点存在1类漏洞，其中0类危险程度为高的漏洞，0类危害程度为中的漏洞，1类危害程度为低的漏洞。

3.12.2.1 渗透测试过程说明

方案制定：

在得到委托单位的书面授权许可后，才进行渗透测试的实施。并且将实施范围、方法、时间、人员等具体的方案委托单位进行交流，并得到委托单位的认同。在测试实施之前，会做到让委托单位对渗透测试过程和风险的知晓，使随后的正式测试流程都在委托单位的管控下。

信息收集：

此阶段中，渗透测试人员对目标信息系统进行必要的信息收集，如操作系统类型、开放的端口和服务、中间件信息、后台数据库类型、web开发语言等，即收集有利于漏洞挖掘的相关信息，为渗透测试做准备。

漏洞挖掘方法：

此阶段中，渗透测试人员对目标信息系统开始进行渗透测试，利用已知信息和现有条件及技术进行漏洞挖掘，尽可能发现目标信息系统中存在的所有安全风险，并进行记录。

漏洞利用：

此阶段中，渗透测试人员对目标信息系统对上一阶段漏洞挖掘中发现的漏洞进行必要的利用以证明其危害性，再对渗透测试过程所产生的测试数据进行清除。

输出报告：

此阶段中，渗透测试人员把渗透测试记录、截图等相关信息进行整理，然后撰写渗透测试报告，最终提交给委托单位。

漏洞修复：

此阶段中，委托单位依据收到的渗透测试报告对其中所提出的漏洞进行整改，可参考报告中所提出的修复建议，整改完成后联系本单位相关人员准备回归测试。

回归测试：

此阶段中，渗透测试人员对整改后的目标信息系统进行复测，以确定报告中提出的漏洞是否已被修复，若已被修复，则进入下一阶段；否则，返回上一阶段。

测试工具：

序号	工具	工具用途
1	Burpsuite Pro	用于攻击Web应用程序的集成软件
2	Sqlmap	开源的自动化SQL注入工具
3	Nmap	开源的网络发现和安全审计工具
4	OWASP ZAP	自动化Web应用漏洞扫描工具
5	其他测试工具	根据信息系统的类别选择不同的工具（如自写脚本、目录扫描器、木马扫描器、其它开源工具等）

3.12.2.2 渗透测试问题描述

通过渗透测试发现，财务管理系统存在的安全问题汇总如下表所示。

表 3-5 渗透测试结果汇总表

序号	安全问题	关联资产/域名	严重程度
1	缺少“X-Content-Type-Options”响应头 此类漏洞涉及业务应用软件平台。	https://s.mmpt.edu.cn/财务管理系统	低

3.13 单项测评小结

3.13.1 控制点符合情况汇总

根据单项测评结果汇总控制点符合情况如下表所示。（表格以不同颜色对测评结果进行区分，不符合的安全控制点采用红色标识，部分符合的采用黄色标识，不适用的采用蓝色标识且不做勾选。）

表 3-6 控制点符合情况汇总表

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
1	安全通用要求	安全物理环境	物理位置选择	√		
2			物理访问控制		√	
3			防盗窃和防破坏	√		
4			防雷击	√		
5			防火		√	
6			防水和防潮	√		
7			防静电			√
8			温湿度控制	√		
9			电力供应	√		
10			电磁防护	√		
11	安全通用要求	安全通信网络	网络架构		√	
12			通信传输	√		
13			可信验证			√
14	安全通用要求	安全区域边界	边界防护	√		
15			访问控制	√		
16			入侵防范		√	
17			恶意代码和垃圾邮件防范		√	
18			安全审计	√		
19			可信验证			√

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
20	安全通用要求	安全计算环境	身份鉴别	√		
21			访问控制	√		
22			安全审计	√		
23			入侵防范	√		
24			恶意代码防范	√		
25			可信验证			√
26			数据完整性	√		
27			数据备份恢复		√	
28			剩余信息保护	√		
29			个人信息保护	√		
30	安全通用要求	安全管理中心	系统管理		√	
31			审计管理	√		
32	安全通用要求	安全管理制度	安全策略	√		
33			管理制度	√		
34			制定和发布	√		
35			评审和修订	√		
36	安全通用要求	安全管理机构	岗位设置	√		
37			人员配备	√		
38			授权和审批	√		
39			沟通和合作	√		

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
40			审核和检查		√	
41	安全通用要求	安全管理人员	人员录用	√		
42			人员离岗	√		
43			安全意识教育和培训	√		
44			外部人员访问管理		√	
45	安全通用要求	安全建设管理	定级和备案	√		
46			安全方案设计			√
47			产品采购和使用	√		
48			自行软件开发			
49			外包软件开发		√	
50			工程实施	√		
51			测试验收		√	
52			系统交付	√		
53			等级测评	√		
54			服务供应商选择	√		
55	安全通用要求	安全运维管理	环境管理	√		
56			资产管理	√		
57			介质管理	√		
58			设备维护管理	√		
59			漏洞和风险管理			√

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
60			网络和系统安全管理	√		
61			恶意代码防范管理		√	
62			配置管理	√		
63			密码管理			√
64			变更管理	√		
65			备份与恢复管理	√		
66			安全事件处置	√		
67			应急预案管理	√		
68			外包运维管理			
安全通用要求控制点符合情况数量统计				47	12	7
控制点符合情况数量统计				47	12	7

3.13.2 安全问题汇总

针对单项测评结果中存在的部分符合和不符合项进行汇总，形成了安全问题如下表所示。

表 3-7 安全问题汇总表

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T1	（1）机房出入口未配置电子门禁系统。	信息化机房	安全通用要求	安全物理环境	物理访问控制	机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。
T2	（1）机房建设未完全采用符合耐火等级的建筑材料； （2）机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级。	信息化机房	安全通用要求	安全物理环境	防火	b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T3	（1）机房内缺乏防静电措施（如防静电地板或铺设防静电地毯 ）。	信息化机房	安全通用要求	安全物理环境	防静电	应采用防静电地板或地面并采用必要的接地防静电措施。
T4	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	安全通用要求	安全通信网络	网络架构	a）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
T5	（1）缺乏对通信设备可信验证方面的安全设计要求； （2）现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况。	安全通信网络	安全通用要求	安全通信网络	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T6	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	安全通用要求	安全区域边界	入侵防范	应在关键网络节点处监视网络攻击行为。
T7	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	安全通用要求	安全区域边界	恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。
T8	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	办公网区域 外网边界区域 安全管理区域 服务器存储区域	安全通用要求	安全区域边界	可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T9	（1）设备不具备相关可信验证的技术措施。	WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统	安全通用要求	安全计算环境	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
		核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2				警，并将验证结果形成审计记录送至安全管理中心。
T10	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。	业务终端-1 业务终端-2 应用服务器 数据库服务器-1 数据库服务器-2 运维及管理终端-1 运维及管理终端-2	安全通用要求	安全计算环境	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T11	（1）未能提供中间件重要数据的异地定时数据备份功能。	应用服务器-Tomcat	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T12	（1）未能提供数据库系统重要数据的异地定时数据备份功能。	数据库服务器-1-MSSQL 数据库服务器-2-Oracle	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T13	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	财务管理系统	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T14	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	重要业务数据 重要个人信息	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T15	（1）系统管理的资源、运行及配置管理不够全面。	管理中心	安全通用要求	安全管理中心	系统管理	b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T16	（1）单位开展的检查工作不够完善。	制度文件、执行/记录文件	安全通用要求	安全管理机构	审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。
T17	（1）单位未完全按管理规范开展人员离场后的清理工作。	制度文件、执行/记录文件	安全通用要求	安全管理人员	外部人员访问管理	c）外部人员离场后应及时清除其所有的访问权限。
T18	（1）单位未具备适用于被测系统的安全规划设计方案。	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
T19	（1）单位未具备完整的安全设计方案相关的文档； （2）单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	b）应根据保护对象的安全保护等级进行安全方案设计；
T20	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； （2）单位未对相关论证过程及内容进行完整的记录。	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	c）应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。
T21	（1）单位未在软件开发过程中对所有软件安全性进行测试； （2）单位未在软件安装之前按要求对所有软件开展恶意代码检测。	制度文件、执行/记录文件	安全通用要求	安全建设管理	外包软件开发	a）应在软件交付前检测其中可能存在的恶意代码；
T22	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	安全通用要求	安全建设管理	测试验收	a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；
T23	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	安全通用要求	安全建设管理	测试验收	b）应进行上线前的安全性测试，并出具安全测试报告。
T24	（1）单位未严格按规范开展漏洞及安全隐患检测工作。	制度文件、执行/记录文件	安全通用要求	安全运维管理	漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。
T25	（1）单位未严格按规范要求，针对防范恶意代码攻	制度文件、执行/记录文件	安全通用要求	安全运维管理	恶意代码防范管理	c）应定期检查恶意代码库的升级情况，对截

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
	击的技术措施的有效性验证，开展工作。					获的恶意代码进行及时分析处理。
T26	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	制度文件、执行/记录文件	安全通用要求	安全运维管理	密码管理	a）应遵循密码相关国家标准和行业标准；

4 整体测评

从安全控制间、区域间和验证测试等方面对单元测评的结果进行验证、分析和整体评价。

具体内容参见《GB/T 28448-2019信息安全技术 网络安全等级保护测评要求》。

4.1 安全控制点间安全测评

安全控制间的安全测评主要考虑同一区域内、同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用。安全功能上的增强和补充可以使两个不同强度、不同等级的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。

4.1.1 安全建设管理

4.1.1.1 安全通用要求

（T22）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。

单位未具备适用于被测系统的安全规划设计方案。安全方案设计不完善，导致规划设计需求不全面，信息系统存在安全缺陷。可升高单位未完全根据测试验收方案组织相关部门和人员开展验收工作的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

（T23）针对系统上线前的安全性测试工作存在问题。

单位未在软件交付之前按要求对所有软件开展恶意代码检测，导致在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。可升高针对系统上线前的安全性测试工作存在问题的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

4.1.2 安全运维管理

4.1.2.1 安全通用要求

（T25）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。

单位未严格按规范开展漏洞及安全隐患检测工作，漏洞检测工作不到位，导致存在未授权人员利用漏洞攻击信息系统的风险。可升高单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

4.2 区域间安全测评

区域间的安全测评主要考虑互连互通（包括物理上和逻辑上的互连互通等）的不同区域之间存在的安全功能增强、补充和削弱等关联作用，特别是有数据交换的两个不同区域。

4.2.1 安全物理环境

4.2.1.1 安全通用要求

（T1）机房出入口未配置电子门禁系统。

机房所在位置处于内部受控区域，非授权人员无法随意通过现有控制措施（如机械锁）进出机房，且具备相对完善的机房出入管理要求（具备《机房安全管理制度》），

并实际执行措施效果良好（具备《机房出入登记表》），可降低机房出入口访问控制措施缺失的问题严重程度（如信息化机房）。根据整体测评分析，问题严重程度变化为降低。

4.2.2 安全通信网络

4.2.2.1 安全通用要求

（T4）关键的应用服务和数据库服务网段未独立进行子网划分的情况。

单位有完整的IP地址规范，对IP地址的使用、回收均有记录《资产清单》，且系统具备相对完善的设备自身访问控制策略管理要求（具备《网络安全管理规范》、《设备及系统软件配置和操作手册》），措施效果良好，有助于部分补充未划分子网的安全功能不足（如安全通信网络）。根据整体测评分析，问题严重程度变化为降低。

4.2.3 安全区域边界

4.2.3.1 安全通用要求

（T6）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。

网络环境划分了相应的安全区域，区域间具备有效的访问控制措施，区域内各主机设备部署深信服EDR单机版，策略库、规则库更新及时，能够对攻击行为进行检测、阻断或限制，实际措施效果良好，且系统具备相对完善的策略库、规则库更新/校准管理要求，管理措施效果良好且及时检查更新有效性（具备《漏洞检测报告》、《主机安全管理规范》），可降低外部网络攻击防御措施缺失的问题严重程度（如办公网区域、安全管理区域）。根据整体测评分析，问题严重程度变化为降低。

（T7）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。

系统部署于可控的网络环境内（具备有效的访问控制、入侵防护措施）限制相关主机对象访问非受控网络，操作系统层面配置防御策略（具备本地防火墙策略、核心交换机地址限制策略、部署深信服EDR单机版），恶意代码入侵的可能性相对较低，可降低恶意代码防范措施缺失的问题严重程度（如办公网区域、安全管理区域）。根据整体测评分析，问题严重程度变化为降低。

4.3 整体测评结果汇总

经整体测评后安全问题严重程度变化情况如下表所示

表 4-1 整体测评结果汇总表

问题编号	安全问题描述	测评对象	整体测评描述	严重程度变化
T1	（1）机房出入口未配置电子门禁系统。	信息化机房	（1）机房所在位置处于内部受控区域，非授权人员无法随意通过现有控制措施（如机械锁）进出机房，且具备相对完善的机房出入管理要求（具备《机房安全管理制度》），并实际执行措施效果良好（具备《机房出入登记表》），可降低机房出入口访问控制措施缺失的问题严重程度。	□升高 ☑降低
T4	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	（1）单位有完整的IP地址规范，对IP地址的使用、回收均有记录《资产清单》，且系统具备相对完善的设备自身访问控制策略管理要求（具备《网络安全管理规范》、《设备及系统软件配置和操作手册》），措施效果良好，有助于部分补充未划分子网的安全功能不足。	□升高 ☑降低
T6	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	（1）网络环境划分了相应的安全区域，区域间具备有效的访问控制措施，区域内各主机设备部署深信服EDR单机版，策略库、规则库更新及时，能够对攻击行为进行检测、阻断或限制，实际措施效果良好，且系统具备相对完善的策略库、规则库更新/校准管理要求，管理措施	□升高 ☑降低

问题编号	安全问题描述	测评对象	整体测评描述	严重程度变化
			效果良好且及时检查更新有效性（具备《漏洞检测报告》、《主机安全管理规范》），可降低外部网络攻击防御措施缺失的问题严重程度。	
T7	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	（1）系统部署于可控的网络环境内（具备有效的访问控制、入侵防护措施）限制相关主机对象访问非受控网络，操作系统层面配置防御策略（具备本地防火墙策略、核心交换机地址限制策略、部署深信服EDR单机版），恶意代码入侵的可能性相对较低，可降低恶意代码防范措施缺失的问题严重程度。	□升高 ☑降低
T22	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	（1）单位未具备适用于被测系统的安全规划设计方案。安全方案设计不完善，导致规划设计需求不全面，信息系统存在安全缺陷。可升高单位未完全根据测试验收方案组织相关部门和人员开展验收工作的问题严重程度。	☑升高 □降低
T23	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	（1）单位未在软件交付之前按要求对所有软件开展恶意代码检测，导致在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。可升高针对系统上线前的安全性测试工作存在问题的问题严重程度。	☑升高 □降低
T25	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	（1）单位未严格按规范开展漏洞及安全隐患检测工作，漏洞检测工作不到位，导致存在未授权人员利用漏洞攻击信息系统的风险。可升高单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作的问题严重程度。	☑升高 □降低

5 安全问题风险分析

针对等级测评结果中存在的所有安全问题,结合关联资产和威胁分别分析安全问题可能产生的危害结果,找出可能对系统、单位、社会及国家造成的最大安全危害(损失),并根据最大安全危害(损失)的严重程度进一步确定安全问题的风险等级,结果为“高”、“中”或“低”。最大安全危害（损失）结果应结合安全问题所影响业务的重要程度、相关系统组件的重要程度、安全问题严重程度以及安全事件影响范围等进行综合分析。

表 5-1 安全问题风险分析

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
1	安全物理环境	（1）机房出入口未配置电子门禁系统。	信息化机房	物理攻击	（1）上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域，可能对系统的平稳运行造成影响。	中风险
2	安全物理环境	（1）机房建设未完全采用符合耐火等级的建筑材料; （2）机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级。	信息化机房	物理环境影响	（1）存在发生火情时助燃火灾的风险。	低风险
3	安全物理环境	（1）机房内缺乏防静电措施(如防静电地板或铺设防静电地毯 ）。	信息化机房	软硬件故障	（1）存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。	中风险
4	安全通信网络	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	恶意攻击	（1）上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变得更为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。	中风险
5	安全通信网络	（1）缺乏对通信设备可信验证方面的安全设计要求; （2）现有的通信设备存	安全通信网络	恶意攻击	（1）缺乏对系统可执行程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将	低风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
		在对系统运行过程中的可信检验完全缺失的情况。			导致计算资源被干扰和破坏造成损失。	
6	安全区域边界	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	恶意攻击	（1）存在不能及时发现内部主机作为攻击跳板，或网络攻击行为而造成系统损坏/网络资源浪费的风险。	中风险
7	安全区域边界	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	恶意攻击	（1）无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。	中风险
8	安全区域边界	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	办公网区域 外网边界区域 安全管理区域 服务器存储区域	恶意攻击	（1）缺乏对边界设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险
9	安全计算环境	（1）设备不具备相关可信验证的技术措施。	WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2	恶意攻击	（1）缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险
10	安全计算环境	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。	业务终端-1 业务终端-2 应用服务器 数据库服务器-1 数据库服务器-2 运维及管理终端-1 运维及管理终端-2	恶意攻击	（1）缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险
11	安全计算环境	（1）未能提供中间件重要数据的异地定时数据备份功能。	应用服务器-Tomcat	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的	中风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
					持续提供。	
12	安全计算环境	（1）未能提供数据库系统重要数据的异地定时数据备份功能。	数据库服务器-1-MSSQL 数据库服务器-2-Oracle	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供，使企业的经济利益或声誉受到损害。	中风险
13	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	财务管理系统	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。	中风险
14	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	重要业务数据 重要个人信息	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。	中风险
15	安全管理中心	（1）系统管理的资源、运行及配置管理不够全面。	管理中心	恶意攻击	（1）系统的资源和运行缺少统一的管理，将导致系统可能无法按规划实现基于资源配置、 系统加载、异常处理、及备份/恢复等的安全控制措施。	低风险
16	安全管理机构	（1）单位开展的检查工作不够完善。	制度文件、执行/记录文件	管理不到位	（1）检查工作开展不仔细，可能对存在或潜在的安全风险不能被及时发现并进行处理。	低风险
17	安全管理人员	（1）单位未完全按管理规范开展人员离场后的清理工作。	制度文件、执行/记录文件	管理不到位	（1）人员离场后的清理工作开展不规范，可能导致遗留外部人员访问受控区域的记录，存在被二次非法利用，造成泄密。	低风险
18	安全建设管理	（1）单位未具备适用于被测系统的安全规划设计方案。	制度文件、执行/记录文件	管理不到位	（1）规划设计需求不全面，可能导致安全方案设计不完善，信息系统存在安全缺陷。	低风险
19	安全建设管理	（1）单位未具备完整的安全设计方案相关的文档; （2）单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	管理不到位	（1）相关合规的规划配套文件缺失，可能导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。	中风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
20	安全建设管理	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； （2）单位未对相关论证过程及内容进行完整的记录。	制度文件、执行/记录文件	管理不到位	（1）未开展规范的审批过程，可能存在安全整体规划缺乏合理性和可行性，导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。	低风险
21	安全建设管理	（1）单位未在软件开发过程中对所有软件安全性进行测试； （2）单位未在软件安装之前按要求对所有软件开展恶意代码检测。	制度文件、执行/记录文件	管理不到位	（1）软件交付前恶意代码检测不规范，可能在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。	低风险
22	安全建设管理	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	管理不到位	（1）可能由于验收测试不严谨，造成测试过程缺乏计划性及操作性，无法保证经过测试验收的系统达到既定的安全性等目标。	低风险
23	安全建设管理	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	管理不到位	（1）未按规定开展上线前测试，安全隐患可能在系统上线运行前未被发现并作出相应处理。	低风险
24	安全运维管理	（1）单位未严格按规范开展漏洞及安全隐患检测工作。	制度文件、执行/记录文件	管理不到位	（1）漏洞检测、修补工作不到位，可能存在未授权人员利用漏洞攻击信息系统的风险。	低风险
25	安全运维管理	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	管理不到位	（1）可能导致系统恶意代码检测管理不到位，存在信息系统感染恶意代码，从而导致严重的信息安全风险。	低风险
26	安全运维管理	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	制度文件、执行/记录文件	管理不到位	（1）密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不到位，存在违反国家政策的风险。	中风险

6 等级测评结论

等级测评结论由安全问题风险分析结果和综合得分共同确定，判定依据如下表所示。

表 6-1 等级测评结论判别依据

测评结论	判别依据
优	被测对象中存在安全问题，但不会导致被测对象面临中、高等级安全风险，且系统综合得分 90 分以上（含90 分）。
良	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分 80分以上（含 80分）。
中	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分 70分以上（含 70分）
差	被测对象中存在安全问题，而且会导致被测对象面临高等级安全风险，或被测对象综合得分低于 70 分。

综合得分计算方法如下：

设M为被测对象的综合得分，$M = V_t + V_m$，V_t和V_m根据下列公式计算。

$$V_t = \begin{cases} 100 \cdot y - \sum_{k=1}^{t} f(\omega_k) \cdot (1 - x_k) \cdot S, & V_t > 0 \\ 0, & V_t \le 0 \end{cases}$$

$$V_m = \begin{cases} 100 \cdot (1 - y) - \sum_{k=1}^{m} f(\omega_k) \cdot (1 - x_k) \cdot S, & V_m > 0 \\ 0, & V_m \le 0 \end{cases}$$

$$0 \le x_k \le 1,\ S = 100 \cdot \frac{1}{n},\ f(\omega_k) = \begin{cases} 1, & \omega_k = \text{一般} \\ 2, & \omega_k = \text{重要} \\ 3, & \omega_k = \text{关键} \end{cases}$$

其中，y为关注系数，取值在0至1之间，由等级保护工作管理部门给出，默认值为0.5。n为被测对象涉及的总测评项数（不含不适用项，下同），t为技术方面对应的总测评项数，V_t为技术方面的得分，m为管理方面对应的总测评项数，V_m为管理方面的得

分，ω_k为测评项k的重要程度（分为一般、重要和关键），x_k为测评项k的得分，如果测评项k涉及多测评项对象，则x_k取值为多测评对象得分的算术平均值。

x_k的得分计算如下：

测评项k涉及对象 / 测评项k定性判定	只涉及单个对象	涉及多个对象
符合	1	1
部分符合	0.5	计算测评对象平均分，取值在0至1之间
不符合	0	0

注：当测评项k涉及多个对象时，针对每个对象的得分取值为1、0.5和0。

根据第5章安全问题风险分析结果统计高、中、低风险安全问题的数量，利用综合得分计算公式计算出被测对象的综合得分，并将相关结果填入下表。

表 6-2 安全问题统计和综合得分

被测对象名称	安全问题数量			综合得分
	高风险	中风险	低风险	
财务管理系统	0	11	15	73.85

依据 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》和GB/T 28448—2019《信息安全技术 网络安全等级保护测评要求》的第二级要求，经对财务管理系统的安全保护状况进行综合分析评价，等级测评结论如下：

财务管理系统本次等级测评的综合得分为73.85，且不存在高等级安全风险，等级测评结论为中。

7 安全问题整改建议

表 7-1 安全问题整改建议

序号	安全类	安全问题	关联资产	整改建议
1	安全物理环境	(1)机房出入口未配置电子门禁系统。	信息化机房	(1) 采用电子门禁系统严格控制机房其他出入口的进出，或安排专人值守； (2) 采用电子门禁系统，对机房所有人员出入进行登记记录，并保存。
2	安全物理环境	(1)机房建设未完全采用符合耐火等级的建筑材料； (2)机房建设不具备防火设计/验收文档,或机房验收文档未明确相关建筑材料的耐火等级。	信息化机房	(1) 机房及相关的工作房间和辅助房采用具有耐火等级的建筑材料； (2) 机房建设采用符合相关耐火等级（二级）的建筑材料。（内外墙壁均应采用具有防火涂料、隔热板、铝板、钢板等阻燃或不燃的材料）； (3) 机房耐火等级建筑材料有相关合格证，并留存机房验收文档。
3	安全物理环境	(1)机房内缺乏防静电措施（如防静电地板或铺设防静电地毯）。	信息化机房	(1) 机房铺设防静电地板或铺设防静电地毯； (2) 机房房静电设计可依据GB50174-2008和GB50314-2006相关规定进行机房设计和验收。
4	安全通信网络	(1)关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	(1) 建议独立划分出应用服务器网段、数据库服务器网段。
5	安全通信网络	(1)缺乏对通信设备可信验证方面的安全设计要求； (2)现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况。	安全通信网络	(1) 建议在管理规范文档内对通信设备可信验证方面的安全设计提出要求； (2) 建议系统实现对所有可执行环节进行可信验证，包括: 运行过程中的可信检验: ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■通信应用连接过程。
6	安全区域边界	(1) 网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	(1) 建议网络层部署的防火墙配置对内部发起的攻击行为实现防范功能策略，实现检测、防止或限制从内部发起的网络攻击行为； (2) 内部安全防范措施能检测以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、碎片攻击、网络蠕虫攻击、应用漏洞攻击。
7	安全区域	(1)现有部署的恶意代码防	办公网区域	(1) 建议现有部署的恶意代码防范措

序号	安全类	安全问题	关联资产	整改建议
	边界	范措施存在不合规的问题，网络边界覆盖不全面。	安全管理区域	施网络边界覆盖全面，及时对恶意代码及逆行检测和清除。
8	安全区域边界	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）建议对边界设备系统程序的可信验证设计并保存设计文件； （2）建议系统实现对所有可执行环节进行可信验证。
9	安全计算环境	（1）设备不具备相关可信验证的技术措施。	WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2	（1）建议通过设备的启动过程和运行过程中对预装软件（包括系统引导程序、系统程序、相关应用程序和重要配置参数）的完整性验证或检测，确保对系统引导程序、系统程序、重要配置参数和关键应用程序可信根验证； （2）建议设备启用在检测到其可信性受到破坏后进行报警的相关功能。
10	安全计算环境	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。	业务终端-1 业务终端-2 应用服务器 数据库服务器-1 数据库服务器-2 运维及管理终端-1 运维及管理终端-2	（1）建议对计算设备系统程序的可信验证设计并保存设计文件； （2）建议系统实现对所有可执行环节进行可信验证。
11	安全计算环境	（1）未能提供中间件重要数据的异地定时数据备份功能。	应用服务器-Tomcat	（1）建议设置异地灾备机房，并利用通信网络将中间件重要数据定时备份至备份场地； （2）异地备份的中间件数据范围（不限于）包括系统的： ■配置数据 ■重要日志数据。
12	安全计算环境	（1）未能提供数据库系统重要数据的异地定时数据备份功能。	数据库服务器-2-Oracle	（1）建议设置异地灾备机房，并利用通信网络将重要数据定时备份至备份场地； （2）异地备份的数据范围（不限于）

序号	安全类	安全问题	关联资产	整改建议
				包括系统的： ■配置数据 ■重要业务数据。
			数据库服务器-1-MSSQL	（1）建议设置异地灾备机房，并利用通信网络将重要数据定时备份至备份场地； （2）异地备份的数据范围（不限于）包括系统的： ■配置数据 ■重要业务数据。
13	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	财务管理系统	（1）建议设置异地灾备机房，并利用通信网络将应用软件系统重要数据定时备份至备份场地； （2）异地备份的应用软件系统数据范围（不限于）包括系统的：配置数据、重要日志数据，业务数据。
14	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	重要业务数据 重要个人信息	（1）建议设置异地灾备机房，并利用通信网络将应用软件系统重要数据定时备份至备份场地。
15	安全管理中心	（1）系统管理的资源、运行及配置管理不够全面。	管理中心	（1）需实现系统包括对可信证书管理、可信基准库的管理。
16	安全管理机构	（1）单位开展的检查工作不够完善。	制度文件、执行/记录文件	（1）建议单位按要求提供安全检查报告。
17	安全管理人员	（1）单位未完全按管理规范开展人员离场后的清理工作。	制度文件、执行/记录文件	（1）建议单位按管理规范开展人员离场后的清理工作。至少包括：保留清理记录、及时清除离场后的所有访问权限、记录访问权限清除时间。
18	安全建设管理	（1）单位未具备适用于被测系统的安全规划设计方案。	制度文件、执行/记录文件	（1）建议单位根据等保要求进行过全面的自查或对比，根据系统的安全级别选择基本安全措施； （2）建议规划方案需根据风险分析结果对系统安全措施进行补充和整，并在系统建设\\整改方案中有详细描述。
19	安全建设管理	（1）单位未具备完整的安全设计方案相关的文档； （2）单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	（1）建议单位根据信息系统的等级划分情况，准备安全设计方案、安全管理策略、安全建设规划文档等； （2）建议相关文档内容应完善，包括统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、密码技术要求、总体建设规划和详细设计方案，并形成一致性的配套文件。

序号	安全类	安全问题	关联资产	整改建议
20	安全建设管理	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； （2）单位未对相关论证过程及内容进行完整的记录。	制度文件、执行/记录文件	（1）建议单位组织相关部门和安全技术专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定； （2）保存论证和审定记录，记录包括批准时间、批准人员签字； （3）文件经过批准后，才能正式实施。
21	安全建设管理	（1）单位未在软件开发过程中对所有软件安全性进行测试； （2）单位未在软件安装之前按要求对所有软件开展恶意代码检测。	制度文件、执行/记录文件	（1）建议开发商提供软件源代码，软件安装前检测软件中的恶意代码； （2）输出检测报告（或提供第三方检测报告），内容包括测试时间、测试地点、测试对象、测试结论、测试人员。
22	安全建设管理	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	（1）建议根据测试验收过程记录与结果，形成测试验收报告。
23	安全建设管理	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	（1）建议系统建设完成后，委托第三方测试单位对系统进行安全性测试，并出具安全性测试报告； （2）测试报告内容至少包括测试时间、测试地点、测试人、测试对象、测试方法、测试过程、测试发现的安全问题、整改建议、测试结论，并有第三方测试机构的签字盖章。
24	安全运维管理	（1）单位未严格按规范开展漏洞及安全隐患检测工作。	制度文件、执行/记录文件	（1）建议单位定期开展漏洞扫描，对发现的安全漏洞和隐患进行及时修补评估； （2）对必需修补的安全漏洞和隐患进行加固测试，测试无误后，备份系统数据，再从生产环境进行修补； （3）对于剩余安全漏洞和隐患进行残余风险分析，明确安全风险整改原则。
25	安全运维管理	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	（1）建议单位按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。包括;定期对相关产品的恶意代码库进行升级；对相关设备升级情况进行记录；对各类防病毒产品上截获的恶意代码进行分析并汇总上报； （2）单位需保留完整的恶意代码检测/升级的记录。至少具备：执行人、升级结果/检测结果、处理方式、负责人签字 。

序号	安全类	安全问题	关联资产	整改建议
26	安全运维管理	(1)单位不了解现有密码相关的国家标准和行业标准； (2)单位缺乏密码管理要求的制度文档。	制度文件、执行/记录文件	（1）建议单位学习现有密码相关的国家标准和行业标准。建立密码管理要求的制度文档。

漏洞安全问题整改建议

序号	安全类	安全问题	关联资产	整改建议
1	安全计算环境	允许Traceroute探测 此类漏洞涉及网络设备、安全设备、服务器存储设备。	10.2.4.14/数据库服务器-2 10.2.4.12/数据库服务器-1 10.2.4.13/应用服务器 10.2.1.4/运维安全管理系统 10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/上网行为管理系统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/汇聚交换机 172.16.1.2/核心交换机	在防火墙出站规则中禁用echo-reply（type 0）、time-exceeded（type 11）、destination-unreachable（type 3）类型的ICMP包。
2	安全计算环境	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161) 此类漏洞涉及网络设备。	172.16.1.2/核心交换机	临时解决方法：* 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://downloads.ssh.com/ 对于具体Linux发行版中使用的版本，可以参考如下链接,确认系统是否受该漏洞影响:

序号	安全类	安全问题	关联资产	整改建议
				Redhat ------- https://rhn.redhat.com/errata/RHSA-2009-1287.html Suse ------- http://support.novell.com/security/cve/CVE-2008-5161.html Ubuntu ------- http://people.canonical.com/~ubuntu-security/cve/2008/CVE-2008-5161.html
3	安全计算环境	缺少“X-Content-Type-Options”响应头 此类漏洞涉及业务应用软件平台。	https://s.mmpt.edu.cn/财务管理系统	在服务器中配置X-Content-Type-Options响应头为“nosniff”。

【正文结束】

附录A 被测对象资产

A.1 物理机房

附录A 表- 1物理机房

序号	机房名称	物理位置	重要程度
1	信息化机房	茂名市茂南区文明北路232号大院大楼	关键

A.2 网络设备

附录A 表- 2网络设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度	备注
1	核心交换机	否	H3C version 7.1.070, Release 7585P07	H3C S7500E-X	核心数据交换、访问控制	关键	
2	汇聚交换机	否	H3C version 7.1.070, Release 6126P20	H3C S5560X-30C-EI	数据交换	重要	

A.3 安全设备

附录A 表- 3安全设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度	备注
1	防火墙-1	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键	
2	WEB应用防火墙	否	深信服AF 8.0.9	深信服WAF-2000-H642	应用防护、入侵防范、病毒防护	重要	
3	运维安全管理系统	否	深信服V3.0.6	深信服AC-1000-D603-PT	运维审计	重要	
4	基线核查系统	否	深信服V3.0.3	深信服AC-1000-D602-PT	漏洞扫描	重要	
5	日志审计系统	否	深信服LAS 3.0.5	深信服AC-1000-D601-PT	日志审计	重要	
6	上网行为管理系统	否	深信服AC12.0.26	深信服AC-1000-D600-PT	上网行为管理及终端准入控制	重要	
7	防火墙-2	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键	

A.4 服务器

附录A 表-4服务器

序号	设备名称	所属业务应用系统/平台名称	是否虚拟设备	操作系统及版本	数据库管理系统及版本	中间件及版本	重要程度	备注
1	应用服务器	财务管理系统	否	Windows Server 2016 R2	/	Tomcat 9.0.13	关键	
2	数据库服务器-1	财务管理系统	否	Windows Server 2016 R2	MSSQL 2014 R2	/	关键	
3	数据库服务器-2	财务管理系统	否	Windows Server 2016 R2	Oracle 11.2.0.1.0	/	关键	

A.5 终端设备

附录A 表-5终端设备

序号	设备名称	是否虚拟设备	操作系统/控制软件及版本	用途	重要程度	备注
1	业务终端-2	否	Windows 10 （版本 20H2 （内部版本 19044.1889）	业务管理	一般	
2	运维及管理终端-2	否	Windows 10 （版本 21H2 （内部版本 19044.1889）））	运维管理、系统管理	一般	
3	运维及管理终端-1	否	Windows 10 （版本 20H2 （内部版本 19044.1889）	运维管理、系统管理	一般	
4	业务终端-1	否	Windows 10 （版本 20H2 （内部版本 19044.1889）	业务管理	一般	

A.6 其他系统或设备

附录A 表-6其他系统或设备

序号	设备名称	是否虚拟设备	操作系统/控制软件及版本	用途	重要程度	备注
/	/	/	/	/	/	/

注释：本次测评对象中不涉及专用移动互联终端等，不开展抽测。

A.7 系统管理软件/平台

附录A 表-7系统管理软件/平台

序号	系统管理软件/平台名称	所在设备名称	版本	主要功能	重要程度	备注
1	数据库服务器-2-Oracle	应用/数据库服务器	11.2.0.1.0	数据生产、存储	关键	
2	应用服务器-Tomcat	应用/数据库服务器	9.0.13	页面发布	关键	
3	数据库服务器-1-MSSQL	应用/数据库服务器	2014 R2	数据生产、存储	关键	

A.8 业务应用软件/平台

附录A 表-8业务应用系统/平台

序号	业务应用系统/平台名称	主要功能	业务应用软件及版本	开发厂商	重要程度
1	财务管理系统	财务管理系统包含财务核算、学生收费、预算管理、结算、工资管理功能模块，年终结转该系统通过专网与财政系统进行联通通信，涵盖学生收费、奖贷学金发放、预算管理、工资管理、工资结算等业务，是学校财务流转的核心业务系统。	V3.0	天津神州浩天科技有限公司	关键

A.9 数据资源

附录A 表-9数据资源

序号	数据类别	所属业务应用	安全防护需求	重要程度
1	重要业务数据	财务管理系统	完整性、保密性	关键
2	重要个人信息	财务管理系统	完整性、保密性	关键
3	鉴别数据	财务管理系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性、保密性	关键
4	重要审计数据	财务管理系统（安全管理中心）	完整性	重要
5	重要配置数据	财务管理系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/	完整性	关键

序号	数据类别	所属业务应用	安全防护需求	重要程度
		平台)		

注释：网络设备、安全设备、服务器、终端、系统管理软件/平台和业务应用系统等所涉及的鉴别数据和重要配置数据分别在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。重要审计数据在安全管理中心进行汇总测评证据，包括数据完整性。重要业务数据和重要个人信息分别在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。

A.10 密码产品

附录A 表- 10密码产品

序号	产品/模块名称	生成厂商	商密型号	密码算法	用途	重要程度
/	/	/	/	/	/	/

注释：本次测评不存在加密机等密码产品。

A.11 安全相关人员

附录A 表- 11安全相关人员

序号	姓名	岗位/角色	联系方式	所属单位
1	叶永利	安全管理员	0668-2920122	茂名职业技术学院
2	杨云	审计管理员	0668-2920122	茂名职业技术学院
3	杨云	资产管理员	0668-2920122	茂名职业技术学院
4	吴国华	系统管理员	0668-2920122	茂名职业技术学院
5	吴国华	机房管理员	0668-2920122	茂名职业技术学院
6	龙恒	数据管理员	13377766618	茂名职业技术学院
7	龙恒	应用管理员	13377766618	茂名职业技术学院
8	龙恒	网络管理员	13377766618	茂名职业技术学院

A.12 安全管理文档

附录A 表- 12安全管理文档

序号	文档名称	主要内容
1	制度类文档-恶意代码	关于单位恶意代码工作管理制度文档

序号	文档名称	主要内容
	防范管理制度	
2	制度类文档-测试及验收方案	关于单位测试验收方案文档
3	制度类文档-变更控制管理制度	关于单位变更流程、控制管理制度文档
4	制度类文档-信息安全总体策略	关于单位网络安全方针、策略制度文档
5	制度类文档-授权和审批管理规定	关于单位授权审批、审批流程规范制度文档
6	制度类文档-工程实施管理制度	关于单位工程实施工作管理制度文档
7	制度类文档-安全审查和检查管理规范	关于单位安全检查、审查工作规范制度文档
8	制度类文档-信息系统外包运维管理制度	关于单位外包运维工作管理制度文档
9	制度类文档-系统安全管理制度	关于单位系统安全管理、安全服务管理制度文档
10	制度类文档-介质管理制度	关于单位介质安全管理工制度文档
11	制度类文档-信息系统恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
12	制度类文档-人员管理制度	关于单位人员录用、调岗、离岗管理制度文档
13	制度类文档-备份与恢复管理制度	关于单位数据备份、恢复管理制度文档
14	制度类文档-设备安全管理制度	关于单位设备安全管理制度文档
15	制度类文档-工程测试验收管理	关于单位工程测试工作管理制度文档
16	制度类文档-外部服务人员管理规范	关于单位针对外部人员工作管理规范制度文档
17	制度类文档-安全管理组织规范	关于单位组织结构管理规范制度文档
18	制度类文档-网络安全管理制度	关于单位网络安全工作管理制度文档
19	制度类文档-网络安全事件应急预案	关于单位网络安全事件应急处理、流程、培训等管理制度文档
20	制度类文档-应用系统业务用户密码设置规定	关于单位用户密码管理制度文档
21	制度类文档-岗位安排及岗位职责	关于单位岗位职责、岗位安排制度文档

序号	文档名称	主要内容
22	制度类文档-系统及应用数据备份管理规范	关于单位数据备份、恢复管理制度文档
23	制度类文档-办公环境保密管理	关于单位办公环境管理制度文档
24	制度类文档-制度制定、发布、评审和修订管理制度	关于单位制度制定、发布、评审和修订等管理文档
25	制度类文档-安全漏洞管理制度	关于单位安全漏洞管理工作制度文档
26	制度类文档-服务供应商选择安全管理制度	关于单位安全服务供应商管理规定制度文档
27	制度类文档-信息安全奖惩办法	关于单位人员奖惩制度文档
28	制度类文档-数据安全管理规范	关于保障关键数据安全，从数据库本身、数据加密、数据备份恢复三个方面对数据安全进行规范的制度文档
29	制度类文档-离岗人员工作交接规范	关于单位离岗交接工作规范制度文档
30	制度类文档-外部接入受控网络访问系统管理规范	关于单位针对外部人员工作接入规范制度文档
31	制度类文档-信息安全漏洞扫描规范	关于单位安全漏洞工作规范制度文档
32	制度类文档-安全事件报告和处置	关于单位网络安全事件管理、处置、流程等报告制度文档
33	制度类文档-物理安全管理规范	关于加强单位办公区域及电子计算机机房的管理和设备运行安全，规范办公区域及机房建设，使人员办公高效及机房设备安全、稳定运行的制度文档
34	制度类文档-组织安全结构和人员职责制度	关于单位安全结构、人员职责
35	制度类文档-组织安全结构和人员职责制度	关于单位组织结构、人员安排、人员职责制度文档
36	制度类文档-网络与信息系统安全设计规范	关于单位网络与信息化安全设计制度文档
37	制度类文档-网络安全管理规范	关于保障单位网络系统的安全稳定运行，抵御内部和外部各种形式的网络攻击或威胁制定的管理文档
38	制度类文档-外包开发软件管理规定	关于单位外包项目管理工作制度文档
39	制度类文档-办公环境管理制度	关于单位办公环境管理制度文档
40	制度类文档-员工考核管理制度	关于单位人员考核工作管理制度文档
41	制度类文档-恶意代码防范管理制度	关于单位恶意代码防范工作制度文档

序号	文档名称	主要内容
42	制度类文档-网络安全事件报告制度	关于单位网络安全事件管理报告文档
43	制度类文档-外部人员访问管理制度	关于单位针对外来人员访问管控制度文档
44	制度类文档-机房安全管理制度	关于单位机房安全管理工作制度文档
45	制度类文档-主机安全管理规范	关于规定单位主机系统安全管理要求规范，指导业务平台主机的安全配置和维护的制度文档
46	制度类文档-系统交付管理	关于单位交付工作管理制度文档
47	制度类文档-安全教育和培训制度	关于单位安全培训、安全交流工作制度文档
48	制度类文档-应用安全管理规范	关于规定单位应用安全管理要求及规范的制度文档
49	操作类文档-设备及系统软件配置和操作手册	关于单位安全设备操作、Linux服务器配置手册、主机运维操作手册、软件操作手册、防火墙配置和操作手册、数据库日常运维操作手册等指导文档
50	操作类文档-软硬件日常维护管理规程	关于单位计算机网络系统使用、管理、信息安全、资源共享有所遵循,规范上网操作流程,提高网络系统安全性的指导文档
51	操作类文档-设备操作规程	关于单位相关设备操作指导文档
52	操作类文档-数据备份策略	关于单位数据备份策略文件
53	记录类文档-存储介质目录清单	关于备份介质存储工作清单
54	记录类文档-通用变更记录表	关于单位变更工作记录
55	记录类文档-软件交付清单	关于单位交付工作记录
56	记录类文档-机房维护日志	关于机房维护工作记录
57	记录类文档-机房巡检记录表	关于单位机房环境巡检记录
58	记录类文档-技能培训记录	关于单位系统培训工作、考核工作记录
59	记录类文档-离职员工物品交回登记表	关于人员离岗工物交接工作记录
60	记录类文档-系统交付清单	关于单位交付工作记录
61	记录类文档-评审和修订记录	关于单位变更评审、修订工作记录
62	记录类文档-应急预案培训记录表	关于单位应急预案培训工作记录

序号	文档名称	主要内容
63	记录类文档-收发文登记记录	关于单位文档签发记录
64	记录类文档-设备维修申请表	关于单位设备维护工作申请记录
65	记录类文档-外部会议文件和记录	关于单位外部联系、交流及会议工作记录
66	记录类文档-信息安全检查记录表	关于单位安全检查工作记录
67	记录类文档-专家论证记录表	关于单位网络方案论证记录
68	记录类文档-备份介质使用记录	关于备份介质使用登记工作记录
69	记录类文档-网络配置信息	关于单位配置信息登记工作记录
70	记录类文档-网络信息安全事件记录表	关于单位网络安全事件工作记录
71	记录类文档-信息系统存储介质使用清单	关于备份介质存储使用清单
72	记录类文档-人员培训及考核记录表	关于人员培训、考核等工作记录
73	记录类文档-监理审批表	关于单位监理审核工作记录
74	记录类文档-设备操作维护记录	关于单位设备维护工作记录
75	记录类文档-外部人员访问记录表	关于外来人员访问登记工作记录
76	记录类文档-重要操作审批表	关于单位审批工作记录
77	记录类文档-机房设备维护记录表	关于设备维护登记工作记录
78	记录类文档-漏洞检测报告	关于单位安全漏洞检测报告文档
79	记录类文档-机房设备维修记录表	关于单位机房设备维修工作记录
80	记录类文档-信息管理系统漏洞检查表	关于单位安全漏洞工作检测记录表
81	记录类文档-外部人员访问申请表	关于外来人员访问申请流程工作记录
82	记录类文档-数据恢复申请表	关于单位数据恢复工作申请表
83	记录类文档-机房出入登记表	关于人员进出机房登记工作记录
84	记录类文档-人员离岗	关于人员离岗申请记录

序号	文档名称	主要内容
	申请表	
85	记录类文档-数据备份记录表	关于单位数据备份工作记录
86	记录类文档-设备出入登记记录表	关于设备进出机房登记工作记录
87	记录类文档-信息安全会议记录	关于单位安全培训、安全交流会议记录
88	记录类文档-安全建设方案评审纪录	关于单位网络与信息化安全设计方案评审工作记录
89	记录类文档-接入受控网络申请表	关于外来人员接入工作记录
90	记录类文档-信息系统存储介质销毁申请表	关于备份介质销毁申请工作记录
91	记录类文档-人员入职考核记录	关于人员录用、考核工作记录
92	记录类文档-关键岗位人员考核记录	关于关键岗位考核工作记录
93	记录类文档-访问记录表	关于人员访问工作记录
94	记录类文档-安全管理制度评审记录	关于单位制度审计记录
95	记录类文档-离场信息资料交接表	关于人员离岗交接工作记录
96	记录类文档-备份工作汇总表	关于单位数据备份工作总结表
97	证据类文档-信息安全事件分析报告表	关于单位安全事件分析报告
98	证据类文档-定级备案	关于单位系统定级报告、备案证文件
99	证据类文档-外部联系表	关于单位内部联系及外部联系名单
100	证据类文档-网络安全等级保护测评服务合同	关于单位与安全服务商签定的安全服务合同文件
101	证据类文档-网络安全等级保护工作小组名单	关于单位网络安全等级保护工作小组人员名单文件
102	证据类文档-工程项目实施方案	关于单位工程实施方案文档
103	证据类文档-深信服安全采购合同	关于单位与安全厂家服务采购、产品选择合同文件
104	证据类文档-安全职位人员	关于单位人员岗位安排名单
105	证据类文档-网络安全	关于单位网络与信息化安全设计方案文档

序号	文档名称	主要内容
	系统设计方案	
106	证据类文档-资产清单	关于单位信息系统资产清单统计表

附录B 上次测评问题整改情况说明

此次为财务管理系统初次等级测评，之前未实施过等级保护测评工作。

附录B 表- 1上次测评问题整改情况

序号	主要安全问题	整改情况	情况说明
/	/	□已整改 □未整改	/

附录C 单项测评结果汇总

C.1 安全物理环境

附录 C 表-1 安全物理环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			物理位置选择	物理访问控制	防盗窃和防破坏	防雷击	防火	防水和防潮	防静电	温湿度控制	电力供应	电磁防护
1	信息化机房	符合	2	0	2	1	1	2	0	1	2	1
		部分符合	0	1	0	0	0	0	0	0	0	0
		不符合	0	0	0	0	1	0	1	0	0	0
		不适用	0	0	0	0	0	0	0	0	0	0

附录 C 表-2 安全物理环境单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.2 安全通信网络

附录 C 表-3 安全通信网络单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求		
			网络架构	通信传输	可信验证
1	安全通信网络	符合	1	1	0
		部分符合	1	0	0
		不符合	0	0	1
		不适用	0	0	0

附录 C 表-4 安全通信网络单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.3 安全区域边界

附录 C 表-5 安全区域边界单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求					
			边界防护	访问控制	入侵防范	恶意代码和垃圾邮件防范	安全审计	可信验证
1	外网边界区域	符合	1	4	1	1	3	0
		部分符合	0	0	0	0	0	0
		不符合	0	0	0	0	0	1
		不适用	0	0	0	0	0	0
2	安全管理区域	符合	1	4	0	0	3	0
		部分符合	0	0	0	1	0	0
		不符合	0	0	1	0	0	1
		不适用	0	0	0	0	0	0
3	服务器存储区域	符合	1	4	1	1	3	0
		部分符合	0	0	0	0	0	0
		不符合	0	0	0	0	0	1
		不适用	0	0	0	0	0	0
4	办公网区域	符合	1	4	0	0	3	0
		部分符合	0	0	0	1	0	0
		不符合	0	0	1	0	0	1
		不适用	0	0	0	0	0	0

附录 C 表-6 安全区域边界单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.4 安全计算环境

C.4.1 网络设备

附录 C 表-7 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	汇聚交换机	符合	3	4	3	4	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	1	0	0	1	1	--
2	核心交换机	符合	3	4	3	4	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	1	0	0	1	1	--

C.4.2 安全设备

附录 C 表-8 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	基线核查系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
2	上网行为管理系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
3	WEB应用防火墙	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
4	防火墙-1	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
5	防火墙-2	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
6	日志	符合	3	4	3	5	0	0	1	1	0	--

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
	审计系统	部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
7	运维安全管理系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--

C.4.3 服务器和终端

附录 C 表-9 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	数据库服务器-1	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
2	应用服务器	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
3	数据库服务器-2	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
4	业务终端-2	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
5	业务终端-1	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
		不适用	0	0	0	1	0	0	0	1	0	--
6	运维及管理终端-2	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
7	运维及管理终端-1	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--

C.4.4 系统管理软件/平台

附录 C 表-10 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	应用服务器-Tomcat	符合	0	4	3	2	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	3	0	0	3	1	1	0	0	0	--
2	数据库服务器-1-MSSQL	符合	3	4	3	2	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	0	0	0	3	1	1	0	0	0	--
3	数据库服务器-2-Oracle	符合	3	4	3	2	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	0	0	0	3	1	1	0	0	0	--

C.4.5 业务应用系统/平台

附录 C 表-11 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	财务管理系统	符合	3	4	3	3	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	0	0	0	2	1	1	0	0	0	--

C.4.6 数据资源

附录 C 表-12 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	重要个人信息	符合	--	--	--	--	--	--	1	1	0	2
		部分符合	--	--	--	--	--	--	0	0	0	0
		不符合	--	--	--	--	--	--	0	1	0	0
		不适用	--	--	--	--	--	--	0	0	1	0
2	重要业务数据	符合	--	--	--	--	--	--	1	1	0	0
		部分符合	--	--	--	--	--	--	0	0	0	0
		不符合	--	--	--	--	--	--	0	1	0	0
		不适用	--	--	--	--	--	--	0	0	1	2

C.4.7 其他系统或设备

附录 C 表-13 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	--	符合	--	--	--	--	--	--	--	--	--	--
		部分符合	--	--	--	--	--	--	--	--	--	--
		不符合	--	--	--	--	--	--	--	--	--	--
		不适用	--	--	--	--	--	--	--	--	--	--

C.5 安全管理中心

附录 C 表-14 安全管理中心单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求	
			系统管理	审计管理
1	管理中心	符合	1	2
		部分符合	0	0
		不符合	1	0
		不适用	0	0

附录 C 表-15 安全管理中心单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.6 安全管理制度

附录 C 表-16 安全管理制度单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求			
			安全策略	管理制度	制定和发布	评审和修订
1	制度文件、执行/记录文件	符合	1	2	2	1
		部分符合	0	0	0	0
		不符合	0	0	0	0
		不适用	0	0	0	0

C.7 安全管理机构

附录 C 表-17 安全管理机构单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求				
			岗位设置	人员配备	授权和审批	沟通和合作	审核和检查
1	制度文件、执行/记录文件	符合	2	1	2	3	0
		部分符合	0	0	0	0	1
		不符合	0	0	0	0	0
		不适用	0	0	0	0	0

C.8 安全管理人员

附录 C 表-18 安全管理人员单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求			
			人员录用	人员离岗	安全意识教育和培训	外部人员访问管理
1	制度文件、执行/记录文件	符合	2	1	1	2
		部分符合	0	0	0	0
		不符合	0	0	0	1
		不适用	0	0	0	0

C.9 安全建设管理

附录 C 表-19 安全建设管理单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			定级和备案	安全方案设计	产品采购和使用	自行软件开发	外包软件开发	工程实施	测试验收	系统交付	等级测评	服务供应商选择
1	制度文件、执行/记录文件	符合	4	0	2	0	1	2	0	3	3	2
		部分符合	0	0	0	0	0	0	1	0	0	0
		不符合	0	3	0	0	1	0	1	0	0	0
		不适用	0	0	0	2	0	0	0	0	0	0

附录 C 表-20 安全建设管理单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.10 安全运维管理

附录 C 表-21 安全运维管理单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求												
			环境管理	资产管理	介质管理	设备维护管理	漏洞和风险管理	网络和系统安全管理	恶意代码防范管理	配置管理	密码管理	变更管理	备份与恢复管理	安全事件处置	应急预案管理	外包运维管理
1	制度文件、执行/记录文件	符合	3	1	2	2	0	5	2	1	0	1	3	3	2	0
		部分符合	0	0	0	0	0	0	1	0	0	0	0	0	0	0
		不符合	0	0	0	0	1	0	0	0	1	0	0	0	0	0
		不适用	0	0	0	0	0	0	0	0	1	0	0	0	0	2

附录 C 表-22 安全运维管理单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.11 其他安全要求指标

附录 C 表-23 其他指标单项测评结果汇总表

序号	测评对象	符合情况
本报告不涉及		

附录D 单项测评结果记录

D.1 安全物理环境

D.1.1 安全通用要求

D.1.1.1 信息化机房

安全控制点	测评指标	结果结论	符合程度
物理位置选择	a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；	（1）机房和办公场地场所在建筑物具有建筑验收文档，包含对防震、防风和防雨能力的说明； ■机房建设地址为：茂名市茂南区文明北路232号大院大楼 （2）机房和办公场地未出严重的问题。 ■无雨水渗透痕迹 ■无因风导致的较严重尘土 ■无屋顶、墙体、地面等破损开裂	符合
	b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	（1）机房未部署在易发生问题的位置； （2）机房对于空调设备的排水管等部位采取密封防漏处理； （3）机房对于楼板进行了防护措施。	符合
物理访问控制	机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。	（1）制定了《机房安全管理制度》，内容包含机房出入方面的管理规定； （2）对未配置电子门禁系统的出入口指定专人7*24小时负责机房出入，对出入的人员进行身份鉴别和登记，可查出入记录，且出入有专人陪同； (3)机房存在未配置门禁系统的开放出入口。	部分符合
防盗窃和防破坏	a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识；	（1）机房设备或主要部件都固定在机架上； （2）机房内对主要部件已绑定相应不易除去的标签； ■包括网络设备 ■包括安全设备 ■包括服务器 ■包括网络线缆	符合

安全控制点	测评指标	结果结论	符合程度
		（3）重要机柜已进行上锁处理。	
	b）应将通信线缆铺设在隐蔽安全处。	（1）通信线缆铺设在下走线槽隐蔽处中； （2）通信线缆设有明显的源目的标识； （3）通信线缆均铺设整齐、规范。	符合
防雷击	应将各类机柜、设施和设备等通过接地系统安全接地。	（1）机房设置专用地线； （2）机房内机柜、设施和设备等进行接地处理； （3）交流电源接地验收检测结果符合要求。	符合
防火	a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；	（1）机房采用经消防检测部门检测合格并在有效期内的（如 七氟丙烷）气体自动灭火设备，火灾自动报警类型为烟感+红外； （2）自动消防系统工作状态正常，有定期巡检和维护记录《机房巡检记录表》； （3）建立机房消防的管理制度相关文档《机房安全管理制度》，按管理要求机房无人情况下气体灭火配置为自动模式，进入机房调整为手动模式，机房报警有7*24小时值班人员进行监控。	符合
	b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。	（1）机房及相关的工作房间和辅助房没有采用具有耐火等级的建筑材料； （2）缺乏机房防火设计文档； （3）缺乏机房防火验收文档。	不符合
防水和防潮	a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	（1）机房不存在雨水渗透、破损等不合规情况； （2）机房不位于建筑的顶层、边缘区域。	符合
	b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。	（1）机房区域范围已部署1台科华品牌（精密）空调，机房内分别配置1组温湿度传感器监控； （2）机房内空调下方已铺设安装好挡水和排水设施； （3）机房墙壁或楼板的管道采取必要的防渗防漏等防水保护措施； （4）机房安装检测设备（如：漏水检测绳）检测地下积水，及时处理机房水蒸气结露和地下积水的转移与渗透； （5）目前防水\防潮检测未发现异常情况，并且有防水防潮的运维记录《机房维护日志》。	符合
防静电	应采用防静电地板或地面并采用必要的接地防静电措施。	（1）对机房内设备（可导电金属线槽）采用了接地静电泄放措施； （2）机房未采用防静电地板或铺设防静电地毯。	不符合
温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围	（1）机房范围已部署1组科华品牌精密空调进行温湿度调节； （2）机房范围已部署空调及加湿机进行温湿	符合

安全控制点	测评指标	结果结论	符合程度
	之内。	度调节； （3）温湿度自动调节设施运作正常，有运行和维护记录《机房维护日志》； （4）机房温度能保持在24摄氏度到28摄氏度之间； （5）机房湿度能保持在40%到65%之间。	
电力供应	a）应在机房供电线路上配置稳压器和过电压防护设备；	（1）机房配备了稳压器和过电压防护设备； （2）稳压器和过电压防护设备正常工作； （3）机房具备电力供应安全设计，并在其中标明配备稳压器、过电压防护设备等要求。	符合
	b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。	（1）机房配备了1组科华品牌UPS； （2）UPS正常工作，可满足主要设备断电情况下的至少1小时正常运行要求； （3）UPS有定期（至少每年）检查和维护，有运行和维护记录《机房巡检记录表》。	符合
电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。	（1）通信线缆铺设采用独立的具有电磁屏蔽作用线槽； （2）电源线缆铺设采用独立的具有电磁屏蔽作用线槽； （3）弱电线缆隔离铺设，没有干扰。	符合

D.2 安全通信网络

D.2.1 安全通用要求

D.2.1.1 安全通信网络

安全控制点	测评指标	结果结论	符合程度
网络架构	a）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；	（1）已对网络地址划分，且便于管理和控制； （2）网络地址划分采用核心交换机实现外网边界区域、服务器存储区域等的划分； （3）重要核心网络区域与非重要网络在同一网段； （4）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	部分符合
	b）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	（1）网络内重要网段未部署在网络边界处，且未直接连接外部信息系统； （2）系统通过防火墙对重要网段采取访问控制策略； （3）各安全域（子网）的出口唯一。	符合
通信传输	应采用校验技术保证通信过程中数据的完整性。	（1）网络系统中未涉及完整性保障设备，但在安全计算环境方面网络设备采用SSH协议、安全设备采用HTTPS协议、操作系统采用SSH协议、应用系统采用HTTPS协议来保证通信过程中数据的完整性。	符合

安全控制点	测评指标	结果结论	符合程度
可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对通信设备可信验证方面的安全设计要求； （2）现有的通信设备存在未能实现操作系统到上层应用的信任链的情况，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■通信应用连接过程	不符合

D.3 安全区域边界

D.3.1 安全通用要求

D.3.1.1 办公网区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■办公网区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	符合
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是	符合

安全控制点	测评指标	结果结论	符合程度
		拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	
	d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制,能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略,无法检测、防止或限制从内部发起的网络攻击行为。	不符合
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试； （4）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	部分符合
安全审计	a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间	符合

安全控制点	测评指标	结果结论	符合程度
	他与审计相关的信息；	■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.3.1.2 外网边界区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■外网边界区域 （2）网络边界处部署了可提供访问控制功能的设备； ■防火墙 ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	符合
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■防火墙 ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条	符合

安全控制点	测评指标	结果结论	符合程度
		显示禁止所有通信网络。	
	b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署支持对内部发起的攻击行为进行防范的设备； ■防火墙(带入侵防御模块) ■WEB应用防火墙 （2）现有的防范措施满足相应防护要求； ■所有关键网络边界均有检测措施 ■设备的规则库及时更新 ■检测(模块)符合国家相关产品检测要求 ■其安全策略有效 (3)内部安全防范措施能检测相应攻击行为。 ■端口扫描 ■强力攻击 ■木马后门攻击 ■拒绝服务攻击 ■缓冲区溢出攻击 ■碎片攻击 ■网络蠕虫攻击	符合

安全控制点	测评指标	结果结论	符合程度
		■应用漏洞攻击	
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试。	符合
安全审计	a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数	不符合

安全控制点	测评指标	结果结论	符合程度
	录送至安全管理中心。	■边界防护应用程序	

D.3.1.3 安全管理区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■安全管理区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	符合
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■防火墙（状态检测防火墙）	符合

安全控制点	测评指标	结果结论	符合程度
		（3）访问控制设备支持并启用基于连接状态的检测机制,能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略,无法检测、防止或限制从内部发起的网络攻击行为。	不符合
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试； （4）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	部分符合
安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个	符合

安全控制点	测评指标	结果结论	符合程度
		月； （5）定期收集日志记录并定期备份。	
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.3.1.4 服务器存储区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■服务器存储区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	符合
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址	符合

安全控制点	测评指标	结果结论	符合程度
		■目的地址 ■源端口 ■目的端口 ■协议	
	d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■WEB应用防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制,能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署支持对内部发起的攻击行为进行防范的设备； ■WEB应用防火墙 （2）现有的防范措施满足相应防护要求； ■所有关键网络边界均有检测措施 ■设备的规则库及时更新 ■检测(模块)符合国家相关产品检测要求 ■其安全策略有效 (3)内部安全防范措施能检测相应攻击行为。 ■端口扫描 ■强力攻击 ■木马后门攻击 ■拒绝服务攻击 ■缓冲区溢出攻击 ■碎片攻击 ■网络蠕虫攻击 ■应用漏洞攻击	符合
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■WEB应用防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试。	符合
安全审计	a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■WEB应用防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块)	符合

安全控制点	测评指标	结果结论	符合程度
		■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.4 安全计算环境

D.4.1 安全通用要求

D.4.1.1 网络设备

D.4.1.1.1 核心交换机

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括VTY认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有	符合

安全控制点	测评指标	结果结论	符合程度
		唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的全局密码策略； ■Password control:Enabled ■Password aging:Enabled (180 days) ■Password length:Enabled (8 characters) ■Password composition:Enabled (4 types, 1 characters per type) （6）设备配置加密的super认证。	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备配置合规的全局登录失败处理策略； ■Password control: Enabled ■Maximum login attempts: 5 ■Action for exceeding login attempts: Lock user for 5 minutes （2）设备配置合规的操作超时退出措施。 ■VTY配置idle-timeout 15 0	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式。 ■未启用TELNET ■启用SSH	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般	符合

安全控制点	测评指标	结果结论	符合程度
		用户管理员权限,不赋予用户不必要的操作权限。	
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； ■Information Center: Enabled ■Console: Enabled ■Monitor: Enabled ■Log host: Enabled 10.2.1.2 ■Security log file: Enabled （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制； ■对ssh 登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合

安全控制点	测评指标	结果结论	符合程度
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）网络层相关设备不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的交换功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规	符合

安全控制点	测评指标	结果结论	符合程度
		范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.1.2 汇聚交换机

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括VTY认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的全局密码策略； ■Password control:Enabled ■Password aging:Enabled (180 days) ■Password length:Enabled (8 characters) ■Password composition:Enabled (4 types, 1 characters per type) （6）设备配置加密的super认证。	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备配置合规的全局登录失败处理策略； ■Password control: Enabled ■Maximum login attempts: 5 ■Action for exceeding login attempts: Lock user for 5 minutes （2）设备配置合规的操作超时退出措施。	符合

安全控制点	测评指标	结果结论	符合程度
		■VTY配置idle-timeout 15 0	
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式。 ■未启用TELNET ■启用SSH	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； ■Information Center: Enabled ■Console: Enabled ■Monitor: Enabled ■Log host: Enabled 10.2.1.2 ■Security log file: Enabled （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型	符合

安全控制点	测评指标	结果结论	符合程度
		■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制； ■对ssh 登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）网络层相关设备不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的交换功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备	（1）设备不具备相关可信验证的技术措施；	不符合

安全控制点	测评指标	结果结论	符合程度
	的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2 安全设备

D.4.1.2.1 WEB应用防火墙

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； (2)登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令	符合

安全控制点	测评指标	结果结论	符合程度
		■未设置空口令	
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合

安全控制点	测评指标	结果结论	符合程度
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据	符合

安全控制点	测评指标	结果结论	符合程度
		（2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.2 上网行为管理系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b）应具有登录失败处理功	（1）设备启用合规登录失败处理策略；	符合

安全控制点	测评指标	结果结论	符合程度
	能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间	符合

安全控制点	测评指标	结果结论	符合程度
		■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备	（1）设备不具备相关可信验证的技术措施；	不符合

安全控制点	测评指标	结果结论	符合程度
	的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.3 基线核查系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合

安全控制点	测评指标	结果结论	符合程度
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方	（1）设备通过核心交换机的访问控制策略，	符合

安全控制点	测评指标	结果结论	符合程度
	式或网络地址范围对通过网络进行管理的管理终端进行限制；	通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的基线核查功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合

安全控制点	测评指标	结果结论	符合程度
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.4 日志审计系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟	符合

安全控制点	测评指标	结果结论	符合程度
	等相关措施；	（2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识	符合

安全控制点	测评指标	结果结论	符合程度
		■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。	不符合

安全控制点	测评指标	结果结论	符合程度
	结果形成审计记录送至安全管理中心。	■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施; ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施; ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能;	（1）设备定义了相关重要数据; ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范; （3）设备定期完全依照备份策略，采用正确的配置进行本地备份; （4）设备的备份周期为：每月一次; （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息;	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.5 运维安全管理系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员	符合

安全控制点	测评指标	结果结论	符合程度
		■系统操作员 (2)设备不存在多个管理级别高的特权用户； (3) 设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	(1) 设备开启审计功能，审计进程正常； (2) 设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	(1) 设备日期、时间正常； (2) 设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	(1) 设备限制审计文件的访问控制权限，普通用户不可删除及修改； (2) 设备针对日志、审计记录具备充足的存储容量； (3) 对审计记录进行定期存档备份，其备份策略有效； (4) 部署日志审计系统实时对日志进行统一收集存储； (5) 日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	(1) 设备在全局模式下禁用部分不必要的服务； (2) 设备在部分接口模式下禁用部分不必要的服务； (3) 漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	(1) 设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； (3) 漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	(1) 设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制。 ■对Web登录配置管理地址，限制登录范围	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要	(1) 设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 (2) 设备管理的校验接口范围较全面。	符合

安全控制点	测评指标	结果结论	符合程度
	求；	■包括人机接口校验 ■包括通信接口校验	
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份；	符合

安全控制点	测评指标	结果结论	符合程度
		（4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.6 防火墙-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合

安全控制点	测评指标	结果结论	符合程度
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效；	符合

安全控制点	测评指标	结果结论	符合程度
		（4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.7 防火墙-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证	符合

安全控制点	测评指标	结果结论	符合程度
	具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验	符合

安全控制点	测评指标	结果结论	符合程度
		■包括通信接口校验	
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确	符合

安全控制点	测评指标	结果结论	符合程度
		的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.3 服务器和终端

D.4.1.3.1 应用服务器

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏	符合

安全控制点	测评指标	结果结论	符合程度
		幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用‘RDP安全层’参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败	符合

安全控制点	测评指标	结果结论	符合程度
		■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下：运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验	（1）操作系统不存在此部分的控制需求，不	不适用

安全控制点	测评指标	结果结论	符合程度
	功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	适用。	
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施；	符合

安全控制点	测评指标	结果结论	符合程度
		■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.2 数据库服务器-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措	符合

安全控制点	测评指标	结果结论	符合程度
		施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用‘RDP安全层’参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员	符合

安全控制点	测评指标	结果结论	符合程度
		■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下:运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合

安全控制点	测评指标	结果结论	符合程度
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据	符合

安全控制点	测评指标	结果结论	符合程度
		（2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非	（1）操作系统不存在此部分的控制需求，不	不适用

安全控制点	测评指标	结果结论	符合程度
	法使用用户个人信息。	适用。	

D.4.1.3.3 数据库服务器-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 (5)用户属性策略未勾选“密码永不过期”。	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用‘RDP安全层’参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合

安全控制点	测评指标	结果结论	符合程度
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	(1)操作系统采取对审计记录存储容量如下:运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G; （2）限制审计文件的访问控制权限，用户不	符合

安全控制点	测评指标	结果结论	符合程度
		可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的	符合

安全控制点	测评指标	结果结论	符合程度
		危害。	
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请	符合

安全控制点	测评指标	结果结论	符合程度
		表》。	
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施： 安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.4 业务终端-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 (5)用户属性策略未勾选“密码永不过期”。	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用	符合

安全控制点	测评指标	结果结论	符合程度
		■“空闲会话限制”->≤10分钟	
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合

安全控制点	测评指标	结果结论	符合程度
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下：运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据	符合

安全控制点	测评指标	结果结论	符合程度
		■能实现保护措施和恢复措施有效	
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.5 业务终端-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天	符合

安全控制点	测评指标	结果结论	符合程度
		■密码最短使用期限->1天 ■强制密码历史->5次 (5)用户属性策略未勾选“密码永不过期”。	
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操	符合

安全控制点	测评指标	结果结论	符合程度
		作权限。	
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下：运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口；	符合

安全控制点	测评指标	结果结论	符合程度
		■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能	符合

安全控制点	测评指标	结果结论	符合程度
		发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.6 运维及管理终端-1

安全控制点	测评指标	结果结论	符合程度

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 (5)用户属性策略未勾选“密码永不过期”。	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令	符合

安全控制点	测评指标	结果结论	符合程度
		■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下：运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份	符合

安全控制点	测评指标	结果结论	符合程度
		策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信	不符合

安全控制点	测评指标	结果结论	符合程度
	程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备	不适用

安全控制点	测评指标	结果结论	符合程度
	场地。	份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施： 安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.7 运维及管理终端-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”	符合

安全控制点	测评指标	结果结论	符合程度
	听。	参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间	符合

安全控制点	测评指标	结果结论	符合程度
		■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下：运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端	符合

安全控制点	测评指标	结果结论	符合程度
		口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据	符合

安全控制点	测评指标	结果结论	符合程度
		■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.4 系统管理软件/平台

D.4.1.4.1 应用服务器-Tomcat

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）Tomcat中间件关闭web管理控制台，其身份鉴别功能由宿主操作系统实现，不适用。	不适用
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）Tomcat中间件关闭web管理控制台，其身份鉴别功能由宿主操作系统实现，不适用。	不适用
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）Tomcat中间件关闭web管理控制台，其身份鉴别功能由宿主操作系统实现，不适用。	不适用
访问控制	a）应对登录的用户分配账户和权限；	（1）对应不同的账户均按需分配不同的用户权限，不存在中间件用户均属于管理级别、高	符合

安全控制点	测评指标	结果结论	符合程度
		权限的情况； （2）中间件配置可降权启动Tomcat的用户； （3）宿主系统针对中间件用户分别赋予相应的管理操作权限。 ■包括审计权限 ■包括操作权限	
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）中间件不存在除如:Tomcat、admin、manager、role1等默认账户名； （2）中间件账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）中间件不存在多余或过期账户； （2）中间件管理员用户与账户之间一一对应； （3）中间件启用合规的管理用户名配置。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）中间件根据安全策略要求对特权用户及宿主管理用户进行分离； （2）中间件管理不存在多个管理级别高的特权用户； （3）中间件管理按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）中间件开启审计功能，审计进程正常； ■开启Cataline引擎的日志文件 catalina.org.apache.juli.FileHandler.level = FINE ■开启内部代码丢出的日志 localhost.org.apache.juli.FileHandler.level = FINE ■开启manager应用日志 manager.org.apache.juli.FileHandler.level = FINE ■开启控制台输出的日志 java.util.logging.ConsoleHandler.level = FINE ■开启Access访问日志。 server.xml文件配置正常，未被注释标记<!-- -->； （2）系统的日志审计级别满足要求。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）中间件日期、时间正常； （2）中间件审计记录开启审核策略且日志级别正常。 ■日志级别不低于“FINE” ■日志配置pattern值设为common ■日志配置pattern值为自定义格式，至少包含：%h %l %u %t %s	符合

安全控制点	测评指标	结果结论	符合程度
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）中间件限制审计文件的访问控制权限，普通用户不可删除及修改； ■localhost.log 644 ■catalina.log 644 ■host-manager.log 644 ■manager.log 644 （2）宿主系统针对中间件日志、审计记录具备充足的存储容量； ■日志存储在/log/tomcat/目录下 ■日志创建计划为每天/每周/每月 ■不限制最大日志文件大小 （3）对中间件审计记录进行定期存档备份，其备份策略有效； （4）审计记录及日志保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）中间件系统不存在此部分的安装控制需求，不适用。	不适用
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）Tomcat中间件的管理地址限制功能由宿主操作系统实现，故该项不适用。	不适用
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）中间件管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）中间件管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）中间件已根据需要不定期地对已发布的版本进行更新； （2）中间件更新安装前进行安全性和兼容性测试； （3）在系统上线或发生重大变更时测试并安装最新的中间件版本或更新补丁； （4）在不影响业务系统正常运行情况下，对发现的中间件漏洞在确保安全的情况下进行修补； （5）中间件进行扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更	（1）中间件系统不存在此部分的控制需求，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	新防恶意代码库。		
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输 重要配置数据: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份的中间件重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）宿主系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）中间件相关数据的备份周期合理：每天增量一次、每月全备一次； （5）中间件开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配	（1）宿主系统具有清除用户鉴别信息的功能； （2）经测试，宿主系统退出后无法访问先前	符合

安全控制点	测评指标	结果结论	符合程度
	前得到完全清除。	中间件登录过的页面； （3）经测试，宿主系统关闭后无残留的中间件用户鉴别信息。	
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用

D.4.1.4.2 数据库服务器-1-MSSQL

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）数据库系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）数据库系统不存在弱口令用户； ■MS_SQL数据库已修改默认sa口令 ■MS_SQL数据库不存在空口令用户 （3）数据库系统不存在默认信任的登录模式； ■MS_SQL数据库登录未勾选“记住密码” ■MS_SQL数据库系统配置服务器身份验证方式为：SQL Server和Windows身份验证模式” （4）数据库系统为登录用户设置的身份标识具有唯一性； （5）数据库系统配置合规的密码长度及复杂度策略； ■MS_SQL数据库系统勾选“强制实施密码策略” ■MS_SQL数据库宿主系统配置合规密码复杂度策略 （6）数据库系统配置合规的密码有效周期策略。 ■MS_SQL数据库系统勾选“强制密码过期策略” ■MS_SQL数据库宿主系统配置合规密码有效期策略	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）数据库系统启用合规登录失败处理策略； ■MS_SQL数据库系统勾选“强制实施密码策略” ■宿主操作系统启用“账户锁定策略” （2）数据库系统执行合规的锁定策略； ■复位帐号锁定计数器=30（分钟） ■账户锁定时间=30（分钟）	符合

安全控制点	测评指标	结果结论	符合程度
		■账户锁定阀值=15 （3）数据库系统配置合规的操作超时锁定。 ■“连接”--“远程查询超时值”<900秒	
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）宿主操作系统配置合规的远程管理模式； ■主机启用了安全的远程管理模式（如 RDP 高密级 ），且只能通过本地对数据库进行管理 （2）使用运维安全管理系统统一管理操作系统远程登录，运维安全管理系统采用了 HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供数据库系统权限表； （2）登录数据库系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在所有用户均属于sysadmin的情况； （4）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）数据库系统对多余帐户进行删除、锁定或禁止其登录； （2）数据库系统账户口令设置合规。 ■MS_SQL数据库系统勾选“强制实施密码策略”	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）数据库系统不存在多余或过期账户； （2）数据库系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）数据库系统根据安全策略要求对特权用户进行分离； ■配置系统管理员 ■配置安全审计员 ■配置系统操作员 （2）数据库系统不存除sa外的特权用户； （3）数据库系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）数据库系统开启审计功能，审计进程正常； ■MS_SQL 数据库系统审计级别为“失败和成功的登陆” ■MS_SQL 数据库系统启用C2审核跟踪 （2）审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的	（1）数据库宿主系统日期、时间正常；	符合

安全控制点	测评指标	结果结论	符合程度
	日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（2）数据库系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括重要用户行为 ■包括系统资源的异常使用情况 ■包括重要系统命令的使用 ■包括重要的安全相关事件	
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）数据库系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）数据库系统针对日志、审计记录具备充足的存储容量； （3）MS_SQL数据库系统日志文件安装路径下的log文件（\SQL Server\MSSQLMSSQLSERVER\MSSQL\Log\ERRORLOG）everyone用户没有写权限； （4）日志及审计记录保存大于6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）数据库系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）补丁安装前进行安全性和兼容性测试； （3）在系统上线或发生重大变更时测试并安装数据库安全补丁； （4）MS_SQL分离默认安装的示例数据库； （5）数据库系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）数据库系统不存在此部分的控制需求，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■使用数据库级的加密（TDE） 重要配置数据: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■使用数据库级的加密（TDE）	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）数据库系统定义了相关重要数据； ■包括鉴别数据 ■包括重要配置数据 ■包括重要审计数据 （2）单位具备合理的重要数据的备份策略规范； （3）数据库系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	(1)数据库系统未能提供异地数据备份功能。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）数据库系统不保存终端历史记录； （3）MS_SQL引用产品测试结果，信息删除	符合

安全控制点	测评指标	结果结论	符合程度
		后可法保证完全清除。	
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）数据库存储的用户个人信息均为业务应用必需的环节。	符合
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； ■包括信息采集 ■包括信息保存 ■包括信息访问 ■包括信息使用 （2）数据库具备控制措施禁止未授权访问用户个人信息表单； （3）数据库具备控制措施禁止非法使用用户个人信息表单。	符合

D.4.1.4.3 数据库服务器-2-Oracle

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）数据库系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）数据库系统不存在弱口令用户； ■ORACLE数据库已修改默认口令 ■ORACLE数据库不存在空口令用户 （3）数据库系统为登录用户设置的身份标识具有唯一性； （4）数据库系统配置合规的密码长度及复杂度策略； ■PASSWORD_VERIFY_FUNCTION ，LIMIT=VERIFY_FUNCTION ■IF LENGTH(password) 值为8 ■PASSWORD_REUSE_MAX值为5 （5）数据库系统配置合规的密码有效周期策略。 ■PASSWORD_LIFE_TIME值为 180	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）数据库系统启用合规登录失败处理策略； ■ORACLE 数据库系统FAILED_LOGIN_ATTEMPTS= 10 （2）数据库系统执行合规的锁定策略。 ■PASSWORD_LOCK_TIME=1	符合
	c) 当进行远程管理时，应	（1）数据库系统配置合规的远程管理模式。	符合

安全控制点	测评指标	结果结论	符合程度
	采取必要措施防止鉴别信息在网络传输过程中被窃听。	■ORACLE 数据库系统sqlnet.encryption为true ■ORACLE 数据库系统采用sqlplus连接数据库，客户端与服务器端之间通信是加密的	
访问控制	a) 应对登录的用户分配账户和权限；	（1）登录数据库系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （2）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在多用户均与sys、DBA用户权限一致的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）数据库系统对多余帐户进行删除、锁定或禁止其登录； ■数据库系统账户禁用不常用的默认用户 （2）数据库系统账户口令设置合规。 ■数据库系统各用户未使用空口令 ■数据库系统未使用弱口令或默认与用户名相同的口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）数据库系统不存在多余或过期账户； （2）数据库系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）数据库系统根据安全策略要求对特权用户进行分离； ■配置系统管理员 ■配置安全审计员 ■配置系统操作员 （2）数据库系统用户权限合理，非管理员未设置过大权限； ■具备DBA角色的用户仅为 SYS、SYSTEM （3）数据库系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）数据库系统开启审计功能，审计进程正常； ■ORACLE 数据库系统audit_sys_operations=TRUE ■ORACLE 数据库系统audit_trail=DB （2）ORACLE数据库系统启动数据库日志模式和自动归档； ■Automatic archival=Enabled （3）审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的	（1）数据库宿主系统日期、时间正常；	符合

安全控制点	测评指标	结果结论	符合程度
	日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（2）数据库系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括重要用户行为 ■包括系统资源的异常使用情况 ■包括重要系统命令的使用 ■包括重要的安全相关事件	
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）数据库系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）数据库系统针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）日志及审计记录保存大于6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）网络设备ACL策略有效限制访问本机的IP地址及管理模式。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）数据库系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）数据库宿主系统不存在启用未加控制的高危端口； （3）MY_SQL分离默认安装的示例数据库； （4）数据库系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用	（1）数据库系统不存在此部分的控制需求，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。		
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■SQLNET.ENCRYPTION_SERVER = REQUIRED ■SQLNET.ENCRYPTION_TYPES_SERVER = RC4_256 ■SQLNET.CRYPTO_CHECKSUM_SERVER = REQUIRED 重要配置数据: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■SQLNET.ENCRYPTION_SERVER = REQUIRED ■SQLNET.ENCRYPTION_TYPES_SERVER = RC4_256 ■SQLNET.CRYPTO_CHECKSUM_SERVER = REQUIRED	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）数据库系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）数据库系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功	(1)数据库系统未能提供异地数据备份功能。	不符合

安全控制点	测评指标	结果结论	符合程度
	能，利用通信网络将重要数据定时批量传送至备用场地。		
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）数据库系统不保存终端历史记录。	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）数据库存储的用户个人信息均为业务应用必需的环节。	符合
	b）应禁止未授权访问和非法使用用户个人信息。	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； ■包括信息采集 ■包括信息保存 ■包括信息访问 ■包括信息使用 （2）数据库具备控制措施禁止未授权访问用户个人信息表单； （3）数据库具备控制措施禁止非法使用用户个人信息表单。	符合

D.4.1.5 业务应用系统/平台

D.4.1.5.1 财务管理系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）系统对各登录模式均启用身份鉴别； ■包括管理后台认证 （2）系统对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）系统登录用户设置的身份标识具有唯一性； （4）系统不存在空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）系统启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）系统配置合规的操作超时退出措施。 ■管理后台配置超时15分钟	符合

安全控制点	测评指标	结果结论	符合程度
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）应用系统的用户鉴别数据采用SHA-512算法在可控网络环境中传输； （2）系统配置合规的远程管理模式。 ■启用HTTPS	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供系统权限分配表； （2）登录系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需分配不同的用户权限，不存在所有用户均属于管理级别、高权限的情况。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）系统禁用默认账户名； （2）系统账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）系统不存在多余或过期账户； （2）系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）系统不存在多个管理级别高的特权用户； （2）系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）系统开启审计功能，审计进程正常； （2）系统的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）系统日期、时间正常； （2）系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）系统针对日志、审计记录具备充足的存储容量； （3）审计记录及日志保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和	（1）应用软件系统不存在此部分的安装控制需求，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	应用程序；		
	b) 应关闭不需要的系统服务、默认共享和高危端口；	(1)应用软件系统不存在此部分的控制需求，不适用。	不适用
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）系统自身设定有效的终端访问策略，通过访问措施进行管理地址的限制。 ■系统管理页面仅能内网登录	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）系统具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）系统的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）系统已根据需要不定期地对已发布的版本进行更新； （2）在系统上线或发生重大变更时测试并安装最新的版本或更新补丁； （3）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	(1)应用软件系统不存在此部分的控制需求，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	(1)应用软件系统不存在此部分的控制需求，不适用。	不适用
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据	符合

安全控制点	测评指标	结果结论	符合程度
		（2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）系统具有清除用户鉴别信息的功能； （2）经测试，系统退出后无法访问先前登录过的页面； （3）经测试，系统关闭后无残留的用户鉴别信息。	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息； （3）系统采集的用户个人信息均为业务应用必需的环节。	符合
	b）应禁止未授权访问和非法使用用户个人信息。	（1）系统不采集和保存任何形式的用户个人信息； （2）系统对所有涉及个人信息的环节均有明确的授权同意过程； ■包括信息采集 ■包括信息保存 ■包括信息访问 ■包括信息使用 （3）系统具备控制措施禁止未授权访问用户个人信息； （4）系统具备控制措施禁止非法使用用户个	符合

安全控制点	测评指标	结果结论	符合程度
		人信息。	

D.4.1.6 数据资源

D.4.1.6.1 重要业务数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	（1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要业务数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份重要数据； ■包括重要业务数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）该测评项测评对象鉴别数据，已在安全计算环境层面其他对象判定，此项不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）该测评项测评对象为重要个人信息的内容，已在安全计算环境层面其他对象判定，该项不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）该测评项测评对象为重要个人信息的内容，已在安全计算环境层面其他对象判定，该项不适用。	不适用

D.4.1.6.2 重要个人信息

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	（1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要个人信息 （2）系统对重要数据在传输过程中采取必要	符合

安全控制点	测评指标	结果结论	符合程度
		的完整性保护措施。 ■使用HTTPS加密协议进行传输	
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份重要数据； ■包括重要个人信息 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）该测评项测评对象鉴别数据，已在安全计算环境层面其他对象判定，此项不适用。	不适用
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息； （3）系统采集的用户个人信息均为业务应用必需的环节。	符合
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； ■包括信息采集 ■包括信息保存 ■包括信息访问 ■包括信息使用 （2）系统具备控制措施禁止未授权访问用户个人信息； （3）系统具备控制措施禁止非法使用用户个人信息。	符合

D.4.1.6.3 鉴别数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	数据库服务器-2-Oracle: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施；	符合

安全控制点	测评指标	结果结论	符合程度
		■包括鉴别数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■SQLNET.ENCRYPTION_SERVER = REQUIRED ■SQLNET.ENCRYPTION_TYPES_SERVER = RC4_256 ■SQLNET.CRYPTO_CHECKSUM_SERVER = REQUIRED 应用服务器-Tomcat: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输 业务终端-1、业务终端-2、应用服务器、数据库服务器-1、数据库服务器-2、运维及管理终端-1、运维及管理终端-2: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 数据库服务器-1-MSSQL: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据	

安全控制点	测评指标	结果结论	符合程度
		（2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■使用数据库级的加密（TDE） 财务管理系统: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	该测评项在各系统及设备已做判定,数据资源针对鉴别数据不做判定	不适用
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	该测评项在各系统及设备已做判定,数据资源针对鉴别数据不做判定，不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	应用服务器-Tomcat: （1）宿主系统具有清除用户鉴别信息的功能； （2）经测试，宿主系统退出后无法访问先前中间件登录过的页面； （3）经测试，宿主系统关闭后无残留的中间件用户鉴别信息。 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）网络层设备不适用。 业务终端-1、业务终端-2、应用服务器、数据库服务器-1、数据库服务器-2、运维及管理终端-1、运维及管理终端-2: （1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施： 安全选项“不显示上次的用户名”->启用 财务管理系统: （1）系统具有清除用户鉴别信息的功能； （2）经测试，系统退出后无法访问先前登录过的页面； （3）经测试，系统关闭后无残留的用户鉴别信息。 数据库服务器-1-MSSQL: （1）身份鉴别信息释放或清除机制正常且满足要求；	符合

安全控制点	测评指标	结果结论	符合程度
		（2）数据库系统不保存终端历史记录； （3）MS_SQL引用产品测试结果，信息删除后可法保证完全清除。 数据库服务器-2-Oracle: （1）身份鉴别信息释放或清除机制正常且满足要求； （2）数据库系统不保存终端历史记录。	
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	鉴别数据不存在此部分的控制需求,故此项不适用	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	鉴别数据不存在此部分的控制需求,故此项不适用	不适用

D.4.1.6.4 重要配置数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	数据库服务器-2-Oracle: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■SQLNET.ENCRYPTION_SERVER = REQUIRED ■SQLNET.ENCRYPTION_TYPES_SERVER = RC4_256 ■SQLNET.CRYPTO_CHECKSUM_SERVER = REQUIRED 财务管理系统: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输 应用服务器-Tomcat: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火	符合

安全控制点	测评指标	结果结论	符合程度
		墙-2: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 数据库服务器-1-MSSQL: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■使用数据库级的加密（TDE） 业务终端-1、业务终端-2、应用服务器、数据库服务器-1、数据库服务器-2、运维及管理终端-1、运维及管理终端-2: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）设备定义了相关重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 应用服务器-Tomcat: （1）系统定义了相关需要备份的中间件重要	符合

安全控制点	测评指标	结果结论	符合程度
		数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）宿主系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）中间件相关数据的备份周期合理：每天增量一次、每月全备一次； （5）中间件开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 业务终端-1、业务终端-2、应用服务器、数据库服务器-1、数据库服务器-2、运维及管理终端-1、运维及管理终端-2: （1）操作系统定义了相关重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 财务管理系统: （1）系统定义了相关需要备份重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 数据库服务器-1-MSSQL、数据库服务器-2-Oracle: （1）数据库系统定义了相关重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范；	

安全控制点	测评指标	结果结论	符合程度
		（3）数据库系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	应用服务器、数据库服务器-1、数据库服务器-2: （1）设备为服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、运维安全管理系统、防火墙-1、防火墙-2: （1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 数据库服务器-1-MSSQL、数据库服务器-2-Oracle: （1）数据库系统未能提供异地数据备份功能。 应用服务器-Tomcat、财务管理系统: （1）单位未能提供异地数据备份措施。 业务终端-1、业务终端-2、运维及管理终端-1、运维及管理终端-2: （1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 核心交换机、汇聚交换机: （1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	重要配置数据不存在此部分的控制需求,故此项不适用	不适用

安全控制点	测评指标	结果结论	符合程度
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	重要配置数据不存在此部分的控制需求,故此项不适用	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	重要配置数据不存在此部分的控制需求,故此项不适用	不适用

D.4.1.7 其他系统或设备

无

D.5 安全管理中心

D.5.1 安全通用要求

D.5.1.1 管理中心

安全控制点	测评指标	结果结论	符合程度
系统管理	a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；	（1）网络中部署运维安全管理系统实现集中的系统管理； （2）系统对登录用户进行身份鉴别； ■包括合规的用户名 ■包括合规的口令策略 （3）系统用户标识具有唯一性； ■不存在多人共享 ■增加、删除用户或权限变更需经过审批 （4）系统可实现对账户的身份鉴别数据进行保密性和完整性保护； （5）系统管理操作模式具备控制措施； ■只允许系统管理员登录 ■具备特定的登录命令 ■具备特定的登录操作界面 （6）系统具备相应的管理操作审计措施。 ■可实现对系统管理操作进行审计 ■审计范围覆盖所有用户 ■操作审计不可被删除	符合
	b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。	（1）系统管理员对系统的资源和运行进行配置、控制和管理； ■包括用户身份管理 ■包括资源配置管理 ■包括系统加载和启动管理 ■包括系统运行的异常处理管理 ■包括数据和设备的备份与恢复管理 （2）系统的资源、运行及配置管理不够全面。 ■缺乏可信证书管理 ■缺乏可信基准库管理	不符合
审计管理	a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行	（1）网络中部署运维安全管理系统实现集中安全审计功能； （2）审计系统对审计管理员进行身份鉴别；	符合

安全控制点	测评指标	结果结论	符合程度
	安全审计操作，并对这些操作进行审计；	■包括合规的用户名 ■包括合规的口令策略 （3）审计系统用户标识具有唯一性； ■不存在多人共享 ■增加、删除用户或权限变更需经过审批 （4）审计系统管理操作模式具备控制措施； ■只允许审计管理员登录 ■具备特定的登录命令 ■具备特定的登录操作界面 （5）审计系统具备相应的管理操作审计措施。 ■可实现对安全审计操作进行审计 ■审计范围覆盖所有审计管理用户 ■操作审计不可被删除	
	b）应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	财务管理系统: （1）审计管理员定期对审计记录进行分析，对发现的安全可疑事件及时处理； （2）单位具有安全审计策略文件，规范审计记录的存储、管理和查询要求； （3）审计管理员按规范要求对审计记录进行管理。 ■审计记录不可随意删除/修改 ■定期备份、存储审计记录 ■审计记录存储周期满足6个月要求 重要审计数据: 日志审计系统、运维安全管理系统: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要审计数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■网络设备、安全设备使用rsyslog协议进行传输 ■Windows操作系统使用插件+SSL协议进行传输	符合

D.6 安全管理制度

D.6.1 安全通用要求

D.6.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
安全策略	应制定网络安全工作的总	（1）单位具有网络安全工作的总体方针和安	符合

安全控制点	测评指标	结果结论	符合程度
	体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。	全策略文件； ■具备独立的网络安全总体方针文件 ■具备涵盖网络安全总体方针策略要求的相关管理文件 ■具备安全策略文件 （2）制度内容包括明确的单位安全工作要求； ■安全目标 ■安全范围 ■安全原则 ■安全框架 ■各类安全策略 （3）管理文件详见《信息安全总体策略》。	
管理制度	a）应对安全管理活动中的主要管理内容建立安全管理制度；	（1）单位有针对安全管理活动中的各类管理内容建立安全管理制度； （2）现有制度已覆盖管理活动的主要的方面； ■具备文件控制管理 ■具备安全检查管理 ■具备人力资源及培训 ■具备设备管理 ■具备软件开发/外包开发项目管理 ■具备机房安全管理 ■具备信息分类及管理 ■具备网络安全管理 ■具备系统安全管理 ■具备恶意代码管理 ■具备变更控制 ■具备备份及介质管理 ■具备事件管理 ■具备应急预案 （3）制度详见：《信息安全总体策略》、《网络安全管理规范》、《组织安全结构和人员职责制度》、《人员管理制度》、《员工考核管理制度》。	符合
	b）应对管理人员或操作人员执行的日常管理操作建立操作规程。	（1）单位针对相关业务日常管理的操作建立规程类管理制度； （2）现有制度已覆盖重要管理方面的系统维护手册和用户操作规程等； ■具备网络/安全管理 ■具备服务器管理 ■具备数据库管理 ■具备机房硬件设施管理 ■具备业务应用管理 （3）管理文件详见《设备及系统软件配置和	符合

安全控制点	测评指标	结果结论	符合程度
		操作手册》。	
制定和发布	a) 应指定或授权专门的部门或人员负责安全管理制度的制定；	（1）单位针对安全管理制度的制定，指定教育信息与网络中心部主要负责； （2）在已制定的相关制度中可查阅到被授权制定管理制度的部门/人员信息； （3）管理文件详见《安全管理组织规范》。	符合
	b) 安全管理制度应通过正式、有效的方式发布，并进行版本控制。	（1）单位针对制度的制定和发布要求，制定管理规范文件； （2）管理规范文件对文件制定及发布定义了规范要求； ■包括安全管理制度的制定和发布程序 ■包括格式要求 ■包括版本编号要求 （3）安全管理制度的收发登记记录有效； ■具备通过正式、有效的方式收发 ■具备正式发文 ■具备领导签署、单位盖章等 （4）管理文件详见《制度制定、发布、评审和修订管理制度》、《收发文登记记录》。	符合
评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	（1）单位针对制度的合理性和适用性需进行论证和审定及修订的要求，制定管理规范文件； （2）管理规范文件对制度的评审及修订定义了规范要求； （3）单位具有安全管理制度的审定或论证的过程记录； （4）单位对做过修订的制度，具备有修订版本的安全管理过程记录； （5）管理文件详见《制度制定、发布、评审和修订管理制度》及 《安全管理制度评审记录》。	符合

D.7 安全管理机构

D.7.1 安全通用要求

D.7.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
岗位设置	a) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；	（1）单位已明确网络安全管理工作的职能部门，并明确了各岗位职责； ■已设置机房管理员 ■已设置网络管理员 ■已设置安全管理员 （2）单位各部门职责文档已明确网络安全管	符合

安全控制点	测评指标	结果结论	符合程度
		理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备网络安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	
	b）应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。	（1）单位已明确系统安全管理工作的职能部门，并明确了各岗位职责； ■已设置系统管理员 ■已设置数据管理员 ■已设置审计管理员 ■已设置应用管理员 （2）单位各部门职责文档已明确系统安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备系统安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	符合
人员配备	应配备一定数量的系统管理员、审计管理员和安全管理员等。	（1）单位针对人员配备要求，制定了管理制度； （2）单位按要求配备一定数量的重要岗位管理人员； （3）单位针对各岗位人员，制定并维护人员档案； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	符合
授权和审批	a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；	（1）单位在制度中用文字描述或在流程图中明确，对关键活动进行审批； ■具备部门职责文档明确各部门审批事项 ■具备岗位职责文档明确各岗位审批事项 （2）单位对审批过程明确审批权限，对各项信息系统的重要操作与变更明确审批部门和批准人； （3）管理文件详见《授权和审批管理规定》。	符合
	b）应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。	（1）单位针对各项业务操作及变更等建立了审批程序规定； ■包括系统变更 ■包括重要操作 ■包括物理访问 ■包括系统接入 （2）单位针对系统变更、系统接入、物理范围等事项已明确按审批程序执行,记录有批准人签字； （3）管理文件详见《授权和审批管理规定》。	符合

安全控制点	测评指标	结果结论	符合程度
沟通和合作	a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；	（1）单位针对机构内部管理人员之间、部门之间的沟通与合作，制定了管理制度； （2）单位的管理制度规范了合作和沟通的方式和周期； （3）单位有组织机构内部人员联系表； （4）单位有定期召开信息安全会议，保存有会议纪要； （5）管理文件详见《安全教育和培训制度》、《技能培训记录》《外部联系表》。	符合
	b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；	（1）单位针对加强与外部单位的合作与沟通，制定了管理制度规定； ■包括公安机关 ■包括网络安全职能部门 ■包括职能监管机构 ■包括各类供应商 ■包括业界专家 ■包括安全组织 （2）单位能按要求与相关单位保持沟通合作，并提供相关单位联系方式和交流会议纪要； （3）管理文件详见《安全教育和培训制度》、《技能培训记录》、《外部联系表》。	符合
	c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	（1）单位建立了完善的对外联单位的联系列表； ■记录单位名称 ■记录合作内容 ■记录联系人 ■记录联系方式 （2）管理文件详见《外部联系表》。	符合
审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。	（1）单位针对定期开展常规安全检查，制定了管理制度； （2）单位对检查工作的范围、过程、要求等管理的比较完善； ■系统日常运行 ■系统漏洞 ■数据备份 ■包括敏感系统检查人员 （3）单位已按要求由安全管理员定期检查，检查内容需覆盖系统运行相关的管理活动，并能提供安全检查报告； （4）管理文件详见《安全审查和检查管理规范》； （5）单位开展的检查工作不够完善。 ■未定期检查	部分符合

D.8 安全管理人员

D.8.1 安全通用要求

D.8.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
人员录用	a) 应指定或授权专门的部门或人员负责人员录用；	（1）单位授权专门的部门负责人员录用工作，制定了管理制度规范； （2）由人力资源保障科负责人员录用工作； （3）管理文件详见《人员管理制度》。	符合
	b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查。	（1）单位针对人员录用过程，制定了明确要求，并形成人员安全管理制度； （2）单位现有管理制度明确说明录用人员应具备的条件； ■包括学历/学位要求 ■包括技术人员的专业技术要求 ■包括管理人员的安全管理要求 （3）单位按规定执行人员录用的相关审查过程； ■包括录用人身份 ■包括安全背景 ■包括专业资格 ■包括资质 （4）管理文件详见《人员管理制度》、《人员入职考核记录》。	符合
人员离岗	应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。	（1）单位针对离岗人员权限终止及取回机构提供的各种设施的要求，制定了管理制度； （2）单位按规范开展对离岗人员的相关管理工作； ■明确负责部门 ■及时终止其访问权限 ■交还身份证件 ■交还软硬件设备 （3）管理文件详见《人员管理度》、《人员离岗申请表》、《离场信息资料交接表》。	符合
安全意识教育和培训	应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。	（1）单位针对人员安全培训及责任和惩戒措施，制定了管理制度； （2）单位已开展安全意识教育及岗位技能培训 ■具备明确培训周期 ■具备有效的培训方式 ■具备清晰的培训内容 ■具备考核要求 （3）管理文件详见《安全教育和培训制度》。	符合
外部人员访问	a) 应在外部人员物理访问	（1）单位针对外部人员物理访问，制定了外	符合

安全控制点	测评指标	结果结论	符合程度
管理	受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；	部人员访问管理文档； ■明确允许外部人员访问的范围 ■明确外部人员进入的条件 ■明确外部人员进入的访问控制措施 （2）单位具备有效的外部人员访问重要区域的书面申请文档； ■具有申请人 ■具有申请原因 ■具有范围 ■具有日期 ■具有批准人签字 （3）单位具备外部人员访问重要区域的登记记录； ■记录进入时间、 ■记录离开时间 ■记录访问区域 ■记录陪同人信息 （4)管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。	
	b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；	（1）单位针对外部接入受控网络访问系统，制定了管理制度； （2）单位具备外部人员接入受控网络前的申请审批流程； （3）单位具备外部人员接入及访问系统的书面申请文档； ■具有申请人 ■具有申请原因 ■具有访问权限 ■具有日期 ■具有批准人签字 （4）单位具备外部人员接入及访问系统的登记记录； ■记录访问权限 ■记录访问时限 ■记录账户 （5)管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。	符合
	c) 外部人员离场后应及时清除其所有的访问权限。	（1）单位针对人员离场后的清理工作，制定了管理制度；	不符合

安全控制点	测评指标	结果结论	符合程度
		(2)管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》； (3) 单位未完全按管理规范开展人员离场后的清理工作。 ■缺乏清理记录 ■未及时清除离场后的所有访问权限 ■未记录访问权限清除时间	

D.9 安全建设管理

D.9.1 安全通用要求

D.9.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
定级和备案	a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；	(1) 单位的被测系统于2022年4月已完成备案； (2) 系统备案相关文档（定级报告）中明确等级划分方法和理由,SAG三个方面的级别描述清晰； (3) 管理文件详见《定级备案》。	符合
	b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；	(1) 单位针对系统定级结果的审批及评审工作等要求，制定了管理制度； (2) 现有系统的定级已具备合理性和正确性审定； ■具备单位部门审定 (3) 管理文件详见《定级备案》。	符合
	c) 应保证定级结果经过相关部门的批准；	(1)单位针对系统定级结果的上级批准要求,制定了管理制度； (2)现有系统的定级获得了相关部门的批准； (3) 管理文件详见《定级备案》。	符合
	d) 应将备案材料报主管部门和相应公安机关备案。	(1) 单位对被测系统的等级备案表、定级报告等备案材料已经报相应公安机关备案； (2) 单位具备公安机关出具的备案号； (3) 管理文件详见《定级备案》。	符合
安全方案设计	a) 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；	(1) 单位未具备适用于被测系统的安全规划设计方案； (2) 现有方案文档未能完全按照规范要求选择安全措施。 ■缺乏安全保护等级的要求 ■缺乏风险分析结果的要求 ■缺乏实际安全需求	不符合
	b) 应根据保护对象的安全	(1) 单位未具备完整的安全设计方案相关的	不符合

安全控制点	测评指标	结果结论	符合程度
	保护等级进行安全方案设计；	文档。 ■缺乏总体规划 ■缺乏安全设计方案 ■缺乏相关配套文件 ■缺乏保护对象的安全保护等级要求	
	c) 应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； ■缺乏安全整体规划 ■缺乏安全设计方案 ■缺乏安全配套文件 （2）单位未对相关论证过程及内容进行完整的记录。	不符合
产品采购和使用	a) 应确保网络安全产品采购和使用符合国家的有关规定；	（1）单位已建立安全产品管理的相关管理规定； ■包括采购要求 ■包括使用要求 （2）单位具备安全产品采购流程及相关实施文档； （3）被测系统使用的安全产品具备销售许可资质； （4）安全产品具均为国内产品； （5）管理文件详见《设备安全管理制度》。	符合
	b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。	（1）单位已建立密码产品与服务管理的相关管理制度； ■包括采购要求 ■包括使用要求 （2）系统未使用密码产品； （3）管理文件详见《设备安全管理制度》。	符合
自行软件开发	a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。	不适用
	b) 应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。	不适用
外包软件开发	a) 应在软件交付前检测其中可能存在的恶意代码；	（1）单位针对软件交付前测试恶意代码的要求，制定了管理制度； （2）管理文件详见《外包开发软件管理规定》； （3）单位未在软件交付之前按要求对所有软件开展恶意代码检测。 ■缺乏恶意代码检测报告	不符合
	b) 应保证开发单位提供软件设计文档和使用指南。	（1）单位制定软件开发项目验收要求，明确开发单位的提交材料；	符合

安全控制点	测评指标	结果结论	符合程度
		（2）开发单位提供软件日常维护和使用所需的文档； ■包括需求分析说明书 ■包括软件设计说明书 ■包括软件操作手册 （3）管理文件详见《外包开发软件管理规定》、《设备及系统软件配置和操作手册》。	
工程实施	a）应指定或授权专门的部门或人员负责工程实施过程的管理；	（1）单位针对专门的部门负责工程实施过程的管理要求，制定管理度； （2）单位由专岗负责系统建设的工程实施，且按照实施方案的要求对进度和质量进行控制； （3）管理文件详见《工程实施管理制度》。	符合
	b）应制定安全工程实施方案控制工程实施过程。	（1）单位制定了详细的工程实施方案； ■包括工程时间限制 ■包括进度控制 ■包括质量控制 （2）工程实施单位严格按照方案执行，并有过程记录； （3）管理文件详见《测试及验收方案》、《工程项目实施方案》。	符合
测试验收	a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；	（1）单位可提供被测系统的合规测试验收方案； ■包括测试人员 ■包括测试验收内容 ■包括现场操作过程 （2）管理文件详见《测试及验收方案》、《工程项目实施方案》； （3）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。 ■缺乏验收报告 ■缺乏报告审定意见	部分符合
	b）应进行上线前的安全性测试，并出具安全测试报告。	（1）单位对系统上线前需开展安全性测试的要求，制定管理制度； （2）管理文件详见《外包开发软件管理规定》、《系统交付管理》； （3）针对系统上线前的安全性测试工作存在问题。 ■缺乏测试报告	不符合
系统交付	a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；	（1）单位具备系统交付清单； （2）系统交付清单内容较详细； ■包括设备 ■包括软件	符合

安全控制点	测评指标	结果结论	符合程度
		■包括文档 （3）单位的清点工作较合规； ■已依据交付清单开展清点工作 （4）管理文件详见《系统交付管理》、《资产清单》。	
	b）应对负责运行维护的技术人员进行相应的技能培训；	（1）单位已对负责系统运行维护的技术人员进行了技能培训； （2）具备运维人员的培训记录； ■包括培训时间 ■包括培训地点 ■包括培训对象 ■包括培训内容 ■包括培训参与人员签字 （3）管理文件详见《系统交付管理》、《资产清单》、《系统交付清单》、《技能培训记录》。	符合
	c）应提供建设过程文档和运行维护文档。	（1）单位提供了系统建设过程中的文档； （2）单位提供了指导用户进行系统运维的文档和系统培训手册； （3）管理文件详见《系统交付管理》、《系统交付清单》、《设备及系统软件配置和操作手册》。	符合
等级测评	a）应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；	（1）单位针对系统等级测评要求，制定管理制度； （2）系统按要求开展首次测评工作； （3）管理文件详见《系统安全管理制度》。	符合
	b）应在发生重大变更或级别发生变化时进行等级测评；	（1）管理制度中已规定在系统发生变更时及时对系统进行等级测评； （2）系统未发生过重大变更，系统等级未发生变化； （3）管理文件详见《系统安全管理制度》。	符合
	c）应确保测评机构的选择符合国家有关规定。	（1）已选择在“全国等级保护测评机构推荐目录”中的测评单位进行等级测评； （2）管理文件详见《系统安全管理制度》、《网络安全等级保护测评服务合同》。	符合
服务供应商选择	a）应确保服务供应商的选择符合国家的有关规定；	（1）单位在管理制度内明确提出安全服务供应商选择的要求； （2）单位选择的安全服务商符合国家的有关规定，具备相应的安全服务资质； （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。	符合
	b）应与选定的服务供应商签订相关协议，明确整个	（1）单位的管理制度中已规定，需与安全服务商签订安全相关的协议并明确整个服务供	符合

安全控制点	测评指标	结果结论	符合程度
	服务供应链各方需履行的网络安全相关义务。	应链各方需履行的网络安全相关义务； （2）单位已按规定与选定的安全服务商签订合规的协议； ■明确整个服务供应链各方需履行的网络安全相关义务 ■包括保密范围 ■包括安全责任 ■包括违约责任 ■包括协议的有效期限 ■包括责任人签字 （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。	

D.10 安全运维管理

D.10.1 安全通用要求

D.10.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
环境管理	a）应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；	（1）单位建立机房安全方面的管理制度，对有关运维方面的管理作出规定； ■指定教育信息与网络中心部门负责管理 ■包括出入管理要求 ■包括定期维护要求 ■包括空调要求 ■包括供配电设备要求 ■包括消防设施要求 ■包括温湿度控制要求 （2）单位具备完整的机房出入登记记录； ■记录来访人员 ■记录来访时间 ■记录离开时间 ■记录携带物品 （3）单位具备完整的机房基础设施的维护记录； ■记录维护日期 ■记录维护人 ■记录维护设备 ■记录故障原因 ■记录维护结果 （4）管理文件详见《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。	符合
	b）应对机房的安全管理做	（1）单位建立机房安全方面的管理制度；	符合

安全控制点	测评指标	结果结论	符合程度
	出规定，包括物理访问、物品进出和环境安全等；	■包括物理访问管理 ■包括物品进出管理 ■包括环境安全管理 （2）单位现有机房管理记录与制度相符； ■具备物理访问记录 ■具备物品进出记录 ■具备环境安全相关记录 （3）制度详见：《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。	
	c）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	（1）单位机房安全管理制度已明确来访人员的接待区域的要求； （2）单位按规范要求开展人员来访接待； ■划分来访人员的接待区域 ■记录来访人员的情况 （3）单位办公环境未发现有随意放置含有敏感信息介质的情况； ■无纸档文件 ■无移动介质 （4）制度详见：《机房安全管理制度》、《物理安全管理规范》、《办公环境保密管理》。	符合
资产管理	应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。	（1）单位已建立有效的资产清单； （2）单位现有资产清单内容较全面； ■包括设备设施类别 ■包括软件类别 ■包括文档类别 ■包括资产责任人 ■包括所属级别 ■包括所处位置 ■包括所处部门 （3）制度详见：《设备安全管理制度》、《资产清单》。	符合
介质管理	a）应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；	（1）介质按管理要求放置于受控的环境中（如：机房）； （2）介质管理具备较全面的记录； ■包括介质归档 ■包括使用情况 ■包括定期盘点记录 （3）制度详见：《设备安全管理制度》、《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。	符合

安全控制点	测评指标	结果结论	符合程度
	b) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。	（1）介质管理制度中对介质安全传输有明确规定； ■包括人员选择 ■包括打包要求 ■包括交付要求 （2）存储重要信息的介质在物理传输过程，具备严格的环节控制，无重大环节疏漏； （3）对介质的归档和查询均具备记录； （4）制度详见：《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。	符合
设备维护管理	a) 应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	（1）单位人员岗位职责相关文档已明确设备维护管理的责任部门； （2）单位对各类设施、设备进行定期维护； （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。	符合
	b) 应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。	（1）单位建立了配套设施、软硬件维护管理方面的管理制度； ■包括维护人员的责任 ■包括维修和服务的审批 ■包括维修过程的监督控制 （2）单位开展相关工作与制度相符，且保留记录； ■包括维修和服务审批 ■包括维修过程记录 （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。	符合
漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。	（1）单位制定管理制度，规范对安全漏洞和隐患的检测、识别及评估修补要求； （2）制度详见：《恶意代码防范管理制度》； （3）单位未严格按规范开展漏洞及安全隐患检测工作。 ■未定期开展漏洞扫描	不符合
网络和系统安全管理	a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；	（1）单位建立系统安全管理文档，对系统管理员的管理制定了要求； ■包括角色划分 ■包括角色的责任 ■包括角色权限 （2）单位对各类关键角色建立了相应的工作职责文档；	符合

安全控制点	测评指标	结果结论	符合程度
		■包括安全管理员 ■包括网络管理员 ■包括系统管理员 ■包括数据管理员 ■包括审计管理员 （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	
	b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	（1）单位制定管理制度，对系统账号进行管理； ■指定专人 ■包括申请账户管理 ■包括建立账户管理 ■包括删除账户管理 （2）单位按管理规范开展账号管理工作； ■具备相关审批流程 ■具备相关审批记录 ■具备管理登记记录 （3）账户管理记录内容较完整； ■包括变更日期 ■包括变更时间 ■包括变更人 ■包括变更设备/系统 ■包括变更结果 （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	符合
	c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	（1）单位建立了网络和系统安全管理制度； （2）网络和系统安全管理制度内容较全面； ■包括安全策略要求 ■包括账户管理 ■包括配置文件的生成及备份 ■包括变更审批管理 ■包括授权访问 ■包括最小服务控制 ■包括升级与打补丁管理 ■包括审计日志管理 ■包括口令管理 （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	符合
	d）应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；	（1）单位对重要设备、系统的配置和操作建立配置手册； ■包括操作系统 ■包括数据库 ■包括网络设备	符合

安全控制点	测评指标	结果结论	符合程度
		■包括安全设备 ■包括应用和组件 （2）现有操作配置手册已明确操作步骤、参数配置； （3）制度详见：《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。	
	e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。	（1）单位制定日常运维管理的相关制度规范； （2）单位按制度规范开展日常运维管理工作； （3）单位具备合规的运维记录； ■包括日常巡检记录 ■包括运行维护记录 ■包括参数的设置记录 ■包括参数的修改记录 （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》、《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。	符合
恶意代码防范管理	a）应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	（1）单位制定恶意代码防范管理制度，明确对外来计算机或存储设备接入系统前进行恶意代码检查； （2）单位按外来计算机接入恶意代码检查规范开展工作； ■对外来计算机接入进行恶意代码检查 ■具备合规的检测记录 （3）单位制定培训管理制度，明确需通过培训提升员工的防恶意代码意识； （4）单位按培训管理要求开展工作； ■定期对员工开展防恶意代码意识培训 ■具备合规的培训记录 （5）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申请表》、《信息管理系统漏洞检查表》。	符合
	b）应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；	（1）建立恶意代码防范管理文档； （2）管理制度中覆盖防恶意代码软件的授权使用、恶意代码库升级、定期查杀等内容； （3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》。	符合
	c）应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。	（1）单位指定专门的部门负责定期验证防范恶意代码攻击的技术措施的有效性； （2）单位近期未发生过严重的恶意代码攻击事件； （3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申	部分符合

安全控制点	测评指标	结果结论	符合程度
		请表》、《信息管理系统漏洞检查表》； （4）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。 ■未定期对相关产品的恶意代码库进行升级 ■未对所有防病毒产品上截获的恶意代码进行分析并汇总上报	
配置管理	应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。	（1）单位制定了基本配置信息管理的制度要求； ■包括网络拓扑结构 ■包括设备安装的软件组件 ■包括软件组件的版本 （2）管理文件详见：《主机安全管理规范》、《网络安全管理规范》、《应用安全管理规范》、《网络配置信息》。	符合
密码管理	a）应遵循密码相关国家标准和行业标准；	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	不符合
	b）应使用国家密码管理主管部门认证核准的密码技术和产品。	（1）单位未采购涉及密码技术的产品，不适用。	不适用
变更管理	应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。	（1）单位建立了关于系统变更管理的制度文件； （2）现有变更管理制度覆盖了变更管理的各方面要求； ■包括变更管理要求 ■包括整体变更管理流程 ■包括变更内容分析与论证 ■包括变更方案审批流程 ■包括变更后通报 （3）制度详见：《变更控制管理制度》、《通用变更记录表》。	符合
备份与恢复管理	a）应识别需要定期备份的重要业务信息、系统数据及软件系统等；	（1）单位根据业务重要程度，制定了需要定期备份的重要业务信息列表或清单。清单内需要定期备份的重要数据已经过用户方确认； （2）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。	符合
	b）应规定备份信息的备份方式、备份频度、存储介质、保存期等；	（1）单位建立了备份与恢复管理相关的安全管理制度； （2）备份与恢复管理的相关要求比较明确； ■规定备份方式	符合

安全控制点	测评指标	结果结论	符合程度
		■规定备份频度 ■规定存储介质 ■规定保存期 （3）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。	
	c）应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	（1）单位现有管理制度，明确了数据备份策略和数据恢复策略，以及备份程序和恢复程序； （2）单位可按策略要求实现重要数据的定期备份与恢复性测试； （3）单位现有的备份的数据均经过恢复性测试，可确保备份的数据可用； （4）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。	符合
安全事件处置	a）应及时向安全管理部门报告所发现的安全弱点和可疑事件；	（1）单位已在安全培训及宣传过程中告知用户在发现安全弱点和可疑事件时及时向安全管理部门报告； （2）单位在系统运维过程中对发现的安全弱点和可疑事件均编制了对应的报告或相关文档； （3）单位现有安全弱点和可疑事件报告文档内容较详实； （4）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	符合
	b）应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；	（1）单位制定了安全事件报告和处置管理制度； （2）现有安全事件管理制度内容较完整； ■包括安全事件类型分类 ■包括安全事件有关的工作职责 ■包括安全事件的报告 ■包括安全事件的处置 ■包括安全事件的响应流程 （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	符合
	c）应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。	（1）单位具备对安全事件的分析、处理、总结、防范等的报告／过程文档； （2）单位提供的安全事件报告和响应处置记录内容较完整； ■记录引发安全事件的原因	符合

安全控制点	测评指标	结果结论	符合程度
		■记录事件的证据 ■记录处置过程 ■包括经验教训 ■提出补救措施 （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	
应急预案管理	a）应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；	（1）单位制定重要事件的应急预案； （2）单位现有应急预案涉及的类型范围较全面； ■包括针对机房的预案 ■包括针对网络传输的预案 ■包括针对网络设备的预案 ■包括针对操作系统的预案 ■包括针对数据库的预案 ■包括针对安全漏洞攻击的预案 ■包括针对恶意代码的预案 ■包括针对数据泄露的预案 （3）单位现有应急预案的内容较完整； ■明确重要事件的应急处理流程 ■明确系统恢复流程等内容 （4）制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。	符合
	b）应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。	(1)单位定期对相关人员进行应急预案培训； （2）单位根据不同的应急预案，按要求进行应急演练； （3）单位具备近期应急预案工作开展的相关记录； ■具备培训记录 ■具备演练记录 (4)单位提供的应急预案培训记录比较完整； ■明确培训对象 ■明确培训内容 ■明确培训结果 (5)单位提供的应急预案演练记录比较完整； ■记录演练时间 ■记录主要操作内容 ■记录演练结果 （6）经检查单位目前一旦出现应急事件，可参照预案合理有序的进行应急事件处置过程； （7）制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。	符合
外包运维管理	a）应确保外包运维服务商的选择符合国家的有关规	(1)单位目前未涉及任何外包运维服务情况，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	定；		
	b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。	(1)单位目前未涉及任何外包运维服务情况，不适用。	不适用

D.11 其他安全要求

本次测评不涉及其他安全要求指标。

附录E 漏洞扫描结果记录

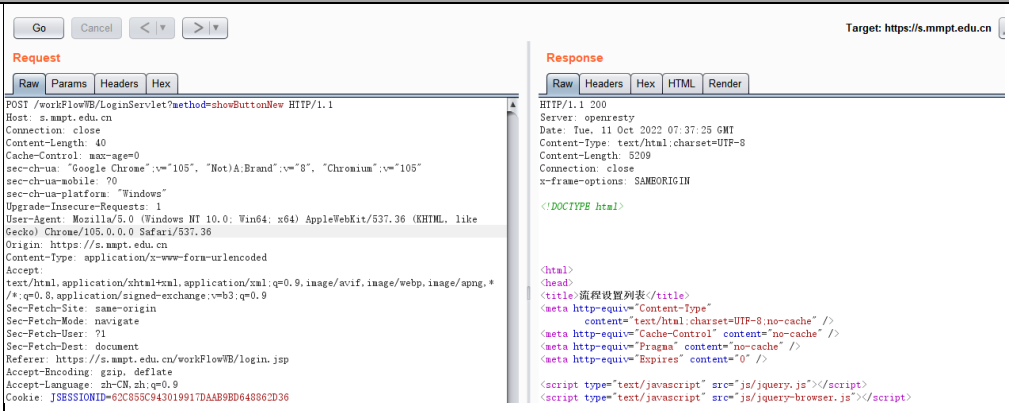
附录E表-1漏洞扫描主要安全漏洞

序号	危险程度	漏洞名称	影响IP
1	低	允许Traceroute探测 此类漏洞涉及网络设备、安全设备、服务器存储设备。	10.2.4.14/数据库服务器-2 10.2.4.12/数据库服务器-1 10.2.4.13/应用服务器 10.2.1.4/运维安全管理系统 10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/上网行为管理系统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/汇聚交换机 172.16.1.2/核心交换机
2	低	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161) 此类漏洞涉及网络设备。	172.16.1.2/核心交换机

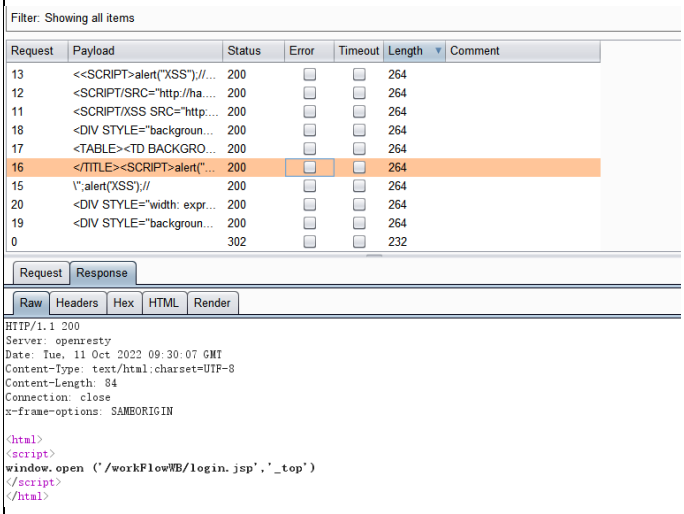
附录F 渗透测试结果记录

F.1 业务应用软件平台 缺少“X-Content-Type-Options”响应头

缺少“X-Content-Type-Options”响应头	
危险程度	低
渗透位置	JB,JC
影响URL实体	https://s.mmpt.edu.cn/workFlowWB/LoginServlet?method=showButtonNew
渗透详情	渗透方法：BurpSuite抓包检测 采用的工具：BurpSuite 测试过程：响应包中没有X-Content-Type-Options响应头，如下图：

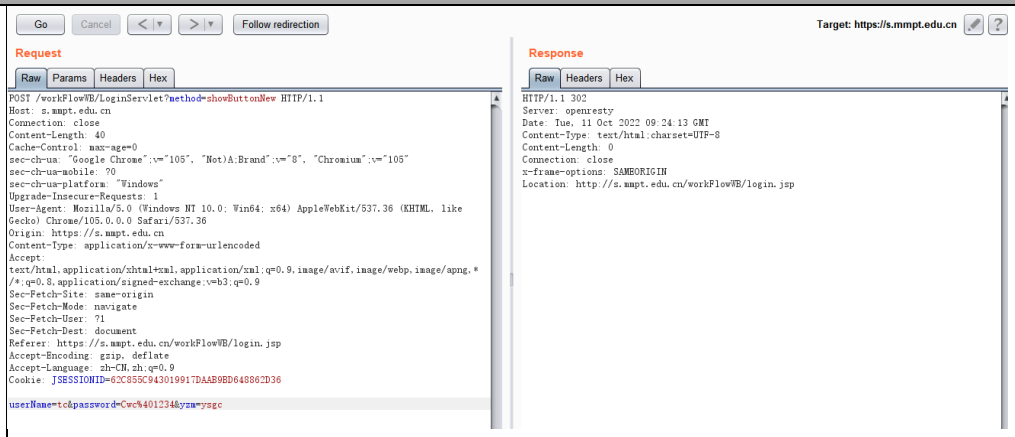
缺少“X-Content-Type-Options”响应头	
	

F.2 业务应用软件平台　　XSS跨站脚本攻击

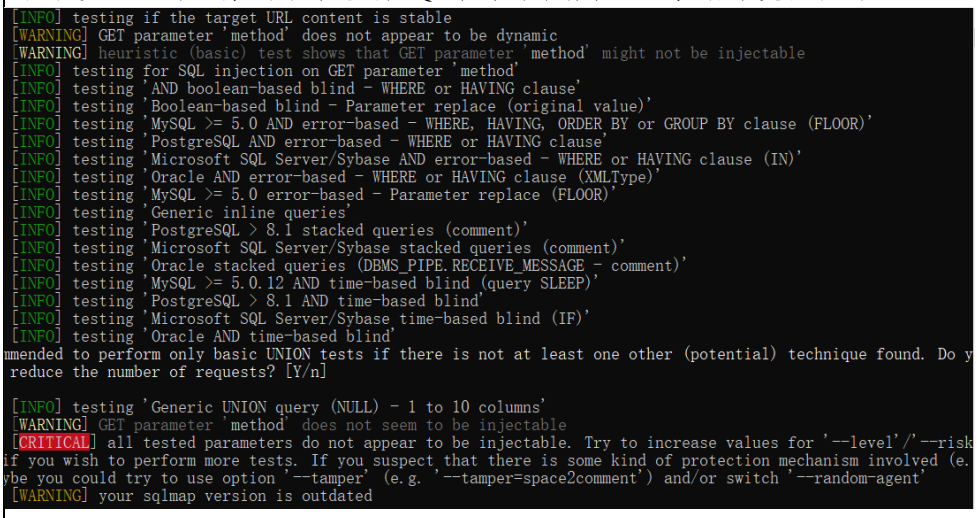
XSS跨站脚本攻击	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：测试是否对客户端输入的HTML代码、客户端脚本进行过滤或限制。 采用的工具：Burpsuite 测试过程：经检测，已对客户端输入的HTML代码、客户端脚本进行过滤或限制，暂未发现该漏洞。 

F.3 业务应用软件平台　　未授权访问

未授权访问	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：测试能否在系统未登录的状态下进行登录后功能访问或操作。 采用的工具：Burpsuite 测试过程：已检测，不能在系统未登录的状态下进行功能访问或操作。

未授权访问	
	

F.4 业务应用软件平台　　SQL注入漏洞

SQL注入漏洞	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：通过手工或工具检测系统在执行SQL语句时是否存在注入。 采用的工具：Sqlmap 测试过程：已检测，系统在执行SQL语句时不存在注入，暂未发现该漏洞。 

附录G 威胁列表

附录G 表- 1威胁列表

序号	威胁列表	描述
1	恶意攻击	利用工具和技术对信息系统进行攻击和入侵。威胁行为包括：恶意代码、邮件勒索、网络攻击等。
2	软硬件故障	对业务实施或系统运行产生影响的设备硬件故障、通讯链路中断、系统本身或软件缺陷造等问题。威胁行为包括：设备故障、软件故障等。
3	管理不到位	由于制度缺失、不完善等原因导致安全管理无法落实

序号	威胁列表	描述
		或者不到位。威胁行为包括：管理不到位、媒体负面报道等。
4	无作为或操作失误	应该执行而没有执行相应的操作，或者无意执行了错误的操作。威胁行为包括：操作失误、维护错误等。
5	敏感信息泄漏	敏感信息泄露给不应了解的他人。威胁行为包括：内部信息泄露、外部信息泄露等。
6	物理环境影响	对信息系统正常运行造成影响的物理环境问题和自然灾害。威胁行为包括：物理损害等。
7	越权或滥用	越权访问本来无权访问的资源，或者滥用自己的权限破坏信息系统。威胁行为包括：未授权的设备使用、权限滥用、权限伪造等。
8	物理攻击	通过物理的接触造成对软件、硬件和数据的破坏。威胁行为包括：设备失效等。
9	篡改	非法修改信息，破坏信息的完整性使系统的安全性降低或信息不可用。威胁行为包括：硬件篡改、数据篡改等。
10	抵赖	否认所做的操作。威胁行为包括：行为否认（抵赖）、媒体负面报道等。

报告编号：44090243008-00007-22-0163-01

网络安全等级保护
档案管理系统等级测评报告

委托单位：茂名职业技术学院

测评单位：广东南方信息安全研究院

报告时间：2022年10月30日

网络安全等级测评基本信息表

被测对象				
被测对象名称	档案管理系统		安全保护等级	第二级（S2A2）
备案证明编号	44090243008-00007			
被测单位				
单位名称	茂名职业技术学院			
单位地址	广东省茂名市茂南区文明北路232号大院		邮政编码	525000
联系人	姓名	龙恒	职务/职称	教师
	所属部门	教育信息与网络中心	办公电话	0668-2920122
	移动电话	13377766618	电子邮件	372383968@qq.com
测评单位				
单位名称	广东南方信息安全研究院		机构代码	SC202127130010163
单位地址	广州市科学城彩频路9号B座12楼1202		邮政编码	510663
联系人	姓名	谢若雨	职务/职称	助理
	所属部门	办公室	办公电话	020-32290702
	移动电话	18819149895	电子邮件	office@cybersec-gd.cn
审核批准	编制人	林炳良	编制日期	2022.10.30
	审核人	谭	审核日期	2022.10.30
	批准人	陈林	批准日期	2022.10.30

声明

本报告是档案管理系统的等级测评报告。

本报告测评结论的有效性建立在被测评单位提供相关证据的真实性基础之上。

本报告中给出的测评结论仅对被测对象当时的安全状态有效。当测评工作完成后，由于被测对象发生变更而涉及到的系统构成组件（或子系统）本报告不再适用。

本报告中给出的测评结论不能作为对被测对象内部部署的相关系统构成组件（或产品）的测评结论。

在任何情况下，若需引用本报告中的测评结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。

单位名称：广东南方信息安全研究院

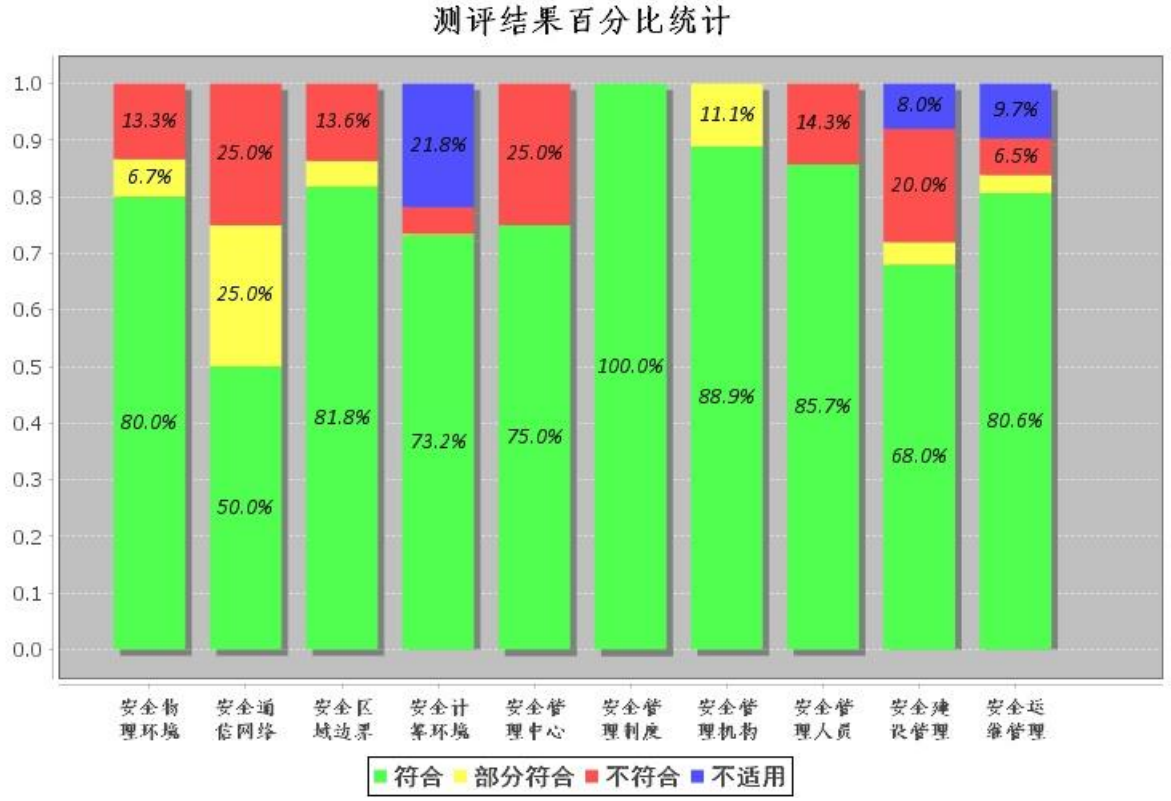
2022年10月30日

等级测评结论

测评结论和综合得分			
被测对象名称	档案管理系统	安全保护等级	第二级（S2A2）
扩展要求应用情况	□云计算 □移动互联 □物联网 □工业控制系统 □大数据		
被测对象描述	档案管理系统是由茂名职业技术学院统一组织规划建设，由同略科技有限公司负责开发，于2019年12月正式投入运行，由教育信息与网络中心负责运行维护。茂名职业技术学院是该信息系统的业务主管部门，茂名职业技术学院为该信息系统定级的责任单位。 档案管理系统网络主要分为4个区域，分别为外网边界区域、安全管理区域、服务器存储区域、办公网区域，主要由网络设备、安全设备组成，不对互联网提供业务访问。档案管理系统为B/S结构，主要由Windows平台的操作系统，MySQL平台的数据库系统，及nginx中间件系统组成。单位采用自主运维模式，通过部署运维及管理终端提供专用运维环境管理，采用运维安全管理系统实现设备的统一管理，并进行操作运维审计，日志审计系统进行设备日志统一收集存储与分析。 档案管理系统包括了档案业务管理、借阅管理、系统管理等模块，系统涵盖档案收、管、存、用整个业务流程，能够实现档案远程归档和服务利用，包括档案的收集、整理、归档、保管、鉴定、发布、利用等全部业务环节，是学院档案全流程管理的高效平台系统。		
安全状况描述	档案管理系统通信传输具备一定的保护措施，安全区域边界较清晰，网络层具备访问控制、安全审计的相应技术措施。各设备在访问控制、安全审计、入侵防范方面具备控制措施。重要数据在数据完整性、个人信息保护方面具备保护措施。在安全管理制度层面较为完善。在网络架构不够完整，网络层在入侵防范、恶意代码和垃圾邮件防范的技术措施存在不足。各设备在身份鉴别方面控制措施存在不足。重要数据在数据备份恢复方面存在不足。 档案管理系统在本次测评中总共出现27类问题，其中0类高风险问题，12类中风险问题，15类低风险问题。在本次测评通过扫描及渗透发现2类漏洞问题，其中0类危险程度为高的漏洞，0类危险程度为中的漏洞，2类危险程度为低的漏洞。 档案管理系统本次等级测评的综合得分为73.8，且不存在高等级安全风险，等级测评结论为中。		
等级测评结论	中	综合得分	73.8

总体评价

通过对信息系统基本安全保护状态的分析，茂名职业技术学院针对档案管理系统面临的主要安全威胁采取了相应的安全机制，基本达到保护信息系统重要资产的作用。档案管理系统在本次测评中采用了GB/T 22239-2019，其中安全通用要求135项，不适用5项。



在安全物理环境方面，针对安全通用要求，基础设施在防雷击、电磁防护、防水和防潮、物理位置选择、电力供应、防盗窃和防破坏、温湿度控制等方面较为完善（如：信息化机房）。在物理访问控制、防静电等方面还不够完善（如：信息化机房），机房出入口未配置电子门禁系统，机房内缺乏防静电措施（如防静电地板或铺设防静电地毯）。

在安全通信网络方面,针对安全通用要求,网络环境在通信传输等方面较为完善(如:安全通信网络)。在网络架构等方面还不够完善（如：安全通信网络），关键的应用服务和数据库服务网段未独立进行子网划分的情况。

在安全区域边界方面，针对安全通用要求，网络环境在边界防护、安全审计、访问控制等方面较为完善（如：外网边界区域，安全管理区域，服务器存储区域等）。在入侵防范、恶意代码和垃圾邮件防范等方面还不够完善(如:安全管理区域,办公网区域),网络层部署防火墙,防火墙未配置对内部发起的攻击行为实现防范功能策略,无法检测、防止或限制从内部发起的网络攻击行为,现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。

在安全计算环境方面，针对安全通用要求，计算环境在个人信息保护、安全审计、数据完整性、访问控制、入侵防范、恶意代码防范、剩余信息保护等方面较为完善。在主机方面，在可信验证等方面还不够完善（如：业务终端-2，业务终端-1，应用/数据库服务器等），缺乏对计算设备可信验证方面的安全设计要求，现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。在应用方面，在身份鉴别、数据备份恢复等方面还不够完善（如：应用/数据库服务器-MySQL），数据库系统配置不合规的密码有效周期策略，未能提供数据库系统重要数据的异地定时数据备份功能。在网络及安全设备方面，在可信验证等方面还不够完善（如：基线核查系统，上网行为管理系统，WEB应用防火墙等），设备不具备相关可信验证的技术措施。在数据保护方面，在数据备份恢复等方面还不够完善（如：重要个人信息，重要业务数据），未能提供应用软件系统重要数据的异地定时数据备份功能。

在安全管理中心方面，针对安全通用要求，安全控制措施在审计管理等方面较为完善（如：管理中心）。在系统管理等方面还不够完善（如：管理中心），系统管理的资源、运行及配置管理不够全面。

在安全管理制度方面，针对安全通用要求，管理制度体系在制定和发布、安全策略、管理制度、评审和修订等方面较为完善（如：制度文件、执行/记录文件）。

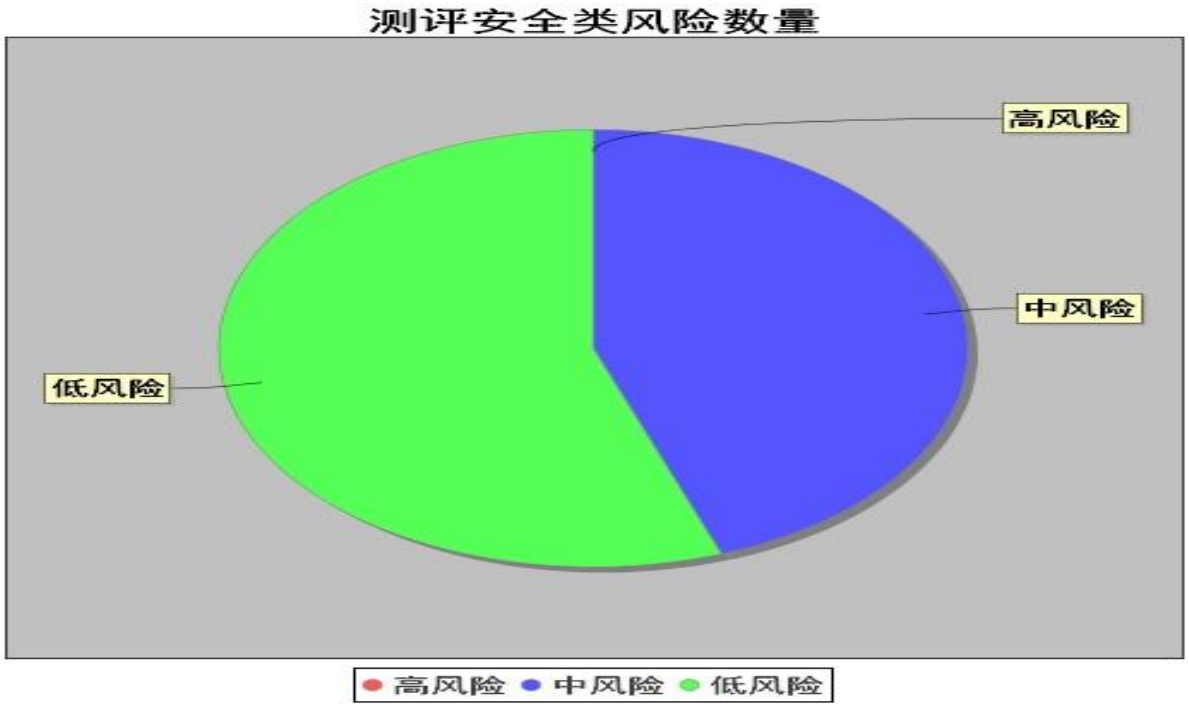
在安全管理机构方面，针对安全通用要求，机构建设在人员配备、沟通和合作、授权和审批、岗位设置等方面较为完善（如：制度文件、执行/记录文件）。在审核和检查等方面还不够完善（如：制度文件、执行/记录文件），单位开展的检查工作不够完善。

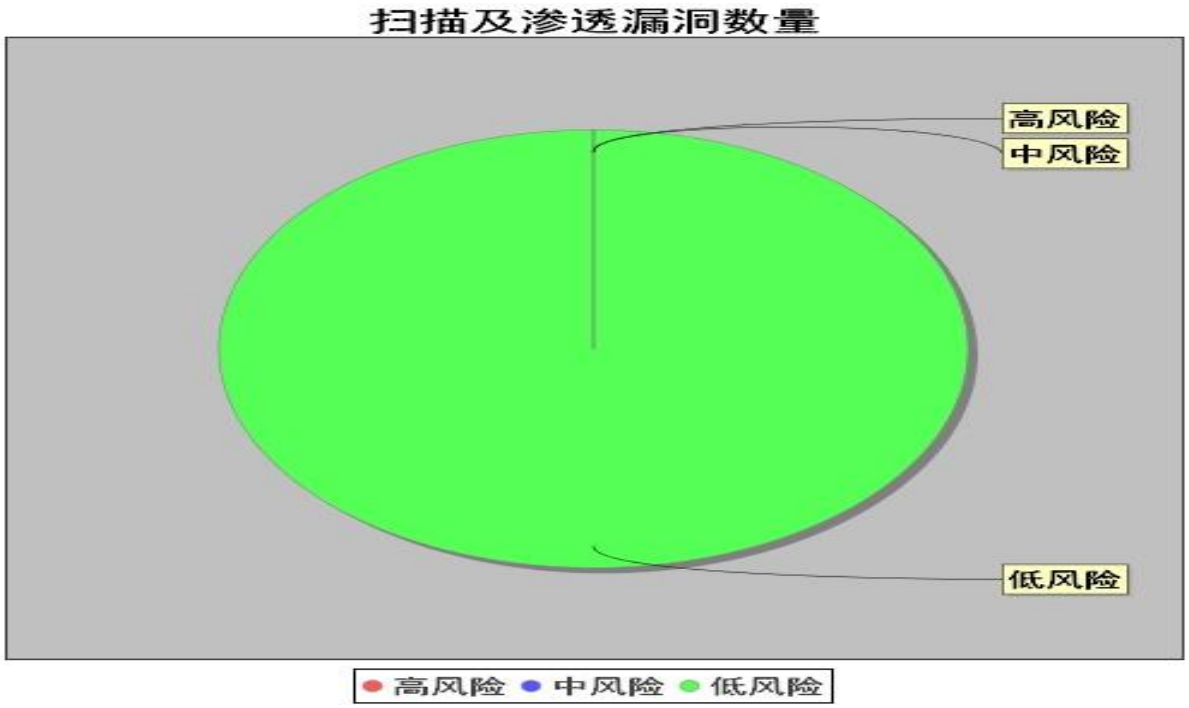
在安全管理人员方面，针对安全通用要求，人员在人员录用、安全意识教育和培训、人员离岗等方面较为完善（如：制度文件、执行/记录文件）。在外部人员访问管理等方面还不够完善（如：制度文件、执行/记录文件），单位未完全按管理规范开展人员离场后的清理工作。

在安全建设管理方面，针对安全通用要求，系统建设在定级和备案、工程实施、等级测评、产品采购和使用、服务供应商选择、系统交付等方面较为完善（如：制度文件、执行/记录文件）。在安全方案设计等方面还不够完善（如：制度文件、执行/记录文件），单位未具备完整的安全设计方案相关的文档，单位相关方案的设计的内容不够完善。

在安全运维管理方面，针对安全通用要求，系统运维在介质管理、设备维护管理、网络和系统安全管理、备份与恢复管理、资产管理、应急预案管理、环境管理、配置管理、安全事件处置、变更管理等方面较为完善（如：制度文件、执行/记录文件）。在密码管理等方面还不够完善（如：制度文件、执行/记录文件），单位不了解现有密码相关的国家标准和行业标准，单位缺乏密码管理要求的制度文档。

档案管理系统在本次测评中总共出现27类问题，其中0类高风险问题,12类中风险问题，15类低风险问题。在本次测评通过扫描及渗透发现2类漏洞问题，其中0类危险程度为高的漏洞，0类危险程度为中的漏洞，2类危险程度为低的漏洞。





档案管理系统本次等级测评的综合得分为73.8，且不存在高等级安全风险，等级测评结论为中。

主要安全问题及整改建议

一、安全物理环境

安全通用要求

(1)中风险 机房出入口未配置电子门禁系统（如：信息化机房）。 上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域,可能对系统的平稳运行造成影响。

建议安排专人7*24小时负责机房出入，对出入的人员进行身份鉴别和登记，且出入有专人陪同或在机房出入口配置电子门禁系统，控制、鉴别和记录进入的人员。

(2)中风险 机房内缺乏防静电措施（如防静电地板或铺设防静电地毯 ）（如：信息化机房）。 存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。

建议采用防静电地板或地面并采用必要的接地防静电措施。

二、安全通信网络

安全通用要求

(1)中风险 关键的应用服务和数据库服务网段未独立进行子网划分的情况（如：安全通信网络）。 上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变得更为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。

建议独立划分出应用服务器网段、数据库服务器网段。

三、安全区域边界

安全通用要求

(1)中风险 网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为（如：办公网区域）。 存在不

能及时发现内部主机作为攻击跳板，或网络攻击行为而造成系统损坏/网络资源浪费的风险。

建议网络层部署的防火墙配置对内部发起的攻击行为实现防范功能策略，实现检测、防止或限制从内部发起的网络攻击行为。

(2)中风险 现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面（如：办公网区域）。 无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。

建议现有部署的恶意代码防范措施网络边界覆盖全面，及时对恶意代码及逆行检测和清除。

四、安全计算环境

1、网络设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

2、安全设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

3、服务器和终端

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

4、系统管理软件/平台

安全通用要求

(1)中风险 数据库系统配置不合规的密码有效周期策略（如：应用/数据库服务器

-MySQL）。 上述问题的存在，使恶意用户能够较为容易的访问数据库等资源并实施恶意操作，对相关系统的正常运行造成影响，存在系统被未授权访问、操作的可能性。

建议数据库配置 ‘default_password_lifetime‘；默认密码有效期不为0（具体有效期视业务需求定，一般情况可参考设为90-180天）。

⑵中风险 未能提供数据库系统重要数据的异地定时数据备份功能（如：应用/数据库服务器-MySQL）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供，使企业的经济利益或声誉受到损害。

建议数据库系统利用通信网络将关键数据定时批量传送至备用场地，实现异地数据异地备份。

5、业务应用系统/平台

安全通用要求

⑴中风险 未能提供应用软件系统重要数据的异地定时数据备份功能（如：档案管理系统）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。

建议利用通信网络将应用软件系统关键数据定时批量传送至备用场地，实现异地数据异地备份。

6、数据资源

安全通用要求

重要业务数据

⑴中风险 未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要业务数据）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。

建议利用通信网络将应用软件系统关键数据定时批量传送至备用场地，实现异地数据异地备份。

重要个人信息

(1)中风险 **未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要个人信息）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。**

建议利用通信网络将应用软件系统关键数据定时批量传送至备用场地，实现异地数据异地备份。

7、其他系统或设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

五、安全管理中心

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

六、安全管理制度

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

七、安全管理机构

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

八、安全管理人员

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

九、安全建设管理

安全通用要求

(1)中风险 **单位未具备完整的安全设计方案相关的文档。单位相关方案的设计的内容不够完善（如：制度文件、执行/记录文件）。 相关合规的规划配套文件缺失，可能导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。**

建议根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件。

十、安全运维管理

安全通用要求

(1)中风险 **单位不了解现有密码相关的国家标准和行业标准。单位缺乏密码管理要求的制度文档（如：制度文件、执行/记录文件）。 密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不到位，存在违反国家政策的风险。**

建议单位学习现有密码相关的国家标准和行业标准。建立密码管理要求的制度文档。

目录

网络安全等级测评基本信息表 I
声明 II
等级测评结论 III
总体评价 IV
主要安全问题及整改建议 VIII
一、安全物理环境 VIII
安全通用要求 VIII
二、安全通信网络 VIII
安全通用要求 VIII
三、安全区域边界 VIII
安全通用要求 VIII
四、安全计算环境 IX
1、网络设备 IX
安全通用要求 IX
2、安全设备 IX
安全通用要求 IX
3、服务器和终端 IX
安全通用要求 IX
4、系统管理软件/平台 IX
安全通用要求 IX
5、业务应用系统/平台 X
安全通用要求 X
6、数据资源 X
安全通用要求 X
7、其他系统或设备 XI
安全通用要求 XI
五、安全管理中心 XI
安全通用要求 XI
六、安全管理制度 XI
安全通用要求 XI
七、安全管理机构 XI
安全通用要求 XI
八、安全管理人员 XI
安全通用要求 XI
九、安全建设管理 XII
安全通用要求 XII
十、安全运维管理 XII
安全通用要求 XII

目录.....XIII
1 测评项目概述.....1
1.1 测评目的.....1
1.2 测评依据.....1
1.3 测评过程.....2
1.4 报告分发范围.....5
2 被测对象描述.....5
2.1 被测对象概述.....5
2.1.1 定级结果.....5
2.1.2 业务和采用的技术.....5
2.1.3 网络结构.....5
2.2 测评指标.....7
2.2.1 安全通用要求指标.....7
2.2.2 安全扩展要求指标.....9
2.2.3 其他安全要求指标.....10
2.2.4 不适用安全要求指标.....10
2.3 测评对象.....10
2.3.1 测评对象选择方法.....10
2.3.2 测评对象选择结果.....11
2.3.2.1 物理机房.....12
2.3.2.2 网络设备.....12
2.3.2.3 安全设备.....12
2.3.2.4 服务器.....13
2.3.2.5 终端设备.....13
2.3.2.6 其他系统或设备.....13
2.3.2.7 系统管理软件/平台.....14
2.3.2.8 业务应用软件/平台.....14
2.3.2.9 数据资源.....15
2.3.2.10 安全相关人员.....15
2.3.2.11 安全管理文档.....16
3 单项测评结果分析.....21
3.1 安全物理环境.....21
3.1.1 已有安全控制措施汇总分析.....21
3.1.2 主要安全问题汇总分析.....22
3.2 安全通信网络.....23
3.2.1 已有安全控制措施汇总分析.....23
3.2.2 主要安全问题汇总分析.....23
3.3 安全区域边界.....24
3.3.1 已有安全控制措施汇总分析.....24
3.3.2 主要安全问题汇总分析.....25
3.4 安全计算环境.....26
3.4.1 网络设备.....26

3.4.1.1 已有安全控制措施汇总分析 26
3.4.1.2 主要安全问题汇总分析 28
3.4.2 安全设备 28
3.4.2.1 已有安全控制措施汇总分析 28
3.4.2.2 主要安全问题汇总分析 32
3.4.3 服务器和终端 32
3.4.3.1 已有安全控制措施汇总分析 32
3.4.3.2 主要安全问题汇总分析 35
3.4.4 系统管理软件/平台 36
3.4.4.1 已有安全控制措施汇总分析 36
3.4.4.2 主要安全问题汇总分析 39
3.4.5 业务应用系统/平台 39
3.4.5.1 已有安全控制措施汇总分析 39
3.4.5.2 主要安全问题汇总分析 41
3.4.6 数据资源 41
3.4.6.1 已有安全控制措施汇总分析 41
3.4.6.2 主要安全问题汇总分析 42
3.4.7 其他系统或设备 42
3.4.7.1 已有安全控制措施汇总分析 42
3.4.7.2 主要安全问题汇总分析 43
3.5 安全管理中心 43
3.5.1 已有安全控制措施汇总分析 43
3.5.2 主要安全问题汇总分析 44
3.6 安全管理制度 44
3.6.1 已有安全控制措施汇总分析 44
3.6.2 主要安全问题汇总分析 45
3.7 安全管理机构 45
3.7.1 已有安全控制措施汇总分析 45
3.7.2 主要安全问题汇总分析 47
3.8 安全管理人员 47
3.8.1 已有安全控制措施汇总分析 47
3.8.2 主要安全问题汇总分析 48
3.9 安全建设管理 48
3.9.1 已有安全控制措施汇总分析 48
3.9.2 主要安全问题汇总分析 50
3.10 安全运维管理 51
3.10.1 已有安全控制措施汇总分析 51
3.10.2 主要安全问题汇总分析 55
3.11 其他安全要求指标 56
3.11.1 已有安全控制措施汇总分析 56
3.11.2 主要安全问题汇总分析 56
3.12 验证测试 56
3.12.1 漏洞扫描 56
3.12.1.1 漏洞扫描结果统计 56

3.12.1.2 漏洞扫描问题描述 60
3.12.2 渗透测试 61
3.12.2.1 渗透测试过程说明 61
3.12.2.2 渗透测试问题描述 63
3.13 单项测评小结 63
3.13.1 控制点符合情况汇总 63
3.13.2 安全问题汇总 67
4 整体测评 70
4.1 安全控制点间安全测评 71
4.1.1 安全建设管理 71
4.1.1.1 安全通用要求 71
4.1.2 安全运维管理 71
4.1.2.1 安全通用要求 72
4.2 区域间安全测评 72
4.2.1 安全物理环境 72
4.2.1.1 安全通用要求 72
4.2.2 安全通信网络 72
4.2.2.1 安全通用要求 72
4.2.3 安全区域边界 73
4.2.3.1 安全通用要求 73
4.2.4 安全计算环境 73
4.2.4.1 安全通用要求 73
4.3 整体测评结果汇总 74
5 安全问题风险分析 76
6 等级测评结论 80
7 安全问题整改建议 82
附录A 被测对象资产 88
A.1 物理机房 88
A.2 网络设备 88
A.3 安全设备 88
A.4 服务器 89
A.5 终端设备 89
A.6 其他系统或设备 89
A.7 系统管理软件/平台 89
A.8 业务应用软件/平台 90
A.9 数据资源 90
A.10 密码产品 91
A.11 安全相关人员 91
A.12 安全管理文档 91
附录B 上次测评问题整改情况说明 96
附录C 单项测评结果汇总 97

C.1 安全物理环境 97
C.2 安全通信网络 97
C.3 安全区域边界 97
C.4 安全计算环境 98
C.4.1 网络设备 98
C.4.2 安全设备 99
C.4.3 服务器和终端 100
C.4.4 系统管理软件/平台 100
C.4.5 业务应用系统/平台 101
C.4.6 数据资源 101
C.4.7 其他系统或设备 102
C.5 安全管理中心 102
C.6 安全管理制度 102
C.7 安全管理机构 102
C.8 安全管理人员 103
C.9 安全建设管理 103
C.10 安全运维管理 103
C.11 其他安全要求指标 104
附录D 单项测评结果记录 104
D.1 安全物理环境 104
D.1.1 安全通用要求 104
D.1.1.1 信息化机房 104
D.2 安全通信网络 107
D.2.1 安全通用要求 107
D.2.1.1 安全通信网络 107
D.3 安全区域边界 107
D.3.1 安全通用要求 107
D.3.1.1 办公网区域 107
D.3.1.2 外网边界区域 110
D.3.1.3 安全管理区域 112
D.3.1.4 服务器存储区域 114
D.4 安全计算环境 117
D.4.1 安全通用要求 117
D.4.1.1 网络设备 117
D.4.1.2 安全设备 124
D.4.1.3 服务器和终端 148
D.4.1.4 系统管理软件/平台 170
D.4.1.5 业务应用系统/平台 177
D.4.1.6 数据资源 181
D.4.1.7 其他系统或设备 188
D.5 安全管理中心 188
D.5.1 安全通用要求 188
D.5.1.1 管理中心 188
D.6 安全管理制度 190

D.6.1 安全通用要求 190
D.6.1.1 制度文件、执行/记录文件 190
D.7 安全管理机构 192
D.7.1 安全通用要求 192
D.7.1.1 制度文件、执行/记录文件 192
D.8 安全管理人员 194
D.8.1 安全通用要求 194
D.8.1.1 制度文件、执行/记录文件 194
D.9 安全建设管理 196
D.9.1 安全通用要求 196
D.9.1.1 制度文件、执行/记录文件 196
D.10 安全运维管理 200
D.10.1 安全通用要求 200
D.10.1.1 制度文件、执行/记录文件 200
D.11 其他安全要求 208
附录E 漏洞扫描结果记录 208
附录F 渗透测试结果记录 209
附录G 威胁列表 211

1 测评项目概述

1.1 测评目的

安全等级测评的目标是通过对目标系统在安全技术及管理方面的测评,对目标系统的安全技术状态及安全管理状况做出初步判断,给出目标系统在安全技术及安全管理方面与其相应安全等级保护要求之间的差距。测评结论作为委托方进一步完善系统安全策略及安全技术防护措施依据。

项目背景是为进一步提高信息系统的保障能力,根据《信息安全等级保护管理办法》（公通字2007【43】号）的精神，茂名职业技术学院委托广东南方信息安全研究院（SC202127130010163）对档案管理系统实施等级测评，以期发现信息系统和等级保护标准的差距以及存在的安全隐患，为后续的安全整改工作提供参考依据。

1.2 测评依据

测评过程中主要依据的标准:

测评标准

（1）GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》

（2）GB/T 28448-2019 《信息安全技术 网络安全等级保护测评要求》

测评参考标准

（1）GB 17859-1999 《计算机信息系统 安全保护等级划分准则》

（2）GB/T 28449-2018 《信息安全技术 网络安全等级保护测评过程指南》

（3）GB/T 20984-2007 《信息安全技术 信息安全风险评估规范》

（4）GB/T 25058-2019 《信息安全技术 网络安全等级保护实施指南》

测评参考法律法规

（1）《中华人民共和国网络安全法》

（2）《中华人民共和国密码法》

（3）《中华人民共和国数据安全法》

1.3 测评过程

本次等级测评分为四个过程：测评准备活动、方案编制活动、测评实施活动、报告编制活动。具体如图 1-1 所示。其中，各阶段的时间安排如下：

⑴ 测评准备活动

测评准备活动的目标是顺利启动测评项目,收集定级对象相关资料,准备测评所需资料,为编制测评方案打下良好的基础。测评准备活动包括工作启动、信息收集和分析、工具和表单准备三项主要任务。

（2）方案编制活动

方案编制活动的目标是整理测评准备活动中获取的定级对象相关资料,为现场测评活动提供最基本的文档和指导方案。方案编制活动包括测评对象确定、测评指标确定、测评内容确定、工具测试方法确定、测评指导书开发及测评方案编制六项主要任务。

（3）现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调,为现场测评的顺利开展打下良好基础,依据测评方案实施现场测评工作,将测评方案和测评方法等内容具体落实到现场测评活动中。现场测评工作应取得报告编制活动所需的、足够的证据和资料。现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

（4）报告编制活动

在现场测评工作结束后,测评机构应对现场测评获得的测评结果(或称测评证据)进行汇总分析,形成等级测评结论,并编制测评报告。测评人员在初步判定单项测评结果后,还需进行单元测评结果判定、整体测评、系统安全保障评估,经过整体测评后,有的单项

测评结果可能会有所变化,需进一步修订单项测评结果,而后针对安全问题进行风险评估,形成等级测评结论。分析与报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、系统安全保障评估、安全问题风险评估、等级测评结论形成及测评报告编制七项主要任务。

各阶段完成的关键任务：

序号	阶段	任务	对象	开始日期	结束日期
1	测评准备活动	工作启动	项目甲乙双方	2022年8月15日	2022年8月19日
2		信息收集与分析	调研表	2022年8月22日	2022年8月25日
3		工具和表单准备	测评工具、测评授权书、文档交接单	2022年8月25日	2022年8月30日
4	方案编制活动	测评对象确认	测评方案-对象列表	2022年8月31日	2022年8月31日
5		测评指标确认	测评方案-指标列表	2022年8月31日	2022年8月31日
6		测评内容确认	测评方案-内容列表	2022年9月1日	2022年9月1日
7		工具测试方法确认	测评方案-工具测试方法列表	2022年9月1日	2022年9月1日
8		测评指导书开发	测评作业指导书	2022年9月2日	2022年9月2日
9		测评方案编制	测评方案	2022年9月5日	2022年9月5日
10	现场测评活动	现场测评准备	工具、人员、表单准备	2022年9月28日	2022年9月28日
11		现场测评和结果记录	安全管理访谈	2022年9月28日	2022年9月28日
12			安全管理文档检查	2022年9月28日	2022年9月28日
13			安全物理环境测评	2022年9月28日	2022年9月28日
14			安全通信网络	2022年9月28日	2022年9月29日
15			安全区域边界	2022年9月28日	2022年9月29日
16			安全计算环境	2022年9月28日	2022年9月29日
17			工具测试	2022年9月29日	2022年10月9日
18		结果确认和资料归还	检测人员出入场确认单、测评现场服务评价单	2022年10月8日	2022年10月9日
19	报告编制活动	单项测评结果	测评报告	2022年10月9日	2022年10月12日

序号	阶段	任务	对象	开始日期	结束日期
		判定			
20		单元测评结果判定		2022年10月9日	2022年10月17日
21		整体测评		2022年10月9日	2022年10月17日
22		系统安全保障评估		2022年10月9日	2022年10月17日
23		安全问题风险分析		2022年10月9日	2022年10月17日
24		等级测评结论形成		2022年10月17日	2022年10月30日
25		测评报告编制		2022年10月17日	2022年10月30日

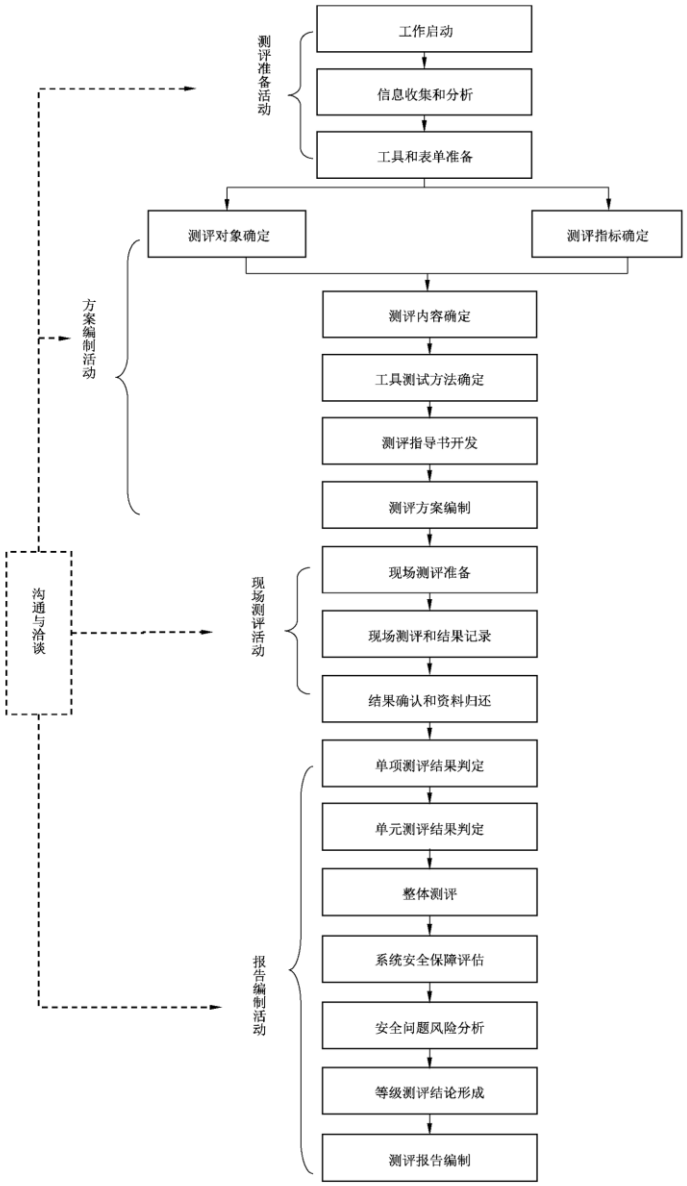


图 1-1 等级保护测评工作流程图

其中，于项目前期召开了项目启动会议，确定了工作方案及项目人员名单；于现场测评完成后召开了项目末次会议，确认了测评发现的问题；于2022年10月30日在对系统的整改情况进行了复核确认后，完成报告编制。

1.4 报告分发范围

等级测评报告正本一式3份，其中茂名职业技术学院1份，广东南方信息安全研究院1份，受理备案的公安机关1份。

2 被测对象描述

2.1 被测对象概述

2.1.1 定级结果

表 2-1定级结果

被测对象名称	安全保护等级	业务信息安全等级	系统服务安全等级
档案管理系统	2	2	2

2.1.2 业务和采用的技术

档案管理系统包括了档案业务管理、借阅管理、系统管理等模块,系统涵盖档案收、管、存、用整个业务流程，能够实现档案远程归档和服务利用，包括档案的收集、整理、归档、保管、鉴定、发布、利用等全部业务环节，是学院档案全流程管理的高效平台系统。

被测对象未采用云计算/移动互联/物联网/工业控制/大数据等技术情况。

2.1.3 网络结构

档案管理系统主要是对内网提供服务，相关设备部署在信息化机房当中,其简要拓扑如下:

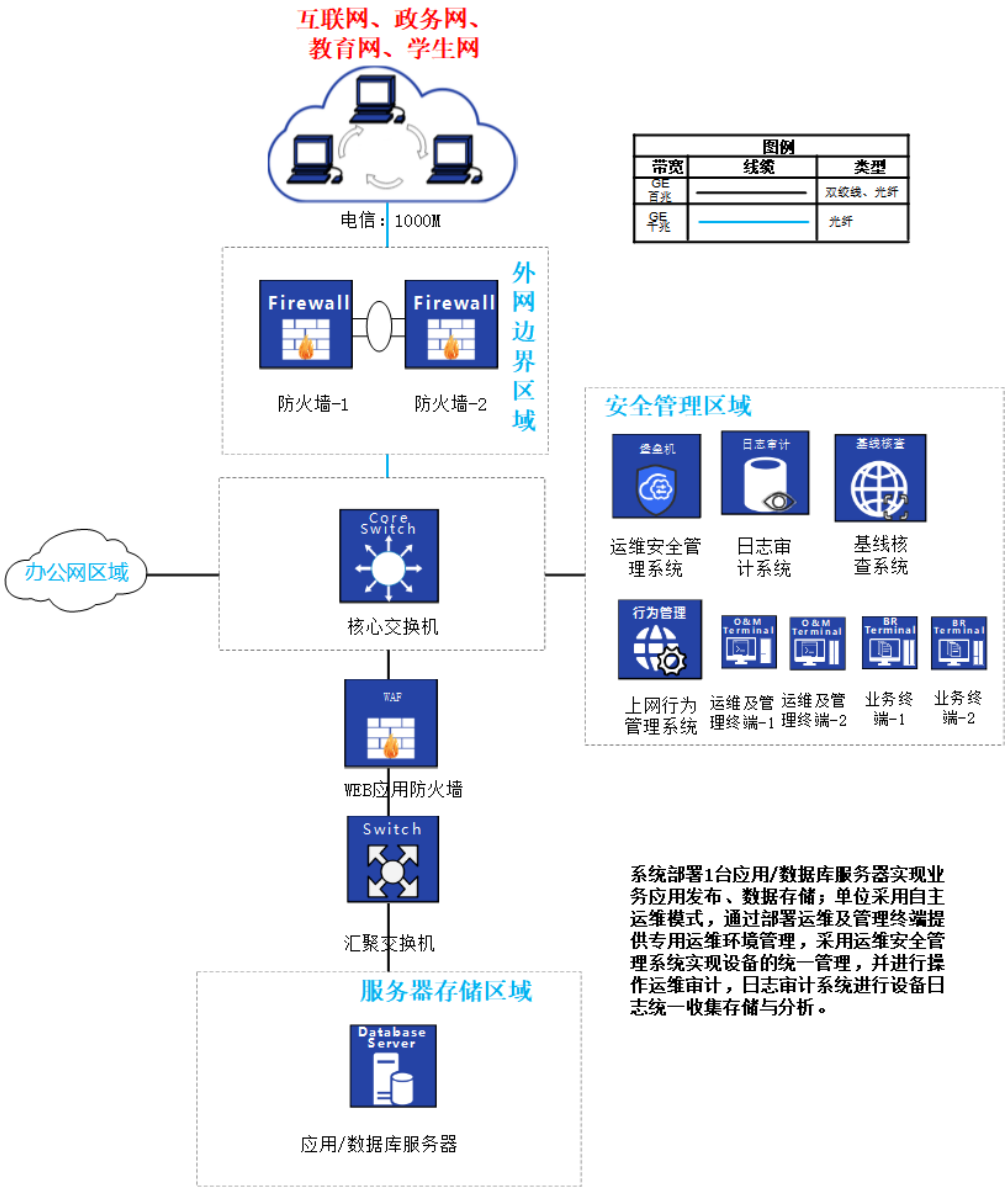


图 2-1 档案管理系统网络拓扑图

如图2-1档案管理系统网络拓扑图所示，档案管理系统网络安全域划分为4个，分别为外网边界区域、安全管理区域、服务器存储区域、办公网区域。

1、外网边界区域：

外网边界区域网络主要包括档案管理系统的业务服务和信息交换应用，是安全管理区域、服务器存储区域、办公网区域的出口边界；其链路接入为光纤线，带宽为1000mb。通过部署核心交换机、防火墙等设备实施网络访问控制，防火墙（入侵防御模块）实现网络入侵攻击行为防御。

2、办公网区域：

办公网区域网络主要包括档案管理系统与办公区域的信息交换应用，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、防火墙、上网行为管理系统等设备实施网络访问控制、防火墙（入侵防御模块）实现网络入侵攻击行为防御。

3、安全管理区域：

安全管理区域网络主要包括日志审计系统、运维安全管理系统、上网行为管理系统，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、上网行为管理系统等设备实施网络访问控制。

4、服务器存储区域：

服务器存储区域网络主要包括档案管理系统的应用服务器、数据库服务器，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、上网行为管理系统等设备实现一定的网络访问控制。

5、服务器部署情况：

档案管理系统由1台应用/数据库服务器实现应用发布、数据处理、存储、维护。

6、灾备及冗余

档案管理系统无异地备份机房，未实现异地备份数据定时传输功能。系统重要数据根据需求采用每天增量、每月全备到本地信息化机房。

档案管理系统未实现冗余措施。

2.2 测评指标

2.2.1 安全通用要求指标

表 2-2 安全通用要求指标

安全类	安全控制点	测评项数
安全物理环境	物理位置选择	2
	物理访问控制	1
	防盗窃和防破坏	2
	防雷击	1
	防火	2
	防水和防潮	2
	防静电	1
	温湿度控制	1
	电力供应	2
	电磁防护	1
安全通信网络	网络架构	2
	通信传输	1
	可信验证	1
安全区域边界	边界防护	1
	访问控制	4
	入侵防范	1
	恶意代码和垃圾邮件防范	1
	安全审计	3
	可信验证	1
安全计算环境	身份鉴别	3
	访问控制	4
	安全审计	3
	入侵防范	5
	恶意代码防范	1
	可信验证	1
	数据完整性	1
	数据备份恢复	2
	剩余信息保护	1
	个人信息保护	2
安全管理中心	系统管理	2
	审计管理	2
安全管理制度	安全策略	1
	管理制度	2
	制定和发布	2
	评审和修订	1
安全管理机构	岗位设置	2
	人员配备	1
	授权和审批	2
	沟通和合作	3

安全类	安全控制点	测评项数
	审核和检查	1
安全管理人员	人员录用	2
	人员离岗	1
	安全意识教育和培训	1
	外部人员访问管理	3
安全建设管理	定级和备案	4
	安全方案设计	3
	产品采购和使用	2
	自行软件开发	2
	外包软件开发	2
	工程实施	2
	测试验收	2
	系统交付	3
	等级测评	3
	服务供应商选择	2
安全运维管理	环境管理	3
	资产管理	1
	介质管理	2
	设备维护管理	2
	漏洞和风险管理	1
	网络和系统安全管理	5
	恶意代码防范管理	3
	配置管理	1
	密码管理	2
	变更管理	1
	备份与恢复管理	3
	安全事件处置	3
	应急预案管理	2
	外包运维管理	2
安全通用要求指标数量统计		135

2.2.2 安全扩展要求指标

表 2-3 安全扩展要求指标

扩展类型	安全类	安全控制点	测评项数
本次测评不涉及安全扩展要求指标			

2.2.3 其他安全要求指标

表 2-4 其他安全要求指标

安全类	安全控制点	测评项数
本次测评不涉及其他安全要求指标		

2.2.4 不适用安全要求指标

表 2-5-1 不适用安全要求指标

安全类	安全控制点	不适用项	不适用原因
安全建设管理	自行软件开发	a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。
安全建设管理	自行软件开发	b) 应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。
安全运维管理	密码管理	b) 应使用国家密码管理主管部门认证核准的密码技术和产品。	（1）单位未采购涉及密码技术的产品，不适用。
安全运维管理	外包运维管理	a) 应确保外包运维服务商的选择符合国家的有关规定；	（1）单位目前未涉及任何外包运维服务情况，不适用。
安全运维管理	外包运维管理	b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。	（1）单位目前未涉及任何外包运维服务情况，不适用。

表 2-5-2 其他不适用安全要求指标

安全类	安全控制点	不适用项	不适用原因
本次测评不涉及其他安全要求指标			

2.3 测评对象

2.3.1 测评对象选择方法

档案管理系统等级测评的测评对象种类上基本覆盖、数量进行抽样，重点抽查主要的设备、设施、人员和文档等。结合档案管理系统的网络拓扑结构和业务情况，本次等级测评的测评对象在抽样时主要考虑以下几个方面：

（1） 主机房（包括其环境、设备和设施等）和灾备机房；

（2） 存储被测系统重要数据的介质的存放环境；

（3） 办公场地；

（4） 整个系统的网络拓扑结构；

（5） 安全设备，包括防火墙等；

（6） 边界网络设备，包括路由器、楼层交换机等；

（7） 对整个信息系统或其局部的安全性起作用的网络互联设备，如核心交换机、路由器等；

（8） 承载业务处理系统主要业务或数据的服务器（包括其操作系统和数据库）；

（9） 管理终端和主要应用系统终端；

（10） 能够完成系统不同业务使命的业务应用系统；

（11） 业务备份系统；

（12） 信息安全主管人员、各方面的负责人员、具体负责安全管理的当事人、业务负责人；

（13） 涉及到信息系统安全的所有管理制度和记录。

抽样原则：在等级测评时，业务处理系统中配置相同的安全设备、边界网络设备、网络互联设备、服务器、终端以及备份设备，每类至少抽查两台作为测评对象。

2.3.2 测评对象选择结果

2.3.2.1 物理机房

表 2-6 物理机房

序号	机房名称	物理位置	重要程度
1	信息化机房	茂名市茂南区文明北路232号大院大楼	关键

2.3.2.2 网络设备

表 2-7 网络设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度
1	核心交换机	否	H3C version 7.1.070, Release 7585P07	H3C S7500E-X	核心数据交换、访问控制	关键
2	汇聚交换机	否	H3C version 7.1.070, Release 6126P20	H3C S5560X-30C-EI	数据交换	重要

2.3.2.3 安全设备

表 2-8 安全设备

序号	设备名称	是否虚拟设备	系统及版本	品牌型号	用途	重要程度
1	防火墙-2	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键
2	运维安全管理系统	否	深信服V3.0.6	深信服AC-1000-D603-PT	运维审计	重要
3	上网行为管理系统	否	深信服AC12.0.26	深信服AC-1000-D600-PT	上网行为管理及终端准入控制	重要
4	WEB应用防火墙	否	深信服AF 8.0.9	深信服WAF-2000-H642	应用防护、入侵防范、病毒防护	重要
5	基线核查系统	否	深信服V3.0.3	深信服AC-1000-D602-PT	漏洞扫描	重要
6	防火墙-1	否	深信服AF 8.0.23	深信服	访问控制、入侵防	关键

序号	设备名称	是否虚拟设备	系统及版本	品牌型号	用途	重要程度
				AF-2000-H642	范、病毒防护	
7	日志审计系统	否	深信服LAS 3.0.5	深信服AC-1000-D601-PT	日志审计	重要

2.3.2.4 服务器

表 2-9 服务器

序号	设备名称	所属业务应用系统/平台	是否虚拟设备	操作系统及版本	数据库管理系统及版本	中间件及版本	重要程度
1	应用/数据库服务器	档案管理系统	否	Windows Server 2008 R2	MySQL 5.7	Tomcat 9.0.13	关键

2.3.2.5 终端设备

表 2-10 终端设备

序号	设备名称	是否虚拟设备	操作系统及版本	用途	重要程度
1	运维及管理终端-2	否	Windows 10 （版本 21H2（内部版本 19044.1889））	运维管理、系统管理	一般
2	业务终端-1	否	Windows 10 （版本 20H2（内部版本 19044.1889）	业务管理	一般
3	运维及管理终端-1	否	Windows 10 （版本 20H2（内部版本 19044.1889）	运维管理、系统管理	一般
4	业务终端-2	否	Windows 10 （版本 20H2（内部版本 19044.1889）	业务管理	一般

2.3.2.6 其他系统或设备

表 2-11 其他系统或设备

序号	设备名称	是否虚拟设备	系统及版本	用途	重要程度
/	/	/	/	/	/

注释：本次测评对象中不涉及专用移动互联终端等，不开展抽测。

2.3.2.7 系统管理软件/平台

表 2-12 系统管理软件/平台

序号	系统管理软件/平台名称	主要功能	版本	所在设备名称	重要程度
1	应用/数据库服务器-MySQL	数据生产、存储	5.7	应用/数据库服务器	关键
2	应用/数据库服务器-Tomcat	页面发布	9.0.13	应用/数据库服务器	关键

2.3.2.8 业务应用软件/平台

表 2-13 业务应用系统/平台

序号	业务应用软件/平台名称	主要功能	业务应用软件及版本	开发厂商	重要程度
1	档案管理系统	档案管理系统包括了档案业务管理、借阅管理、系统管理等模块，系统涵盖档案收、管、存、用整个业务流程，能够实现档案远程归档和服务利用，包括档案的收集、整理、归档、保管、鉴定、发布、利用等全部业务环节，是学院档案全流程管理的高效平台系统。	V6.0	同略科技有限公司	关键

2.3.2.9 数据资源

表 2-14 数据资源

序号	数据类别	所属业务应用	安全防护需求	重要程度
1	重要个人信息	档案管理系统	完整性、保密性	关键
2	重要业务数据	档案管理系统	完整性、保密性	关键
3	鉴别数据	档案管理系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性、保密性	关键
4	重要审计数据	档案管理系统（安全管理中心）	完整性	重要
5	重要配置数据	档案管理系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性	关键

注释：网络设备、安全设备、服务器、终端、系统管理软件/平台和业务应用系统等所涉及的鉴别数据和重要配置数据分别在各自测评对象中汇总测评证据后集中体现,包括数据完整性、数据保密性和备份恢复。重要审计数据在安全管理中心进行汇总测评证据，包括数据完整性。重要业务数据和重要个人信息分别在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。

2.3.2.10 安全相关人员

表 2-15 安全相关人员

序号	姓名	岗位/角色	联系方式	所属单位
1	叶永利	安全管理员	0668-2920122	茂名职业技术学院
2	龙恒	数据管理员	13377766618	茂名职业技术学院
3	杨云	资产管理员	0668-2920122	茂名职业技术学院
4	龙恒	网络管理员	13377766618	茂名职业技术学院
5	吴国华	机房管理员	0668-2920122	茂名职业技术学院

序号	姓名	岗位/角色	联系方式	所属单位
6	龙恒	应用管理员	13377766618	茂名职业技术学院
7	吴国华	系统管理员	0668-2920122	茂名职业技术学院
8	杨云	审计管理员	0668-2920122	茂名职业技术学院

2.3.2.11 安全管理文档

表 2-16 安全管理文档

序号	文档名称	主要内容
1	制度类文档-网络与信息系统安全设计规范	关于单位网络与信息化安全设计制度文档
2	制度类文档-安全漏洞管理制度	关于单位安全漏洞管理工作制度文档
3	制度类文档-恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
4	制度类文档-网络安全事件应急预案	关于单位网络安全事件应急处理、流程、培训等管理制度文档
5	制度类文档-办公环境管理制度	关于单位办公环境管理制度文档
6	制度类文档-数据安全管理规范	关于保障关键数据安全，从数据库本身、数据加密、数据备份恢复三个方面对数据安全进行规范的制度文档
7	制度类文档-备份与恢复管理制度	关于单位数据备份、恢复管理制度文档
8	制度类文档-系统安全管理制度	关于单位系统安全管理、安全服务管理制度文档
9	制度类文档-工程实施管理制度	关于单位工程实施工作管理制度文档
10	制度类文档-安全教育和培训制度	关于单位安全培训、安全交流工作制度文档
11	制度类文档-物理安全管理规范	关于加强单位办公区域及电子计算机机房的管理和设备运行安全，规范办公区域及机房建设，使人员办公高效及机房设备安全、稳定运行的制度文档
12	制度类文档-测试及验收方案	关于单位测试验收方案文档
13	制度类文档-网络安全事件报告制度	关于单位网络安全事件管理报告文档
14	制度类文档-恶意代码防范管理制度	关于单位恶意代码防范工作制度文档

序号	文档名称	主要内容
15	制度类文档-工程测试验收管理	关于单位工程测试工作管理制度文档
16	制度类文档-安全管理组织规范	关于单位组织结构管理规范制度文档
17	制度类文档-系统及应用数据备份管理规范	关于单位数据备份、恢复管理制度文档
18	制度类文档-组织安全结构和人员职责制度	关于单位组织结构、人员安排、人员职责制度文档
19	制度类文档-外包开发软件管理规定	关于单位外包项目管理工作制度文档
20	制度类文档-离岗人员工作交接规范	关于单位离岗交接工作规范制度文档
21	制度类文档-主机安全管理规范	关于规定单位主机系统安全管理要求规范，指导业务平台主机的安全配置和维护的制度文档
22	制度类文档-信息安全奖惩办法	关于单位人员奖惩制度文档
23	制度类文档-外部服务人员管理规范	关于单位针对外部人员工作管理规范制度文档
24	制度类文档-员工考核管理制度	关于单位人员考核工作管理制度文档
25	制度类文档-变更控制管理制度	关于单位变更流程、控制管理制度文档
26	制度类文档-组织安全结构和人员职责制度	关于单位安全结构、人员职责
27	制度类文档-人员管理制度	关于单位人员录用、调岗、离岗管理制度文档
28	制度类文档-系统交付管理	关于单位交付工作管理制度文档
29	制度类文档-设备安全管理制度	关于单位设备安全管理制度文档
30	制度类文档-安全事件报告和处置	关于单位网络安全事件管理、处置、流程等报告制度文档
31	制度类文档-办公环境保密管理	关于单位办公环境管理制度文档
32	制度类文档-服务供应商选择安全管理制度	关于单位安全服务供应商管理规定制度文档
33	制度类文档-外部接入受控网络访问系统管理规范	关于单位针对外部人员工作接入规范制度文档
34	制度类文档-授权和审批管理规定	关于单位授权审批、审批流程规范制度文档
35	制度类文档-应用系统业务用户密码设置规定	关于单位用户密码管理制度文档
36	制度类文档-网络安全管理规范	关于保障单位网络系统的安全稳定运行，抵御内部和外部各种形式的网络攻击或威胁制定的管理文档

序号	文档名称	主要内容
37	制度类文档-信息安全漏洞扫描规范	关于单位安全漏洞工作规范制度文档
38	制度类文档-安全审查和检查管理规范	关于单位安全检查、审查工作规范制度文档
39	制度类文档-网络安全管理制度	关于单位网络安全工作管理制度文档
40	制度类文档-岗位安排及岗位职责	关于单位岗位职责、岗位安排制度文档
41	制度类文档-外部人员访问管理制度	关于单位针对外来人员访问管控制度文档
42	制度类文档-应用安全管理规范	关于规定单位应用安全管理要求及规范的制度文档
43	制度类文档-信息安全总体策略	关于单位网络安全方针、策略制度文档
44	制度类文档-信息系统恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
45	制度类文档-介质管理制度	关于单位介质安全管理工制度文档
46	制度类文档-制度制定、发布、评审和修订管理制度	关于单位制度制定、发布、评审和修订等管理文档
47	制度类文档-信息系统外包运维管理制度	关于单位外包运维工作管理制度文档
48	制度类文档-机房安全管理制度	关于单位机房安全管理工作制度文档
49	操作类文档-数据备份策略	关于单位数据备份策略文件
50	操作类文档-软硬件日常维护管理规程	关于单位计算机网络系统使用、管理、信息安全、资源共享有所遵循,规范上网操作流程,提高网络系统安全性的指导文档
51	操作类文档-设备操作规程	关于单位相关设备操作指导文档
52	操作类文档-设备及系统软件配置和操作手册	关于单位安全设备操作、Linux服务器配置手册、主机运维操作手册、软件操作手册、防火墙配置和操作手册、数据库日常运维操作手册等指导文档
53	记录类文档-外部人员访问记录表	关于外来人员访问登记工作记录
54	记录类文档-信息系统存储介质销毁申请表	关于备份介质销毁申请工作记录
55	记录类文档-信息管理系统漏洞检查表	关于单位安全漏洞工作检测记录表
56	记录类文档-数据恢复申请表	关于单位数据恢复工作申请表
57	记录类文档-软件交付清单	关于单位交付工作记录
58	记录类文档-机房出入登记表	关于人员进出机房登记工作记录
59	记录类文档-收发文登记记	关于单位文档签发记录

序号	文档名称	主要内容
	录	
60	记录类文档-专家论证记录表	关于单位网络方案论证记录
61	记录类文档-机房巡检记录表	关于单位机房环境巡检记录
62	记录类文档-机房设备维修记录表	关于单位机房设备维修工作记录
63	记录类文档-设备出入登记记录表	关于设备进出机房登记工作记录
64	记录类文档-关键岗位人员考核记录	关于关键岗位考核工作记录
65	记录类文档-离场信息资料交接表	关于人员离岗交接工作记录
66	记录类文档-设备维修申请表	关于单位设备维护工作申请记录
67	记录类文档-备份介质使用记录	关于备份介质使用登记工作记录
68	记录类文档-安全管理制度评审记录	关于单位制度审计记录
69	记录类文档-信息系统存储介质使用清单	关于备份介质存储使用清单
70	记录类文档-外部人员访问申请表	关于外来人员访问申请流程工作记录
71	记录类文档-离职员工物品交回登记表	关于人员离岗工物交接工作记录
72	记录类文档-人员培训及考核记录表	关于人员培训、考核等工作记录
73	记录类文档-通用变更记录表	关于单位变更工作记录
74	记录类文档-系统交付清单	关于单位交付工作记录
75	记录类文档-接入受控网络申请表	关于外来人员接入工作记录
76	记录类文档-人员入职考核记录	关于人员录用、考核工作记录
77	记录类文档-信息安全检查记录表	关于单位安全检查工作记录
78	记录类文档-存储介质目录清单	关于备份介质存储工作清单
79	记录类文档-技能培训记录	关于单位系统培训工作、考核工作记录
80	记录类文档-网络配置信息	关于单位配置信息登记工作记录
81	记录类文档-评审和修订记录	关于单位变更评审、修订工作记录

序号	文档名称	主要内容
82	记录类文档-重要操作审批表	关于单位审批工作记录
83	记录类文档-安全建设方案评审纪录	关于单位网络与信息化安全设计方案评审工作记录
84	记录类文档-人员离岗申请表	关于人员离岗申请记录
85	记录类文档-应急预案培训记录表	关于单位应急预案培训工作记录
86	记录类文档-外部会议文件和记录	关于单位外部联系、交流及会议工作记录
87	记录类文档-漏洞检测报告	关于单位安全漏洞检测报告文档
88	记录类文档-机房设备维护记录表	关于设备维护登记工作记录
89	记录类文档-网络信息安全事件记录表	关于单位网络安全事件工作记录
90	记录类文档-机房维护日志	关于机房维护工作记录
91	记录类文档-访问记录表	关于人员访问工作记录
92	记录类文档-设备操作维护记录	关于单位设备维护工作记录
93	记录类文档-监理审批表	关于单位监理审核工作记录
94	记录类文档-数据备份记录表	关于单位数据备份工作记录
95	记录类文档-备份工作汇总表	关于单位数据备份工作总结表
96	记录类文档-信息安全会议记录	关于单位安全培训、安全交流会议记录
97	证据类文档-网络安全等级保护工作小组名单	关于单位网络安全等级保护工作小组人员名单文件
98	证据类文档-工程项目实施方案	关于单位工程实施方案文档
99	证据类文档-定级备案	关于单位系统定级报告、备案证文件
100	证据类文档-资产清单	关于单位信息系统资产清单统计表
101	证据类文档-网络安全等级保护测评服务合同	关于单位与安全服务商签定的安全服务合同文件
102	证据类文档-外部联系表	关于单位内部联系及外部联系名单
103	证据类文档-深信服安全采购合同	关于单位与安全厂家服务采购、产品选择合同文件
104	证据类文档-信息安全事件分析报告表	关于单位安全事件分析报告
105	证据类文档-安全职位人员	关于单位人员岗位安排名单
106	证据类文档-网络安全系统设计方案	关于单位网络与信息化安全设计方案文档

3 单项测评结果分析

3.1 安全物理环境

3.1.1 已有安全控制措施汇总分析

安全通用要求

物理位置选择	
a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；	
信息化机房	（1）机房和办公场地场所在建筑物具有建筑验收文档，包含对防震、防风和防雨能力的说明； （2）机房和办公场地未出严重的问题。
b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	
信息化机房	（1）机房未部署在易发生问题的位置； （2）机房对于空调设备的排水管等部位采取密封防漏处理； （3）机房对于楼板进行了防护措施。
防盗窃和防破坏	
a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识；	
信息化机房	（1）机房设备或主要部件都固定在机架上； （2）机房内对主要部件已绑定相应不易除去的标签； （3）重要机柜已进行上锁处理。
b) 应将通信线缆铺设在隐蔽安全处。	
信息化机房	（1）通信线缆铺设在下走线槽隐蔽处中； （2）通信线缆设有明显的源目的标识； （3）通信线缆均铺设整齐、规范。
防雷击	
应将各类机柜、设施和设备等通过接地系统安全接地。	
信息化机房	（1）机房设置专用地线； （2）机房内机柜、设施和设备等进行接地处理； （3）交流电源接地验收检测结果符合要求。
防火	
a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；	
信息化机房	（1）机房采用经消防检测部门检测合格并在有效期内的（如 七氟丙烷）气体自动灭火设备，火灾自动报警类型为烟感+红外； （2）自动消防系统工作状态正常，有定期巡检和维护记录《机房巡检记录表》； （3）建立机房消防的管理制度相关文档《机房安全管理制度》，按管理要求机房无人情况下气体灭火配置为自动模式，进入机房调整为手动模式，机房报警有7*24小时值班人员进行监控。
防水和防潮	

a) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	
信息化机房	（1）机房不存在雨水渗透、破损等不合规情况； （2）机房不位于建筑的顶层、边缘区域。
b) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。	
信息化机房	（1）机房区域范围已部署1台科华品牌（精密）空调，机房内分别配置1组温湿度传感器监控； （2）机房内空调下方已铺设安装好挡水和排水设施； （3）机房墙壁或楼板的管道采取必要的防渗防漏等防水保护措施； （4）机房安装检测设备（如：漏水检测绳）检测地下积水，及时处理机房水蒸气结露和地下积水的转移与渗透； （5）目前防水\防潮检测未发现异常情况，并且有防水防潮的运维记录《机房维护日志》。
温湿度控制	
应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。	
信息化机房	（1）机房范围已部署1组科华品牌精密空调进行温湿度调节； （2）机房范围已部署空调及加湿机进行温湿度调节； (3)温湿度自动调节设施运作正常,有运行和维护记录《机房维护日志》; （4）机房温度能保持在24摄氏度到28摄氏度之间； （5）机房湿度能保持在40%到65%之间。
电力供应	
a) 应在机房供电线路上配置稳压器和过电压防护设备；	
信息化机房	（1）机房配备了稳压器和过电压防护设备； （2）稳压器和过电压防护设备正常工作； （3）机房具备电力供应安全设计，并在其中标明配备稳压器、过电压防护设备等要求。
b) 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。	
信息化机房	（1）机房配备了1组科华品牌UPS； （2）UPS正常工作，可满足主要设备断电情况下的至少1小时正常运行要求； （3）UPS有定期（至少每年）检查和维护，有运行和维护记录《机房巡检记录表》。
电磁防护	
电源线和通信线缆应隔离铺设，避免互相干扰。	
信息化机房	（1）通信线缆铺设采用独立的具有电磁屏蔽作用线槽； （2）电源线缆铺设采用独立的具有电磁屏蔽作用线槽； （3）弱电线缆隔离铺设，没有干扰。

3.1.2 主要安全问题汇总分析

安全通用要求

（1）机房出入口未配置电子门禁系统（如：信息化机房）。上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域,可能对系统的平稳运行造成影响。中风险。

（2）机房建设未完全采用符合耐火等级的建筑材料。机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级（如：信息化机房）。存在发生火情时助燃火灾的风险。 低风险。

（3）机房内缺乏防静电措施（如防静电地板或铺设防静电地毯 ）（如：信息化机房）。存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。 中风险。

3.2 安全通信网络

3.2.1 已有安全控制措施汇总分析

安全通用要求

网络架构	
b) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	
安全通信网络	(1)网络内重要网段未部署在网络边界处,且未直接连接外部信息系统; (2) 系统通过防火墙对重要网段采取访问控制策略; (3) 各安全域（子网）的出口唯一。
通信传输	
应采用校验技术保证通信过程中数据的完整性。	
安全通信网络	(1) 网络系统中未涉及完整性保障设备，但在安全计算环境方面网络设备采用SSH协议、安全设备采用HTTPS协议、操作系统采用SSH协议、应用系统采用HTTPS协议来保证通信过程中数据的完整性。

3.2.2 主要安全问题汇总分析

安全通用要求

（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况（如：安全通信网络）。上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变得更

为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。 中风险。

（2）缺乏对通信设备可信验证方面的安全设计要求。现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况（如：安全通信网络）。缺乏对系统可执行程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致计算资源被干扰和破坏造成损失。 低风险。

3.3 安全区域边界

3.3.1 已有安全控制措施汇总分析

安全通用要求

边界防护	
应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络存在受保护的边界； （2）网络边界处部署了可提供访问控制功能的设备； （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。
访问控制	
a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。
b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。
c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	
办公网区域 外网边界区域 安全管理区域	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数

服务器存储区域	据包是被接收还是拒绝通过特定指示条件来决定。
d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	(1) 网络内支持状态检测和会话机制检测的区域及边界； (2) 网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； (3) 访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。
入侵防范	
应在关键网络节点处监视网络攻击行为。	
外网边界区域 服务器存储区域	(1) 网络层部署支持对内部发起的攻击行为进行防范的设备； (2) 现有的防范措施满足相应防护要求； (3) 内部安全防范措施能检测相应攻击行为。
恶意代码和垃圾邮件防范	
应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	
外网边界区域 服务器存储区域	(1) 在关键网络节点处部署合规的防恶意代码措施； (2) 恶意代码防护机制的代码库运作正常，定期更新恶意代码库； (3) 有对恶意代码库更新前的安全性及兼容性进行测试。
安全审计	
a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	(1) 网络层相关设备均开启本地审计功能； (2) 网络内部署审计措施对网络边界、重要网络节点进行安全审计； (3) 现有的审计措施满足相应的审计要求。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	(1) 设备均开启日志记录功能； (2) 现有环境内日志信息较全面； (3) 设备本地时间正常。
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	(1) 网络层部署日志审计系统，统一接收及保存相关设备的审计记录； (2) 相关网络及安全设备的本地日志文件不可删除修改； (3) 审计记录的备份机制符合信息安全管理要求； (4) 日志及审计记录的保存能力可超过6个月； (5) 定期收集日志记录并定期备份。

3.3.2 主要安全问题汇总分析

安全通用要求

(1)网络层部署防火墙,防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为（如：办公网区域）。存在不能及时发现内部主机作为攻击跳板，或网络攻击行为而造成系统损坏/网络资源浪费的风险。中风险。

(2)现有部署的恶意代码防范措施存在不合规的问题,网络边界覆盖不全面(如：办公网区域）。无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。 中风险。

(3) 缺乏对边界设备可信验证方面的安全设计要求。现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况（如：办公网区域）。缺乏对边界设备的相关程序的可信性验证,无法保证系统始终运行于可信环境中,运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4 安全计算环境

3.4.1 网络设备

3.4.1.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
核心交换机 汇聚交换机	(1) 设备对各登录模式均启用身份鉴别； (2) 设备对登录管理的用户进行身份鉴别； (3) 设备名及登录用户设置的身份标识具有唯一性； (4) 设备不存在明文或空口令用户； (5) 设备配置合规的全局密码策略； (6) 设备配置加密的super认证。
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
核心交换机 汇聚交换机	(1) 设备配置合规的全局登录失败处理策略； (2) 设备配置合规的操作超时退出措施。

c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
核心交换机 汇聚交换机	（1）设备配置合规的远程管理模式。
访问控制	
a) 应对登录的用户分配账户和权限；	
核心交换机 汇聚交换机	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。
b) 应重命名或删除默认账户，修改默认账户的默认口令；	
核心交换机 汇聚交换机	（1）设备不存在默认账户名； （2）设备账户口令设置合规。
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
核心交换机 汇聚交换机	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	
核心交换机 汇聚交换机	（1）设备根据安全策略要求对特权用户进行分离； （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
核心交换机 汇聚交换机	（1）设备开启审计功能，审计进程正常； （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
核心交换机 汇聚交换机	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
核心交换机 汇聚交换机	（1）设备限制审计文件的访问控制权限，普通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效； （5）日志及审计记录保存大于6个月。
入侵防范	
a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	
核心交换机 汇聚交换机	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。
b) 应关闭不需要的系统服务、默认共享和高危端口；	
核心交换机	（1）设备采用安全策略限制部分高危端口；

汇聚交换机	（2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。
c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
核心交换机 汇聚交换机	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
核心交换机 汇聚交换机	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
核心交换机 汇聚交换机	鉴别数据、重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； （2）设备对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a）应提供重要数据的本地数据备份与恢复功能；	
核心交换机 汇聚交换机	（1）设备定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。

3.4.1.2 主要安全问题汇总分析

安全通用要求

（1）设备不具备相关可信验证的技术措施（如：核心交换机）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.2 安全设备

3.4.2.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别

a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备对各登录模式均启用身份鉴别； （2）设备对登录管理的用户进行身份鉴别； （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备启用合规登录失败处理策略； （2）设备配置合规的操作超时退出措施。
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备配置合规的远程管理模式； （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。
访问控制	
a) 应对登录的用户分配账户和权限；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。
b) 应重命名或删除默认账户，修改默认账户的默认口令；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备不存在默认账户名； （2）设备账户口令设置合规。
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	

WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备不存在多余或过期账户； (2) 设备管理员用户与账户之间一一对应。
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备根据安全策略要求对特权用户进行分离； (2) 设备不存在多个管理级别高的特权用户； (3) 设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备开启审计功能，审计进程正常； (2)设备的日志审计级别满足要求,审计覆盖所有用户操作审计和记录。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备日期、时间正常； (2) 设备审计记录内容基本完整。
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
WEB应用防火墙 上网行为管理系统 基线核查系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备限制审计文件的访问控制权限，普通用户不可删除及修改； (2) 设备针对日志、审计记录具备充足的存储容量； (3) 对审计记录进行定期存档备份，其备份策略有效； (4) 部署日志审计系统实时对日志进行统一收集存储； (5) 日志及审计记录保存大于6个月。
日志审计系统	(1) 设备限制审计文件的访问控制权限，普通用户不可删除及修改； (2) 设备针对日志、审计记录具备充足的存储容量； (3) 对审计记录进行定期存档备份，其备份策略有效； (4) 日志及审计记录保存大于6个月。
入侵防范	

a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。
b) 应关闭不需要的系统服务、默认共享和高危端口；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。
c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 防火墙-1 防火墙-2	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
运维安全管理系统	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制。
d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备管理具备数据有效性检验功能； （2）设备管理的校验接口范围较全面。
e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。
恶意代码防范	
应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	

WEB应用防火墙 防火墙-1 防火墙-2	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	鉴别数据、重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； （2）设备对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a）应提供重要数据的本地数据备份与恢复功能；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。

3.4.2.2 主要安全问题汇总分析

安全通用要求

（1）设备不具备相关可信验证的技术措施（如：WEB应用防火墙）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.3 服务器和终端

3.4.3.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别
a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统对登录系统的用户进行身份鉴别； （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； （5）用户属性策略未勾选“密码永不过期”。
b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统启用登录失败处理策略。 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略。
c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS的管理。
应用/数据库服务器	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用‘RDP安全层’参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS的管理。
访问控制	
a）应对登录的用户分配账户和权限；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。
b）应重命名或删除默认账户，修改默认账户的默认口令；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统针对默认账户采用相应的安全策略配置； （2）操作系统账户不存在弱口令或空口令。
c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。
d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	
业务终端-1 业务终端-2	（1）操作系统根据安全策略要求对特权用户进行分离； （2）操作系统不存在特权用户；

应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（3）操作系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统开启审计策略，操作系统审计策略基本完整； （2）审计覆盖所有用户操作审计和记录。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。
c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统采取对审计记录存储容量如下： 运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。
入侵防范	
a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。
b）应关闭不需要的系统服务、默认共享和高危端口；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统不存在多余的默认共享及其它文件共享； （2）操作系统关闭不必要端口； （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。
c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。

e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。
恶意代码防范	
应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	鉴别数据、重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施: 安全选项“不显示上次的用户名”->启用

3.4.3.2 主要安全问题汇总分析

安全通用要求

（1）缺乏对计算设备可信验证方面的安全设计要求。现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况（如：业务终端-1）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.4 系统管理软件/平台

3.4.4.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
应用/数据库服务器-MySQL	（1）数据库系统启用合规登录失败处理策略； （2）数据库系统执行合规的锁定策略； （3）数据库系统配置合规的操作超时锁定。
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
应用/数据库服务器-MySQL	（1）数据库系统配置合规的远程管理模式。
访问控制	
a) 应对登录的用户分配账户和权限；	
应用/数据库服务器-MySQL	（1）登录数据库系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （2）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在多用户均与root用户权限一致的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。
应用/数据库服务器-Tomcat	（1）对应不同的账户均按需分配不同的用户权限，不存在中间件用户均属于管理级别、高权限的情况； （2）中间件配置可降权启动Tomcat的用户； （3）宿主系统针对中间件用户分别赋予相应的管理操作权限。
b) 应重命名或删除默认账户，修改默认账户的默认口令；	
应用/数据库服务器-MySQL	（1）数据库系统对多余帐户进行删除、锁定或禁止其登录； （2）数据库系统账户口令设置合规。
应用/数据库服务器-Tomcat	（1）中间件不存在除如:Tomcat、admin、manager、role1等默认账户名； （2）中间件账户口令设置合规。
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
应用/数据库服务器-MySQL	（1）数据库系统不存在多余或过期账户； （2）数据库系统管理员用户与账户之间一一对应。
应用/数据库服务器-Tomcat	（1）中间件不存在多余或过期账户；

	（2）中间件管理员用户与账户之间一一对应； （3）中间件启用合规的管理用户名配置。
d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	
应用/数据库服务器-MySQL	（1）数据库系统根据安全策略要求对特权用户进行分离； （2）数据库系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限； （3）数据库账户和系统管理员账户未处于同一个用户组中； （4）宿主操作系统管理员与数据库管理员为不同的人员，且使用不同的帐户登录系统。
应用/数据库服务器-Tomcat	（1）中间件根据安全策略要求对特权用户及宿主管理用户进行分离； （2）中间件管理不存在多个管理级别高的特权用户； （3）中间件管理按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
应用/数据库服务器-MySQL	（1）数据库系统开启审计功能，审计进程正常。
应用/数据库服务器-Tomcat	（1）中间件开启审计功能，审计进程正常； （2）系统的日志审计级别满足要求。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
应用/数据库服务器-MySQL	（1）数据库宿主系统日期、时间正常； （2）数据库系统审计记录内容基本完整。
应用/数据库服务器-Tomcat	（1）中间件日期、时间正常； （2）中间件审计记录开启审核策略且日志级别正常。
c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
应用/数据库服务器-MySQL	（1）数据库系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）数据库系统针对日志、审计记录具备充足的存储容量； （3）日志及审计记录保存大于6个月。
应用/数据库服务器-Tomcat	（1）中间件限制审计文件的访问控制权限，普通用户不可删除及修改； （2）宿主系统针对中间件日志、审计记录具备充足的存储容量； （3）对中间件审计记录进行定期存档备份，其备份策略有效； （4）审计记录及日志保存大于6个月。
入侵防范	
c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
应用/数据库服务器-MySQL	（1）数据库系统设定有效的终端接入策略，对通过网络进行管理的终端进行限制； （2）核心交换机设备ACL策略有效限制访问本机的IP地址及管理模式。
e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
应用/数据库服务器-MySQL	（1）数据库系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）数据库宿主系统不存在启用未加控制的高危端口； （3）MYSQL分离默认安装的示例数据库； （4）数据库系统进行渗透及扫描未发现存在可造成高风险的漏洞。
应用/数据库服务器-Tomcat	（1）中间件已根据需要不定期地对已发布的版本进行更新； （2）中间件更新安装前进行安全性和兼容性测试；

	(3)在系统上线或发生重大变更时测试并安装最新的中间件版本或更新补丁； (4)在不影响业务系统正常运行情况下，对发现的中间件漏洞在确保安全的情况下进行修补； (5)中间件进行扫描未发现存在可造成高风险的漏洞。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
应用/数据库服务器-MySQL	鉴别数据、重要配置数据: (1)数据库系统在通信传输过程中对相关数据采取完整性保护措施； (2)数据库系统重要数据在传输过程中采取必要的完整性保护措施。
应用/数据库服务器-Tomcat	鉴别数据、重要配置数据: (1)中间件管理在通信传输过程中对相关数据采取完整性保护措施； (2)中间件对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a)应提供重要数据的本地数据备份与恢复功能；	
应用/数据库服务器-MySQL	(1)数据库系统定义了相关重要数据； (2)数据库系统定期完全依照备份策略,采用正确的配置进行本地备份； (3)系统的备份周期为：每天一次增量、每月一次全备； (4)数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
应用/数据库服务器-Tomcat	(1)系统定义了相关需要备份的中间件重要数据； (2)单位具备合理的重要数据的备份策略规范； (3)宿主系统定期完全依照备份策略，采用正确的配置进行本地备份； (4)中间件相关数据的备份周期合理：每天增量一次、每月全备一次； (5)中间件开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	
应用/数据库服务器-MySQL	(1)身份鉴别信息释放或清除机制正常且满足要求； (2)数据库系统不保存终端历史记录。
应用/数据库服务器-Tomcat	(1)宿主系统具有清除用户鉴别信息的功能； (2)经测试，宿主系统退出后无法访问先前中间件登录过的页面； (3)经测试，宿主系统关闭后无残留的中间件用户鉴别信息。
个人信息保护	
a)应仅采集和保存业务必需的用户个人信息；	
应用/数据库服务器-MySQL	(1)单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； (2)数据库存储的用户个人信息均为业务应用必需的环节。
b)应禁止未授权访问和非法使用用户个人信息。	
应用/数据库服务器-MySQL	(1)系统对所有涉及个人信息的环节均有明确的授权同意过程； (2)数据库具备控制措施禁止未授权访问用户个人信息表单； (3)数据库具备控制措施禁止非法使用用户个人信息表单。

3.4.4.2 主要安全问题汇总分析

安全通用要求

（1）数据库系统配置不合规的密码有效周期策略（如:应用/数据库服务器-MySQL）。上述问题的存在，使恶意用户能够较为容易的访问数据库等资源并实施恶意操作，对相关系统的正常运行造成影响，存在系统被未授权访问、操作的可能性。 中风险。

（2）未能提供数据库系统重要数据的异地定时数据备份功能（如：应用/数据库服务器-MySQL）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供，使企业的经济利益或声誉受到损害。 中风险。

3.4.5 业务应用系统/平台

3.4.5.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
档案管理系统	（1）系统对各登录模式均启用身份鉴别； （2）系统对登录管理的用户进行身份鉴别； （3）系统登录用户设置的身份标识具有唯一性； （4）系统不存在空口令用户； （5）设备配置合规的密码策略。
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
档案管理系统	（1）系统启用合规登录失败处理策略； （2）系统配置合规的操作超时退出措施。
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
档案管理系统	(1)应用系统的用户鉴别数据采用SHA-512算法在可控网络环境中传输; （2）系统配置合规的远程管理模式。
访问控制	
a) 应对登录的用户分配账户和权限；	
档案管理系统	（1）可提供系统权限分配表； （2）登录系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需分配不同的用户权限，不存在所有用户均属

	于管理级别、高权限的情况。
b) 应重命名或删除默认账户，修改默认账户的默认口令；	
档案管理系统	（1）系统禁用默认账户名； （2）系统账户口令设置合规。
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
档案管理系统	（1）系统不存在多余或过期账户； （2）系统管理员用户与账户之间一一对应。
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	
档案管理系统	（1）系统不存在多个管理级别高的特权用户； （2）系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
档案管理系统	（1）系统开启审计功能，审计进程正常； (2)系统的日志审计级别满足要求,审计覆盖所有用户操作审计和记录。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
档案管理系统	（1）系统日期、时间正常； （2）系统审计记录内容基本完整。
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
档案管理系统	（1）系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）系统针对日志、审计记录具备充足的存储容量； （3）审计记录及日志保存大于6个月。
入侵防范	
c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
档案管理系统	（1）系统自身设定有效的终端访问策略，通过访问措施进行管理地址的限制。
d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	
档案管理系统	（1）系统具备数据有效性检验功能； （2）系统的校验接口范围较全面。
e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
档案管理系统	（1）系统已根据需要不定期地对已发布的版本进行更新； （2）在系统上线或发生重大变更时测试并安装最新的版本或更新补丁； （3）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
档案管理系统	鉴别数据、重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； （2）系统对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
档案管理系统	（1）系统定义了相关需要备份重要数据；

	（2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	
档案管理系统	（1）系统具有清除用户鉴别信息的功能； （2）经测试，系统退出后无法访问先前登录过的页面； （3）经测试，系统关闭后无残留的用户鉴别信息。
个人信息保护	
a) 应仅采集和保存业务必需的用户个人信息；	
档案管理系统	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息； （3）系统采集的用户个人信息均为业务应用必需的环节。
b) 应禁止未授权访问和非法使用用户个人信息。	
档案管理系统	（1）系统不采集和保存任何形式的用户个人信息； （2）系统对所有涉及个人信息的环节均有明确的授权同意过程； （3）系统具备控制措施禁止未授权访问用户个人信息； （4）系统具备控制措施禁止非法使用用户个人信息。

3.4.5.2 主要安全问题汇总分析

安全通用要求

（1）未能提供应用软件系统重要数据的异地定时数据备份功能（如：档案管理系统）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

3.4.6 数据资源

3.4.6.1 已有安全控制措施汇总分析

安全通用要求

数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
重要业务数据 重要个人信息	（1）系统在通信传输过程中对相关数据采取完整性保护措施； （2）系统对重要数据在传输过程中采取必要的完整性保护措施。

数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
重要业务数据 重要个人信息	（1）系统定义了相关需要备份重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
个人信息保护	
a) 应仅采集和保存业务必需的用户个人信息；	
重要个人信息	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息； （3）系统采集的用户个人信息均为业务应用必需的环节。
b) 应禁止未授权访问和非法使用用户个人信息。	
重要个人信息	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； （2）系统具备控制措施禁止未授权访问用户个人信息； （3）系统具备控制措施禁止非法使用用户个人信息。

3.4.6.2 主要安全问题汇总分析

安全通用要求

重要业务数据

（1）未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要业务数据）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

重要个人信息

（1）未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要个人信息）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

3.4.7 其他系统或设备

3.4.7.1 已有安全控制措施汇总分析

安全通用要求

无其他系统或设备，不涉及相关测评

3.4.7.2 主要安全问题汇总分析

安全通用要求

无其他系统或设备，不涉及相关测评

3.5 安全管理中心

3.5.1 已有安全控制措施汇总分析

安全通用要求

系统管理	
a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；	
管理中心	（1）网络中部署运维安全管理系统实现集中的系统管理； （2）系统对登录用户进行身份鉴别； （3）系统用户标识具有唯一性； （4）系统可实现对账户的身份鉴别数据进行保密性和完整性保护； （5）系统管理操作模式具备控制措施； （6）系统具备相应的管理操作审计措施。
审计管理	
a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；	
管理中心	（1）网络中部署运维安全管理系统实现集中安全审计功能； （2）审计系统对审计管理员进行身份鉴别； （3）审计系统用户标识具有唯一性； （4）审计系统管理操作模式具备控制措施； （5）审计系统具备相应的管理操作审计措施。
b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	
管理中心	档案管理系统: （1）审计管理员定期对审计记录进行分析，对发现的安全可疑事件及时处理； （2）单位具有安全审计策略文件，规范审计记录的存储、管理和查询要求； （3）审计管理员按规范要求对审计记录进行管理。

	重要审计数据: 日志审计系统、运维安全管理系统: （1）设备在通信传输过程中对相关数据采取完整性保护措施; （2）设备对重要数据在传输过程中采取必要的完整性保护措施。

3.5.2 主要安全问题汇总分析

安全通用要求

（1）系统管理的资源、运行及配置管理不够全面（如：管理中心）。系统的资源和运行缺少统一的管理，将导致系统可能无法按规划实现基于资源配置、 系统加载、异常处理、及备份/恢复等的安全控制措施。 低风险。

3.6 安全管理制度

3.6.1 已有安全控制措施汇总分析

安全通用要求

安全策略	
应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。	
制度文件、执行/记录文件	（1）单位具有网络安全工作的总体方针和安全策略文件; （2）制度内容包括明确的单位安全工作要求; （3）管理文件详见《信息安全总体策略》。
管理制度	
a) 应对安全管理活动中的主要管理内容建立安全管理制度;	
制度文件、执行/记录文件	（1）单位有针对安全管理活动中的各类管理内容建立安全管理制度; （2）现有制度已覆盖管理活动的主要的方面; （3）制度详见：《信息安全总体策略》、《网络安全管理规范》、《组织安全结构和人员职责制度》、《人员管理制度》、《员工考核管理制度》。
b) 应对管理人员或操作人员执行的日常管理操作建立操作规程。	
制度文件、执行/记录文件	（1）单位针对相关业务日常管理的操作建立规程类管理制度; （2）现有制度已覆盖重要管理方面的系统维护手册和用户操作规程等; （3）管理文件详见《设备及系统软件配置和操作手册》。
制定和发布	
a) 应指定或授权专门的部门或人员负责安全管理制度的制定;	
制度文件、执行/记录文件	（1）单位针对安全管理制度的制定，指定教育信息与网络中心部主要负责;

	（2）在已制定的相关制度中可查阅到被授权制定管理制度的部门/人员信息； （3）管理文件详见《安全管理组织规范》。
b）安全管理制度应通过正式、有效的方式发布，并进行版本控制。	
制度文件、执行/记录文件	（1）单位针对制度的制定和发布要求，制定管理规范文件； （2）管理规范文件对文件制定及发布定义了规范要求； （3）安全管理制度的收发登记记录有效； （4）管理文件详见《制度制定、发布、评审和修订管理制度》、《收发文登记记录》。
评审和修订	
应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	
制度文件、执行/记录文件	（1）单位针对制度的合理性和适用性需进行论证和审定及修订的要求，制定管理规范文件； （2）管理规范文件对制度的评审及修订定义了规范要求； （3）单位具有安全管理制度的审定或论证的过程记录； （4）单位对做过修订的制度，具备有修订版本的安全管理过程记录； （5）管理文件详见《制度制定、发布、评审和修订管理制度》及 《安全管理制度评审记录》。

3.6.2 主要安全问题汇总分析

安全通用要求

档案管理系统针对安全管理制度层面的安全通用要求采取的安全措施比较完善，未发现不符合项。

3.7 安全管理机构

3.7.1 已有安全控制措施汇总分析

安全通用要求

岗位设置	
a）应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；	
制度文件、执行/记录文件	（1）单位已明确网络安全管理工作的职能部门，并明确了各岗位职责； （2）单位各部门职责文档已明确网络安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备网络安全岗位划分情况和岗位职责的详细说明；

	（4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。
b）应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。	
制度文件、执行/记录文件	（1）单位已明确系统安全管理工作的职能部门，并明确了各岗位职责； （2）单位各部门职责文档已明确系统安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备系统安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。
人员配备	
应配备一定数量的系统管理员、审计管理员和安全管理员等。	
制度文件、执行/记录文件	（1）单位针对人员配备要求，制定了管理制度； （2）单位按要求配备一定数量的重要岗位管理人员； （3）单位针对各岗位人员，制定并维护人员档案； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。
授权和审批	
a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；	
制度文件、执行/记录文件	（1）单位在制度中用文字描述或在流程图中明确，对关键活动进行审批； （2）单位对审批过程明确审批权限，对各项信息系统的重要操作与变更明确审批部门和批准人； （3）管理文件详见《授权和审批管理规定》。
b）应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。	
制度文件、执行/记录文件	（1）单位针对各项业务操作及变更等建立了审批程序规定； （2）单位针对系统变更、系统接入、物理范围等事项已明确按审批程序执行，记录有批准人签字； （3）管理文件详见《授权和审批管理规定》。
沟通和合作	
a）应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；	
制度文件、执行/记录文件	（1）单位针对机构内部管理人员之间、部门之间的沟通与合作，制定了管理制度； （2）单位的管理制度规范了合作和沟通的方式和周期； （3）单位有组织机构内部人员联系表； （4）单位有定期召开信息安全会议，保存有会议纪要； （5）管理文件详见《安全教育和培训制度》、《技能培训记录》《外部联系表》。
b）应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；	
制度文件、执行/记录文件	（1）单位针对加强与外部单位的合作与沟通，制定了管理制度规定； （2）单位能按要求与相关单位保持沟通合作，并提供相关单位联系方式和交流会议纪要； （3）管理文件详见《安全教育和培训制度》、《技能培训记录》、《外部联系表》。

c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	
制度文件、执行/记录文件	（1）单位建立了完善的对外联单位的联系列表； （2）管理文件详见《外部联系表》。

3.7.2 主要安全问题汇总分析

安全通用要求

（1）单位开展的检查工作不够完善（如：制度文件、执行/记录文件）。检查工作开展不仔细，可能对存在或潜在的安全风险不能被及时发现并进行处理。 低风险。

3.8 安全管理人员

3.8.1 已有安全控制措施汇总分析

安全通用要求

人员录用	
a) 应指定或授权专门的部门或人员负责人员录用；	
制度文件、执行/记录文件	（1）单位授权专门的部门负责人员录用工作，制定了管理制度规范； （2）由人力资源保障科负责人员录用工作； （3）管理文件详见《人员管理制度》。
b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查。	
制度文件、执行/记录文件	（1）单位针对人员录用过程，制定了明确要求，并形成人员安全管理制度； （2）单位现有管理制度明确说明录用人员应具备的条件； （3）单位按规定执行人员录用的相关审查过程； （4）管理文件详见《人员管理制度》、《人员入职考核记录》。
人员离岗	
应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。	
制度文件、执行/记录文件	（1）单位针对离岗人员权限终止及取回机构提供的各种设施的要求，制定了管理制度； （2）单位按规范开展对离岗人员的相关管理工作； （3）管理文件详见《人员管理度》、《人员离岗申请表》、《离场信息资料交接表》。
安全意识教育和培训	
应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。	
制度文件、执行/记录文件	（1）单位针对人员安全培训及责任和惩戒措施，制定了管理制度； （2）单位已开展安全意识教育及岗位技能培训。 （3）管理文件详见《安全教育和培训制度》。

外部人员访问管理	
a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；	
制度文件、执行/记录文件	（1）单位针对外部人员物理访问，制定了外部人员访问管理文档； （2）单位具备有效的外部人员访问重要区域的书面申请文档； （3）单位具备外部人员访问重要区域的登记记录； （4）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。
b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；	
制度文件、执行/记录文件	（1）单位针对外部接入受控网络访问系统，制定了管理制度； （2）单位具备外部人员接入受控网络前的申请审批流程； （3）单位具备外部人员接入及访问系统的书面申请文档； （4）单位具备外部人员接入及访问系统的登记记录； （5）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。

3.8.2 主要安全问题汇总分析

安全通用要求

（1）单位未完全按管理规范开展人员离场后的清理工作（如：制度文件、执行/记录文件）。人员离场后的清理工作开展不规范，可能导致遗留外部人员访问受控区域的记录，存在被二次非法利用，造成泄密。 低风险。

3.9 安全建设管理

3.9.1 已有安全控制措施汇总分析

安全通用要求

定级和备案	
a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；	
制度文件、执行/记录文件	（1）单位的被测系统于2022年4月已完成备案； （2）系统备案相关文档（定级报告）中明确等级划分方法和理由，SAG三个方面的级别描述清晰； （3）管理文件详见《定级备案》。
b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；	
制度文件、执行/记录文件	(1)单位针对系统定级结果的审批及评审工作等要求,制定了管理制度;

	（2）现有系统的定级已具备合理性和正确性审定； （3）管理文件详见《定级备案》。
c）应保证定级结果经过相关部门的批准；	
制度文件、执行/记录文件	（1）单位针对系统定级结果的上级批准要求，制定了管理制度； （2）现有系统的定级获得了相关部门的批准； （3）管理文件详见《定级备案》。
d）应将备案材料报主管部门和相应公安机关备案。	
制度文件、执行/记录文件	（1）单位对被测系统的等级备案表、定级报告等备案材料已经报相应公安机关备案； （2）单位具备公安机关出具的备案号； （3）管理文件详见《定级备案》。
产品采购和使用	
a）应确保网络安全产品采购和使用符合国家的有关规定；	
制度文件、执行/记录文件	（1）单位已建立安全产品管理的相关管理规定； （2）单位具备安全产品采购流程及相关实施文档； （3）被测系统使用的安全产品具备销售许可资质； （4）安全产品具均为国内产品； （5）管理文件详见《设备安全管理制度》。
b）应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。	
制度文件、执行/记录文件	（1）单位已建立密码产品与服务管理的相关管理制度； （2）系统未使用密码产品； （3）管理文件详见《设备安全管理制度》。
外包软件开发	
b）应保证开发单位提供软件设计文档和使用指南。	
制度文件、执行/记录文件	（1）单位制定软件开发项目验收要求，明确开发单位的提交材料； （2）开发单位提供软件日常维护和使用所需的文档； （3）管理文件详见《外包开发软件管理规定》、《设备及系统软件配置和操作手册》。
工程实施	
a）应指定或授权专门的部门或人员负责工程实施过程的管理；	
制度文件、执行/记录文件	（1）单位针对专门的部门负责工程实施过程的管理要求，制定管理度； （2）单位由专岗负责系统建设的工程实施，且按照实施方案的要求对进度和质量进行控制； （3）管理文件详见《工程实施管理制度》。
b）应制定安全工程实施方案控制工程实施过程。	
制度文件、执行/记录文件	（1）单位制定了详细的工程实施方案； （2）工程实施单位严格按照方案执行，并有过程记录； （3）管理文件详见《测试及验收方案》、《工程项目实施方案》。
系统交付	
a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；	
制度文件、执行/记录文件	（1）单位具备系统交付清单； （2）系统交付清单内容较详细； （3）单位的清点工作较合规； （4）管理文件详见《系统交付管理》、《资产清单》。

b) 应对负责运行维护的技术人员进行相应的技能培训；	
制度文件、执行/记录文件	(1) 单位已对负责系统运行维护的技术人员进行了技能培训； (2) 具备运维人员的培训记录； (3) 管理文件详见《系统交付管理》、《资产清单》、《系统交付清单》、《技能培训记录》。
c) 应提供建设过程文档和运行维护文档。	
制度文件、执行/记录文件	(1) 单位提供了系统建设过程中的文档； (2) 单位提供了指导用户进行系统运维的文档和系统培训手册； (3) 管理文件详见《系统交付管理》、《系统交付清单》、《设备及系统软件配置和操作手册》。
等级测评	
a) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；	
制度文件、执行/记录文件	(1) 单位针对系统等级测评要求，制定管理制度； (2) 系统按要求开展首次测评工作； (3) 管理文件详见《系统安全管理制度》。
b) 应在发生重大变更或级别发生变化时进行等级测评；	
制度文件、执行/记录文件	(1) 管理制度中已规定在系统发生变更时及时对系统进行等级测评； (2) 系统未发生过重大变更，系统等级未发生变化； (3) 管理文件详见《系统安全管理制度》。
c) 应确保测评机构的选择符合国家有关规定。	
制度文件、执行/记录文件	(1) 已选择在“全国等级保护测评机构推荐目录”中的测评单位进行等级测评； (2) 管理文件详见《系统安全管理制度》、《网络安全等级保护测评服务合同》。
服务供应商选择	
a) 应确保服务供应商的选择符合国家的有关规定；	
制度文件、执行/记录文件	(1) 单位在管理制度内明确提出安全服务供应商选择的要求； (2) 单位选择的安全服务商符合国家的有关规定，具备相应的安全服务资质； (3) 管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。
b) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。	
制度文件、执行/记录文件	(1) 单位的管理制度中已规定，需与安全服务商签订安全相关的协议并明确整个服务供应链各方需履行的网络安全相关义务； (2) 单位已按规定与选定的安全服务商签订合规的协议； (3) 管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。

3.9.2 主要安全问题汇总分析

安全通用要求

（1）单位未具备适用于被测系统的安全规划设计方案（如：制度文件、执行/记录文件）。规划设计需求不全面，可能导致安全方案设计不完善，信息系统存在安全缺陷。低风险。

（2）单位未具备完整的安全设计方案相关的文档。单位相关方案的设计的内容不够完善（如：制度文件、执行/记录文件）。相关合规的规划配套文件缺失，可能导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。 中风险。

（3）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定。单位未对相关论证过程及内容进行完整的记录（如：制度文件、执行/记录文件）。未开展规范的审批过程，可能存在安全整体规划缺乏合理性和可行性，导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。 低风险。

（4）单位未在软件开发过程中对所有软件安全性进行测试。单位未在软件安装之前按要求对所有软件开展恶意代码检测（如：制度文件、执行/记录文件）。软件交付前恶意代码检测不规范，可能在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。 低风险。

（5）单位未完全根据测试验收方案组织相关部门和人员开展验收工作（如：制度文件、执行/记录文件）。可能由于验收测试不严谨，造成测试过程缺乏计划性及操作性，无法保证经过测试验收的系统达到既定的安全性等目标。 低风险。

(6)针对系统上线前的安全性测试工作存在问题(如:制度文件、执行/记录文件)。未按规定开展上线前测试，安全隐患可能在系统上线运行前未被发现并作出相应处理。低风险。

3.10 安全运维管理

3.10.1 已有安全控制措施汇总分析

安全通用要求

环境管理	
a) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；	
制度文件、执行/记录文件	（1）单位建立机房安全方面的管理制度，对有关运维方面的管理作出规定； （2）单位具备完整的机房出入登记记录； （3）单位具备完整的机房基础设施的维护记录； （4）管理文件详见《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。
b) 应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；	
制度文件、执行/记录文件	（1）单位建立机房安全方面的管理制度； （2）单位现有机房管理记录与制度相符； （3）制度详见：《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。
c) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	
制度文件、执行/记录文件	（1）单位机房安全管理制度已明确来访人员的接待区域的要求； （2）单位按规范要求开展人员来访接待； （3）单位办公环境未发现有随意放置含有敏感信息介质的情况； （4）制度详见：《机房安全管理制度》、《物理安全管理规范》、《办公环境保密管理》。
资产管理	
应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。	
制度文件、执行/记录文件	（1）单位已建立有效的资产清单； （2）单位现有资产清单内容较全面； （3）制度详见：《设备安全管理制度》、《资产清单》。
介质管理	
a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；	
制度文件、执行/记录文件	（1）介质按管理要求放置于受控的环境中（如：机房）； （2）介质管理具备较全面的记录； （3）制度详见：《设备安全管理制度》、《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。
b) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。	
制度文件、执行/记录文件	（1）介质管理制度中对介质安全传输有明确规定； （2）存储重要信息的介质在物理传输过程，具备严格的环节控制，无重大环节疏漏； （3）对介质的归档和查询均具备记录；

	（4）制度详见：《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。
设备维护管理	
a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	
制度文件、执行/记录文件	（1）单位人员岗位职责相关文档已明确设备维护管理的责任部门； （2）单位对各类设施、设备进行定期维护； （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。
b）应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。	
制度文件、执行/记录文件	（1）单位建立了配套设施、软硬件维护管理方面的管理制度； （2）单位开展相关工作与制度相符，且保留记录； （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。
网络和系统安全管理	
a）应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；	
制度文件、执行/记录文件	（1）单位建立系统安全管理文档，对系统管理员的管理制定了要求； （2）单位对各类关键角色建立了相应的工作职责文档； （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。
b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	
制度文件、执行/记录文件	（1）单位制定管理制度，对系统账号进行管理； （2）单位按管理规范开展账号管理工作； （3）账户管理记录内容较完整； （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。
c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	
制度文件、执行/记录文件	（1）单位建立了网络和系统安全管理制度； （2）网络和系统安全管理制度内容较全面； （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。
d）应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；	
制度文件、执行/记录文件	（1）单位对重要设备、系统的配置和操作建立配置手册； （2）现有操作配置手册已明确操作步骤、参数配置； （3）制度详见：《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。
e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。	
制度文件、执行/记录文件	（1）单位制定日常运维管理的相关制度规范； （2）单位按制度规范开展日常运维管理工作； （3）单位具备合规的运维记录； （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》、《设备及系统软件配置和操作手册》、《软硬件日

	常维护管理规程》。
恶意代码防范管理	
a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	
制度文件、执行/记录文件	（1）单位制定恶意代码防范管理制度，明确对外来计算机或存储设备接入系统前进行恶意代码检查； （2）单位按外来计算机接入恶意代码检查规范开展工作； （3）单位制定培训管理制度，明确需通过培训提升员工的防恶意代码意识； （4）单位按培训管理要求开展工作； （5）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申请表》、《信息管理系统漏洞检查表》。
b) 应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；	
制度文件、执行/记录文件	（1）建立恶意代码防范管理文档； （2）管理制度中覆盖防恶意代码软件的授权使用、恶意代码库升级、定期查杀等内容； （3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》。
配置管理	
应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。	
制度文件、执行/记录文件	（1）单位制定了基本配置信息管理的制度要求； （2）管理文件详见：《主机安全管理规范》、《网络安全管理规范》、《应用安全管理规范》、《网络配置信息》。
变更管理	
应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。	
制度文件、执行/记录文件	（1）单位建立了关于系统变更管理的制度文件； （2）现有变更管理制度覆盖了变更管理的各方面要求； （3）制度详见：《变更控制管理制度》、《通用变更记录表》。
备份与恢复管理	
a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；	
制度文件、执行/记录文件	（1）单位根据业务重要程度，制定了需要定期备份的重要业务信息列表或清单。清单内需要定期备份的重要数据已经过用户方确认； （2）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。
b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等；	
制度文件、执行/记录文件	（1）单位建立了备份与恢复管理相关的安全管理制度； （2）备份与恢复管理的相关要求比较明确； （3）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。
c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	
制度文件、执行/记录文件	（1）单位现有管理制度，明确了数据备份策略和数据恢复策略，以及备份程序和恢复程序； （2）单位可按策略要求实现重要数据的定期备份与恢复性测试；

	(3)单位现有的备份的数据均经过恢复性测试,可确保备份的数据可用; (4) 制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。
安全事件处置	
a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件;	
制度文件、执行/记录文件	(1)单位已在安全培训及宣传过程中告知用户在发现安全弱点和可疑事件时及时向安全管理部门报告; (2)单位在系统运维过程中对发现的安全弱点和可疑事件均编制了对应的报告或相关文档; (3) 单位现有安全弱点和可疑事件报告文档内容较详实; (4) 制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。
b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等;	
制度文件、执行/记录文件	(1) 单位制定了安全事件报告和处置管理制度; (2) 现有安全事件管理制度内容较完整; (3) 制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。
c) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。	
制度文件、执行/记录文件	(1) 单位具备对安全事件的分析、处理、总结、防范等的报告／过程文档; (2) 单位提供的安全事件报告和响应处置记录内容较完整; (3) 制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。
应急预案管理	
a) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容;	
制度文件、执行/记录文件	(1) 单位制定重要事件的应急预案; (2) 单位现有应急预案涉及的类型范围较全面; (3) 单位现有应急预案的内容较完整; (4) 制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。
b) 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。	
制度文件、执行/记录文件	(1) 单位定期对相关人员进行应急预案培训; (2) 单位根据不同的应急预案，按要求进行应急演练; (3) 单位具备近期应急预案工作开展的相关记录; (4) 单位提供的应急预案培训记录比较完整; (5) 单位提供的应急预案演练记录比较完整; (6) 经检查单位目前一旦出现应急事件，可参照预案合理有序的进行应急事件处置过程; (7) 制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。

3.10.2 主要安全问题汇总分析

安全通用要求

（1）单位未严格按规范开展漏洞及安全隐患检测工作（如：制度文件、执行/记录文件）。漏洞检测、修补工作不到位，可能存在未授权人员利用漏洞攻击信息系统的风险。 低风险。

（2）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作（如：制度文件、执行/记录文件）。可能导致系统恶意代码检测管理不到位，存在信息系统感染恶意代码，从而导致严重的信息安全风险。 低风险。

（3）单位不了解现有密码相关的国家标准和行业标准。单位缺乏密码管理要求的制度文档（如：制度文件、执行/记录文件）。密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不到位，存在违反国家政策的风险。 中风险。

3.11 其他安全要求指标

3.11.1 已有安全控制措施汇总分析

本次测评未涉及其他安全要求指标。

3.11.2 主要安全问题汇总分析

本次测评未涉及其他安全要求指标。

3.12 验证测试

验证测试包括漏洞扫描，渗透测试等，验证测试发现的安全问题对应到相应的测评项的结果记录中。详细验证测试报告见报告附录。

3.12.1 漏洞扫描

3.12.1.1 漏洞扫描结果统计

本次测评主要使用了[绿盟远程安全评估系统]对系统的设备进行了安全扫描，其所涉及的系统版本为：[V6.0R04F01SP06]，规则库版本为：[V6.0R02F01.2900]。扫描结果如下：

经分析统计，共发现各接入点存在1类漏洞，其中0类危险程度为高的漏洞，0类危害程度为中的漏洞，1类危害程度为低的漏洞。

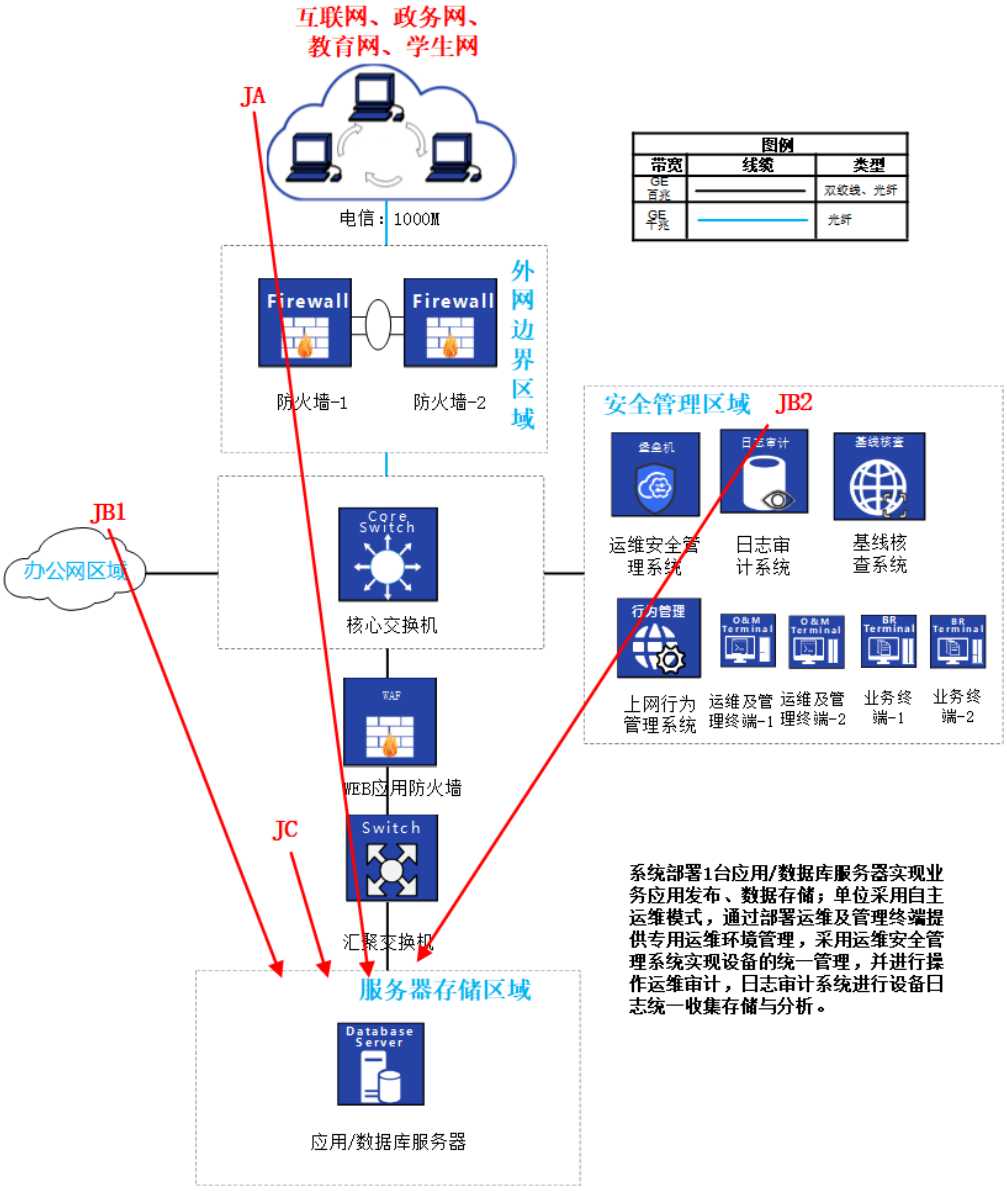


图 3-1 漏洞扫描工具接入测试示意图

接入点JA：在防火墙外侧接入，开展扫描/渗透主要目的是，探测对外服务功能区上各服务器、应用系统对外部网络边界暴露的安全漏洞情况，并根据漏洞扫描的结果接入渗透测试工具集，试图利用服务器、应用的安全漏洞入侵网络的行为。

接入点JB：在办公网区域VLAN段、安全管理区域VLAN段接入，开展扫描/渗透主要目的是，模拟外联单位/内部恶意用户发现操作系统、数据库、Web应用、第三方产

品等安全漏洞的过程，并尝试利用以上漏洞实施诸如获取系统控制权（GetShell）、获得大量敏感信息（DragLibrary）等模拟攻击行为。

接入点JC：在系统所在VLAN的交换机接入，开展扫描/渗透主要目的是，直接测试对服务功能区上各服务器在最小化防御的基础上，对网络暴露的安全漏洞情况。

（1）接入点A漏洞扫描结果统计

根据在接入点A对14台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-1 接入点 A 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	0	0	0	0
2	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	0	0	0	0
3	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	0	0	0	0
4	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	0	0	0	0
5	172.16.1.14/上网行为管理系统	(安全设备)深信服 AC12.0.26	0	0	0	0
6	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	0	0	0	0
7	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	0	0	0	0
8	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	0	0	0	0
9	192.168.33.11/业务终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
10	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
11	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
12	192.168.33.10/业务终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
13	10.2.4.11/应用/数据库服务器	(服务器存储设备)Windows Server 2008 R2	0	0	0	0
14	https://arch.mmpt.edu.cn/档案管理系统	(业务应用软件平台) V6.0	0	0	0	0

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
安全漏洞数量小计			0	0	0	0

（2）接入点B漏洞扫描结果统计

根据在接入点B对14台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-2 接入点 B 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	1	0	0	1
2	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	1	0	0	1
3	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	1	0	0	1
4	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	2	0	0	2
5	172.16.1.14/上网行为管理系统	(安全设备)深信服AC12.0.26	1	0	0	1
6	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	1	0	0	1
7	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	1	0	0	1
8	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	1	0	0	1
9	192.168.33.11/业务终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
10	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
11	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
12	192.168.33.10/业务终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
13	10.2.4.11/应用/数据库服务器	(服务器存储设备)Windows Server 2008 R2	1	0	0	1
14	https://arch.mmpt.edu.cn/档案管理系统	(业务应用软件平台) V6.0	0	0	0	0
安全漏洞数量小计			10	0	0	10

（3）接入点C漏洞扫描结果统计

根据在接入点C对14台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-3 接入点 C 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	1	0	0	1
2	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	1	0	0	1
3	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	1	0	0	1
4	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	2	0	0	2
5	172.16.1.14/上网行为管理系统	(安全设备)深信服 AC12.0.26	1	0	0	1
6	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	1	0	0	1
7	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	1	0	0	1
8	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	1	0	0	1
9	192.168.33.11/业务终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
10	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
11	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
12	192.168.33.10/业务终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
13	10.2.4.11/应用/数据库服务器	(服务器存储设备)Windows Server 2008 R2	1	0	0	1
14	https://arch.mmpt.edu.cn/档案管理系统	(业务应用软件平台) V6.0	0	0	0	0
安全漏洞数量小计			10	0	0	10

3.12.1.2 漏洞扫描问题描述

通过对漏洞扫描结果进行分析,档案管理系统存在的主要安全漏洞汇总如下表所示

表 3-4 主要安全漏洞汇总表

序号	安全漏洞名称	关联资产/域名	严重程度
1	允许Traceroute探测 此类漏洞涉及服务器存储设备、安全设备、网络设备。	10.2.4.11/应用/数据库服务器 10.2.1.4/运维安全管理系统 10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/上网行为管理系统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/汇聚交换机 172.16.1.2/核心交换机	低
2	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161) 此类漏洞涉及网络设备。	172.16.1.2/核心交换机	低

3.12.2 渗透测试

经分析统计，共发现各接入点存在1类漏洞，其中0类危险程度为高的漏洞，0类危害程度为中的漏洞，1类危害程度为低的漏洞。

3.12.2.1 渗透测试过程说明

方案制定：

在得到委托单位的书面授权许可后，才进行渗透测试的实施。并且将实施范围、方法、时间、人员等具体的方案委托单位进行交流，并得到委托单位的认同。在测试实施之前，会做到让委托单位对渗透测试过程和风险的知晓，使随后的正式测试流程都在委托单位的管控下。

信息收集：

此阶段中，渗透测试人员对目标信息系统进行必要的信息收集，如操作系统类型、开放的端口和服务、中间件信息、后台数据库类型、web开发语言等，即收集有利于漏洞挖掘的相关信息，为渗透测试做准备。

漏洞挖掘方法：

此阶段中，渗透测试人员对目标信息系统开始进行渗透测试，利用已知信息和现有条件及技术进行漏洞挖掘，尽可能发现目标信息系统中存在的所有安全风险，并进行记录。

漏洞利用：

此阶段中，渗透测试人员对目标信息系统对上一阶段漏洞挖掘中发现的漏洞进行必要的利用以证明其危害性，再对渗透测试过程所产生的测试数据进行清除。

输出报告：

此阶段中，渗透测试人员把渗透测试记录、截图等相关信息进行整理，然后撰写渗透测试报告，最终提交给委托单位。

漏洞修复：

此阶段中，委托单位依据收到的渗透测试报告对其中所提出的漏洞进行整改，可参考报告中所提出的修复建议，整改完成后联系本单位相关人员准备回归测试。

回归测试：

此阶段中，渗透测试人员对整改后的目标信息系统进行复测，以确定报告中提出的漏洞是否已被修复，若已被修复，则进入下一阶段；否则，返回上一阶段。

测试工具：

序号	工具	工具用途
1	Burpsuite Pro	用于攻击Web应用程序的集成软件
2	Sqlmap	开源的自动化SQL注入工具

序号	工具	工具用途
3	Nmap	开源的网络发现和安全审计工具
4	OWASP ZAP	自动化Web应用漏洞扫描工具
5	其他测试工具	根据信息系统的类别选择不同的工具（如自写脚本、目录扫描器、木马扫描器、其它开源工具等）

3.12.2.2 渗透测试问题描述

通过渗透测试发现，档案管理系统存在的安全问题汇总如下表所示。

表 3-5 渗透测试结果汇总表

序号	安全问题	关联资产/域名	严重程度
1	缺少“X-Content-Type-Options”响应头 此类漏洞涉及业务应用软件平台。	https://arch.mmpt.edu.cn/档案管理系统	低

3.13 单项测评小结

3.13.1 控制点符合情况汇总

根据单项测评结果汇总控制点符合情况如下表所示。（表格以不同颜色对测评结果进行区分，不符合的安全控制点采用红色标识，部分符合的采用黄色标识，不适用的采用蓝色标识且不做勾选。）

表 3-6 控制点符合情况汇总表

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
1	安全通用要求	安全物理环境	物理位置选择	√		
2			物理访问控制		√	
3			防盗窃和防破坏	√		
4			防雷击	√		
5			防火		√	
6			防水和防潮	√		

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
7			防静电			√
8			温湿度控制	√		
9			电力供应	√		
10			电磁防护	√		
11	安全通用要求	安全通信网络	网络架构		√	
12			通信传输	√		
13			可信验证			√
14	安全通用要求	安全区域边界	边界防护	√		
15			访问控制	√		
16			入侵防范		√	
17			恶意代码和垃圾邮件防范		√	
18			安全审计	√		
19			可信验证			√
20	安全通用要求	安全计算环境	身份鉴别		√	
21			访问控制	√		
22			安全审计	√		
23			入侵防范	√		
24			恶意代码防范	√		
25			可信验证			√
26			数据完整性	√		

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
27			数据备份恢复		√	
28			剩余信息保护	√		
29			个人信息保护	√		
30	安全通用要求	安全管理中心	系统管理		√	
31			审计管理	√		
32	安全通用要求	安全管理制度	安全策略	√		
33			管理制度	√		
34			制定和发布	√		
35			评审和修订	√		
36	安全通用要求	安全管理机构	岗位设置	√		
37			人员配备	√		
38			授权和审批	√		
39			沟通和合作	√		
40			审核和检查		√	
41	安全通用要求	安全管理人员	人员录用	√		
42			人员离岗	√		
43			安全意识教育和培训	√		
44			外部人员访问管理		√	
45	安全通用要求	安全建设管理	定级和备案	√		
46			安全方案设计			√

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
47			产品采购和使用	√		
48			自行软件开发			
49			外包软件开发		√	
50			工程实施	√		
51			测试验收		√	
52			系统交付	√		
53			等级测评	√		
54			服务供应商选择	√		
55	安全通用要求	安全运维管理	环境管理	√		
56			资产管理	√		
57			介质管理	√		
58			设备维护管理	√		
59			漏洞和风险管理			√
60			网络和系统安全管理	√		
61			恶意代码防范管理		√	
62			配置管理	√		
63			密码管理			√
64			变更管理	√		
65			备份与恢复管理	√		
66			安全事件处置	√		

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
67			应急预案管理	√		
68			外包运维管理			
安全通用要求控制点符合情况数量统计				46	13	7
控制点符合情况数量统计				46	13	7

3.13.2 安全问题汇总

针对单项测评结果中存在的部分符合和不符合项进行汇总，形成了安全问题如下表所示。

表 3-7 安全问题汇总表

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T1	（1）机房出入口未配置电子门禁系统。	信息化机房	安全通用要求	安全物理环境	物理访问控制	机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。
T2	（1）机房建设未完全采用符合耐火等级的建筑材料； （2）机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级。	信息化机房	安全通用要求	安全物理环境	防火	b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。
T3	（1）机房内缺乏防静电措施（如防静电地板或铺设防静电地毯）。	信息化机房	安全通用要求	安全物理环境	防静电	应采用防静电地板或地面并采用必要的接地防静电措施。
T4	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	安全通用要求	安全通信网络	网络架构	a）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
T5	（1）缺乏对通信设备可信验证方面的安全设计要求； （2）现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况。	安全通信网络	安全通用要求	安全通信网络	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
						形成审计记录送至安全管理中心。
T6	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	安全通用要求	安全区域边界	入侵防范	应在关键网络节点处监视网络攻击行为。
T7	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	安全通用要求	安全区域边界	恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。
T8	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	办公网区域 外网边界区域 安全管理区域 服务器存储区域	安全通用要求	安全区域边界	可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T9	（1）数据库系统配置不合规的密码有效周期策略。	应用/数据库服务器-MySQL	安全通用要求	安全计算环境	身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
T10	（1）设备不具备相关可信验证的技术措施。	WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2	安全通用要求	安全计算环境	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T11	（1）缺乏对计算设备可信验证方面的安全设计要求；	业务终端-1 业务终端-2 应用/数据库	安全通用要求	安全计算环境	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
	（2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。	服务器 运维及管理终端-1 运维及管理终端-2				和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T12	（1）未能提供数据库系统重要数据的异地定时数据备份功能。	应用/数据库服务器-MySQL	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T13	（1）未能提供中间件重要数据的异地定时数据备份功能。	应用/数据库服务器-Tomcat	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T14	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	档案管理系统	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T15	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	重要业务数据 重要个人信息	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T16	（1）系统管理的资源、运行及配置管理不够全面。	管理中心	安全通用要求	安全管理中心	系统管理	b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
T17	（1）单位开展的检查工作不够完善。	制度文件、执行/记录文件	安全通用要求	安全管理机构	审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。
T18	（1）单位未完全按管理规范开展人员离场后的清理工作。	制度文件、执行/记录文件	安全通用要求	安全管理人员	外部人员访问管理	c）外部人员离场后应及时清除其所有的访问权限。
T19	（1）单位未具备适用于被测系统的安全规划设计方案。	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T20	（1）单位未具备完整的安全设计方案相关的文档； （2）单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	b）应根据保护对象的安全保护等级进行安全方案设计；
T21	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； （2）单位未对相关论证过程及内容进行完整的记录。	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	c）应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。
T22	（1）单位未在软件开发过程中对所有软件安全性进行测试； （2）单位未在软件安装之前按要求对所有软件开展恶意代码检测。	制度文件、执行/记录文件	安全通用要求	安全建设管理	外包软件开发	a）应在软件交付前检测其中可能存在的恶意代码；
T23	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	安全通用要求	安全建设管理	测试验收	a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；
T24	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	安全通用要求	安全建设管理	测试验收	b）应进行上线前的安全性测试，并出具安全测试报告。
T25	（1）单位未严格按规范开展漏洞及安全隐患检测工作。	制度文件、执行/记录文件	安全通用要求	安全运维管理	漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。
T26	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	安全通用要求	安全运维管理	恶意代码防范管理	c）应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。
T27	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	制度文件、执行/记录文件	安全通用要求	安全运维管理	密码管理	a）应遵循密码相关国家标准和行业标准；

4 整体测评

从安全控制间、区域间和验证测试等方面对单元测评的结果进行验证、分析和整体评价。

具体内容参见《GB/T 28448-2019信息安全技术 网络安全等级保护测评要求》。

4.1 安全控制点间安全测评

安全控制间的安全测评主要考虑同一区域内、同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用。安全功能上的增强和补充可以使两个不同强度、不同等级的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。

4.1.1 安全建设管理

4.1.1.1 安全通用要求

（T23）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。

单位未具备适用于被测系统的安全规划设计方案。安全方案设计不完善，导致规划设计需求不全面，信息系统存在安全缺陷。可升高单位未完全根据测试验收方案组织相关部门和人员开展验收工作的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

（T24）针对系统上线前的安全性测试工作存在问题。

单位未在软件交付之前按要求对所有软件开展恶意代码检测，导致在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。可升高针对系统上线前的安全性测试工作存在问题的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

4.1.2 安全运维管理

4.1.2.1 安全通用要求

（T26）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。

单位未严格按规范开展漏洞及安全隐患检测工作，漏洞检测工作不到位，导致存在未授权人员利用漏洞攻击信息系统的风险。可升高单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

4.2 区域间安全测评

区域间的安全测评主要考虑互连互通（包括物理上和逻辑上的互连互通等）的不同区域之间存在的安全功能增强、补充和削弱等关联作用，特别是有数据交换的两个不同区域。

4.2.1 安全物理环境

4.2.1.1 安全通用要求

（T1）机房出入口未配置电子门禁系统。

机房所在位置处于内部受控区域，非授权人员无法随意通过现有控制措施（如机械锁）进出机房，且具备相对完善的机房出入管理要求（具备《机房安全管理制度》），并实际执行措施效果良好（具备《机房出入登记表》），可降低机房出入口访问控制措施缺失的问题严重程度（如信息化机房）。根据整体测评分析，问题严重程度变化为降低。

4.2.2 安全通信网络

4.2.2.1 安全通用要求

（T4）关键的应用服务和数据库服务网段未独立进行子网划分的情况。

单位有完整的IP地址规范，对IP地址的使用、回收均有记录《资产清单》，且系统具备相对完善的设备自身访问控制策略管理要求（具备《网络安全管理规范》、《设备及系统软件配置和操作手册》），措施效果良好，有助于部分补充未划分子网的安全功能不足（如安全通信网络）。根据整体测评分析，问题严重程度变化为降低。

4.2.3 安全区域边界

4.2.3.1 安全通用要求

（T6）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。

网络环境划分了相应的安全区域，区域间具备有效的访问控制措施，区域内各主机设备部署深信服EDR单机版，策略库、规则库更新及时，能够对攻击行为进行检测、阻断或限制，实际措施效果良好，且系统具备相对完善的策略库、规则库更新/校准管理要求，管理措施效果良好且及时检查更新有效性（具备《漏洞检测报告》、《主机安全管理规范》），可降低外部网络攻击防御措施缺失的问题严重程度（如办公网区域、安全管理区域）。根据整体测评分析，问题严重程度变化为降低。

（T7）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。

系统部署于可控的网络环境内（具备有效的访问控制、入侵防护措施）限制相关主机对象访问非受控网络，操作系统层面配置防御策略（具备本地防火墙策略、核心交换机地址限制策略、部署深信服EDR单机版），恶意代码入侵的可能性相对较低，可降低恶意代码防范措施缺失的问题严重程度（如办公网区域、安全管理区域）。根据整体测评分析，问题严重程度变化为降低。

4.2.4 安全计算环境

4.2.4.1 安全通用要求

（T9）数据库系统配置不合规的密码有效周期策略。

单位管理制度中明确规定密码长度、复杂度及有效期要求《应用安全管理规范》、《设备及系统软件配置和操作手册》，且有按照管理规定对设备密码定期更换，减轻设备存在弱口令或相同口令的风险,综合考虑风险后可降低数据库系统配置不合规的密码长度及复杂度策略的问题严重程度（如应用/数据库服务器-MySQL）。根据整体测评分析，问题严重程度变化为降低。

4.3 整体测评结果汇总

经整体测评后安全问题严重程度变化情况如下表所示

表 4-1 整体测评结果汇总表

问题编号	安全问题描述	测评对象	整体测评描述	严重程度变化
T1	（1）机房出入口未配置电子门禁系统。	信息化机房	（1）机房所在位置处于内部受控区域，非授权人员无法随意通过现有控制措施（如机械锁）进出机房，且具备相对完善的机房出入管理要求（具备《机房安全管理制度》），并实际执行措施效果良好（具备《机房出入登记表》），可降低机房出入口访问控制措施缺失的问题严重程度。	□升高 ☑降低
T4	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	（1）单位有完整的IP地址规范，对IP地址的使用、回收均有记录《资产清单》，且系统具备相对完善的设备自身访问控制策略管理要求（具备《网络安全管理规范》、《设备及系统软件配置和操作手册》），措施效果良好，有助于部分补充未划分子网的安全功能不足。	□升高 ☑降低
T6	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略,无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	（1）网络环境划分了相应的安全区域，区域间具备有效的访问控制措施，区域内各主机设备部署深信服EDR单机版，策略库、规则库更新及时，能够对攻击行为进行检测、阻断或限制，实际措施效果良好，	□升高 ☑降低

问题编号	安全问题描述	测评对象	整体测评描述	严重程度变化
			且系统具备相对完善的策略库、规则库更新/校准管理要求，管理措施效果良好且及时检查更新有效性（具备《漏洞检测报告》、《主机安全管理规范》），可降低外部网络攻击防御措施缺失的问题严重程度。	
T7	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域安全管理区域	（1）系统部署于可控的网络环境内（具备有效的访问控制、入侵防护措施）限制相关主机对象访问非受控网络，操作系统层面配置防御策略（具备本地防火墙策略、核心交换机地址限制策略、部署深信服EDR单机版），恶意代码入侵的可能性相对较低，可降低恶意代码防范措施缺失的问题严重程度。	□升高 ☑降低
T9	（1）数据库系统配置不合规的密码有效周期策略。	应用/数据库服务器-MySQL	（1）单位管理制度中明确规定密码长度、复杂度及有效期要求《应用安全管理规范》、《设备及系统软件配置和操作手册》，且有按照管理规定对设备密码定期更换，减轻设备存在弱口令或相同口令的风险，综合考虑风险后可降低数据库系统配置不合规的密码长度及复杂度策略的问题严重程度。	□升高 ☑降低
T23	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	（1）单位未具备适用于被测系统的安全规划设计方案。安全方案设计不完善，导致规划设计需求不全面，信息系统存在安全缺陷。可升高单位未完全根据测试验收方案组织相关部门和人员开展验收工作的问题严重程度。	☑升高 □降低
T24	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	（1）单位未在软件交付之前按要求对所有软件开展恶意代码检测，导致在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。可升高针对系统上线前的安全性测试工作存在问题的问题严重程度。	☑升高 □降低
T26	（1）单位未严格按规范要求，针对防范恶意代码攻击的技	制度文件、执行/记录文件	（1）单位未严格按规范开展漏洞及安全隐患检测工作，漏洞检测工作	☑升高

问题编号	安全问题描述	测评对象	整体测评描述	严重程度变化
	术措施的有效性验证,开展工作。		不到位，导致存在未授权人员利用漏洞攻击信息系统的风险。可升高单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作的问题严重程度。	□降低

5 安全问题风险分析

针对等级测评结果中存在的所有安全问题,结合关联资产和威胁分别分析安全问题可能产生的危害结果,找出可能对系统、单位、社会及国家造成的最大安全危害(损失),并根据最大安全危害(损失)的严重程度进一步确定安全问题的风险等级,结果为“高”、“中”或“低”。最大安全危害（损失）结果应结合安全问题所影响业务的重要程度、相关系统组件的重要程度、安全问题严重程度以及安全事件影响范围等进行综合分析。

表 5-1 安全问题风险分析

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
1	安全物理环境	（1）机房出入口未配置电子门禁系统。	信息化机房	物理攻击	（1）上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域，可能对系统的平稳运行造成影响。	中风险
2	安全物理环境	（1）机房建设未完全采用符合耐火等级的建筑材料; （2）机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级。	信息化机房	物理环境影响	（1）存在发生火情时助燃火灾的风险。	低风险
3	安全物理环境	（1）机房内缺乏防静电措施(如防静电地板或铺设防静电地毯 ）。	信息化机房	软硬件故障	（1）存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。	中风险
4	安全通信网络	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	恶意攻击	（1）上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变	中风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
					得更为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。	
5	安全通信网络	（1）缺乏对通信设备可信验证方面的安全设计要求； （2）现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况。	安全通信网络	恶意攻击	（1）缺乏对系统可执行程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致计算资源被干扰和破坏造成损失。	低风险
6	安全区域边界	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	恶意攻击	（1）存在不能及时发现内部主机作为攻击跳板，或网络攻击行为而造成系统损坏/网络资源浪费的风险。	中风险
7	安全区域边界	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	恶意攻击	（1）无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。	中风险
8	安全区域边界	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	办公网区域 外网边界区域 安全管理区域 服务器存储区域	恶意攻击	（1）缺乏对边界设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险
9	安全计算环境	（1）数据库系统配置不合规的密码有效周期策略。	应用/数据库服务器-MySQL	恶意攻击	（1）上述问题的存在，使恶意用户能够较为容易的访问数据库等资源并实施恶意操作，对相关系统的正常运行造成影响，存在系统被未授权访问、操作的可能性。	中风险
10	安全计算环境	（1）设备不具备相关可信验证的技术措施。	WEB应用防火墙 上网行为管理系统	恶意攻击	（1）缺乏对计算设备的相关程序的可信性验证，无	低风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
			基线核查系统 日志审计系统 核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2		法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	
11	安全计算环境	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。	业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	恶意攻击	（1）缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险
12	安全计算环境	（1）未能提供数据库系统重要数据的异地定时数据备份功能。	应用/数据库服务器-MySQL	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供，使企业的经济利益或声誉受到损害。	中风险
13	安全计算环境	（1）未能提供中间件重要数据的异地定时数据备份功能。	应用/数据库服务器-Tomcat	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。	中风险
14	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	档案管理系统	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。	中风险
15	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	重要业务数据 重要个人信息	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。	中风险
16	安全管理中心	（1）系统管理的资源、运行及配置管理不够全面。	管理中心	恶意攻击	（1）系统的资源和运行缺少统一的管理，将导致系统可能无法按规划实现基于资源配置、 系统加载、异常处理、及备份/恢复等的安全控制措施。	低风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
17	安全管理机构	（1）单位开展的检查工作不够完善。	制度文件、执行/记录文件	管理不到位	（1）检查工作开展不仔细，可能对存在或潜在的安全风险不能被及时发现并进行处理。	低风险
18	安全管理人员	（1）单位未完全按管理规范开展人员离场后的清理工作。	制度文件、执行/记录文件	管理不到位	（1）人员离场后的清理工作开展不规范，可能导致遗留外部人员访问受控区域的记录，存在被二次非法利用，造成泄密。	低风险
19	安全建设管理	（1）单位未具备适用于被测系统的安全规划设计方案。	制度文件、执行/记录文件	管理不到位	（1）规划设计需求不全面，可能导致安全方案设计不完善，信息系统存在安全缺陷。	低风险
20	安全建设管理	（1）单位未具备完整的安全设计方案相关的文档； （2）单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	管理不到位	（1）相关合规的规划配套文件缺失，可能导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。	中风险
21	安全建设管理	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； （2）单位未对相关论证过程及内容进行完整的记录。	制度文件、执行/记录文件	管理不到位	（1）未开展规范的审批过程，可能存在安全整体规划缺乏合理性和可行性，导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。	低风险
22	安全建设管理	（1）单位未在软件开发过程中对所有软件安全性进行测试； （2）单位未在软件安装之前按要求对所有软件开展恶意代码检测。	制度文件、执行/记录文件	管理不到位	（1）软件交付前恶意代码检测不规范，可能在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。	低风险
23	安全建设管理	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	管理不到位	（1）可能由于验收测试不严谨，造成测试过程缺乏计划性及操作性，无法保证经过测试验收的系统达到既定的安全性等目标。	低风险
24	安全建设管理	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	管理不到位	（1）未按规定开展上线前测试，安全隐患可能在系统上线运行前未被发现并作出相应处理。	低风险
25	安全运维	（1）单位未严格按规范	制度文件、执行/	管理	（1）漏洞检测、修补工作	低风

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
	管理	开展漏洞及安全隐患检测工作。	记录文件	不到位	不到位，可能存在未授权人员利用漏洞攻击信息系统的风险。	险
26	安全运维管理	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	管理不到位	（1）可能导致系统恶意代码检测管理不到位，存在信息系统感染恶意代码，从而导致严重的信息安全风险。	低风险
27	安全运维管理	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	制度文件、执行/记录文件	管理不到位	（1）密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不到位，存在违反国家政策的风险。	中风险

6 等级测评结论

等级测评结论由安全问题风险分析结果和综合得分共同确定，判定依据如下表所示。

表 6-1 等级测评结论判别依据

测评结论	判别依据
优	被测对象中存在安全问题，但不会导致被测对象面临中、高等级安全风险，且系统综合得分 90 分以上（含90 分）。
良	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分 80分以上（含 80分）。
中	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分 70分以上（含 70分）
差	被测对象中存在安全问题，而且会导致被测对象面临高等级安全风险，或被测对象综合得分低于 70 分。

综合得分计算方法如下：

设M为被测对象的综合得分，$M = V_t + V_m$，V_t和V_m根据下列公式计算。

$$V_t=\begin{cases}100\cdot y-\sum_{k=1}^{t} f(\omega_k)\cdot(1-x_k)\cdot S, & V_t>0\\ 0, & V_t\le 0\end{cases}$$

$$V_m=\begin{cases}100\cdot(1-y)-\sum_{k=1}^{m} f(\omega_k)\cdot(1-x_k)\cdot S, & V_m>0\\ 0, & V_m\le 0\end{cases}$$

$$0\le x_k\le 1,\ S=100\cdot\frac{1}{n},\ f(\omega_k)=\begin{cases}1, & \omega_k=\text{一般}\\ 2, & \omega_k=\text{重要}\\ 3, & \omega_k=\text{关键}\end{cases}$$

其中，y为关注系数，取值在0至1之间，由等级保护工作管理部门给出，默认值为0.5。n为被测对象涉及的总测评项数（不含不适用项，下同），t为技术方面对应的总测评项数，V_t为技术方面的得分，m为管理方面对应的总测评项数，V_m为管理方面的得分，ω_k为测评项k的重要程度（分为一般、重要和关键），x_k为测评项k的得分，如果测评项k涉及多测评项对象，则x_k取值为多测评对象得分的算术平均值。

x_k的得分计算如下：

测评项k涉及对象 / 测评项k定性判定	只涉及单个对象	涉及多个对象
符合	1	1
部分符合	0.5	计算测评对象平均分，取值在0至1之间
不符合	0	0

注：当测评项k涉及多个对象时，针对每个对象的得分取值为1、0.5和0。

根据第5章安全问题风险分析结果统计高、中、低风险安全问题的数量，利用综合得分计算公式计算出被测对象的综合得分，并将相关结果填入下表。

表 6-2 安全问题统计和综合得分

被测对象名称	安全问题数量			综合得分
	高风险	中风险	低风险	
档案管理系统	0	12	15	73.8

依据 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》和GB/T 28448—2019《信息安全技术 网络安全等级保护测评要求》的第二级要求，经对档案管理系统的安全保护状况进行综合分析评价，等级测评结论如下：

档案管理系统本次等级测评的综合得分为73.8，且不存在高等级安全风险，等级测评结论为中。

7 安全问题整改建议

表 7-1 安全问题整改建议

序号	安全类	安全问题	关联资产	整改建议
1	安全物理环境	(1)机房出入口未配置电子门禁系统。	信息化机房	(1) 采用电子门禁系统严格控制机房其他出入口的进出，或安排专人值守； (2) 采用电子门禁系统，对机房所有人员出入进行登记记录，并保存。
2	安全物理环境	(1)机房建设未完全采用符合耐火等级的建筑材料； (2)机房建设不具备防火设计/验收文档,或机房验收文档未明确相关建筑材料的耐火等级。	信息化机房	(1) 机房及相关的工作房间和辅助房采用具有耐火等级的建筑材料； (2) 机房建设采用符合相关耐火等级（二级）的建筑材料。（内外墙壁均应采用具有防火涂料、隔热板、铝板、钢板等阻燃或不燃的材料）； (3) 机房耐火等级建筑材料有相关合格证，并留存机房验收文档。
3	安全物理环境	(1)机房内缺乏防静电措施（如防静电地板或铺设防静电地毯）。	信息化机房	(1) 机房铺设防静电地板或铺设防静电地毯； (2) 机房房静电设计可依据GB50174-2008和GB50314-2006相关规定进行机房设计和验收。
4	安全通信网络	(1)关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	(1) 建议独立划分出应用服务器网段、数据库服务器网段。
5	安全通信网络	(1)缺乏对通信设备可信验证方面的安全设计要求；	安全通信网络	(1) 建议在管理规范文档内对通信设备可信验证方面的安全设计提出要求；

序号	安全类	安全问题	关联资产	整改建议
		(2)现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况。		（2）建议系统实现对所有可执行环节进行可信验证，包括： 运行过程中的可信检验： ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■通信应用连接过程。
6	安全区域边界	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	（1）建议网络层部署的防火墙配置对内部发起的攻击行为实现防范功能策略，实现检测、防止或限制从内部发起的网络攻击行为； （2）内部安全防范措施能检测以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、碎片攻击、网络蠕虫攻击、应用漏洞攻击。
7	安全区域边界	(1)现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	（1）建议现有部署的恶意代码防范措施网络边界覆盖全面，及时对恶意代码及逆行检测和清除。
8	安全区域边界	(1)缺乏对边界设备可信验证方面的安全设计要求； (2)现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）建议对边界设备系统程序的可信验证设计并保存设计文件； （2）建议系统实现对所有可执行环节进行可信验证。
9	安全计算环境	(1)数据库系统配置不合规的密码有效周期策略。	应用/数据库服务器-MySQL	（1）建议数据库配置‘default_password_lifetime‘；默认密码有效期不为0（具体有效期视业务需求定，一般情况可参考设为90-180天）。
10	安全计算环境	(1)设备不具备相关可信验证的技术措施。	WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2	（1）建议通过设备的启动过程和运行过程中对预装软件（包括系统引导程序、系统程序、相关应用程序和重要配置参数）的完整性验证或检测，确保对系统引导程序、系统程序、重要配置参数和关键应用程序可信根验证； （2）建议设备启用在检测到其可信性受到破坏后进行报警的相关功能。
11	安全计算	(1)缺乏对计算设备可信验	业务终端-1	（1）建议对计算设备系统程序的可信

序号	安全类	安全问题	关联资产	整改建议
	环境	证方面的安全设计要求； (2)现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。	业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	验证设计并保存设计文件； （2）建议系统实现对所有可执行环节进行可信验证。
12	安全计算环境	(1)未能提供数据库系统重要数据的异地定时数据备份功能。	应用/数据库服务器-MySQL	（1）建议设置异地灾备机房，并利用通信网络将重要数据定时备份至备份场地； （2）异地备份的数据范围（不限于）包括系统的： ■配置数据 ■重要业务数据。
13	安全计算环境	(1)未能提供中间件重要数据的异地定时数据备份功能。	应用/数据库服务器-Tomcat	（1）建议设置异地灾备机房，并利用通信网络将中间件重要数据定时备份至备份场地； （2）异地备份的中间件数据范围（不限于）包括系统的： ■配置数据 ■重要日志数据。
14	安全计算环境	(1)未能提供应用软件系统重要数据的异地定时数据备份功能。	档案管理系统	（1）建议设置异地灾备机房，并利用通信网络将应用软件系统重要数据定时备份至备份场地； （2）异地备份的应用软件系统数据范围（不限于）包括系统的：配置数据、重要日志数据，业务数据。
15	安全计算环境	(1)未能提供应用软件系统重要数据的异地定时数据备份功能。	重要业务数据 重要个人信息	（1）建议设置异地灾备机房，并利用通信网络将应用软件系统重要数据定时备份至备份场地。
16	安全管理中心	（1）系统管理的资源、运行及配置管理不够全面。	管理中心	（1）需实现系统包括对可信证书管理、可信基准库的管理。
17	安全管理机构	(1)单位开展的检查工作不够完善。	制度文件、执行/记录文件	（1）建议单位按要求提供安全检查报告。
18	安全管理人员	(1)单位未完全按管理规范开展人员离场后的清理工作。	制度文件、执行/记录文件	（1）建议单位按管理规范开展人员离场后的清理工作。至少包括：保留清理记录、及时清除离场后的所有访问权限、记录访问权限清除时间。
19	安全建设管理	(1)单位未具备适用于被测系统的安全规划设计方案。	制度文件、执行/记录文件	（1）建议单位根据等保要求进行过全面的自查或对比，根据系统的安全级别选择基本安全措施；

序号	安全类	安全问题	关联资产	整改建议
				（2）建议规划方案需根据风险分析结果对系统安全措施进行补充和整，并在系统建设\\整改方案中有详细描述。
20	安全建设管理	（1）单位未具备完整的安全设计方案相关的文档； （2）单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	（1）建议单位根据信息系统的等级划分情况，准备安全设计方案、安全管理策略、安全建设规划文档等； （2）建议相关文档内容应完善，包括统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、密码技术要求、总体建设规划和详细设计方案，并形成一致性的配套文件。
21	安全建设管理	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； （2）单位未对相关论证过程及内容进行完整的记录。	制度文件、执行/记录文件	（1）建议单位组织相关部门和安全技术专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定； （2）保存论证和审定记录，记录包括批准时间、批准人员签字； （3）文件经过批准后，才能正式实施。
22	安全建设管理	（1）单位未在软件开发过程中对所有软件安全性进行测试； （2）单位未在软件安装之前按要求对所有软件开展恶意代码检测。	制度文件、执行/记录文件	（1）建议开发商提供软件源代码，软件安装前检测软件中的恶意代码； （2）输出检测报告（或提供第三方检测报告），内容包括测试时间、测试地点、测试对象、测试结论、测试人员。
23	安全建设管理	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	（1）建议根据测试验收过程记录与结果，形成测试验收报告。
24	安全建设管理	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	（1）建议系统建设完成后，委托第三方测试单位对系统进行安全性测试，并出具安全性测试报告； （2）测试报告内容至少包括测试时间、测试地点、测试人、测试对象、测试方法、测试过程、测试发现的安全问题、整改建议、测试结论，并有第三方测试机构的签字盖章。
25	安全运维管理	（1）单位未严格按规范开展漏洞及安全隐患检测工作。	制度文件、执行/记录文件	（1）建议单位定期开展漏洞扫描，对发现的安全漏洞和隐患进行及时修补评估； （2）对必需修补的安全漏洞和隐患进行加固测试，测试无误后，备份系统数据，再从生产环境进行修补； （3）对于剩余安全漏洞和隐患进行残

序号	安全类	安全问题	关联资产	整改建议
				余风险分析，明确安全风险整改原则。
26	安全运维管理	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	（1）建议单位按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。包括;定期对相关产品的恶意代码库进行升级；对相关设备升级情况进行记录；对各类防病毒产品上截获的恶意代码进行分析并汇总上报； （2）单位需保留完整的恶意代码检测/升级的记录。至少具备：执行人、升级结果/检测结果、处理方式、负责人签字 。
27	安全运维管理	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	制度文件、执行/记录文件	（1）建议单位学习现有密码相关的国家标准和行业标准。建立密码管理要求的制度文档。

漏洞安全问题整改建议

序号	安全类	安全问题	关联资产	整改建议
1	安全计算环境	允许Traceroute探测 此类漏洞涉及服务器存储设备、安全设备、网络设备。	10.2.4.11/应用/数据库服务器 10.2.1.4/运维安全管理系统 10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/ 上网行为管理系统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/ 汇聚交换机 172.16.1.2/核心交换机	在防火墙出站规则中禁用echo-reply（type 0）、time-exceeded（type 11）、destination-unreachable（type 3）类型的ICMP包。
2	安全计算	OpenSSH CBC模式信息泄露	172.16.1.2/核心	临时解决方法：* 在SSH会话中仅使用

序号	安全类	安全问题	关联资产	整改建议
	环境	漏洞(CVE-2008-5161) 此类漏洞涉及网络设备。	交换机	CTR模式加密算法，如AES-CTR。 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://downloads.ssh.com/ 对于具体Linux发行版中使用的版本，可以参考如下链接,确认系统是否受该漏洞影响: Redhat ------- https://rhn.redhat.com/errata/RHSA-2009-1287.html Suse ------- http://support.novell.com/security/cve/CVE-2008-5161.html Ubuntu ------- http://people.canonical.com/~ubuntu-security/cve/2008/CVE-2008-5161.html
3	安全计算环境	缺少“X-Content-Type-Options”响应头 此类漏洞涉及业务应用软件平台。	https://arch.mmpt.edu.cn/ 档案管理系统	在服务器中配置X-Content-Type-Options响应头为“nosniff”。

【正文结束】

附录A 被测对象资产

A.1 物理机房

附录A 表- 1物理机房

序号	机房名称	物理位置	重要程度
1	信息化机房	茂名市茂南区文明北路232号大院大楼	关键

A.2 网络设备

附录A 表- 2网络设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度	备注
1	核心交换机	否	H3C version 7.1.070, Release 7585P07	H3C S7500E-X	核心数据交换、访问控制	关键	
2	汇聚交换机	否	H3C version 7.1.070, Release 6126P20	H3C S5560X-30C-EI	数据交换	重要	

A.3 安全设备

附录A 表- 3安全设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度	备注
1	防火墙-2	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键	
2	运维安全管理系统	否	深信服V3.0.6	深信服AC-1000-D603-PT	运维审计	重要	
3	上网行为管理系统	否	深信服AC12.0.26	深信服AC-1000-D600-PT	上网行为管理及终端准入控制	重要	
4	WEB应用防火墙	否	深信服AF 8.0.9	深信服WAF-2000-H642	应用防护、入侵防范、病毒防护	重要	
5	基线核查系统	否	深信服V3.0.3	深信服AC-1000-D602-PT	漏洞扫描	重要	
6	防火墙-1	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键	
7	日志审计系统	否	深信服LAS 3.0.5	深信服AC-1000-D601-PT	日志审计	重要	

A.4 服务器

附录A 表-4服务器

序号	设备名称	所属业务应用系统/平台名称	是否虚拟设备	操作系统及版本	数据库管理系统及版本	中间件及版本	重要程度	备注
1	应用/数据库服务器	档案管理系统	否	Windows Server 2008 R2	MySQL 5.7	Tomcat 9.0.13	关键	

A.5 终端设备

附录A 表-5终端设备

序号	设备名称	是否虚拟设备	操作系统/控制软件及版本	用途	重要程度	备注
1	运维及管理终端-2	否	Windows 10（版本21H2（内部版本19044.1889））	运维管理、系统管理	一般	
2	业务终端-1	否	Windows 10（版本20H2（内部版本19044.1889）	业务管理	一般	
3	运维及管理终端-1	否	Windows 10（版本20H2（内部版本19044.1889）	运维管理、系统管理	一般	
4	业务终端-2	否	Windows 10（版本20H2（内部版本19044.1889）	业务管理	一般	

A.6 其他系统或设备

附录A 表-6其他系统或设备

序号	设备名称	是否虚拟设备	操作系统/控制软件及版本	用途	重要程度	备注
/	/	/	/	/	/	/

注释：本次测评对象中不涉及专用移动互联终端等，不开展抽测。

A.7 系统管理软件/平台

附录A 表-7系统管理软件/平台

序号	系统管理软件/平台名称	所在设备名称	版本	主要功能	重要程度	备注
1	应用/数据库服务器-MySQL	应用/数据库服务器	5.7	数据生产、存储	关键	

序号	系统管理软件/平台名称	所在设备名称	版本	主要功能	重要程度	备注
2	应用/数据库服务器-Tomcat	应用/数据库服务器	9.0.13	页面发布	关键	

A.8 业务应用软件/平台

附录A 表- 8业务应用系统/平台

序号	业务应用系统/平台名称	主要功能	业务应用软件及版本	开发厂商	重要程度
1	档案管理系统	档案管理系统包括了档案业务管理、借阅管理、系统管理等模块，系统涵盖档案收、管、存、用整个业务流程，能够实现档案远程归档和服务利用，包括档案的收集、整理、归档、保管、鉴定、发布、利用等全部业务环节，是学院档案全流程管理的高效平台系统。	V6.0	同略科技有限公司	关键

A.9 数据资源

附录A 表- 9数据资源

序号	数据类别	所属业务应用	安全防护需求	重要程度
1	重要个人信息	档案管理系统	完整性、保密性	关键
2	重要业务数据	档案管理系统	完整性、保密性	关键
3	鉴别数据	档案管理系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性、保密性	关键
4	重要审计数据	档案管理系统（安全管理中心）	完整性	重要
5	重要配置数据	档案管理系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性	关键

注释：网络设备、安全设备、服务器、终端、系统管理软件/平台和业务应用系统等所涉及的鉴别数据和重要配置数据分别在各自测评对象中汇总测评证据后集中体现，包括

数据完整性、数据保密性和备份恢复。重要审计数据在安全管理中心进行汇总测评证据，包括数据完整性。重要业务数据和重要个人信息分别在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。

A.10 密码产品

附录A 表-10密码产品

序号	产品/模块名称	生成厂商	商密型号	密码算法	用途	重要程度
/	/	/	/	/	/	/

注释：本次测评不存在加密机等密码产品。

A.11 安全相关人员

附录A 表-11安全相关人员

序号	姓名	岗位/角色	联系方式	所属单位
1	叶永利	安全管理员	0668-2920122	茂名职业技术学院
2	龙恒	数据管理员	13377766618	茂名职业技术学院
3	杨云	资产管理员	0668-2920122	茂名职业技术学院
4	龙恒	网络管理员	13377766618	茂名职业技术学院
5	吴国华	机房管理员	0668-2920122	茂名职业技术学院
6	龙恒	应用管理员	13377766618	茂名职业技术学院
7	吴国华	系统管理员	0668-2920122	茂名职业技术学院
8	杨云	审计管理员	0668-2920122	茂名职业技术学院

A.12 安全管理文档

附录A 表-12安全管理文档

序号	文档名称	主要内容
1	制度类文档-网络与信息系统安全设计规范	关于单位网络与信息化安全设计制度文档
2	制度类文档-安全漏洞管理制度	关于单位安全漏洞管理工作制度文档
3	制度类文档-恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
4	制度类文档-网络安全	关于单位网络安全事件应急处理、流程、培训等管理制度文档

序号	文档名称	主要内容
	事件应急预案	
5	制度类文档-办公环境管理制度	关于单位办公环境管理制度文档
6	制度类文档-数据安全管理规范	关于保障关键数据安全，从数据库本身、数据加密、数据备份恢复三个方面对数据安全进行规范的制度文档
7	制度类文档-备份与恢复管理制度	关于单位数据备份、恢复管理制度文档
8	制度类文档-系统安全管理制度	关于单位系统安全管理、安全服务管理制度文档
9	制度类文档-工程实施管理制度	关于单位工程实施工作管理制度文档
10	制度类文档-安全教育和培训制度	关于单位安全培训、安全交流工作制度文档
11	制度类文档-物理安全管理规范	关于加强单位办公区域及电子计算机机房的管理和设备运行安全，规范办公区域及机房建设，使人员办公高效及机房设备安全、稳定运行的制度文档
12	制度类文档-测试及验收方案	关于单位测试验收方案文档
13	制度类文档-网络安全事件报告制度	关于单位网络安全事件管理报告文档
14	制度类文档-恶意代码防范管理制度	关于单位恶意代码防范工作制度文档
15	制度类文档-工程测试验收管理	关于单位工程测试工作管理制度文档
16	制度类文档-安全管理组织规范	关于单位组织结构管理规范制度文档
17	制度类文档-系统及应用数据备份管理规范	关于单位数据备份、恢复管理制度文档
18	制度类文档-组织安全结构和人员职责制度	关于单位组织结构、人员安排、人员职责制度文档
19	制度类文档-外包开发软件管理规定	关于单位外包项目管理工作制度文档
20	制度类文档-离岗人员工作交接规范	关于单位离岗交接工作规范制度文档
21	制度类文档-主机安全管理规范	关于规定单位主机系统安全管理要求规范，指导业务平台主机的安全配置和维护的制度文档
22	制度类文档-信息安全奖惩办法	关于单位人员奖惩制度文档
23	制度类文档-外部服务人员管理规范	关于单位针对外部人员工作管理规范制度文档
24	制度类文档-员工考核管理制度	关于单位人员考核工作管理制度文档
25	制度类文档-变更控制	关于单位变更流程、控制管理制度文档

序号	文档名称	主要内容
	管理制度	
26	制度类文档-组织安全结构和人员职责制度	关于单位安全结构、人员职责
27	制度类文档-人员管理制度	关于单位人员录用、调岗、离岗管理制度文档
28	制度类文档-系统交付管理	关于单位交付工作管理制度文档
29	制度类文档-设备安全管理制度	关于单位设备安全管理制度文档
30	制度类文档-安全事件报告和处置	关于单位网络安全事件管理、处置、流程等报告制度文档
31	制度类文档-办公环境保密管理	关于单位办公环境管理制度文档
32	制度类文档-服务供应商选择安全管理制度	关于单位安全服务供应商管理规定制度文档
33	制度类文档-外部接入受控网络访问系统管理规范	关于单位针对外部人员工作接入规范制度文档
34	制度类文档-授权和审批管理规定	关于单位授权审批、审批流程规范制度文档
35	制度类文档-应用系统业务用户密码设置规定	关于单位用户密码管理制度文档
36	制度类文档-网络安全管理规范	关于保障单位网络系统的安全稳定运行，抵御内部和外部各种形式的网络攻击或威胁制定的管理文档
37	制度类文档-信息安全漏洞扫描规范	关于单位安全漏洞工作规范制度文档
38	制度类文档-安全审查和检查管理规范	关于单位安全检查、审查工作规范制度文档
39	制度类文档-网络安全管理制度	关于单位网络安全工作管理制度文档
40	制度类文档-岗位安排及岗位职责	关于单位岗位职责、岗位安排制度文档
41	制度类文档-外部人员访问管理制度	关于单位针对外来人员访问管控制度文档
42	制度类文档-应用安全管理规范	关于规定单位应用安全管理要求及规范的制度文档
43	制度类文档-信息安全总体策略	关于单位网络安全方针、策略制度文档
44	制度类文档-信息系统恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
45	制度类文档-介质管理	关于单位介质安全管理工制度文档

序号	文档名称	主要内容
	制度	
46	制度类文档-制度制定、发布、评审和修订管理制度	关于单位制度制定、发布、评审和修订等管理文档
47	制度类文档-信息系统外包运维管理制度	关于单位外包运维工作管理制度文档
48	制度类文档-机房安全管理制度	关于单位机房安全管理工作制度文档
49	操作类文档-数据备份策略	关于单位数据备份策略文件
50	操作类文档-软硬件日常维护管理规程	关于单位计算机网络系统使用、管理、信息安全、资源共享有所遵循,规范上网操作流程,提高网络系统安全性的指导文档
51	操作类文档-设备操作规程	关于单位相关设备操作指导文档
52	操作类文档-设备及系统软件配置和操作手册	关于单位安全设备操作、Linux服务器配置手册、主机运维操作手册、软件操作手册、防火墙配置和操作手册、数据库日常运维操作手册等指导文档
53	记录类文档-外部人员访问记录表	关于外来人员访问登记工作记录
54	记录类文档-信息系统存储介质销毁申请表	关于备份介质销毁申请工作记录
55	记录类文档-信息管理系统漏洞检查表	关于单位安全漏洞工作检测记录表
56	记录类文档-数据恢复申请表	关于单位数据恢复工作申请表
57	记录类文档-软件交付清单	关于单位交付工作记录
58	记录类文档-机房出入登记表	关于人员进出机房登记工作记录
59	记录类文档-收发文登记记录	关于单位文档签发记录
60	记录类文档-专家论证记录表	关于单位网络方案论证记录
61	记录类文档-机房巡检记录表	关于单位机房环境巡检记录
62	记录类文档-机房设备维修记录表	关于单位机房设备维修工作记录
63	记录类文档-设备出入登记记录表	关于设备进出机房登记工作记录
64	记录类文档-关键岗位人员考核记录	关于关键岗位考核工作记录
65	记录类文档-离场信息资料交接表	关于人员离岗交接工作记录

序号	文档名称	主要内容
66	记录类文档-设备维修申请表	关于单位设备维护工作申请记录
67	记录类文档-备份介质使用记录	关于备份介质使用登记工作记录
68	记录类文档-安全管理制度评审记录	关于单位制度审计记录
69	记录类文档-信息系统存储介质使用清单	关于备份介质存储使用清单
70	记录类文档-外部人员访问申请表	关于外来人员访问申请流程工作记录
71	记录类文档-离职员工物品交回登记表	关于人员离岗工物交接工作记录
72	记录类文档-人员培训及考核记录表	关于人员培训、考核等工作记录
73	记录类文档-通用变更记录表	关于单位变更工作记录
74	记录类文档-系统交付清单	关于单位交付工作记录
75	记录类文档-接入受控网络申请表	关于外来人员接入工作记录
76	记录类文档-人员入职考核记录	关于人员录用、考核工作记录
77	记录类文档-信息安全检查记录表	关于单位安全检查工作记录
78	记录类文档-存储介质目录清单	关于备份介质存储工作清单
79	记录类文档-技能培训记录	关于单位系统培训工作、考核工作记录
80	记录类文档-网络配置信息	关于单位配置信息登记工作记录
81	记录类文档-评审和修订记录	关于单位变更评审、修订工作记录
82	记录类文档-重要操作审批表	关于单位审批工作记录
83	记录类文档-安全建设方案评审纪录	关于单位网络与信息化安全设计方案评审工作记录
84	记录类文档-人员离岗申请表	关于人员离岗申请记录
85	记录类文档-应急预案培训记录表	关于单位应急预案培训工作记录
86	记录类文档-外部会议文件和记录	关于单位外部联系、交流及会议工作记录
87	记录类文档-漏洞检测	关于单位安全漏洞检测报告文档

序号	文档名称	主要内容
	报告	
88	记录类文档-机房设备维护记录表	关于设备维护登记工作记录
89	记录类文档-网络信息安全事件记录表	关于单位网络安全事件工作记录
90	记录类文档-机房维护日志	关于机房维护工作记录
91	记录类文档-访问记录表	关于人员访问工作记录
92	记录类文档-设备操作维护记录	关于单位设备维护工作记录
93	记录类文档-监理审批表	关于单位监理审核工作记录
94	记录类文档-数据备份记录表	关于单位数据备份工作记录
95	记录类文档-备份工作汇总表	关于单位数据备份工作总结表
96	记录类文档-信息安全会议记录	关于单位安全培训、安全交流会议记录
97	证据类文档-网络安全等级保护工作小组名单	关于单位网络安全等级保护工作小组人员名单文件
98	证据类文档-工程项目实施方案	关于单位工程实施方案文档
99	证据类文档-定级备案	关于单位系统定级报告、备案证文件
100	证据类文档-资产清单	关于单位信息系统资产清单统计表
101	证据类文档-网络安全等级保护测评服务合同	关于单位与安全服务商签定的安全服务合同文件
102	证据类文档-外部联系表	关于单位内部联系及外部联系名单
103	证据类文档-深信服安全采购合同	关于单位与安全厂家服务采购、产品选择合同文件
104	证据类文档-信息安全事件分析报告表	关于单位安全事件分析报告
105	证据类文档-安全职位人员	关于单位人员岗位安排名单
106	证据类文档-网络安全系统设计方案	关于单位网络与信息化安全设计方案文档

附录B 上次测评问题整改情况说明

此次为档案管理系统初次等级测评，之前未实施过等级保护测评工作。

附录B 表- 1上次测评问题整改情况

序号	主要安全问题	整改情况	情况说明
/	/	□已整改 □未整改	/

附录C 单项测评结果汇总

C.1 安全物理环境

附录 C 表-1 安全物理环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			物理位置选择	物理访问控制	防盗窃和防破坏	防雷击	防火	防水和防潮	防静电	温湿度控制	电力供应	电磁防护
1	信息化机房	符合	2	0	2	1	1	2	0	1	2	1
		部分符合	0	1	0	0	0	0	0	0	0	0
		不符合	0	0	0	0	1	0	1	0	0	0
		不适用	0	0	0	0	0	0	0	0	0	0

附录 C 表-2 安全物理环境单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.2 安全通信网络

附录 C 表-3 安全通信网络单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求		
			网络架构	通信传输	可信验证
1	安全通信网络	符合	1	1	0
		部分符合	1	0	0
		不符合	0	0	1
		不适用	0	0	0

附录 C 表-4 安全通信网络单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.3 安全区域边界

附录 C 表-5 安全区域边界单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求					
			边界防护	访问控制	入侵防范	恶意代码和垃圾邮件防范	安全审计	可信验证
1	外网边界区域	符合	1	4	1	1	3	0
		部分符合	0	0	0	0	0	0
		不符合	0	0	0	0	0	1
		不适用	0	0	0	0	0	0
2	安全管理区域	符合	1	4	0	0	3	0
		部分符合	0	0	0	1	0	0
		不符合	0	0	1	0	0	1
		不适用	0	0	0	0	0	0
3	服务器存储区域	符合	1	4	1	1	3	0
		部分符合	0	0	0	0	0	0
		不符合	0	0	0	0	0	1
		不适用	0	0	0	0	0	0
4	办公网区域	符合	1	4	0	0	3	0
		部分符合	0	0	0	1	0	0
		不符合	0	0	1	0	0	1
		不适用	0	0	0	0	0	0

附录 C 表-6 安全区域边界单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.4 安全计算环境

C.4.1 网络设备

附录 C 表-7 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	汇聚交换机	符合	3	4	3	4	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	1	0	0	1	1	--
2	核心交换机	符合	3	4	3	4	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
		不适用	0	0	0	1	1	0	0	1	1	--

C.4.2 安全设备

附录 C 表-8 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	基线核查系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
2	上网行为管理系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
3	WEB应用防火墙	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
4	防火墙-1	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
5	防火墙-2	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
6	日志审计系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
7	运维安全	符合	3	4	3	5	0	0	1	1	0	--
		部分符	0	0	0	0	0	0	0	0	0	--

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
	管理系统	合										
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--

C.4.3 服务器和终端

附录 C 表-9 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	应用/数据库服务器	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
2	业务终端-2	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
3	业务终端-1	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
4	运维及管理终端-2	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
5	运维及管理终端-1	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--

C.4.4 系统管理软件/平台

附录 C 表-10 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	应用/数据库服务器-MySQL	符合	2	4	3	2	0	0	1	1	1	--
		部分符合	1	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	0	0	0	3	1	1	0	0	0	--
2	应用/数据库服务器-Tomcat	符合	0	4	3	1	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	3	0	0	4	1	1	0	0	0	--

C.4.5 业务应用系统/平台

附录 C 表-11 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	档案管理系统	符合	3	4	3	3	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	0	0	0	2	1	1	0	0	0	--

C.4.6 数据资源

附录 C 表-12 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	重要个人信息	符合	--	--	--	--	--	--	1	1	0	2
		部分符合	--	--	--	--	--	--	0	0	0	0
		不符合	--	--	--	--	--	--	0	1	0	0
		不适用	--	--	--	--	--	--	0	0	1	0
2	重要业务数据	符合	--	--	--	--	--	--	1	1	0	0
		部分符合	--	--	--	--	--	--	0	0	0	0

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
		不符合	--	--	--	--	--	--	0	1	0	0
		不适用	--	--	--	--	--	--	0	0	1	2

C.4.7 其他系统或设备

附录 C 表-13 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	--	符合	--	--	--	--	--	--	--	--	--	--
		部分符合	--	--	--	--	--	--	--	--	--	--
		不符合	--	--	--	--	--	--	--	--	--	--
		不适用	--	--	--	--	--	--	--	--	--	--

C.5 安全管理中心

附录 C 表-14 安全管理中心单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求	
			系统管理	审计管理
1	管理中心	符合	1	2
		部分符合	0	0
		不符合	1	0
		不适用	0	0

附录 C 表-15 安全管理中心单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.6 安全管理制度

附录 C 表-16 安全管理制度单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求			
			安全策略	管理制度	制定和发布	评审和修订
1	制度文件、执行/记录文件	符合	1	2	2	1
		部分符合	0	0	0	0
		不符合	0	0	0	0
		不适用	0	0	0	0

C.7 安全管理机构

附录 C 表-17 安全管理机构单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求				
			岗位设置	人员配备	授权和审批	沟通和合作	审核和检查
1	制度文件、执行/记录文件	符合	2	1	2	3	0
		部分符合	0	0	0	0	1
		不符合	0	0	0	0	0
		不适用	0	0	0	0	0

C.8 安全管理人员

附录 C 表-18 安全管理人员单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求			
			人员录用	人员离岗	安全意识教育和培训	外部人员访问管理
1	制度文件、执行/记录文件	符合	2	1	1	2
		部分符合	0	0	0	0
		不符合	0	0	0	1
		不适用	0	0	0	0

C.9 安全建设管理

附录 C 表-19 安全建设管理单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			定级和备案	安全方案设计	产品采购和使用	自行软件开发	外包软件开发	工程实施	测试验收	系统交付	等级测评	服务供应商选择
1	制度文件、执行/记录文件	符合	4	0	2	0	1	2	0	3	3	2
		部分符合	0	0	0	0	0	0	1	0	0	0
		不符合	0	3	0	0	1	0	1	0	0	0
		不适用	0	0	0	2	0	0	0	0	0	0

附录 C 表-20 安全建设管理单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.10 安全运维管理

附录 C 表-21 安全运维管理单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求												
			环境管理	资产管理	介质管理	设备维护管理	漏洞和风险管理	网络和系统安全管理	恶意代码防范管理	配置管理	密码管理	变更管理	备份与恢复管理	安全事件处置	应急预案管理	外包运维管理
1	制度文件、执行/记录文件	符合	3	1	2	2	0	5	2	1	0	1	3	3	2	0
		部分符合	0	0	0	0	0	0	1	0	0	0	0	0	0	0
		不符合	0	0	0	0	1	0	0	0	1	0	0	0	0	0
		不适用	0	0	0	0	0	0	0	0	1	0	0	0	0	2

附录 C 表-22 安全运维管理单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.11 其他安全要求指标

附录 C 表-23 其他指标单项测评结果汇总表

序号	测评对象	符合情况
本报告不涉及		

附录D 单项测评结果记录

D.1 安全物理环境

D.1.1 安全通用要求

D.1.1.1 信息化机房

安全控制点	测评指标	结果结论	符合程度
物理位置选择	a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；	（1）机房和办公场地场所在建筑物具有建筑验收文档，包含对防震、防风和防雨能力的说明；	符合

安全控制点	测评指标	结果结论	符合程度
		■机房建设地址为：茂名市茂南区文明北路232号大院大楼 （2）机房和办公场地未出严重的问题。 ■无雨水渗透痕迹 ■无因风导致的较严重尘土 ■无屋顶、墙体、地面等破损开裂	
	b）机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	（1）机房未部署在易发生问题的位置； （2）机房对于空调设备的排水管等部位采取密封防漏处理； （3）机房对于楼板进行了防护措施。	符合
物理访问控制	机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。	（1）制定了《机房安全管理制度》，内容包含机房出入方面的管理规定； （2）对未配置电子门禁系统的出入口指定专人7*24小时负责机房出入，对出入的人员进行身份鉴别和登记，可查出入记录，且出入有专人陪同； （3）机房存在未配置门禁系统的开放出入口。	部分符合
防盗窃和防破坏	a）应将设备或主要部件进行固定，并设置明显的不易除去的标识；	（1）机房设备或主要部件都固定在机架上； （2）机房内对主要部件已绑定相应不易除去的标签； ■包括网络设备 ■包括安全设备 ■包括服务器 ■包括网络线缆 （3）重要机柜已进行上锁处理。	符合
	b）应将通信线缆铺设在隐蔽安全处。	（1）通信线缆铺设在下走线槽隐蔽处中； （2）通信线缆设有明显的源目的标识； （3）通信线缆均铺设整齐、规范。	符合
防雷击	应将各类机柜、设施和设备等通过接地系统安全接地。	（1）机房设置专用地线； （2）机房内机柜、设施和设备等进行接地处理； （3）交流电源接地验收检测结果符合要求。	符合
防火	a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；	（1）机房采用经消防检测部门检测合格并在有效期内的（如 七氟丙烷）气体自动灭火设备，火灾自动报警类型为烟感+红外； （2）自动消防系统工作状态正常，有定期巡检和维护记录《机房巡检记录表》； （3）建立机房消防的管理制度相关文档《机房安全管理制度》，按管理要求机房无人情况下气体灭火配置为自动模式，进入机房调整为手动模式，机房报警有7*24小时值班人员进行监控。	符合
	b）机房及相关的工作房间	（1）机房及相关的工作房间和辅助房没有采	不符合

安全控制点	测评指标	结果结论	符合程度
	和辅助房应采用具有耐火等级的建筑材料。	用具有耐火等级的建筑材料； （2）缺乏机房防火设计文档； （3）缺乏机房防火验收文档。	
防水和防潮	a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	（1）机房不存在雨水渗透、破损等不合规情况； （2）机房不位于建筑的顶层、边缘区域。	符合
	b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。	（1）机房区域范围已部署1台科华品牌（精密）空调，机房内分别配置1组温湿度传感器监控； （2）机房内空调下方已铺设安装好挡水和排水设施； （3）机房墙壁或楼板的管道采取必要的防渗防漏等防水保护措施； （4）机房安装检测设备（如：漏水检测绳）检测地下积水，及时处理机房水蒸气结露和地下积水的转移与渗透； （5）目前防水\防潮检测未发现异常情况，并且有防水防潮的运维记录《机房维护日志》。	符合
防静电	应采用防静电地板或地面并采用必要的接地防静电措施。	（1）对机房内设备（可导电金属线槽）采用了接地静电泄放措施； （2）机房未采用防静电地板或铺设防静电地毯。	不符合
温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。	（1）机房范围已部署1组科华品牌精密空调进行温湿度调节； （2）机房范围已部署空调及加湿机进行温湿度调节； （3）温湿度自动调节设施运作正常，有运行和维护记录《机房维护日志》； （4）机房温度能保持在24摄氏度到28摄氏度之间； （5）机房湿度能保持在40%到65%之间。	符合
电力供应	a）应在机房供电线路上配置稳压器和过电压防护设备；	（1）机房配备了稳压器和过电压防护设备； （2）稳压器和过电压防护设备正常工作； （3）机房具备电力供应安全设计，并在其中标明配备稳压器、过电压防护设备等要求。	符合
	b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。	（1）机房配备了1组科华品牌UPS； （2）UPS正常工作，可满足主要设备断电情况下的至少1小时正常运行要求； （3）UPS有定期（至少每年）检查和维护，有运行和维护记录《机房巡检记录表》。	符合
电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。	（1）通信线缆铺设采用独立的具有电磁屏蔽作用线槽； （2）电源线缆铺设采用独立的具有电磁屏蔽作用线槽；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）弱电线缆隔离铺设，没有干扰。	

D.2 安全通信网络

D.2.1 安全通用要求

D.2.1.1 安全通信网络

安全控制点	测评指标	结果结论	符合程度
网络架构	a）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；	（1）已对网络地址划分，且便于管理和控制； （2）网络地址划分采用核心交换机实现外网边界区域、服务器存储区域等的划分； （3）重要核心网络区域与非重要网络在同一网段； （4）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	部分符合
	b）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	（1）网络内重要网段未部署在网络边界处，且未直接连接外部信息系统； （2）系统通过防火墙对重要网段采取访问控制策略； （3）各安全域（子网）的出口唯一。	符合
通信传输	应采用校验技术保证通信过程中数据的完整性。	（1）网络系统中未涉及完整性保障设备，但在安全计算环境方面网络设备采用SSH协议、安全设备采用HTTPS协议、操作系统采用SSH协议、应用系统采用HTTPS协议来保证通信过程中数据的完整性。	符合
可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对通信设备可信验证方面的安全设计要求； （2）现有的通信设备存在未能实现操作系统到上层应用的信任链的情况，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■通信应用连接过程	不符合

D.3 安全区域边界

D.3.1 安全通用要求

D.3.1.1 办公网区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■办公网区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机	符合

安全控制点	测评指标	结果结论	符合程度
		（3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	不符合
恶意代码和垃		（1）在关键网络节点处部署合规的防恶意代	部分符合

安全控制点	测评指标	结果结论	符合程度
圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试； （4）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	
安全审计	a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数	不符合

安全控制点	测评指标	结果结论	符合程度
	录送至安全管理中心。	■边界防护应用程序	

D.3.1.2 外网边界区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■外网边界区域 （2）网络边界处部署了可提供访问控制功能的设备； ■防火墙 ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	符合
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■防火墙 ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和	符合

安全控制点	测评指标	结果结论	符合程度
		会话机制检测的访问控制设备； ■防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制,能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署支持对内部发起的攻击行为进行防范的设备； ■防火墙(带入侵防御模块) ■WEB应用防火墙 （2）现有的防范措施满足相应防护要求； ■所有关键网络边界均有检测措施 ■设备的规则库及时更新 ■检测(模块)符合国家相关产品检测要求 ■其安全策略有效 （3）内部安全防范措施能检测相应攻击行为。 ■端口扫描 ■强力攻击 ■木马后门攻击 ■拒绝服务攻击 ■缓冲区溢出攻击 ■碎片攻击 ■网络蠕虫攻击 ■应用漏洞攻击	符合
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试。	符合
安全审计	a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合

安全控制点	测评指标	结果结论	符合程度
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.3.1.3 安全管理区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■安全管理区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	符合
访问控制	a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能；	符合

安全控制点	测评指标	结果结论	符合程度
		（4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	不符合
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试； （4）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	部分符合
安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计；	符合

安全控制点	测评指标	结果结论	符合程度
	要的用户行为和重要安全事件进行审计；	■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.3.1.4 服务器存储区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■服务器存储区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略；	符合

安全控制点	测评指标	结果结论	符合程度
		（4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■WEB应用防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署支持对内部发起的攻击行为进行防范的设备； ■WEB应用防火墙 （2）现有的防范措施满足相应防护要求； ■所有关键网络边界均有检测措施 ■设备的规则库及时更新 ■检测(模块)符合国家相关产品检测要求	符合

安全控制点	测评指标	结果结论	符合程度
		■其安全策略有效 （3）内部安全防范措施能检测相应攻击行为。 ■端口扫描 ■强力攻击 ■木马后门攻击 ■拒绝服务攻击 ■缓冲区溢出攻击 ■碎片攻击 ■网络蠕虫攻击 ■应用漏洞攻击	
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■WEB应用防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试。	符合
安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■WEB应用防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个	符合

安全控制点	测评指标	结果结论	符合程度
		月； （5）定期收集日志记录并定期备份。	
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.4 安全计算环境

D.4.1 安全通用要求

D.4.1.1 网络设备

D.4.1.1.1 核心交换机

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括VTY认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的全局密码策略； ■Password control:Enabled ■Password aging:Enabled (180 days) ■Password length:Enabled (8 characters) ■Password composition:Enabled (4 types, 1 characters per type) （6）设备配置加密的super认证。	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备配置合规的全局登录失败处理策略； ■Password control: Enabled ■Maximum login attempts: 5 ■Action for exceeding login attempts: Lock user for 5 minutes （2）设备配置合规的操作超时退出措施。 ■VTY配置idle-timeout 15 0	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式。 ■未启用TELNET ■启用SSH	符合

安全控制点	测评指标	结果结论	符合程度
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； ■Information Center: Enabled ■Console: Enabled ■Monitor: Enabled ■Log host: Enabled 10.2.1.2 ■Security log file: Enabled （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保	（1）设备限制审计文件的访问控制权限，普	符合

安全控制点	测评指标	结果结论	符合程度
	护，定期备份，避免受到未预期的删除、修改或覆盖等。	通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效； （5）日志及审计记录保存大于6个月。	
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制； ■对ssh 登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）网络层相关设备不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的交换功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。	不符合

安全控制点	测评指标	结果结论	符合程度
	结果形成审计记录送至安全管理中心。	■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施; ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施; ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能;	（1）设备定义了相关重要数据; ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范; （3）设备定期完全依照备份策略，采用正确的配置进行本地备份; （4）设备的备份周期为：每月一次; （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息;	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.1.2 汇聚交换机

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括VTY认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的全局密码策略； ■Password control:Enabled ■Password aging:Enabled (180 days) ■Password length:Enabled (8 characters) ■Password composition:Enabled (4 types, 1 characters per type) （6）设备配置加密的super认证。	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备配置合规的全局登录失败处理策略； ■Password control: Enabled ■Maximum login attempts: 5 ■Action for exceeding login attempts: Lock user for 5 minutes （2）设备配置合规的操作超时退出措施。 ■VTY配置idle-timeout 15 0	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式。 ■未启用TELNET ■启用SSH	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户	（1）设备根据安全策略要求对特权用户进行分离；	符合

安全控制点	测评指标	结果结论	符合程度
	的权限分离。	■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； ■Information Center: Enabled ■Console: Enabled ■Monitor: Enabled ■Log host: Enabled 10.2.1.2 ■Security log file: Enabled （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）漏洞扫描未发现设备启用高危端口。	
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制； ■对ssh 登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）网络层相关设备不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的交换功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。	符合

安全控制点	测评指标	结果结论	符合程度
		■使用SSH加密协议进行传输	
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2 安全设备

D.4.1.2.1 WEB应用防火墙

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会	（1）设备启用合规登录失败处理策略； ■启用登录失败策略	符合

安全控制点	测评指标	结果结论	符合程度
	话、限制非法登录次数和当登录连接超时自动退出等相关措施；	■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型	符合

安全控制点	测评指标	结果结论	符合程度
		■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合

安全控制点	测评指标	结果结论	符合程度
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配	（1）网络层设备不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	前得到完全清除。		
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.2 上网行为管理系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令	符合

安全控制点	测评指标	结果结论	符合程度
		■未设置空口令	
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合

安全控制点	测评指标	结果结论	符合程度
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。	符合

安全控制点	测评指标	结果结论	符合程度
		■使用SSH加密协议进行传输	
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.3 基线核查系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次	符合

安全控制点	测评指标	结果结论	符合程度
	当登录连接超时自动退出等相关措施；	■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识	符合

安全控制点	测评指标	结果结论	符合程度
		■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的基线核查功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施	不符合

安全控制点	测评指标	结果结论	符合程度
	程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.4 日志审计系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合

安全控制点	测评指标	结果结论	符合程度
	享账户的存在；		
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合

安全控制点	测评指标	结果结论	符合程度
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据	符合

安全控制点	测评指标	结果结论	符合程度
		（2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.5 运维安全管理系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信	（1）设备配置合规的远程管理模式； ■未启用HTTP	符合

安全控制点	测评指标	结果结论	符合程度
	息在网络传输过程中被窃听。	■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改；	符合

安全控制点	测评指标	结果结论	符合程度
	未预期的删除、修改或覆盖等。	（2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制。 ■对Web登录配置管理地址，限制登录范围	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数	不符合

安全控制点	测评指标	结果结论	符合程度
		■缺乏关键应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.6 防火墙-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身	（1）设备对各登录模式均启用身份鉴别；	符合

安全控制点	测评指标	结果结论	符合程度
	份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员	符合

安全控制点	测评指标	结果结论	符合程度
		(2)设备不存在多个管理级别高的特权用户; (3) 设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计;	(1) 设备开启审计功能，审计进程正常; (2) 设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息;	(1) 设备日期、时间正常; (2) 设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	(1) 设备限制审计文件的访问控制权限，普通用户不可删除及修改; (2) 设备针对日志、审计记录具备充足的存储容量; (3) 对审计记录进行定期存档备份，其备份策略有效; (4) 部署日志审计系统实时对日志进行统一收集存储; (5) 日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序;	(1) 设备在全局模式下禁用部分不必要的服务; (2) 设备在部分接口模式下禁用部分不必要的服务; (3) 漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口;	(1) 设备采用安全策略限制部分高危端口; (2)设备采用安全策略限制部分不必要服务; (3) 漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制;	(1) 设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制; ■对Web登录配置管理地址，限制登录范围 (2) 通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要	(1) 设备管理具备数据有效性检验功能; ■可校验录入数据 ■可校验文档内容 (2) 设备管理的校验接口范围较全面。	符合

安全控制点	测评指标	结果结论	符合程度
	求；	■包括人机接口校验 ■包括通信接口校验	
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.7 防火墙-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS	符合

安全控制点	测评指标	结果结论	符合程度
		（2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序	不符合

安全控制点	测评指标	结果结论	符合程度
		■缺乏重要设备配置参数 ■缺乏关键应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施; ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施; ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能;	（1）设备定义了相关重要数据; ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范; （3）设备定期完全依照备份策略，采用正确的配置进行本地备份; （4）设备的备份周期为：每月一次; （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息;	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.3 服务器和终端

D.4.1.3.1 应用/数据库服务器

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 (5)用户属性策略未勾选“密码永不过期”。	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用‘RDP安全层’参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令	符合

安全控制点	测评指标	结果结论	符合程度
		■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	(1)操作系统采取对审计记录存储容量如下:运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份	符合

安全控制点	测评指标	结果结论	符合程度
		策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信	不符合

安全控制点	测评指标	结果结论	符合程度
	程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用	（1）设备为服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要	不适用

安全控制点	测评指标	结果结论	符合程度
	场地。	求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施： 安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.2 业务终端-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”	符合

安全控制点	测评指标	结果结论	符合程度
	听。	参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间	符合

安全控制点	测评指标	结果结论	符合程度
		■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下：运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端	符合

安全控制点	测评指标	结果结论	符合程度
		口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据	符合

安全控制点	测评指标	结果结论	符合程度
		■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.3 业务终端-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	符合
	b）应具有登录失败处理功	（1）操作系统启用登录失败处理策略，且配	符合

安全控制点	测评指标	结果结论	符合程度
	能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败	符合

安全控制点	测评指标	结果结论	符合程度
	全事件进行审计；	■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下：运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合

安全控制点	测评指标	结果结论	符合程度
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据:	符合

安全控制点	测评指标	结果结论	符合程度
		（1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.4 运维及管理终端-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码	符合

安全控制点	测评指标	结果结论	符合程度
	更换；	（2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c）应及时删除或停用多余的、过期的账户，避免共	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对	符合

安全控制点	测评指标	结果结论	符合程度
	享账户的存在；	应。	
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下：运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合

安全控制点	测评指标	结果结论	符合程度
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数	不符合

安全控制点	测评指标	结果结论	符合程度
	全管理中心。	■业务应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配	（1）身份鉴别信息释放或清除机制正常且满足要求；	符合

安全控制点	测评指标	结果结论	符合程度
	前得到完全清除。	（2）操作系统用户的鉴别信息释放措施： 安全选项“不显示上次的用户名”->启用	
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.5 运维及管理终端-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账	（1）可提供操作系统权限表；	符合

安全控制点	测评指标	结果结论	符合程度
	户和权限；	（2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功）	符合

安全控制点	测评指标	结果结论	符合程度
		■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	(1)操作系统采取对审计记录存储容量如下:运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G; (2) 限制审计文件的访问控制权限，用户不可删除及修改; (3) “管理审核和安全日志”，除审计员、administrators外其他用户无权限; (4) 对审计记录进行定期存档备份，其备份策略有效; (5) 部署日志审计系统实时对日志进行统一收集存储; (6) 日志及审计记录保存6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序;	(1) 操作系统仅安装必需的组件; (2) 操作系统仅安装必需的应用程序; (3) 操作系统遵循最小安装的原则，仅启用必需的功能软件; (4) 漏洞扫描未发现高风险主机漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口;	(1) 操作系统不存在多余的默认共享及其它文件共享; ■如：C$、D$、E$ (2) 操作系统关闭不必要端口; ■如：137，138、139、445、123、1900 (3) 操作系统禁用不必要服务; (4) 操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制;	(1) 安全设备ACL策略有效限制访问本机的IP地址及管理模式; (2) 通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求;	(1) 操作系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	(1)操作系统已安装最新的SP及后续的hotfix补丁; (2) 补丁安装前进行安全性和兼容性测试; (3) 操作系统不存在启用未加控制的高危端口; (4) 操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或	(1) 操作系统安装深信服EDR防恶意代码软	符合

安全控制点	测评指标	结果结论	符合程度
	配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确	符合

安全控制点	测评指标	结果结论	符合程度
		的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.4 系统管理软件/平台

D.4.1.4.1 应用/数据库服务器-MySQL

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）数据库系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）数据库系统不存在弱口令用户； ■MySQL数据库已修改默认root口令 ■MySQL数据库不存在空口令用户 （3）数据库系统不存在默认信任的登录模式； ■MySQL数据库登录未设置skip-grant-tables （4）数据库系统为登录用户设置的身份标识具有唯一性； （5）数据库系统配置合规的密码长度及复杂度策略； ■MySQL数据库系统启用“validate_password” ■validate_password_length 8 ■validate_password_mixed_case_count 1 ■validate_password_number_count 1 ■validate_password_special_char_count 1 （6）不存在空口令或弱口令帐户；	部分符合

安全控制点	测评指标	结果结论	符合程度
		（7）数据库系统配置合规的密码有效周期策略。 ■MySQL 数据库配置未合理的“password_lifetime”参数	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）数据库系统启用合规登录失败处理策略； ■MySQL 数据库系统启用“connection_control” （2）数据库系统执行合规的锁定策略； ■Connection_control_failed_connections_threshold 3 ■Connection_control_min_connection_delay 1000 （3）数据库系统配置合规的操作超时锁定。 ■interactive_timeout 1800	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）数据库系统配置合规的远程管理模式。 ■MySQL 数据库系统have_openssl为YES	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）登录数据库系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （2）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在多用户均与root用户权限一致的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）数据库系统对多余帐户进行删除、锁定或禁止其登录； ■数据库系统账户禁用不常用的默认用户 （2）数据库系统账户口令设置合规。 ■数据库系统各用户未使用空口令 ■数据库系统未使用弱口令或默认与用户名相同的口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）数据库系统不存在多余或过期账户； （2）数据库系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）数据库系统根据安全策略要求对特权用户进行分离； （2）数据库系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限； （3）数据库账户和系统管理员账户未处于同一个用户组中；	符合

安全控制点	测评指标	结果结论	符合程度
		（4）宿主操作系统管理员与数据库管理员为不同的人员，且使用不同的帐户登录系统。	
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）数据库系统开启审计功能，审计进程正常。 ■MySQL 数据库系统log_bin=ON	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）数据库宿主系统日期、时间正常； （2）数据库系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括重要用户行为 ■包括系统资源的异常使用情况 ■包括重要系统命令的使用 ■包括重要的安全相关事件	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）数据库系统限制审计文件的访问控制权限，普通用户不可删除及修改； ■MySQL数据库系统日志文件安装路径下的log文件 用户权限为640 （2）数据库系统针对日志、审计记录具备充足的存储容量； （3）日志及审计记录保存大于6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）数据库系统设定有效的终端接入策略，对通过网络进行管理的终端进行限制； ■数据库系统对帐号进行IP限制，host ≠ % （2）核心交换机设备ACL策略有效限制访问本机的IP地址及管理模式。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）数据库系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）数据库宿主系统不存在启用未加控制的高危端口； （3）MYSQL分离默认安装的示例数据库； （4）数据库系统进行渗透及扫描未发现存在	符合

安全控制点	测评指标	结果结论	符合程度
		可造成高风险的漏洞。	
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■使用数据库内置的SSL协议加密 重要配置数据: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■使用数据库内置的SSL协议加密	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）数据库系统定义了相关重要数据； ■包括鉴别数据 ■包括重要配置数据 ■包括重要审计数据 （2）数据库系统定期完全依照备份策略，采用正确的配置进行本地备份； （3）系统的备份周期为：每天一次增量、每月一次全备； （4）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	(1)数据库系统未能提供异地数据备份功能。	不符合
剩余信息保护	应保证鉴别信息所在的存	（1）身份鉴别信息释放或清除机制正常且满	符合

安全控制点	测评指标	结果结论	符合程度
	储空间被释放或重新分配前得到完全清除。	足要求； （2）数据库系统不保存终端历史记录。	
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）数据库存储的用户个人信息均为业务应用必需的环节。	符合
	b）应禁止未授权访问和非法使用用户个人信息。	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； ■包括信息采集 ■包括信息保存 ■包括信息访问 ■包括信息使用 （2）数据库具备控制措施禁止未授权访问用户个人信息表单； （3）数据库具备控制措施禁止非法使用用户个人信息表单。	符合

D.4.1.4.2 应用/数据库服务器-Tomcat

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）Tomcat中间件关闭web管理控制台，其身份鉴别功能由宿主操作系统实现，不适用。	不适用
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）Tomcat中间件关闭web管理控制台，其身份鉴别功能由宿主操作系统实现，不适用。	不适用
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）Tomcat中间件关闭web管理控制台，其身份鉴别功能由宿主操作系统实现，不适用。	不适用
访问控制	a）应对登录的用户分配账户和权限；	（1）对应不同的账户均按需分配不同的用户权限，不存在中间件用户均属于管理级别、高权限的情况； （2）中间件配置可降权启动Tomcat的用户； （3）宿主系统针对中间件用户分别赋予相应的管理操作权限。 ■包括审计权限 ■包括操作权限	符合
	b）应重命名或删除默认账	（1）中间件不存在除如:Tomcat、admin、	符合

安全控制点	测评指标	结果结论	符合程度
	户，修改默认账户的默认口令；	manager、role1等默认账户名； （2）中间件账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）中间件不存在多余或过期账户； (2)中间件管理员用户与账户之间一一对应； （3）中间件启用合规的管理用户名配置。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）中间件根据安全策略要求对特权用户及宿主管理用户进行分离； （2）中间件管理不存在多个管理级别高的特权用户； （3）中间件管理按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）中间件开启审计功能，审计进程正常； ■开启Cataline引擎的日志文件 catalina.org.apache.juli.FileHandler.level = FINE ■开启内部代码丢出的日志 localhost.org.apache.juli.FileHandler.level = FINE ■开启manager应用日志 manager.org.apache.juli.FileHandler.level = FINE ■开启控制台输出的日志 java.util.logging.ConsoleHandler.level = FINE ■开启Access访问日志。 server.xml文件配置正常，未被注释标记<!-- -->； （2）系统的日志审计级别满足要求。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）中间件日期、时间正常； （2）中间件审计记录开启审核策略且日志级别正常。 ■日志级别不低于“FINE” ■日志配置pattern值设为common ■日志配置pattern值为自定义格式，至少包含：%h %l %u %t %s	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）中间件限制审计文件的访问控制权限，普通用户不可删除及修改； （2）宿主系统针对中间件日志、审计记录具备充足的存储容量； ■日志创建计划为每天/每周/每月 ■不限制最大日志文件大小 （3）对中间件审计记录进行定期存档备份，	符合

安全控制点	测评指标	结果结论	符合程度
		其备份策略有效； （4）审计记录及日志保存大于6个月。	
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）中间件系统不存在此部分的安装控制需求，不适用。	不适用
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）Tomcat中间件的管理地址限制功能由宿主操作系统实现，故该项不适用。	不适用
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）Tomcat中间件关闭web管理控制台，不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）中间件已根据需要不定期地对已发布的版本进行更新； （2）中间件更新安装前进行安全性和兼容性测试； （3）在系统上线或发生重大变更时测试并安装最新的中间件版本或更新补丁； （4）在不影响业务系统正常运行情况下，对发现的中间件漏洞在确保安全的情况下进行修补； （5）中间件进行扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据	符合

安全控制点	测评指标	结果结论	符合程度
		（2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输 重要配置数据: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份的中间件重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）宿主系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）中间件相关数据的备份周期合理：每天增量一次、每月全备一次； （5）中间件开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）宿主系统具有清除用户鉴别信息的功能； （2）经测试，宿主系统退出后无法访问先前中间件登录过的页面； （3）经测试，宿主系统关闭后无残留的中间件用户鉴别信息。	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用

D.4.1.5 业务应用系统/平台

D.4.1.5.1 档案管理系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识	（1）系统对各登录模式均启用身份鉴别； ■包括管理后台认证	符合

安全控制点	测评指标	结果结论	符合程度
	具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（2）系统对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）系统登录用户设置的身份标识具有唯一性； （4）系统不存在空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）系统启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）系统配置合规的操作超时退出措施。 ■管理后台配置超时15分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）应用系统的用户鉴别数据采用SHA-512算法在可控网络环境中传输； （2）系统配置合规的远程管理模式。 ■启用HTTPS	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供系统权限分配表； （2）登录系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需分配不同的用户权限，不存在所有用户均属于管理级别、高权限的情况。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）系统禁用默认账户名； （2）系统账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）系统不存在多余或过期账户； （2）系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）系统不存在多个管理级别高的特权用户； （2）系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）系统开启审计功能，审计进程正常； （2）系统的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合

安全控制点	测评指标	结果结论	符合程度
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）系统日期、时间正常； （2）系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）系统针对日志、审计记录具备充足的存储容量； （3）审计记录及日志保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）应用软件系统不存在此部分的安装控制需求，不适用。	不适用
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）应用软件系统不存在此部分的控制需求，不适用。	不适用
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）系统自身设定有效的终端访问策略，通过访问措施进行管理地址的限制。 ■系统管理页面仅能内网登录	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）系统具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）系统的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）系统已根据需要不定期地对已发布的版本进行更新； （2）在系统上线或发生重大变更时测试并安装最新的版本或更新补丁； （3）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）应用软件系统不存在此部分的控制需求，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用	（1）应用软件系统不存在此部分的控制需求，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。		
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）系统具有清除用户鉴别信息的功能； （2）经测试，系统退出后无法访问先前登录过的页面； （3）经测试，系统关闭后无残留的用户鉴别信息。	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管	符合

安全控制点	测评指标	结果结论	符合程度
		理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息； （3）系统采集的用户个人信息均为业务应用必需的环节。	
	b）应禁止未授权访问和非法使用用户个人信息。	（1）系统不采集和保存任何形式的用户个人信息； （2）系统对所有涉及个人信息的环节均有明确的授权同意过程； ■包括信息采集 ■包括信息保存 ■包括信息访问 ■包括信息使用 （3）系统具备控制措施禁止未授权访问用户个人信息； （4）系统具备控制措施禁止非法使用用户个人信息。	符合

D.4.1.6 数据资源

D.4.1.6.1 重要业务数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	（1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要业务数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份重要数据； ■包括重要业务数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存	（1）该测评项测评对象鉴别数据，已在安全	不适用

安全控制点	测评指标	结果结论	符合程度
	储空间被释放或重新分配前得到完全清除。	计算环境层面其他对象判定，此项不适用。	
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）该测评项测评对象为重要个人信息的内容，已在安全计算环境层面其他对象判定，该项不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）该测评项测评对象为重要个人信息的内容，已在安全计算环境层面其他对象判定，该项不适用。	不适用

D.4.1.6.2 重要个人信息

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	（1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要个人信息 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份重要数据； ■包括重要个人信息 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）该测评项测评对象鉴别数据，已在安全计算环境层面其他对象判定，此项不适用。	不适用
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息； （3）系统采集的用户个人信息均为业务应用必需的环节。	符合
	b) 应禁止未授权访问和非	（1）系统对所有涉及个人信息的环节均有明	符合

安全控制点	测评指标	结果结论	符合程度
	法使用用户个人信息。	确的授权同意过程； ■包括信息采集 ■包括信息保存 ■包括信息访问 ■包括信息使用 （2）系统具备控制措施禁止未授权访问用户个人信息； （3）系统具备控制措施禁止非法使用用户个人信息。	

D.4.1.6.3 鉴别数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	应用/数据库服务器-Tomcat: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输 业务终端-1、业务终端-2、应用/数据库服务器、运维及管理终端-1、运维及管理终端-2: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 应用/数据库服务器-MySQL: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■使用数据库内置的SSL协议加密 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）设备在通信传输过程中对相关数据采取	符合

安全控制点	测评指标	结果结论	符合程度
		完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 档案管理系统: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	该测评项在各系统及设备已做判定,数据资源针对鉴别数据不做判定	不适用
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	该测评项在各系统及设备已做判定,数据资源针对鉴别数据不做判定，不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	应用/数据库服务器-Tomcat: （1）宿主系统具有清除用户鉴别信息的功能； （2）经测试，宿主系统退出后无法访问先前中间件登录过的页面； （3）经测试，宿主系统关闭后无残留的中间件用户鉴别信息。 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）网络层设备不适用。 业务终端-1、业务终端-2、应用/数据库服务器、运维及管理终端-1、运维及管理终端-2: （1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施： 安全选项“不显示上次的用户名”->启用 档案管理系统: （1）系统具有清除用户鉴别信息的功能； （2）经测试，系统退出后无法访问先前登录过的页面； （3）经测试，系统关闭后无残留的用户鉴别信息。 应用/数据库服务器-MySQL: （1）身份鉴别信息释放或清除机制正常且满	符合

安全控制点	测评指标	结果结论	符合程度
		足要求； （2）数据库系统不保存终端历史记录。	
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	鉴别数据不存在此部分的控制需求，故此项不适用	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	鉴别数据不存在此部分的控制需求，故此项不适用	不适用

D.4.1.6.4 重要配置数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	档案管理系统: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输 应用/数据库服务器-Tomcat: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输 应用/数据库服务器-MySQL: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■使用数据库内置的SSL协议加密 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 业务终端-1、业务终端-2、应用/数据库服务器、运维及管理终端-1、运维及管理终端-2: （1）系统在通信传输过程中对相关数据采取	符合

安全控制点	测评指标	结果结论	符合程度
		完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）设备定义了相关重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 应用/数据库服务器-Tomcat: （1）系统定义了相关需要备份的中间件重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）宿主系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）中间件相关数据的备份周期合理：每天增量一次、每月全备一次； （5）中间件开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 业务终端-1、业务终端-2、应用/数据库服务器、运维及管理终端-1、运维及管理终端-2: （1）操作系统定义了相关重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确	符合

安全控制点	测评指标	结果结论	符合程度
		的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 档案管理系统: （1）系统定义了相关需要备份重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 应用/数据库服务器-MySQL: （1）数据库系统定义了相关重要数据； ■包括重要配置数据 （2）数据库系统定期完全依照备份策略，采用正确的配置进行本地备份； （3）系统的备份周期为：每天一次增量、每月一次全备； （4）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	应用/数据库服务器: （1）设备为服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、运维安全管理系统、防火墙-1、防火墙-2: （1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 应用/数据库服务器-MySQL:	不符合

安全控制点	测评指标	结果结论	符合程度
		(1)数据库系统未能提供异地数据备份功能。 应用/数据库服务器-Tomcat、档案管理系统: （1）单位未能提供异地数据备份措施。 业务终端-1、业务终端-2、运维及管理终端-1、运维及管理终端-2: （1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 核心交换机、汇聚交换机: （1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	重要配置数据不存在此部分的控制需求,故此项不适用	不适用
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	重要配置数据不存在此部分的控制需求,故此项不适用	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	重要配置数据不存在此部分的控制需求,故此项不适用	不适用

D.4.1.7 其他系统或设备

无

D.5 安全管理中心

D.5.1 安全通用要求

D.5.1.1 管理中心

安全控制点	测评指标	结果结论	符合程度
系统管理	a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；	（1）网络中部署运维安全管理系统实现集中的系统管理； （2）系统对登录用户进行身份鉴别； ■包括合规的用户名 ■包括合规的口令策略 （3）系统用户标识具有唯一性； ■不存在多人共享 ■增加、删除用户或权限变更需经过审批 （4）系统可实现对账户的身份鉴别数据进行保密性和完整性保护； （5）系统管理操作模式具备控制措施； ■只允许系统管理员登录	符合

安全控制点	测评指标	结果结论	符合程度
		■具备特定的登录命令 ■具备特定的登录操作界面 （6）系统具备相应的管理操作审计措施。 ■可实现对系统管理操作进行审计 ■审计范围覆盖所有用户 ■操作审计不可被删除	
	b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。	（1）系统管理员对系统的资源和运行进行配置、控制和管理； ■包括用户身份管理 ■包括资源配置管理 ■包括系统加载和启动管理 ■包括系统运行的异常处理管理 ■包括数据和设备的备份与恢复管理 （2）系统的资源、运行及配置管理不够全面。 ■缺乏可信证书管理 ■缺乏可信基准库管理	不符合
审计管理	a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；	（1）网络中部署运维安全管理系统实现集中安全审计功能； （2）审计系统对审计管理员进行身份鉴别； ■包括合规的用户名 ■包括合规的口令策略 （3）审计系统用户标识具有唯一性； ■不存在多人共享 ■增加、删除用户或权限变更需经过审批 （4）审计系统管理操作模式具备控制措施； ■只允许审计管理员登录 ■具备特定的登录命令 ■具备特定的登录操作界面 （5）审计系统具备相应的管理操作审计措施。 ■可实现对安全审计操作进行审计 ■审计范围覆盖所有审计管理用户 ■操作审计不可被删除	符合
	b）应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	档案管理系统: （1）审计管理员定期对审计记录进行分析，对发现的安全可疑事件及时处理； （2）单位具有安全审计策略文件，规范审计记录的存储、管理和查询要求； （3）审计管理员按规范要求对审计记录进行管理。 ■审计记录不可随意删除/修改 ■定期备份、存储审计记录 ■审计记录存储周期满足6个月要求	符合

安全控制点	测评指标	结果结论	符合程度
		重要审计数据: 日志审计系统、运维安全管理系统: （1）设备在通信传输过程中对相关数据采取完整性保护措施; ■包括重要审计数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■网络设备、安全设备使用rsyslog协议进行传输 ■Windows操作系统使用插件+SSL协议进行传输	

D.6 安全管理制度

D.6.1 安全通用要求

D.6.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。	（1）单位具有网络安全工作的总体方针和安全策略文件; ■具备独立的网络安全总体方针文件 ■具备涵盖网络安全总体方针策略要求的相关管理文件 ■具备安全策略文件 (2)制度内容包括明确的单位安全工作要求; ■安全目标 ■安全范围 ■安全原则 ■安全框架 ■各类安全策略 （3）管理文件详见《信息安全总体策略》。	符合
管理制度	a) 应对安全管理活动中的主要管理内容建立安全管理制度;	（1）单位有针对安全管理活动中的各类管理内容建立安全管理制度; (2)现有制度已覆盖管理活动的主要的方面; ■具备文件控制管理 ■具备安全检查管理 ■具备人力资源及培训 ■具备设备管理 ■具备软件开发/外包开发项目管理 ■具备机房安全管理 ■具备信息分类及管理 ■具备网络安全管理 ■具备系统安全管理 ■具备恶意代码管理	符合

安全控制点	测评指标	结果结论	符合程度
		■具备变更控制 ■具备备份及介质管理 ■具备事件管理 ■具备应急预案 （3）制度详见：《信息安全总体策略》、《网络安全管理规范》、《组织安全结构和人员职责制度》、《人员管理制度》、《员工考核管理制度》。	
	b）应对管理人员或操作人员执行的日常管理操作建立操作规程。	（1）单位针对相关业务日常管理的操作建立规程类管理制度； （2）现有制度已覆盖重要管理方面的系统维护手册和用户操作规程等； ■具备网络/安全管理 ■具备服务器管理 ■具备数据库管理 ■具备机房硬件设施管理 ■具备业务应用管理 （3）管理文件详见《设备及系统软件配置和操作手册》。	符合
制定和发布	a）应指定或授权专门的部门或人员负责安全管理制度的制定；	（1）单位针对安全管理制度的制定，指定教育信息与网络中心部主要负责； （2）在已制定的相关制度中可查阅到被授权制定管理制度的部门/人员信息； （3）管理文件详见《安全管理组织规范》。	符合
	b）安全管理制度应通过正式、有效的方式发布，并进行版本控制。	（1）单位针对制度的制定和发布要求，制定管理规范文件； （2）管理规范文件对文件制定及发布定义了规范要求； ■包括安全管理制度的制定和发布程序 ■包括格式要求 ■包括版本编号要求 （3）安全管理制度的收发登记记录有效； ■具备通过正式、有效的方式收发 ■具备正式发文 ■具备领导签署、单位盖章等 （4）管理文件详见《制度制定、发布、评审和修订管理制度》、《收发文登记记录》。	符合
评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	（1）单位针对制度的合理性和适用性需进行论证和审定及修订的要求，制定管理规范文件； （2）管理规范文件对制度的评审及修订定义了规范要求； （3）单位具有安全管理制度的审定或论证的	符合

安全控制点	测评指标	结果结论	符合程度
		过程记录； （4）单位对做过修订的制度，具备有修订版本的安全管理过程记录； （5）管理文件详见《制度制定、发布、评审和修订管理制度》及 《安全管理制度评审记录》。	

D.7 安全管理机构

D.7.1 安全通用要求

D.7.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
岗位设置	a）应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；	（1）单位已明确网络安全管理工作的职能部门，并明确了各岗位职责； ■已设置机房管理员 ■已设置网络管理员 ■已设置安全管理员 （2）单位各部门职责文档已明确网络安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备网络安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	符合
	b）应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。	（1）单位已明确系统安全管理工作的职能部门，并明确了各岗位职责； ■已设置系统管理员 ■已设置数据管理员 ■已设置审计管理员 ■已设置应用管理员 （2）单位各部门职责文档已明确系统安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备系统安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	符合
人员配备	应配备一定数量的系统管理员、审计管理员和安全管理员等。	（1）单位针对人员配备要求，制定了管理制度； （2）单位按要求配备一定数量的重要岗位管理人员； （3）单位针对各岗位人员，制定并维护人员档案； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	符合

安全控制点	测评指标	结果结论	符合程度
授权和审批	a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；	（1）单位在制度中用文字描述或在流程图中明确，对关键活动进行审批； ■具备部门职责文档明确各部门审批事项 ■具备岗位职责文档明确各岗位审批事项 （2）单位对审批过程明确审批权限，对各项信息系统的重要操作与变更明确审批部门和批准人； （3）管理文件详见《授权和审批管理规定》。	符合
	b) 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。	（1）单位针对各项业务操作及变更等建立了审批程序规定； ■包括系统变更 ■包括重要操作 ■包括物理访问 ■包括系统接入 （2）单位针对系统变更、系统接入、物理范围等事项已明确按审批程序执行,记录有批准人签字； （3）管理文件详见《授权和审批管理规定》。	符合
沟通和合作	a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；	（1）单位针对机构内部管理人员之间、部门之间的沟通与合作，制定了管理制度； （2）单位的管理制度规范了合作和沟通的方式和周期； （3）单位有组织机构内部人员联系表； （4）单位有定期召开信息安全会议，保存有会议纪要； （5）管理文件详见《安全教育和培训制度》、《技能培训记录》《外部联系表》。	符合
	b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；	（1）单位针对加强与外部单位的合作与沟通，制定了管理制度规定； ■包括公安机关 ■包括网络安全职能部门 ■包括职能监管机构 ■包括各类供应商 ■包括业界专家 ■包括安全组织 （2）单位能按要求与相关单位保持沟通合作，并提供相关单位联系方式和交流会议纪要； （3）管理文件详见《安全教育和培训制度》、《技能培训记录》、《外部联系表》。	符合
	c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	（1）单位建立了完善的对外联单位的联系列表； ■记录单位名称 ■记录合作内容	符合

安全控制点	测评指标	结果结论	符合程度
		■记录联系人 ■记录联系方式 （2）管理文件详见《外部联系表》。	
审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。	（1）单位针对定期开展常规安全检查，制定了管理制度； （2）单位对检查工作的范围、过程、要求等管理的比较完善； ■系统日常运行 ■系统漏洞 ■数据备份 ■包括敏感系统检查人员 （3）单位已按要求由安全管理员定期检查，检查内容需覆盖系统运行相关的管理活动，并能提供安全检查报告； （4）管理文件详见《安全审查和检查管理规范》； （5）单位开展的检查工作不够完善。 ■未定期检查	部分符合

D.8 安全管理人员

D.8.1 安全通用要求

D.8.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
人员录用	a）应指定或授权专门的部门或人员负责人员录用；	（1）单位授权专门的部门负责人员录用工作，制定了管理制度规范； （2）由人力资源保障科负责人员录用工作； （3）管理文件详见《人员管理制度》。	符合
	b）应对被录用人员的身份、安全背景、专业资格或资质等进行审查。	（1）单位针对人员录用过程，制定了明确要求，并形成人员安全管理制度； （2）单位现有管理制度明确说明录用人员应具备的条件； ■包括学历/学位要求 ■包括技术人员的专业技术要求 ■包括管理人员的安全管理要求 （3）单位按规定执行人员录用的相关审查过程； ■包括录用人身份 ■包括安全背景 ■包括专业资格 ■包括资质 （4）管理文件详见《人员管理制度》、《人员入职考核记录》。	符合

安全控制点	测评指标	结果结论	符合程度
人员离岗	应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。	（1）单位针对离岗人员权限终止及取回机构提供的各种设施的要求，制定了管理制度； （2）单位按规范开展对离岗人员的相关管理工作； ■明确负责部门 ■及时终止其访问权限 ■交还身份证件 ■交还软硬件设备 （3）管理文件详见《人员管理度》、《人员离岗申请表》、《离场信息资料交接表》。	符合
安全意识教育和培训	应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。	（1）单位针对人员安全培训及责任和惩戒措施，制定了管理制度； （2）单位已开展安全意识教育及岗位技能培训 ■具备明确培训周期 ■具备有效的培训方式 ■具备清晰的培训内容 ■具备考核要求 （3）管理文件详见《安全教育和培训制度》。	符合
外部人员访问管理	a）应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；	（1）单位针对外部人员物理访问，制定了外部人员访问管理文档； ■明确允许外部人员访问的范围 ■明确外部人员进入的条件 ■明确外部人员进入的访问控制措施 （2）单位具备有效的外部人员访问重要区域的书面申请文档； ■具有申请人 ■具有申请原因 ■具有范围 ■具有日期 ■具有批准人签字 （3）单位具备外部人员访问重要区域的登记记录； ■记录进入时间、 ■记录离开时间 ■记录访问区域 ■记录陪同人信息 （4）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。	符合
	b）应在外部人员接入受控网络访问系统前先提出书	（1）单位针对外部接入受控网络访问系统，制定了管理制度；	符合

安全控制点	测评指标	结果结论	符合程度
	面申请，批准后由专人开设账户、分配权限，并登记备案；	（2）单位具备外部人员接入受控网络前的申请审批流程； （3）单位具备外部人员接入及访问系统的书面申请文档； ■具有申请人 ■具有申请原因 ■具有访问权限 ■具有日期 ■具有批准人签字 （4）单位具备外部人员接入及访问系统的登记记录； ■记录访问权限 ■记录访问时限 ■记录账户 （5)管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。	
	c）外部人员离场后应及时清除其所有的访问权限。	（1）单位针对人员离场后的清理工作，制定了管理制度； （2)管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》； （3）单位未完全按管理规范开展人员离场后的清理工作。 ■缺乏清理记录 ■未及时清除离场后的所有访问权限 ■未记录访问权限清除时间	不符合

D.9 安全建设管理

D.9.1 安全通用要求

D.9.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
定级和备案	a）应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；	（1）单位的被测系统于2022年4月已完成备案； （2）系统备案相关文档（定级报告）中明确等级划分方法和理由,SAG三个方面的级别描述清晰； （3）管理文件详见《定级备案》。	符合
	b）应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论	（1）单位针对系统定级结果的审批及评审工作等要求，制定了管理制度； （2）现有系统的定级已具备合理性和正确性	符合

安全控制点	测评指标	结果结论	符合程度
	证和审定；	审定； ■具备单位部门审定 （3）管理文件详见《定级备案》。	
	c）应保证定级结果经过相关部门的批准；	（1）单位针对系统定级结果的上级批准要求，制定了管理制度； （2）现有系统的定级获得了相关部门的批准； （3）管理文件详见《定级备案》。	符合
	d）应将备案材料报主管部门和相应公安机关备案。	（1）单位对被测系统的等级备案表、定级报告等备案材料已经报相应公安机关备案； （2）单位具备公安机关出具的备案号； （3）管理文件详见《定级备案》。	符合
安全方案设计	a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；	（1）单位未具备适用于被测系统的安全规划设计方案； （2）现有方案文档未能完全按照规范要求选择安全措施。 ■缺乏安全保护等级的要求 ■缺乏风险分析结果的要求 ■缺乏实际安全需求	不符合
	b）应根据保护对象的安全保护等级进行安全方案设计；	（1）单位未具备完整的安全设计方案相关的文档。 ■缺乏总体规划 ■缺乏安全设计方案 ■缺乏相关配套文件 ■缺乏保护对象的安全保护等级要求	不符合
	c）应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； ■缺乏安全整体规划 ■缺乏安全设计方案 ■缺乏安全配套文件 （2）单位未对相关论证过程及内容进行完整的记录。	不符合
产品采购和使用	a）应确保网络安全产品采购和使用符合国家的有关规定；	（1）单位已建立安全产品管理的相关管理规定； ■包括采购要求 ■包括使用要求 （2）单位具备安全产品采购流程及相关实施文档； （3）被测系统使用的安全产品具备销售许可资质； （4）安全产品具均为国内产品； （5）管理文件详见《设备安全管理制度》。	符合
	b）应确保密码产品与服务的采购和使用符合国家密	（1）单位已建立密码产品与服务管理的相关管理制度；	符合

安全控制点	测评指标	结果结论	符合程度
	码管理主管部门的要求。	■包括采购要求 ■包括使用要求 （2）系统未使用密码产品； （3）管理文件详见《设备安全管理制度》。	
自行软件开发	a）应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。	不适用
	b）应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。	不适用
外包软件开发	a）应在软件交付前检测其中可能存在的恶意代码；	（1）单位针对软件交付前测试恶意代码的要求，制定了管理制度； （2）管理文件详见《外包开发软件管理规定》； （3）单位未在软件交付之前按要求对所有软件开展恶意代码检测。 ■缺乏恶意代码检测报告	不符合
	b）应保证开发单位提供软件设计文档和使用指南。	（1）单位制定软件开发项目验收要求，明确开发单位的提交材料； （2）开发单位提供软件日常维护和使用所需的文档； ■包括需求分析说明书 ■包括软件设计说明书 ■包括软件操作手册 （3）管理文件详见《外包开发软件管理规定》、《设备及系统软件配置和操作手册》。	符合
工程实施	a）应指定或授权专门的部门或人员负责工程实施过程的管理；	（1）单位针对专门的部门负责工程实施过程的管理要求，制定管理度； （2）单位由专岗负责系统建设的工程实施，且按照实施方案的要求对进度和质量进行控制； （3）管理文件详见《工程实施管理制度》。	符合
	b）应制定安全工程实施方案控制工程实施过程。	（1）单位制定了详细的工程实施方案； ■包括工程时间限制 ■包括进度控制 ■包括质量控制 （2）工程实施单位严格按照方案执行，并有过程记录； （3）管理文件详见《测试及验收方案》、《工程项目实施方案》。	符合
测试验收	a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收	（1）单位可提供被测系统的合规测试验收方案； ■包括测试人员	部分符合

安全控制点	测评指标	结果结论	符合程度
	报告；	■包括测试验收内容 ■包括现场操作过程 （2）管理文件详见《测试及验收方案》、《工程项目实施方案》； （3）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。 ■缺乏验收报告 ■缺乏报告审定意见	
	b）应进行上线前的安全性测试，并出具安全测试报告。	（1）单位对系统上线前需开展安全性测试的要求，制定管理制度； （2）管理文件详见《外包开发软件管理规定》、《系统交付管理》； （3）针对系统上线前的安全性测试工作存在问题。 ■缺乏测试报告	不符合
系统交付	a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；	（1）单位具备系统交付清单； （2）系统交付清单内容较详细； ■包括设备 ■包括软件 ■包括文档 （3）单位的清点工作较合规； ■已依据交付清单开展清点工作 （4）管理文件详见《系统交付管理》、《资产清单》。	符合
	b）应对负责运行维护的技术人员进行相应的技能培训；	（1）单位已对负责系统运行维护的技术人员进行了技能培训； （2）具备运维人员的培训记录； ■包括培训时间 ■包括培训地点 ■包括培训对象 ■包括培训内容 ■包括培训参与人员签字 （3）管理文件详见《系统交付管理》、《资产清单》、《系统交付清单》、《技能培训记录》。	符合
	c）应提供建设过程文档和运行维护文档。	（1）单位提供了系统建设过程中的文档； （2）单位提供了指导用户进行系统运维的文档和系统培训手册； （3）管理文件详见《系统交付管理》、《系统交付清单》、《设备及系统软件配置和操作手册》。	符合
等级测评	a）应定期进行等级测评，发现不符合相应等级保护	（1）单位针对系统等级测评要求，制定管理制度；	符合

安全控制点	测评指标	结果结论	符合程度
	标准要求的及时整改；	（2）系统按要求开展首次测评工作； （3）管理文件详见《系统安全管理制度》。	
	b）应在发生重大变更或级别发生变化时进行等级测评；	（1）管理制度中已规定在系统发生变更时及时对系统进行等级测评； （2）系统未发生过重大变更，系统等级未发生变化； （3）管理文件详见《系统安全管理制度》。	符合
	c）应确保测评机构的选择符合国家有关规定。	（1）已选择在“全国等级保护测评机构推荐目录”中的测评单位进行等级测评； （2）管理文件详见《系统安全管理制度》、《网络安全等级保护测评服务合同》。	符合
服务供应商选择	a）应确保服务供应商的选择符合国家的有关规定；	（1）单位在管理制度内明确提出安全服务供应商选择的要求； （2）单位选择的安全服务商符合国家的有关规定，具备相应的安全服务资质； （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。	符合
	b）应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。	（1）单位的管理制度中已规定，需与安全服务商签订安全相关的协议并明确整个服务供应链各方需履行的网络安全相关义务； （2）单位已按规定与选定的安全服务商签订合规的协议； ■明确整个服务供应链各方需履行的网络安全相关义务 ■包括保密范围 ■包括安全责任 ■包括违约责任 ■包括协议的有效期限 ■包括责任人签字 （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。	符合

D.10 安全运维管理

D.10.1 安全通用要求

D.10.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
环境管理	a）应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；	（1）单位建立机房安全方面的管理制度，对有关运维方面的管理作出规定； ■指定教育信息与网络中心部门负责管理 ■包括出入管理要求 ■包括定期维护要求 ■包括空调要求	符合

安全控制点	测评指标	结果结论	符合程度
		■包括供配电设备要求 ■包括消防设施要求 ■包括温湿度控制要求 （2）单位具备完整的机房出入登记记录； ■记录来访人员 ■记录来访时间 ■记录离开时间 ■记录携带物品 （3）单位具备完整的机房基础设施的维护记录； ■记录维护日期 ■记录维护人 ■记录维护设备 ■记录故障原因 ■记录维护结果 （4）管理文件详见《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。	
	b）应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；	（1）单位建立机房安全方面的管理制度； ■包括物理访问管理 ■包括物品进出管理 ■包括环境安全管理 （2）单位现有机房管理记录与制度相符； ■具备物理访问记录 ■具备物品进出记录 ■具备环境安全相关记录 （3）制度详见：《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。	符合
	c）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	（1）单位机房安全管理制度已明确来访人员的接待区域的要求； （2）单位按规范要求开展人员来访接待； ■划分来访人员的接待区域 ■记录来访人员的情况 （3）单位办公环境未发现有随意放置含有敏感信息介质的情况； ■无纸档文件 ■无移动介质 （4）制度详见：《机房安全管理制度》、《物理安全管理规范》、《办公环境保密管理》。	符合
资产管理	应编制并保存与保护对象	（1）单位已建立有效的资产清单；	符合

安全控制点	测评指标	结果结论	符合程度
	相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。	（2）单位现有资产清单内容较全面； ■包括设备设施类别 ■包括软件类别 ■包括文档类别 ■包括资产责任人 ■包括所属级别 ■包括所处位置 ■包括所处部门 （3）制度详见：《设备安全管理制度》、《资产清单》。	
介质管理	a）应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；	（1）介质按管理要求放置于受控的环境中（如：机房）； （2）介质管理具备较全面的记录； ■包括介质归档 ■包括使用情况 ■包括定期盘点记录 （3）制度详见：《设备安全管理制度》、《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。	符合
	b）应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。	（1）介质管理制度中对介质安全传输有明确规定； ■包括人员选择 ■包括打包要求 ■包括交付要求 （2）存储重要信息的介质在物理传输过程，具备严格的环节控制，无重大环节疏漏； （3）对介质的归档和查询均具备记录； （4）制度详见：《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。	符合
设备维护管理	a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	（1）单位人员岗位职责相关文档已明确设备维护管理的责任部门； （2）单位对各类设施、设备进行定期维护； （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。	符合
	b）应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。	（1）单位建立了配套设施、软硬件维护管理方面的管理制度； ■包括维护人员的责任 ■包括维修和服务的审批 ■包括维修过程的监督控制	符合

安全控制点	测评指标	结果结论	符合程度
		（2）单位开展相关工作与制度相符，且保留记录； ■包括维修和服务审批 ■包括维修过程记录 （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。	
漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。	（1）单位制定管理制度，规范对安全漏洞和隐患的检测、识别及评估修补要求； （2）制度详见：《恶意代码防范管理制度》； （3）单位未严格按规范开展漏洞及安全隐患检测工作。 ■未定期开展漏洞扫描	不符合
网络和系统安全管理	a）应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；	（1）单位建立系统安全管理文档，对系统管理员的管理制定了要求； ■包括角色划分 ■包括角色的责任 ■包括角色权限 （2）单位对各类关键角色建立了相应的工作职责文档； ■包括安全管理员 ■包括网络管理员 ■包括系统管理员 ■包括数据管理员 ■包括审计管理员 （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	符合
	b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	（1）单位制定管理制度，对系统账号进行管理； ■指定专人 ■包括申请账户管理 ■包括建立账户管理 ■包括删除账户管理 （2）单位按管理规范开展账号管理工作； ■具备相关审批流程 ■具备相关审批记录 ■具备管理登记记录 （3）账户管理记录内容较完整； ■包括变更日期 ■包括变更时间 ■包括变更人 ■包括变更设备/系统 ■包括变更结果	符合

安全控制点	测评指标	结果结论	符合程度
		（4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	
	c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	（1）单位建立了网络和系统安全管理制度； （2）网络和系统安全管理制度内容较全面； ■包括安全策略要求 ■包括账户管理 ■包括配置文件的生成及备份 ■包括变更审批管理 ■包括授权访问 ■包括最小服务控制 ■包括升级与打补丁管理 ■包括审计日志管理 ■包括口令管理 （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	符合
	d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；	（1）单位对重要设备、系统的配置和操作建立配置手册； ■包括操作系统 ■包括数据库 ■包括网络设备 ■包括安全设备 ■包括应用和组件 （2）现有操作配置手册已明确操作步骤、参数配置； （3）制度详见：《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。	符合
	e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。	(1)单位制定日常运维管理的相关制度规范； (2)单位按制度规范开展日常运维管理工作； （3）单位具备合规的运维记录； ■包括日常巡检记录 ■包括运行维护记录 ■包括参数的设置记录 ■包括参数的修改记录 （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》、《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。	符合
恶意代码防范管理	a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	（1）单位制定恶意代码防范管理制度，明确对外来计算机或存储设备接入系统前进行恶意代码检查； （2）单位按外来计算机接入恶意代码检查规范开展工作； ■对外来计算机接入进行恶意代码检查	符合

安全控制点	测评指标	结果结论	符合程度
		■具备合规的检测记录 （3）单位制定培训管理制度，明确需通过培训提升员工的防恶意代码意识； （4）单位按培训管理要求开展工作； ■定期对员工开展防恶意代码意识培训 ■具备合规的培训记录 （5）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申请表》、《信息管理系统漏洞检查表》。	
	b）应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；	（1）建立恶意代码防范管理文档； （2）管理制度中覆盖防恶意代码软件的授权使用、恶意代码库升级、定期查杀等内容； （3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》。	符合
	c）应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。	（1）单位指定专门的部门负责定期验证防范恶意代码攻击的技术措施的有效性； （2）单位近期未发生过严重的恶意代码攻击事件； （3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申请表》、《信息管理系统漏洞检查表》； （4）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。 ■未定期对相关产品的恶意代码库进行升级 ■未对所有防病毒产品上截获的恶意代码进行分析并汇总上报	部分符合
配置管理	应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。	（1）单位制定了基本配置信息管理的制度要求； ■包括网络拓扑结构 ■包括设备安装的软件组件 ■包括软件组件的版本 （2）管理文件详见：《主机安全管理规范》、《网络安全管理规范》、《应用安全管理规范》、《网络配置信息》。	符合
密码管理	a）应遵循密码相关国家标准和行业标准；	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	不符合
	b）应使用国家密码管理主管部门认证核准的密码技术和产品。	（1）单位未采购涉及密码技术的产品，不适用。	不适用
变更管理	应明确变更需求，变更前根据变更需求制定变更方	（1）单位建立了关于系统变更管理的制度文件；	符合

安全控制点	测评指标	结果结论	符合程度
	案，变更方案经过评审、审批后方可实施。	（2）现有变更管理制度覆盖了变更管理的各方面要求； ■包括变更管理要求 ■包括整体变更管理流程 ■包括变更内容分析与论证 ■包括变更方案审批流程 ■包括变更后通报 （3）制度详见：《变更控制管理制度》、《通用变更记录表》。	
备份与恢复管理	a）应识别需要定期备份的重要业务信息、系统数据及软件系统等；	（1）单位根据业务重要程度，制定了需要定期备份的重要业务信息列表或清单。清单内需要定期备份的重要数据已经过用户方确认； （2）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。	符合
	b）应规定备份信息的备份方式、备份频度、存储介质、保存期等；	（1）单位建立了备份与恢复管理相关的安全管理制度； （2）备份与恢复管理的相关要求比较明确； ■规定备份方式 ■规定备份频度 ■规定存储介质 ■规定保存期 （3）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。	符合
	c）应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	（1）单位现有管理制度，明确了数据备份策略和数据恢复策略，以及备份程序和恢复程序； （2）单位可按策略要求实现重要数据的定期备份与恢复性测试； （3）单位现有的备份的数据均经过恢复性测试，可确保备份的数据可用； （4）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。	符合
安全事件处置	a）应及时向安全管理部门报告所发现的安全弱点和可疑事件；	（1）单位已在安全培训及宣传过程中告知用户在发现安全弱点和可疑事件时及时向安全管理部门报告； （2）单位在系统运维过程中对发现的安全弱点和可疑事件均编制了对应的报告或相关文	符合

安全控制点	测评指标	结果结论	符合程度
		档； （3）单位现有安全弱点和可疑事件报告文档内容较详实； （4）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	
	b）应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；	（1）单位制定了安全事件报告和处置管理制度； （2）现有安全事件管理制度内容较完整； ■包括安全事件类型分类 ■包括安全事件有关的工作职责 ■包括安全事件的报告 ■包括安全事件的处置 ■包括安全事件的响应流程 （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	符合
	c）应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。	（1）单位具备对安全事件的分析、处理、总结、防范等的报告／过程文档； （2）单位提供的安全事件报告和响应处置记录内容较完整； ■记录引发安全事件的原因 ■记录事件的证据 ■记录处置过程 ■包括经验教训 ■提出补救措施 （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	符合
应急预案管理	a）应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；	（1）单位制定重要事件的应急预案； （2）单位现有应急预案涉及的类型范围较全面； ■包括针对机房的预案 ■包括针对网络传输的预案 ■包括针对网络设备的预案 ■包括针对操作系统的预案 ■包括针对数据库的预案 ■包括针对安全漏洞攻击的预案 ■包括针对恶意代码的预案 ■包括针对数据泄露的预案 （3）单位现有应急预案的内容较完整； ■明确重要事件的应急处理流程 ■明确系统恢复流程等内容 （4）制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。	符合
	b）应定期对系统相关的人	（1）单位定期对相关人员进行应急预案培训；	符合

安全控制点	测评指标	结果结论	符合程度
	员进行应急预案培训，并进行应急预案的演练。	（2）单位根据不同的应急预案，按要求进行应急演练； （3）单位具备近期应急预案工作开展的相关记录； ■具备培训记录 ■具备演练记录 （4）单位提供的应急预案培训记录比较完整； ■明确培训对象 ■明确培训内容 ■明确培训结果 （5）单位提供的应急预案演练记录比较完整； ■记录演练时间 ■记录主要操作内容 ■记录演练结果 （6）经检查单位目前一旦出现应急事件，可参照预案合理有序的进行应急事件处置过程； （7）制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。	
外包运维管理	a）应确保外包运维服务商的选择符合国家的有关规定；	（1）单位目前未涉及任何外包运维服务情况，不适用。	不适用
	b）应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。	（1）单位目前未涉及任何外包运维服务情况，不适用。	不适用

D.11 其他安全要求

本次测评不涉及其他安全要求指标。

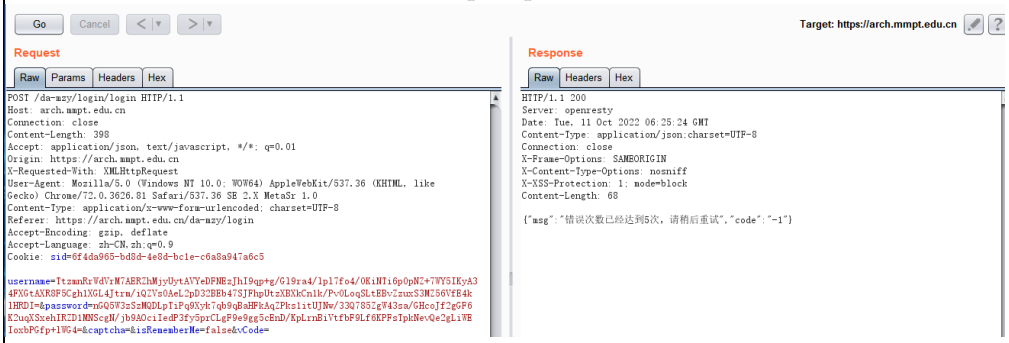
附录E 漏洞扫描结果记录

附录E表-1漏洞扫描主要安全漏洞

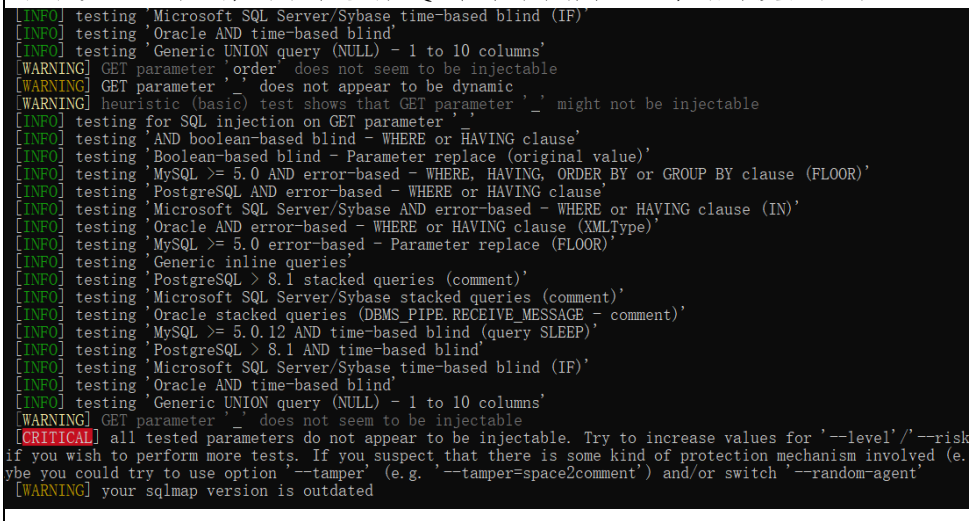
序号	危险程度	漏洞名称	影响IP
1	低	允许Traceroute探测 此类漏洞涉及服务器存储设备、安全设备、网络设备。	10.2.4.11/应用/数据库服务器 10.2.1.4/运维安全管理系统 10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/上网行为管理系统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/汇聚交换机 172.16.1.2/核心交换机
2	低	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161) 此类漏洞涉及网络设备。	172.16.1.2/核心交换机

附录F 渗透测试结果记录

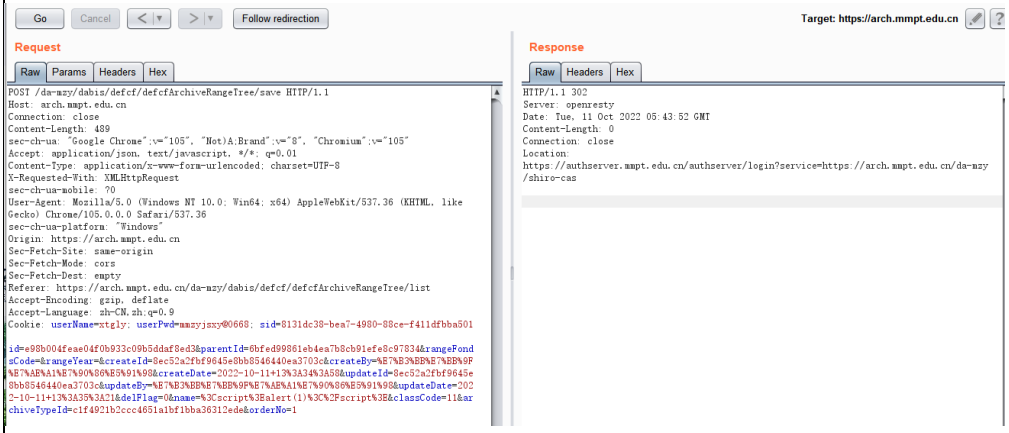
F.1 业务应用软件平台 缺少“X-Content-Type-Options”响应头

缺少“X-Content-Type-Options”响应头	
危险程度	低
渗透位置	JB,JC
影响URL实体	https://arch.mmpt.edu.cn/da-mzy/login/login
渗透详情	渗透方法：BurpSuite抓包检测 采用的工具：BurpSuite 测试过程：响应包中没有X-Content-Type-Options响应头，如下图： 

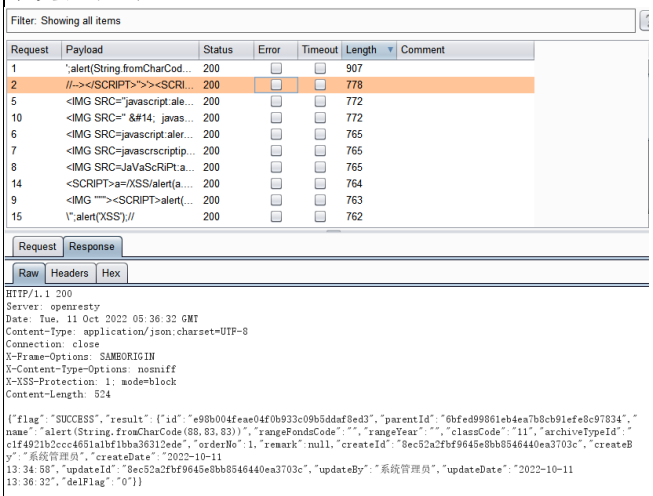
F.2 业务应用软件平台 SQL注入漏洞

SQL注入漏洞	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：通过手工或工具检测系统在执行SQL语句时是否存在注入。 采用的工具：Sqlmap 测试过程：已检测，系统在执行SQL语句时不存在注入，暂未发现该漏洞。 

F.3 业务应用软件平台　未授权访问

未授权访问	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：测试能否在系统未登录的状态下进行登录后功能访问或操作。 采用的工具：Burpsuite 测试过程：已检测，不能在系统未登录的状态下进行功能访问或操作。 

F.4 业务应用软件平台　XSS跨站脚本攻击

XSS跨站脚本攻击	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：测试是否对客户端输入的HTML代码、客户端脚本进行过滤或限制。 采用的工具：Burpsuite 测试过程：经检测，已对客户端输入的HTML代码、客户端脚本进行过滤或限制，暂未发现该漏洞。 

附录G 威胁列表

附录G 表- 1威胁列表

序号	威胁列表	描述
1	恶意攻击	利用工具和技术对信息系统进行攻击和入侵。威胁行为包括：恶意代码、邮件勒索、网络攻击等。
2	软硬件故障	对业务实施或系统运行产生影响的设备硬件故障、通讯链路中断、系统本身或软件缺陷造等问题。威胁行为包括：设备故障、软件故障等。
3	管理不到位	由于制度缺失、不完善等原因导致安全管理无法落实或者不到位。威胁行为包括：管理不到位、媒体负面报道等。
4	无作为或操作失误	应该执行而没有执行相应的操作，或者无意执行了错误的操作。威胁行为包括：操作失误、维护错误等。
5	敏感信息泄漏	敏感信息泄露给不应了解的他人。威胁行为包括：内部信息泄露、外部信息泄露等。
6	物理环境影响	对信息系统正常运行造成影响的物理环境问题和自然灾害。威胁行为包括：物理损害等。
7	越权或滥用	越权访问本来无权访问的资源，或者滥用自己的权限破坏信息系统。威胁行为包括：未授权的设备使用、权限滥用、权限伪造等。
8	物理攻击	通过物理的接触造成对软件、硬件和数据的破坏。威胁行为包括：设备失效等。
9	篡改	非法修改信息，破坏信息的完整性使系统的安全性降低或信息不可用。威胁行为包括：硬件篡改、数据篡改等。
10	抵赖	否认所做的操作。威胁行为包括：行为否认（抵赖）、媒体负面报道等。

报告编号： 44090243008-00006-22-0163-01

网络安全等级保护
教学管理信息服务平台等级测评报告

委托单位： 茂名职业技术学院

测评单位： 广东南方信息安全研究院

报告时间： 2022年10月30日

网络安全等级测评基本信息表

被测对象				
被测对象名称	教学管理信息服务平台		安全保护等级	第二级（S2A2）
备案证明编号	44090243008-00006			
被测单位				
单位名称	茂名职业技术学院			
单位地址	广东省茂名市茂南区文明北路232号大院		邮政编码	525000
联系人	姓名	龙恒	职务/职称	教师
	所属部门	教育信息与网络中心	办公电话	0668-2920122
	移动电话	13377766618	电子邮件	372383968@qq.com
测评单位				
单位名称	广东南方信息安全研究院		机构代码	SC202127130010163
单位地址	广州市科学城彩频路9号B座12楼1202		邮政编码	510663
联系人	姓名	谢若雨	职务/职称	助理
	所属部门	办公室	办公电话	020-32290702
	移动电话	18819149895	电子邮件	office@cybersec-gd.cn
审核批准	编制人	林炳良	编制日期	2022.10.30
	审核人	王络	审核日期	2022.10.30
	批准人	王东林	批准日期	2022.10.30

声明

本报告是教学管理信息服务平台的等级测评报告。

本报告测评结论的有效性建立在被测评单位提供相关证据的真实性基础之上。

本报告中给出的测评结论仅对被测对象当时的安全状态有效。当测评工作完成后，由于被测对象发生变更而涉及到的系统构成组件（或子系统）本报告不再适用。

本报告中给出的测评结论不能作为对被测对象内部部署的相关系统构成组件（或产品）的测评结论。

在任何情况下，若需引用本报告中的测评结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。

单位名称：广东南方信息安全研究院

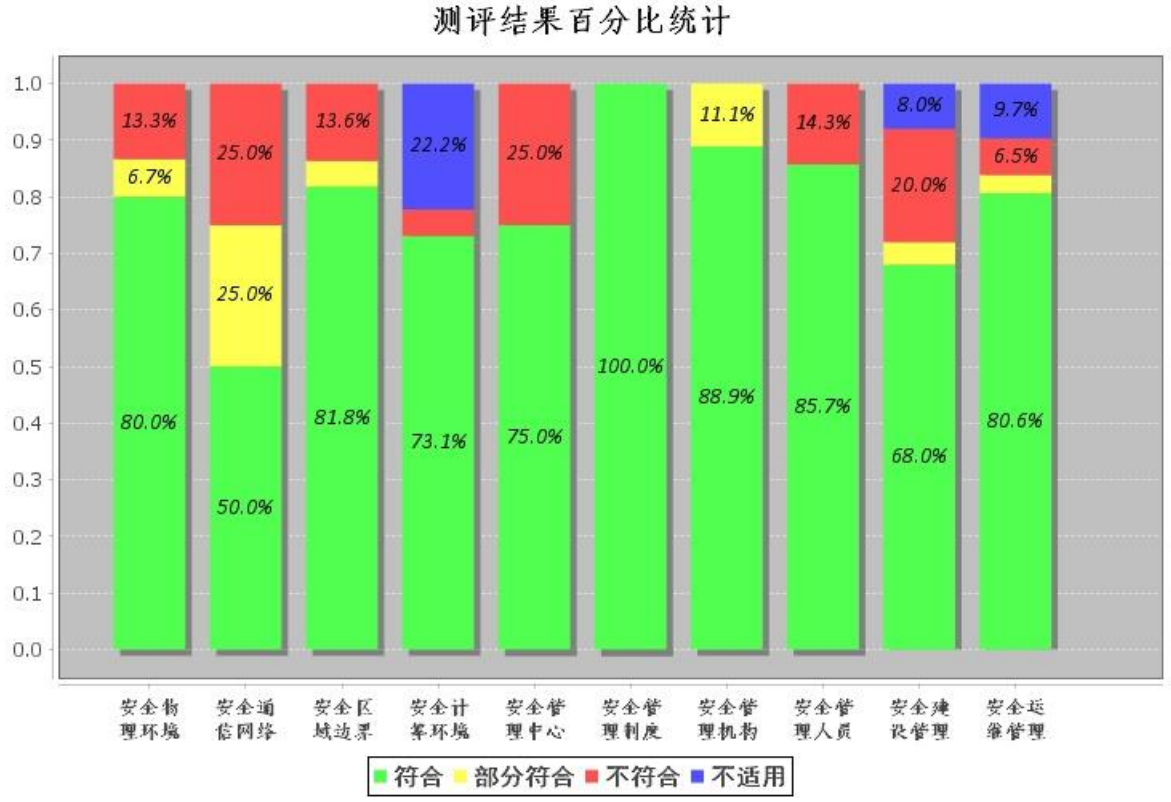
2022年10月30日

等级测评结论

测评结论和综合得分			
被测对象名称	教学管理信息服务平台	安全保护等级	第二级（S2A2）
扩展要求应用情况	□云计算 □移动互联 □物联网 □工业控制系统 □大数据		
被测对象描述	教学管理信息服务平台是由茂名职业技术学院统一组织规划建设，由正方软件股份有限公司负责开发，于2021年9月正式投入运行，由教育信息与网络中心负责运行维护。茂名职业技术学院是该信息系统的业务主管部门，茂名职业技术学院为该信息系统定级的责任单位。 教学管理信息服务平台网络主要分为4个区域，分别为外网边界区域、安全管理区域、服务器存储区域、办公网区域，主要由网络设备、安全设备组成，对互联网提供业务访问。教学管理信息服务平台为B/S结构，主要由Linux平台的操作系统，Orcale平台的数据库系统，及Tomcat中间件系统组成。单位采用自主运维模式，通过部署运维及管理终端提供专用运维环境管理，采用运维安全管理系统实现设备的统一管理，并进行操作运维审计，日志审计系统进行设备日志统一收集存储与分析。 教学管理信息服务平台主要实现教务管理服务，系统包括系统管理、学籍管理、师资管理、教学计划、排课管理、选课管理、成绩管理、考试管理、毕业管理、教学评价等功能模块。教学管理信息服务平台以培养、运行、保障、监控为主线，实现教务工作事务性管理和战略性管理的相互叠加，实现学校培养过程管理、教学质量检查、教学工作管理等日常教学事务管理。		
安全状况描述	教学管理信息服务平台通信传输具备一定的保护措施，安全区域边界较清晰，网络层具备访问控制、安全审计的相应技术措施。各设备在身份鉴别、访问控制、安全审计、入侵防范方面具备控制措施。重要数据在数据完整性、个人信息保护方面具备保护措施。在安全管理制度层面较为完善。在网络架构不够完整，网络层在入侵防范、恶意代码和垃圾邮件防范的技术措施存在不足。重要数据在数据备份恢复方面存在不足。 教学管理信息服务平台在本次测评中总共出现27类问题，其中0类高风险问题,11类中风险问题，16类低风险问题。在本次测评通过扫描及渗透发现3类漏洞问题，其中0类危险程度为高的漏洞，0类危险程度为中的漏洞，3类危险程度为低的漏洞。 教学管理信息服务平台本次等级测评的综合得分为73.85，且不存在高等级安全风险，等级测评结论为中。		
等级测评结论	中	综合得分	73.85

总体评价

通过对信息系统基本安全保护状态的分析，茂名职业技术学院针对教学管理信息服务平台面临的主要安全威胁采取了相应的安全机制，基本达到保护信息系统重要资产的作用。教学管理信息服务平台在本次测评中采用了GB/T 22239-2019，其中安全通用要求135项，不适用5项。



在安全物理环境方面，针对安全通用要求，基础设施在防雷击、电磁防护、防水和防潮、物理位置选择、电力供应、防盗窃和防破坏、温湿度控制等方面较为完善（如：信息化机房）。在物理访问控制、防静电等方面还不够完善（如：信息化机房），机房出入口未配置电子门禁系统，机房内缺乏防静电措施（如防静电地板或铺设防静电地毯）。

在安全通信网络方面,针对安全通用要求,网络环境在通信传输等方面较为完善(如:安全通信网络)。在网络架构等方面还不够完善（如：安全通信网络），关键的应用服务和数据库服务网段未独立进行子网划分的情况。

在安全区域边界方面，针对安全通用要求，网络环境在边界防护、安全审计、访问控制等方面较为完善（如：外网边界区域，安全管理区域，服务器存储区域等）。在入侵防范、恶意代码和垃圾邮件防范等方面还不够完善(如:安全管理区域,办公网区域)，网络层部署防火墙,防火墙未配置对内部发起的攻击行为实现防范功能策略,无法检测、防止或限制从内部发起的网络攻击行为,现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。

在安全计算环境方面，针对安全通用要求，计算环境在个人信息保护、安全审计、数据完整性、访问控制、入侵防范、恶意代码防范、身份鉴别、剩余信息保护等方面较为完善。在主机方面，在可信验证等方面还不够完善（如：业务终端-2，业务终端-1，运维及管理终端-2等），缺乏对计算设备可信验证方面的安全设计要求，现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。在应用方面，在数据备份恢复等方面还不够完善（如：应用服务器-1-Tomcat，应用服务器-2-Tomcat），未能提供中间件重要数据的异地定时数据备份功能。在网络及安全设备方面，在可信验证等方面还不够完善（如：基线核查系统，上网行为管理系统，WEB应用防火墙等），设备不具备相关可信验证的技术措施。在数据保护方面，在数据备份恢复等方面还不够完善（如：重要个人信息，重要业务数据），未能提供应用软件系统重要数据的异地定时数据备份功能。

在安全管理中心方面，针对安全通用要求，安全控制措施在审计管理等方面较为完善（如：管理中心）。在系统管理等方面还不够完善（如：管理中心），系统管理的资源、运行及配置管理不够全面。

在安全管理制度方面，针对安全通用要求，管理制度体系在制定和发布、安全策略、管理制度、评审和修订等方面较为完善（如：制度文件、执行/记录文件）。

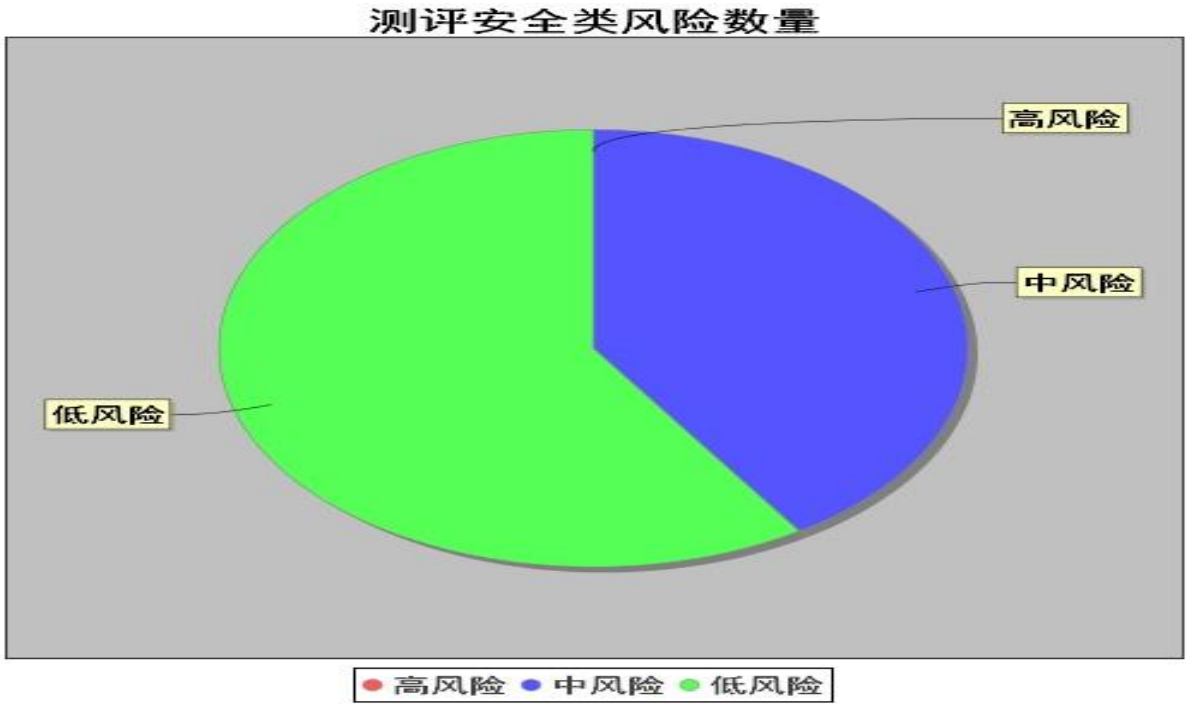
在安全管理机构方面，针对安全通用要求，机构建设在人员配备、沟通和合作、授权和审批、岗位设置等方面较为完善（如：制度文件、执行/记录文件）。在审核和检查等方面还不够完善（如：制度文件、执行/记录文件），单位开展的检查工作不够完善。

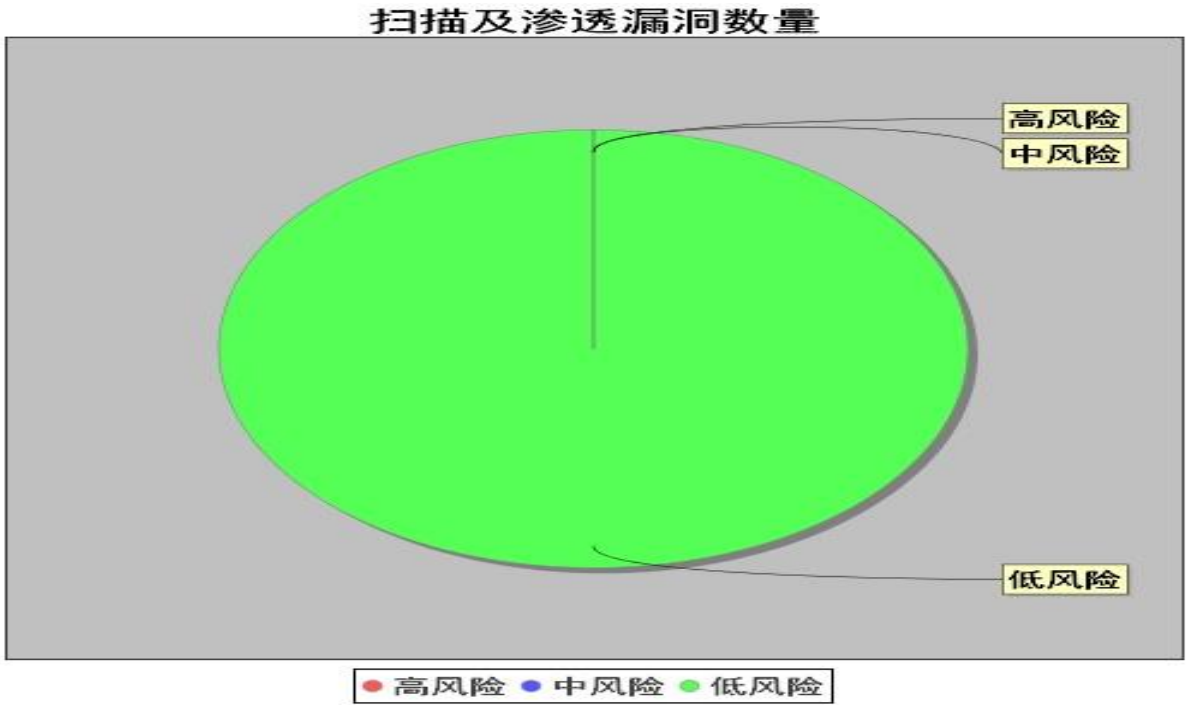
在安全管理人员方面，针对安全通用要求，人员在人员录用、安全意识教育和培训、人员离岗等方面较为完善（如：制度文件、执行/记录文件）。在外部人员访问管理等方面还不够完善（如：制度文件、执行/记录文件），单位未完全按管理规范开展人员离场后的清理工作。

在安全建设管理方面，针对安全通用要求，系统建设在定级和备案、工程实施、等级测评、产品采购和使用、服务供应商选择、系统交付等方面较为完善（如：制度文件、执行/记录文件）。在安全方案设计等方面还不够完善（如：制度文件、执行/记录文件），单位未具备完整的安全设计方案相关的文档，单位相关方案的设计的内容不够完善。

在安全运维管理方面，针对安全通用要求，系统运维在介质管理、设备维护管理、网络和系统安全管理、备份与恢复管理、资产管理、应急预案管理、环境管理、配置管理、安全事件处置、变更管理等方面较为完善（如：制度文件、执行/记录文件）。在密码管理等方面还不够完善（如：制度文件、执行/记录文件），单位不了解现有密码相关的国家标准和行业标准，单位缺乏密码管理要求的制度文档。

教学管理信息服务平台在本次测评中总共出现27类问题，其中0类高风险问题,11类中风险问题，16类低风险问题。在本次测评通过扫描及渗透发现3类漏洞问题，其中0类危险程度为高的漏洞，0类危险程度为中的漏洞，3类危险程度为低的漏洞。





教学管理信息服务平台本次等级测评的综合得分为73.85，且不存在高等级安全风险，等级测评结论为中。

主要安全问题及整改建议

一、安全物理环境

安全通用要求

(1)中风险 机房出入口未配置电子门禁系统（如：信息化机房）。 上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域,可能对系统的平稳运行造成影响。

建议安排专人7*24小时负责机房出入，对出入的人员进行身份鉴别和登记，且出入有专人陪同或在机房出入口配置电子门禁系统，控制、鉴别和记录进入的人员。

(2)中风险 机房内缺乏防静电措施（如防静电地板或铺设防静电地毯 ）（如：信息化机房）。 存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。

建议采用防静电地板或地面并采用必要的接地防静电措施。

二、安全通信网络

安全通用要求

(1)中风险 关键的应用服务和数据库服务网段未独立进行子网划分的情况（如：安全通信网络）。 上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变得更为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。

建议独立划分出应用服务器网段、数据库服务器网段。

三、安全区域边界

安全通用要求

(1)中风险 网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为（如：办公网区域）。 存在不

能及时发现内部主机作为攻击跳板，或网络攻击行为而造成系统损坏/网络资源浪费的风险。

建议网络层部署的防火墙配置对内部发起的攻击行为实现防范功能策略，实现检测、防止或限制从内部发起的网络攻击行为。

(2)中风险 现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面（如：办公网区域）。 无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。

建议现有部署的恶意代码防范措施网络边界覆盖全面，及时对恶意代码及逆行检测和清除。

四、安全计算环境

1、网络设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

2、安全设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

3、服务器和终端

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

4、系统管理软件/平台

安全通用要求

(1)中风险 未能提供中间件重要数据的异地定时数据备份功能（如：应用服务器

-1-Tomcat）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。

建议利用通信网络将中间件关键数据定时批量传送至备用场地，实现异地数据异地备份。

5、业务应用系统/平台

安全通用要求

(1)中风险 未能提供应用软件系统重要数据的异地定时数据备份功能（如：教学管理信息服务平台）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。

建议利用通信网络将应用软件系统关键数据定时批量传送至备用场地，实现异地数据异地备份。

6、数据资源

安全通用要求

重要业务数据

(1)中风险 未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要业务数据）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。

建议利用通信网络将应用软件系统关键数据定时批量传送至备用场地，实现异地数据异地备份。

重要个人信息

(1)中风险 未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要个人信息）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会

影响到业务服务的持续提供。

建议利用通信网络将应用软件系统关键数据定时批量传送至备用场地，实现异地数据异地备份。

7、其他系统或设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

五、安全管理中心

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

六、安全管理制度

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

七、安全管理机构

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

八、安全管理人员

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

九、安全建设管理

安全通用要求

(1)中风险 单位未具备完整的安全设计方案相关的文档。单位相关方案的设计的内容不够完善（如：制度文件、执行/记录文件）。 相关合规的规划配套文件缺失，可能导

致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。

建议根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件。

十、安全运维管理

安全通用要求

(1)中风险 **单位不了解现有密码相关的国家标准和行业标准。单位缺乏密码管理要求的制度文档（如：制度文件、执行/记录文件）。 密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不到位，存在违反国家政策的风险。**

建议单位学习现有密码相关的国家标准和行业标准。建立密码管理要求的制度文档。

目录

网络安全等级测评基本信息表 I
声明 II
等级测评结论 III
总体评价 IV
主要安全问题及整改建议 VIII
一、安全物理环境 VIII
安全通用要求 VIII
二、安全通信网络 VIII
安全通用要求 VIII
三、安全区域边界 VIII
安全通用要求 VIII
四、安全计算环境 IX
1、网络设备 IX
安全通用要求 IX
2、安全设备 IX
安全通用要求 IX
3、服务器和终端 IX
安全通用要求 IX
4、系统管理软件/平台 IX
安全通用要求 IX
5、业务应用系统/平台 X
安全通用要求 X
6、数据资源 X
安全通用要求 X
7、其他系统或设备 XI
安全通用要求 XI
五、安全管理中心 XI
安全通用要求 XI
六、安全管理制度 XI
安全通用要求 XI
七、安全管理机构 XI
安全通用要求 XI
八、安全管理人员 XI
安全通用要求 XI
九、安全建设管理 XI
安全通用要求 XI
十、安全运维管理 XII
安全通用要求 XII

目录.....XIII
1 测评项目概述.....1
1.1 测评目的.....1
1.2 测评依据.....1
1.3 测评过程.....2
1.4 报告分发范围.....5
2 被测对象描述.....5
2.1 被测对象概述.....5
2.1.1 定级结果.....5
2.1.2 业务和采用的技术.....5
2.1.3 网络结构.....5
2.2 测评指标.....7
2.2.1 安全通用要求指标.....7
2.2.2 安全扩展要求指标.....9
2.2.3 其他安全要求指标.....10
2.2.4 不适用安全要求指标.....10
2.3 测评对象.....10
2.3.1 测评对象选择方法.....10
2.3.2 测评对象选择结果.....11
2.3.2.1 物理机房.....12
2.3.2.2 网络设备.....12
2.3.2.3 安全设备.....12
2.3.2.4 服务器.....13
2.3.2.5 终端设备.....13
2.3.2.6 其他系统或设备.....13
2.3.2.7 系统管理软件/平台.....14
2.3.2.8 业务应用软件/平台.....14
2.3.2.9 数据资源.....15
2.3.2.10 安全相关人员.....15
2.3.2.11 安全管理文档.....16
3 单项测评结果分析.....21
3.1 安全物理环境.....21
3.1.1 已有安全控制措施汇总分析.....21
3.1.2 主要安全问题汇总分析.....23
3.2 安全通信网络.....23
3.2.1 已有安全控制措施汇总分析.....23
3.2.2 主要安全问题汇总分析.....24
3.3 安全区域边界.....24
3.3.1 已有安全控制措施汇总分析.....24
3.3.2 主要安全问题汇总分析.....26
3.4 安全计算环境.....26
3.4.1 网络设备.....26

3.4.1.1 已有安全控制措施汇总分析 26
3.4.1.2 主要安全问题汇总分析 28
3.4.2 安全设备 29
3.4.2.1 已有安全控制措施汇总分析 29
3.4.2.2 主要安全问题汇总分析 32
3.4.3 服务器和终端 32
3.4.3.1 已有安全控制措施汇总分析 33
3.4.3.2 主要安全问题汇总分析 37
3.4.4 系统管理软件/平台 37
3.4.4.1 已有安全控制措施汇总分析 37
3.4.4.2 主要安全问题汇总分析 40
3.4.5 业务应用系统/平台 40
3.4.5.1 已有安全控制措施汇总分析 40
3.4.5.2 主要安全问题汇总分析 43
3.4.6 数据资源 43
3.4.6.1 已有安全控制措施汇总分析 43
3.4.6.2 主要安全问题汇总分析 43
3.4.7 其他系统或设备 44
3.4.7.1 已有安全控制措施汇总分析 44
3.4.7.2 主要安全问题汇总分析 44
3.5 安全管理中心 44
3.5.1 已有安全控制措施汇总分析 44
3.5.2 主要安全问题汇总分析 45
3.6 安全管理制度 45
3.6.1 已有安全控制措施汇总分析 45
3.6.2 主要安全问题汇总分析 47
3.7 安全管理机构 47
3.7.1 已有安全控制措施汇总分析 47
3.7.2 主要安全问题汇总分析 48
3.8 安全管理人员 48
3.8.1 已有安全控制措施汇总分析 48
3.8.2 主要安全问题汇总分析 49
3.9 安全建设管理 50
3.9.1 已有安全控制措施汇总分析 50
3.9.2 主要安全问题汇总分析 52
3.10 安全运维管理 53
3.10.1 已有安全控制措施汇总分析 53
3.10.2 主要安全问题汇总分析 57
3.11 其他安全要求指标 57
3.11.1 已有安全控制措施汇总分析 58
3.11.2 主要安全问题汇总分析 58
3.12 验证测试 58
3.12.1 漏洞扫描 58
3.12.1.1 漏洞扫描结果统计 58

3.12.1.2 漏洞扫描问题描述 63
3.12.2 渗透测试 63
3.12.2.1 渗透测试过程说明 64
3.12.2.2 渗透测试问题描述 65
3.13 单项测评小结 65
3.13.1 控制点符合情况汇总 65
3.13.2 安全问题汇总 69
4 整体测评 73
4.1 安全控制点间安全测评 73
4.1.1 安全建设管理 73
4.1.1.1 安全通用要求 73
4.1.2 安全运维管理 74
4.1.2.1 安全通用要求 74
4.2 区域间安全测评 74
4.2.1 安全物理环境 75
4.2.1.1 安全通用要求 75
4.2.2 安全通信网络 75
4.2.2.1 安全通用要求 75
4.2.3 安全区域边界 75
4.2.3.1 安全通用要求 75
4.3 整体测评结果汇总 76
5 安全问题风险分析 78
6 等级测评结论 82
7 安全问题整改建议 84
附录A 被测对象资产 90
A.1 物理机房 90
A.2 网络设备 90
A.3 安全设备 90
A.4 服务器 91
A.5 终端设备 91
A.6 其他系统或设备 91
A.7 系统管理软件/平台 91
A.8 业务应用软件/平台 92
A.9 数据资源 92
A.10 密码产品 93
A.11 安全相关人员 93
A.12 安全管理文档 94
附录B 上次测评问题整改情况说明 99
附录C 单项测评结果汇总 99
C.1 安全物理环境 99

C.2 安全通信网络 99
C.3 安全区域边界 100
C.4 安全计算环境 100
C.4.1 网络设备 100
C.4.2 安全设备 101
C.4.3 服务器和终端 102
C.4.4 系统管理软件/平台 103
C.4.5 业务应用系统/平台 103
C.4.6 数据资源 104
C.4.7 其他系统或设备 104
C.5 安全管理中心 104
C.6 安全管理制度 105
C.7 安全管理机构 105
C.8 安全管理人员 105
C.9 安全建设管理 106
C.10 安全运维管理 106
C.11 其他安全要求指标 107

附录D 单项测评结果记录 107

D.1 安全物理环境 107
D.1.1 安全通用要求 107
D.1.1.1 信息化机房 107
D.2 安全通信网络 109
D.2.1 安全通用要求 109
D.2.1.1 安全通信网络 109
D.3 安全区域边界 110
D.3.1 安全通用要求 110
D.3.1.1 办公网区域 110
D.3.1.2 外网边界区域 112
D.3.1.3 安全管理区域 115
D.3.1.4 服务器存储区域 117
D.4 安全计算环境 119
D.4.1 安全通用要求 119
D.4.1.1 网络设备 119
D.4.1.2 安全设备 127
D.4.1.3 服务器和终端 151
D.4.1.4 系统管理软件/平台 181
D.4.1.5 业务应用系统/平台 192
D.4.1.6 数据资源 196
D.4.1.7 其他系统或设备 204
D.5 安全管理中心 204
D.5.1 安全通用要求 204
D.5.1.1 管理中心 204
D.6 安全管理制度 205
D.6.1 安全通用要求 206

D.6.1.1 制度文件、执行/记录文件 206
D.7 安全管理机构 207
D.7.1 安全通用要求 207
D.7.1.1 制度文件、执行/记录文件 207
D.8 安全管理人员 210
D.8.1 安全通用要求 210
D.8.1.1 制度文件、执行/记录文件 210
D.9 安全建设管理 212
D.9.1 安全通用要求 212
D.9.1.1 制度文件、执行/记录文件 212
D.10 安全运维管理 216
D.10.1 安全通用要求 216
D.10.1.1 制度文件、执行/记录文件 216
D.11 其他安全要求 224
附录E 漏洞扫描结果记录 224
附录F 渗透测试结果记录 224
附录G 威胁列表 228

1 测评项目概述

1.1 测评目的

安全等级测评的目标是通过对目标系统在安全技术及管理方面的测评,对目标系统的安全技术状态及安全管理状况做出初步判断,给出目标系统在安全技术及安全管理方面与其相应安全等级保护要求之间的差距。测评结论作为委托方进一步完善系统安全策略及安全技术防护措施依据。

项目背景是为进一步提高信息系统的保障能力,根据《信息安全等级保护管理办法》（公通字2007【43】号）的精神，茂名职业技术学院委托广东南方信息安全研究院（SC202127130010163）对教学管理信息服务平台实施等级测评，以期发现信息系统和等级保护标准的差距以及存在的安全隐患，为后续的安全整改工作提供参考依据。

1.2 测评依据

测评过程中主要依据的标准:

测评标准

（1）GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》

（2）GB/T 28448-2019 《信息安全技术 网络安全等级保护测评要求》

测评参考标准

（1）GB 17859-1999 《计算机信息系统 安全保护等级划分准则》

（2）GB/T 28449-2018 《信息安全技术 网络安全等级保护测评过程指南》

（3）GB/T 20984-2007 《信息安全技术 信息安全风险评估规范》

（4）GB/T 25058-2019 《信息安全技术 网络安全等级保护实施指南》

测评参考法律法规

（1）《中华人民共和国网络安全法》

（2）《中华人民共和国密码法》

（3）《中华人民共和国数据安全法》

1.3 测评过程

本次等级测评分为四个过程：测评准备活动、方案编制活动、测评实施活动、报告编制活动。具体如图 1-1 所示。其中，各阶段的时间安排如下：

⑴ 测评准备活动

测评准备活动的目标是顺利启动测评项目,收集定级对象相关资料,准备测评所需资料,为编制测评方案打下良好的基础。测评准备活动包括工作启动、信息收集和分析、工具和表单准备三项主要任务。

（2）方案编制活动

方案编制活动的目标是整理测评准备活动中获取的定级对象相关资料,为现场测评活动提供最基本的文档和指导方案。方案编制活动包括测评对象确定、测评指标确定、测评内容确定、工具测试方法确定、测评指导书开发及测评方案编制六项主要任务。

（3）现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调,为现场测评的顺利开展打下良好基础,依据测评方案实施现场测评工作,将测评方案和测评方法等内容具体落实到现场测评活动中。现场测评工作应取得报告编制活动所需的、足够的证据和资料。现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

（4）报告编制活动

在现场测评工作结束后,测评机构应对现场测评获得的测评结果(或称测评证据)进行汇总分析,形成等级测评结论,并编制测评报告。测评人员在初步判定单项测评结果后,还需进行单元测评结果判定、整体测评、系统安全保障评估,经过整体测评后,有的单项

测评结果可能会有所变化,需进一步修订单项测评结果,而后针对安全问题进行风险评估,形成等级测评结论。分析与报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、系统安全保障评估、安全问题风险评估、等级测评结论形成及测评报告编制七项主要任务。

各阶段完成的关键任务：

序号	阶段	任务	对象	开始日期	结束日期
1	测评准备活动	工作启动	项目甲乙双方	2022年8月15日	2022年8月19日
2		信息收集与分析	调研表	2022年8月22日	2022年8月25日
3		工具和表单准备	测评工具、测评授权书、文档交接单	2022年8月25日	2022年8月30日
4	方案编制活动	测评对象确认	测评方案-对象列表	2022年8月31日	2022年8月31日
5		测评指标确认	测评方案-指标列表	2022年8月31日	2022年8月31日
6		测评内容确认	测评方案-内容列表	2022年9月1日	2022年9月1日
7		工具测试方法确认	测评方案-工具测试方法列表	2022年9月1日	2022年9月1日
8		测评指导书开发	测评作业指导书	2022年9月2日	2022年9月2日
9		测评方案编制	测评方案	2022年9月5日	2022年9月5日
10	现场测评活动	现场测评准备	工具、人员、表单准备	2022年9月28日	2022年9月28日
11		现场测评和结果记录	安全管理访谈	2022年9月28日	2022年9月28日
12			安全管理文档检查	2022年9月28日	2022年9月28日
13			安全物理环境测评	2022年9月28日	2022年9月28日
14			安全通信网络	2022年9月28日	2022年9月29日
15			安全区域边界	2022年9月28日	2022年9月29日
16			安全计算环境	2022年9月28日	2022年9月29日
17			工具测试	2022年9月29日	2022年10月9日
18		结果确认和资料归还	检测人员出入场确认单、测评现场服务评价单	2022年10月8日	2022年10月9日
19	报告编制活动	单项测评结果	测评报告	2022年10月9日	2022年10月12日

序号	阶段	任务	对象	开始日期	结束日期
		判定			
20		单元测评结果判定		2022年10月9日	2022年10月17日
21		整体测评		2022年10月9日	2022年10月17日
22		系统安全保障评估		2022年10月9日	2022年10月17日
23		安全问题风险分析		2022年10月9日	2022年10月17日
24		等级测评结论形成		2022年10月17日	2022年10月30日
25		测评报告编制		2022年10月17日	2022年10月30日

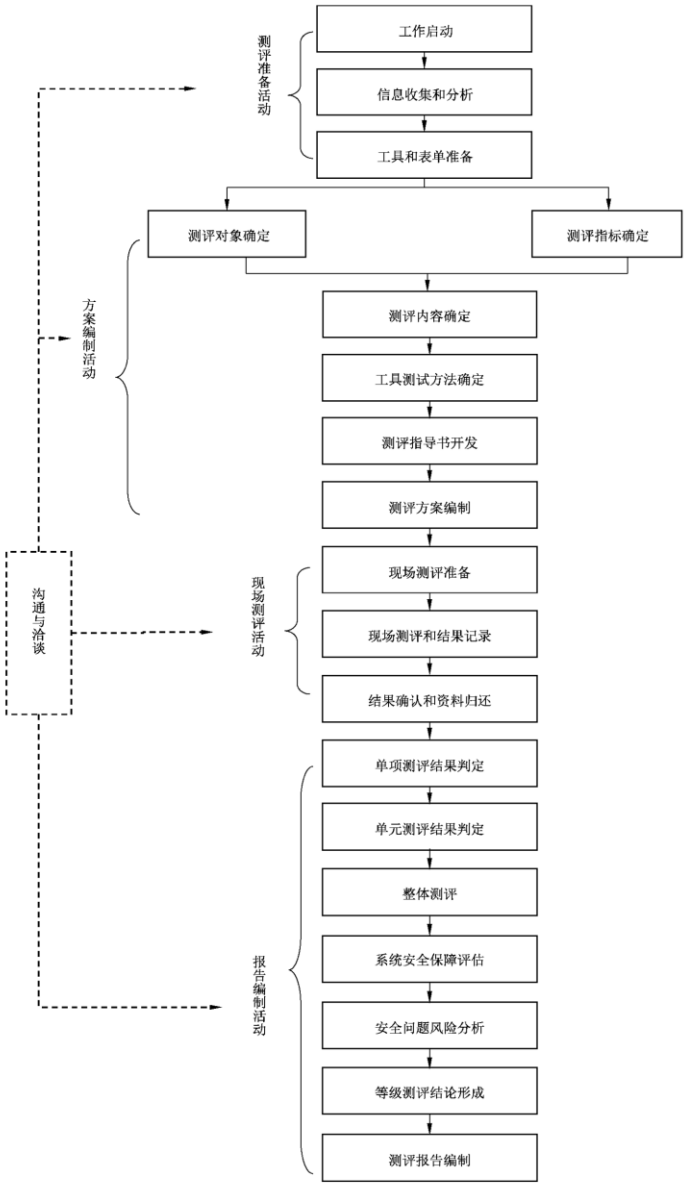


图 1-1 等级保护测评工作流程图

其中，于项目前期召开了项目启动会议，确定了工作方案及项目人员名单；于现场测评完成后召开了项目末次会议，确认了测评发现的问题；于2022年10月30日在对系统的整改情况进行了复核确认后，完成报告编制。

1.4 报告分发范围

等级测评报告正本一式3份，其中茂名职业技术学院1份，广东南方信息安全研究院1份，受理备案的公安机关1份。

2 被测对象描述

2.1 被测对象概述

2.1.1 定级结果

表 2-1定级结果

被测对象名称	安全保护等级	业务信息安全等级	系统服务安全等级
教学管理信息服务平台	2	2	2

2.1.2 业务和采用的技术

教学管理信息服务平台主要实现教务管理服务，系统包括系统管理、学籍管理、师资管理、教学计划、排课管理、选课管理、成绩管理、考试管理、毕业管理、教学评价等功能模块。教学管理信息服务平台以培养、运行、保障、监控为主线，实现教务工作事务性管理和战略性管理的相互叠加，实现学校培养过程管理、教学质量检查、教学工作管理等日常教学事务管理。

被测对象未采用云计算/移动互联/物联网/工业控制/大数据等技术情况。

2.1.3 网络结构

教学管理信息服务平台主要是对互联网提供服务,相关设备部署在信息化机房当中,其简要拓扑如下:

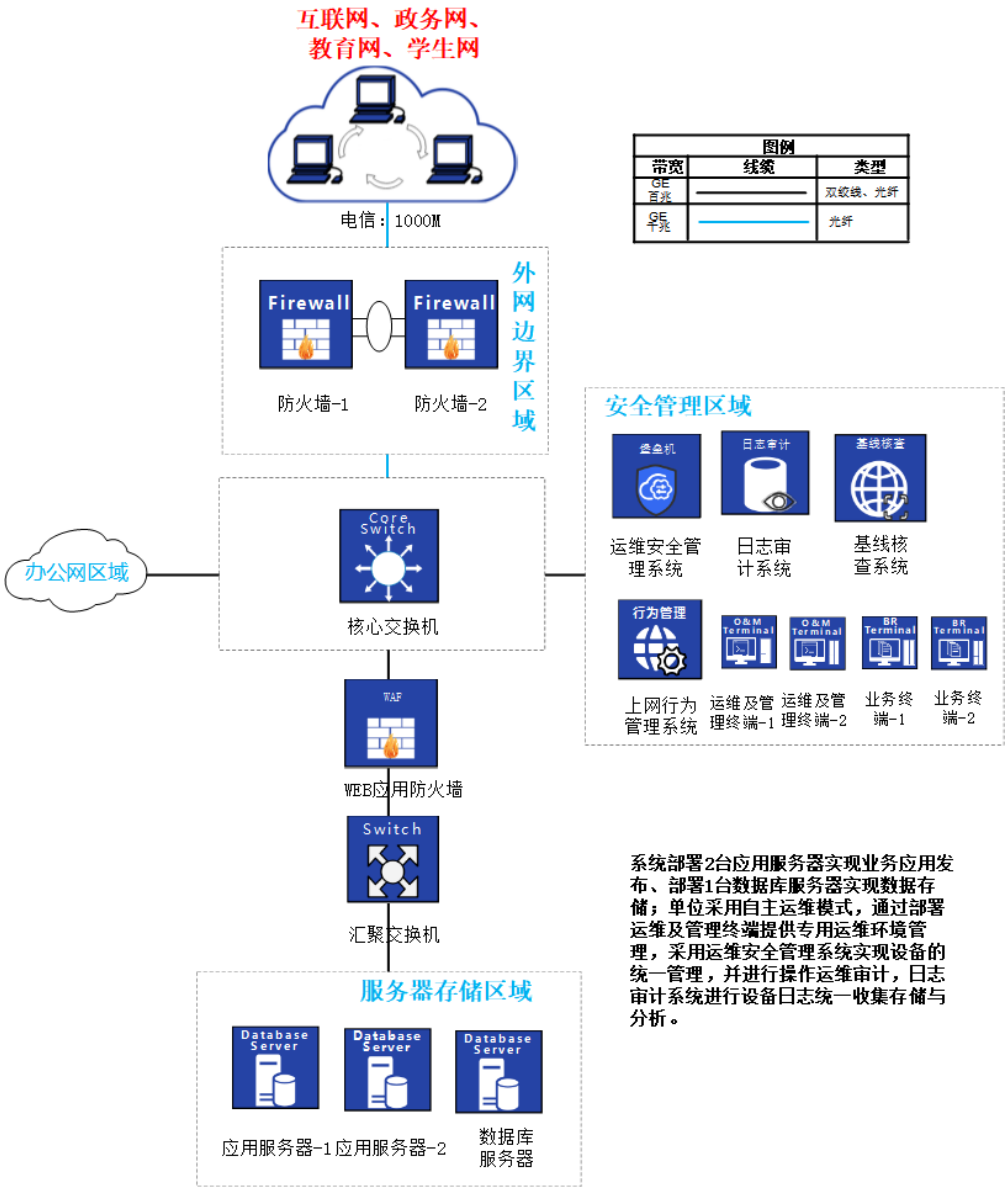


图 2-1 教学管理信息服务平台网络拓扑图

如图2-1教学管理信息服务平台网络拓扑图所示，教学管理信息服务平台网络安全域划分为4个，分别为外网边界区域、安全管理区域、服务器存储区域、办公网区域。

1、外网边界区域：

外网边界区域网络主要包括教学管理信息服务平台的业务服务和信息交换应用，是安全管理区域、服务器存储区域、办公网区域的出口边界；其链路接入为光纤线，带宽为1000mb。通过部署核心交换机、防火墙等设备实施网络访问控制，防火墙（入侵防御模块）实现网络入侵攻击行为防御。

2、办公网区域：

办公网区域网络主要包括教学管理信息服务平台与办公区域的信息交换应用，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、防火墙、上网行为管理系统等设备实施网络访问控制、防火墙（入侵防御模块）实现网络入侵攻击行为防御。

3、安全管理区域：

安全管理区域网络主要包括日志审计系统、运维安全管理系统、上网行为管理系统，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、上网行为管理系统等设备实施网络访问控制。

4、服务器存储区域：

服务器存储区域网络主要包括教学管理信息服务平台的应用服务器、数据库服务器，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、上网行为管理系统等设备实现一定的网络访问控制。

5、服务器部署情况：

教学管理信息服务平台由2台应用服务器实现应用发布；1台数据库服务器实现数据处理、存储、维护。

6、灾备及冗余

教学管理信息服务平台无异地备份机房，未实现异地备份数据定时传输功能。系统重要数据根据需求采用每天增量、每月全备到本地信息化机房。

教学管理信息服务平台未实现冗余措施。

2.2 测评指标

2.2.1 安全通用要求指标

表 2-2 安全通用要求指标

安全类	安全控制点	测评项数
安全物理环境	物理位置选择	2
	物理访问控制	1
	防盗窃和防破坏	2
	防雷击	1
	防火	2
	防水和防潮	2
	防静电	1
	温湿度控制	1
	电力供应	2
	电磁防护	1
安全通信网络	网络架构	2
	通信传输	1
	可信验证	1
安全区域边界	边界防护	1
	访问控制	4
	入侵防范	1
	恶意代码和垃圾邮件防范	1
	安全审计	3
	可信验证	1
安全计算环境	身份鉴别	3
	访问控制	4
	安全审计	3
	入侵防范	5
	恶意代码防范	1
	可信验证	1
	数据完整性	1
	数据备份恢复	2
	剩余信息保护	1
	个人信息保护	2
安全管理中心	系统管理	2
	审计管理	2
安全管理制度	安全策略	1
	管理制度	2
	制定和发布	2
	评审和修订	1
安全管理机构	岗位设置	2
	人员配备	1
	授权和审批	2
	沟通和合作	3

安全类	安全控制点	测评项数
	审核和检查	1
安全管理人员	人员录用	2
	人员离岗	1
	安全意识教育和培训	1
	外部人员访问管理	3
安全建设管理	定级和备案	4
	安全方案设计	3
	产品采购和使用	2
	自行软件开发	2
	外包软件开发	2
	工程实施	2
	测试验收	2
	系统交付	3
	等级测评	3
	服务供应商选择	2
安全运维管理	环境管理	3
	资产管理	1
	介质管理	2
	设备维护管理	2
	漏洞和风险管理	1
	网络和系统安全管理	5
	恶意代码防范管理	3
	配置管理	1
	密码管理	2
	变更管理	1
	备份与恢复管理	3
	安全事件处置	3
	应急预案管理	2
	外包运维管理	2
安全通用要求指标数量统计		135

2.2.2 安全扩展要求指标

表 2-3 安全扩展要求指标

扩展类型	安全类	安全控制点	测评项数
本次测评不涉及安全扩展要求指标			

2.2.3 其他安全要求指标

表 2-4 其他安全要求指标

安全类	安全控制点	测评项数
本次测评不涉及其他安全要求指标		

2.2.4 不适用安全要求指标

表 2-5-1 不适用安全要求指标

安全类	安全控制点	不适用项	不适用原因
安全建设管理	自行软件开发	a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。
安全建设管理	自行软件开发	b) 应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。
安全运维管理	密码管理	b) 应使用国家密码管理主管部门认证核准的密码技术和产品。	（1）单位未采购涉及密码技术的产品，不适用。
安全运维管理	外包运维管理	a) 应确保外包运维服务商的选择符合国家的有关规定；	（1）单位目前未涉及任何外包运维服务情况，不适用。
安全运维管理	外包运维管理	b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。	（1）单位目前未涉及任何外包运维服务情况，不适用。

表 2-5-2 其他不适用安全要求指标

安全类	安全控制点	不适用项	不适用原因
本次测评不涉及其他安全要求指标			

2.3 测评对象

2.3.1 测评对象选择方法

教学管理信息服务平台等级测评的测评对象种类上基本覆盖、数量进行抽样，重点抽查主要的设备、设施、人员和文档等。结合教学管理信息服务平台的网络拓扑结构和业务情况，本次等级测评的测评对象在抽样时主要考虑以下几个方面：

（1） 主机房（包括其环境、设备和设施等）和灾备机房；

（2） 存储被测系统重要数据的介质的存放环境；

（3） 办公场地；

（4） 整个系统的网络拓扑结构；

（5） 安全设备，包括防火墙等；

（6） 边界网络设备，包括路由器、楼层交换机等；

（7） 对整个信息系统或其局部的安全性起作用的网络互联设备，如核心交换机、路由器等；

（8） 承载业务处理系统主要业务或数据的服务器（包括其操作系统和数据库）；

（9） 管理终端和主要应用系统终端；

（10） 能够完成系统不同业务使命的业务应用系统；

（11） 业务备份系统；

（12） 信息安全主管人员、各方面的负责人员、具体负责安全管理的当事人、业务负责人；

（13） 涉及到信息系统安全的所有管理制度和记录。

抽样原则：在等级测评时，业务处理系统中配置相同的安全设备、边界网络设备、网络互联设备、服务器、终端以及备份设备，每类至少抽查两台作为测评对象。

2.3.2 测评对象选择结果

2.3.2.1 物理机房

表 2-6 物理机房

序号	机房名称	物理位置	重要程度
1	信息化机房	茂名市茂南区文明北路232号大院大楼	关键

2.3.2.2 网络设备

表 2-7 网络设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度
1	核心交换机	否	H3C version 7.1.070, Release 7585P07	H3C S7500E-X	核心数据交换、访问控制	关键
2	汇聚交换机	否	H3C version 7.1.070, Release 6126P20	H3C S5560X-30C-EI	数据交换	重要

2.3.2.3 安全设备

表 2-8 安全设备

序号	设备名称	是否虚拟设备	系统及版本	品牌型号	用途	重要程度
1	WEB应用防火墙	否	深信服AF 8.0.9	深信服WAF-2000-H642	应用防护、入侵防范、病毒防护	重要
2	防火墙-2	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键
3	上网行为管理系统	否	深信服AC12.0.26	深信服AC-1000-D600-PT	上网行为管理及终端准入控制	重要
4	基线核查系统	否	深信服V3.0.3	深信服AC-1000-D602-PT	漏洞扫描	重要
5	日志审计系统	否	深信服LAS 3.0.5	深信服AC-1000-D601-PT	日志审计	重要
6	运维安全管理系	否	深信服V3.0.6	深信服	运维审计	重要

序号	设备名称	是否虚拟设备	系统及版本	品牌型号	用途	重要程度
	统			AC-1000-D603-PT		
7	防火墙-1	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键

2.3.2.4 服务器

表 2-9 服务器

序号	设备名称	所属业务应用系统/平台	是否虚拟设备	操作系统及版本	数据库管理系统及版本	中间件及版本	重要程度
1	应用服务器-1	教学管理信息服务平台	否	CentOS 7.7	/	Tomcat 8.5	关键
2	应用服务器-2	教学管理信息服务平台	否	CentOS 7.7	/	Tomcat 8.5	关键
3	数据库服务器	教学管理信息服务平台	否	CentOS 7.7	Oracle 11.2.0.1.0	/	关键

2.3.2.5 终端设备

表 2-10 终端设备

序号	设备名称	是否虚拟设备	操作系统及版本	用途	重要程度
1	运维及管理终端-2	否	Windows 10 （版本 21H2（内部版本 19044.1889））	运维管理、系统管理	一般
2	业务终端-1	否	Windows 10 （版本 20H2（内部版本 19044.1889）	业务管理	一般
3	业务终端-2	否	Windows 10 （版本 20H2（内部版本 19044.1889）	业务管理	一般
4	运维及管理终端-1	否	Windows 10 （版本 20H2（内部版本 19044.1889）	运维管理、系统管理	一般

2.3.2.6 其他系统或设备

表 2-11 其他系统或设备

序号	设备名称	是否虚拟设备	系统及版本	用途	重要程度
/	/	/	/	/	/

注释：本次测评对象中不涉及专用移动互联终端等，不开展抽测。

2.3.2.7 系统管理软件/平台

表 2-12 系统管理软件/平台

序号	系统管理软件/平台名称	主要功能	版本	所在设备名称	重要程度
1	应用服务器-2-Tomcat	页面发布	8.0.37	应用服务器-2	关键
2	数据库服务器-Oracle	数据生产、存储	11.2.0.1.0	数据库服务器	关键
3	应用服务器-1-Tomcat	页面发布	8.0.37	应用服务器-1	关键

2.3.2.8 业务应用软件/平台

表 2-13 业务应用系统/平台

序号	业务应用软件/平台名称	主要功能	业务应用软件及版本	开发厂商	重要程度
1	教学管理信息服务平台	教学管理信息服务平台主要实现教务管理服务，系统包括系统管理、学籍管理、师资管理、教学计划、排课管理、选课管理、成绩管理、考试管理、毕业管理、教学评价等功能模块。教学管理信息服务平台以培养、运行、保障、监控为主线，实现教务工作事务	V6.0	正方软件股份有限公司	关键

序号	业务应用软件/平台名称	主要功能	业务应用软件及版本	开发厂商	重要程度
		性管理和战略性管理的相互叠加，实现学校培养过程管理、教学质量检查、教学工作管理等日常教学事务管理。			

2.3.2.9 数据资源

表 2-14 数据资源

序号	数据类别	所属业务应用	安全防护需求	重要程度
1	重要个人信息	教学管理信息服务平台	完整性、保密性	关键
2	重要业务数据	教学管理信息服务平台	完整性、保密性	关键
3	鉴别数据	教学管理信息服务平台(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性、保密性	关键
4	重要审计数据	教学管理信息服务平台（安全管理中心）	完整性	重要
5	重要配置数据	教学管理信息服务平台(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性	关键

注释：网络设备、安全设备、服务器、终端、系统管理软件/平台和业务应用系统等所涉及的鉴别数据和重要配置数据分别在各自测评对象中汇总测评证据后集中体现,包括数据完整性、数据保密性和备份恢复。重要审计数据在安全管理中心进行汇总测评证据，包括数据完整性。重要业务数据和重要个人信息分别在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。

2.3.2.10 安全相关人员

表 2-15 安全相关人员

序号	姓名	岗位/角色	联系方式	所属单位
1	叶永利	安全管理员	0668-2920122	茂名职业技术学院
2	吴国华	系统管理员	0668-2920122	茂名职业技术学院
3	杨云	审计管理员	0668-2920122	茂名职业技术学院
4	吴国华	机房管理员	0668-2920122	茂名职业技术学院
5	龙恒	网络管理员	13377766618	茂名职业技术学院
6	龙恒	数据管理员	13377766618	茂名职业技术学院
7	龙恒	应用管理员	13377766618	茂名职业技术学院
8	杨云	资产管理员	0668-2920122	茂名职业技术学院

2.3.2.11 安全管理文档

表 2-16 安全管理文档

序号	文档名称	主要内容
1	制度类文档-办公环境保密管理	关于单位办公环境管理制度文档
2	制度类文档-信息安全漏洞扫描规范	关于单位安全漏洞工作规范制度文档
3	制度类文档-安全漏洞管理制度	关于单位安全漏洞管理工作制度文档
4	制度类文档-恶意代码防范管理制度	关于单位恶意代码防范工作制度文档
5	制度类文档-安全事件报告和处置	关于单位网络安全事件管理、处置、流程等报告制度文档
6	制度类文档-外部服务人员管理规范	关于单位针对外部人员工作管理规范制度文档
7	制度类文档-测试及验收方案	关于单位测试验收方案文档
8	制度类文档-办公环境管理制度	关于单位办公环境管理制度文档
9	制度类文档-组织安全结构和人员职责制度	关于单位安全结构、人员职责

序号	文档名称	主要内容
10	制度类文档-员工考核管理制度	关于单位人员考核工作管理制度文档
11	制度类文档-工程测试验收管理	关于单位工程测试工作管理制度文档
12	制度类文档-恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
13	制度类文档-服务供应商选择安全管理制度	关于单位安全服务供应商管理规定制度文档
14	制度类文档-安全审查和检查管理规范	关于单位安全检查、审查工作规范制度文档
15	制度类文档-信息系统恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
16	制度类文档-工程实施管理制度	关于单位工程实施工作管理制度文档
17	制度类文档-系统交付管理	关于单位交付工作管理制度文档
18	制度类文档-介质管理制度	关于单位介质安全管理工制度文档
19	制度类文档-物理安全管理规范	关于加强单位办公区域及电子计算机机房的管理和设备运行安全，规范办公区域及机房建设，使人员办公高效及机房设备安全、稳定运行的制度文档
20	制度类文档-外包开发软件管理规定	关于单位外包项目管理工作制度文档
21	制度类文档-信息安全总体策略	关于单位网络安全方针、策略制度文档
22	制度类文档-岗位安排及岗位职责	关于单位岗位职责、岗位安排制度文档
23	制度类文档-组织安全结构和人员职责制度	关于单位组织结构、人员安排、人员职责制度文档
24	制度类文档-信息安全奖惩办法	关于单位人员奖惩制度文档
25	制度类文档-应用安全管理规范	关于规定单位应用安全管理要求及规范的制度文档
26	制度类文档-授权和审批管理规定	关于单位授权审批、审批流程规范制度文档
27	制度类文档-网络安全管理制度	关于单位网络安全工作管理制度文档
28	制度类文档-网络与信息系统安全设计规范	关于单位网络与信息化安全设计制度文档
29	制度类文档-信息系统外包运维管理制度	关于单位外包运维工作管理制度文档
30	制度类文档-系统安全管理制度	关于单位系统安全管理、安全服务管理制度文档
31	制度类文档-外部人员访问	关于单位针对外来人员访问管控制度文档

序号	文档名称	主要内容
	管理制度	
32	制度类文档-安全教育和培训制度	关于单位安全培训、安全交流工作制度文档
33	制度类文档-制度制定、发布、评审和修订管理制度	关于单位制度制定、发布、评审和修订等管理文档
34	制度类文档-应用系统业务用户密码设置规定	关于单位用户密码管理制度文档
35	制度类文档-备份与恢复管理制度	关于单位数据备份、恢复管理制度文档
36	制度类文档-机房安全管理制度	关于单位机房安全管理工作制度文档
37	制度类文档-安全管理组织规范	关于单位组织结构管理规范制度文档
38	制度类文档-主机安全管理规范	关于规定单位主机系统安全管理要求规范，指导业务平台主机的安全配置和维护的制度文档
39	制度类文档-设备安全管理制度	关于单位设备安全管理制度文档
40	制度类文档-数据安全管理规范	关于保障关键数据安全，从数据库本身、数据加密、数据备份恢复三个方面对数据安全进行规范的制度文档
41	制度类文档-变更控制管理制度	关于单位变更流程、控制管理制度文档
42	制度类文档-系统及应用数据备份管理规范	关于单位数据备份、恢复管理制度文档
43	制度类文档-网络安全事件报告制度	关于单位网络安全事件管理报告文档
44	制度类文档-离岗人员工作交接规范	关于单位离岗交接工作规范制度文档
45	制度类文档-网络安全管理规范	关于保障单位网络系统的安全稳定运行，抵御内部和外部各种形式的网络攻击或威胁制定的管理文档
46	制度类文档-网络安全事件应急预案	关于单位网络安全事件应急处理、流程、培训等管理制度文档
47	制度类文档-外部接入受控网络访问系统管理规范	关于单位针对外部人员工作接入规范制度文档
48	制度类文档-人员管理制度	关于单位人员录用、调岗、离岗管理制度文档
49	操作类文档-设备操作规程	关于单位相关设备操作指导文档
50	操作类文档-软硬件日常维护管理规程	关于单位计算机网络系统使用、管理、信息安全、资源共享有所遵循,规范上网操作流程,提高网络系统安全性的指导文档
51	操作类文档-数据备份策略	关于单位数据备份策略文件
52	操作类文档-设备及系统软件配置和操作手册	关于单位安全设备操作、Linux服务器配置手册、主机运维操作手册、软件操作手册、防火墙配置和操作手册、数据库日常运维操作手册等指导文档
53	记录类文档-人员入职考核	关于人员录用、考核工作记录

序号	文档名称	主要内容
	记录	
54	记录类文档-离场信息资料交接表	关于人员离岗交接工作记录
55	记录类文档-安全管理制度评审记录	关于单位制度审计记录
56	记录类文档-设备维修申请表	关于单位设备维护工作申请记录
57	记录类文档-设备操作维护记录	关于单位设备维护工作记录
58	记录类文档-人员培训及考核记录表	关于人员培训、考核等工作记录
59	记录类文档-设备出入登记记录表	关于设备进出机房登记工作记录
60	记录类文档-接入受控网络申请表	关于外来人员接入工作记录
61	记录类文档-信息系统存储介质销毁申请表	关于备份介质销毁申请工作记录
62	记录类文档-漏洞检测报告	关于单位安全漏洞检测报告文档
63	记录类文档-备份工作汇总表	关于单位数据备份工作总结表
64	记录类文档-收发文登记记录	关于单位文档签发记录
65	记录类文档-应急预案培训记录表	关于单位应急预案培训工作记录
66	记录类文档-技能培训记录	关于单位系统培训工作、考核工作记录
67	记录类文档-离职员工物品交回登记表	关于人员离岗工物交接工作记录
68	记录类文档-外部人员访问记录表	关于外来人员访问登记工作记录
69	记录类文档-网络信息安全事件记录表	关于单位网络安全事件工作记录
70	记录类文档-网络配置信息	关于单位配置信息登记工作记录
71	记录类文档-机房设备维修记录表	关于单位机房设备维修工作记录
72	记录类文档-机房巡检记录表	关于单位机房环境巡检记录
73	记录类文档-系统交付清单	关于单位交付工作记录
74	记录类文档-信息管理系统漏洞检查表	关于单位安全漏洞工作检测记录表
75	记录类文档-访问记录表	关于人员访问工作记录
76	记录类文档-安全建设方案评审纪录	关于单位网络与信息化安全设计方案评审工作记录

序号	文档名称	主要内容
77	记录类文档-关键岗位人员考核记录	关于关键岗位考核工作记录
78	记录类文档-信息安全检查记录表	关于单位安全检查工作记录
79	记录类文档-信息系统存储介质使用清单	关于备份介质存储使用清单
80	记录类文档-外部人员访问申请表	关于外来人员访问申请流程工作记录
81	记录类文档-信息安全会议记录	关于单位安全培训、安全交流会议记录
82	记录类文档-机房设备维护记录表	关于设备维护登记工作记录
83	记录类文档-评审和修订记录	关于单位变更评审、修订工作记录
84	记录类文档-人员离岗申请表	关于人员离岗申请记录
85	记录类文档-数据备份记录表	关于单位数据备份工作记录
86	记录类文档-数据恢复申请表	关于单位数据恢复工作申请表
87	记录类文档-存储介质目录清单	关于备份介质存储工作清单
88	记录类文档-机房维护日志	关于机房维护工作记录
89	记录类文档-通用变更记录表	关于单位变更工作记录
90	记录类文档-专家论证记录表	关于单位网络方案论证记录
91	记录类文档-外部会议文件和记录	关于单位外部联系、交流及会议工作记录
92	记录类文档-软件交付清单	关于单位交付工作记录
93	记录类文档-监理审批表	关于单位监理审核工作记录
94	记录类文档-重要操作审批表	关于单位审批工作记录
95	记录类文档-备份介质使用记录	关于备份介质使用登记工作记录
96	记录类文档-机房出入登记表	关于人员进出机房登记工作记录
97	证据类文档-定级备案	关于单位系统定级报告、备案证文件
98	证据类文档-深信服安全采购合同	关于单位与安全厂家服务采购、产品选择合同文件
99	证据类文档-资产清单	关于单位信息系统资产清单统计表
100	证据类文档-网络安全系统	关于单位网络与信息化安全设计方案文档

序号	文档名称	主要内容
	设计方案	
101	证据类文档-外部联系表	关于单位内部联系及外部联系名单
102	证据类文档-网络安全等级保护工作小组名单	关于单位网络安全等级保护工作小组人员名单文件
103	证据类文档-网络安全等级保护测评服务合同	关于单位与安全服务商签定的安全服务合同文件
104	证据类文档-信息安全事件分析报告表	关于单位安全事件分析报告
105	证据类文档-工程项目实施方案	关于单位工程实施方案文档
106	证据类文档-安全职位人员	关于单位人员岗位安排名单

3 单项测评结果分析

3.1 安全物理环境

3.1.1 已有安全控制措施汇总分析

安全通用要求

物理位置选择	
a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；	
信息化机房	（1）机房和办公场地场所在建筑物具有建筑验收文档，包含对防震、防风和防雨能力的说明； （2）机房和办公场地未出严重的问题。
b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	
信息化机房	（1）机房未部署在易发生问题的位置； （2）机房对于空调设备的排水管等部位采取密封防漏处理； （3）机房对于楼板进行了防护措施。
防盗窃和防破坏	
a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识；	
信息化机房	（1）机房设备或主要部件都固定在机架上； （2）机房内对主要部件已绑定相应不易除去的标签； （3）重要机柜已进行上锁处理。
b) 应将通信线缆铺设在隐蔽安全处。	
信息化机房	（1）通信线缆铺设在下走线槽隐蔽处中； （2）通信线缆设有明显的源目的标识； （3）通信线缆均铺设整齐、规范。
防雷击	
应将各类机柜、设施和设备等通过接地系统安全接地。	

信息化机房	（1）机房设置专用地线； （2）机房内机柜、设施和设备等进行接地处理； （3）交流电源接地验收检测结果符合要求。
防火	
a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；	
信息化机房	（1）机房采用经消防检测部门检测合格并在有效期内的（如 七氟丙烷）气体自动灭火设备，火灾自动报警类型为烟感+红外； （2）自动消防系统工作状态正常，有定期巡检和维护记录《机房巡检记录表》； （3）建立机房消防的管理制度相关文档《机房安全管理制度》，按管理要求机房无人情况下气体灭火配置为自动模式，进入机房调整为手动模式，机房报警有7*24小时值班人员进行监控。
防水和防潮	
a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	
信息化机房	（1）机房不存在雨水渗透、破损等不合规情况； （2）机房不位于建筑的顶层、边缘区域。
b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。	
信息化机房	（1）机房区域范围已部署1台科华品牌（精密）空调，机房内分别配置1组温湿度传感器监控； （2）机房内空调下方已铺设安装好挡水和排水设施； （3）机房墙壁或楼板的管道采取必要的防渗防漏等防水保护措施； （4）机房安装检测设备（如：漏水检测绳）检测地下积水，及时处理机房水蒸气结露和地下积水的转移与渗透； （5）目前防水\防潮检测未发现异常情况，并且有防水防潮的运维记录《机房维护日志》。
温湿度控制	
应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。	
信息化机房	（1）机房范围已部署1组科华品牌精密空调进行温湿度调节； （2）机房范围已部署空调及加湿机进行温湿度调节； （3）温湿度自动调节设施运作正常，有运行和维护记录《机房维护日志》； （4）机房温度能保持在24摄氏度到28摄氏度之间； （5）机房湿度能保持在40%到65%之间。
电力供应	
a）应在机房供电线路上配置稳压器和过电压防护设备；	
信息化机房	（1）机房配备了稳压器和过电压防护设备； （2）稳压器和过电压防护设备正常工作； （3）机房具备电力供应安全设计，并在其中标明配备稳压器、过电压防护设备等要求。
b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。	
信息化机房	（1）机房配备了1组科华品牌UPS； （2）UPS正常工作，可满足主要设备断电情况下的至少1小时正常运行要求； （3）UPS有定期（至少每年）检查和维护，有运行和维护记录《机房巡检记录表》。

电磁防护	
电源线和通信线缆应隔离铺设，避免互相干扰。	
信息化机房	（1）通信线缆铺设采用独立的具有电磁屏蔽作用线槽； （2）电源线缆铺设采用独立的具有电磁屏蔽作用线槽； （3）弱电线缆隔离铺设，没有干扰。

3.1.2 主要安全问题汇总分析

安全通用要求

（1）机房出入口未配置电子门禁系统（如：信息化机房）。上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域,可能对系统的平稳运行造成影响。中风险。

（2）机房建设未完全采用符合耐火等级的建筑材料。机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级（如：信息化机房）。存在发生火情时助燃火灾的风险。 低风险。

（3）机房内缺乏防静电措施（如防静电地板或铺设防静电地毯 ）（如：信息化机房）。存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。 中风险。

3.2 安全通信网络

3.2.1 已有安全控制措施汇总分析

安全通用要求

网络架构	
b) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	
安全通信网络	(1)网络内重要网段未部署在网络边界处,且未直接连接外部信息系统; (2) 系统通过防火墙对重要网段采取访问控制策略; (3) 各安全域（子网）的出口唯一。
通信传输	
应采用校验技术保证通信过程中数据的完整性。	
安全通信网络	(1) 网络系统中未涉及完整性保障设备，但在安全计算环境方面网络设备采用SSH协议、安全设备采用HTTPS协议、操作系统采用SSH协议、应

	用系统采用HTTPS协议来保证通信过程中数据的完整性。

3.2.2 主要安全问题汇总分析

安全通用要求

（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况（如：安全通信网络）。上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变得更为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。 中风险。

（2）缺乏对通信设备可信验证方面的安全设计要求。现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况（如：安全通信网络）。缺乏对系统可执行程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致计算资源被干扰和破坏造成损失。 低风险。

3.3 安全区域边界

3.3.1 已有安全控制措施汇总分析

安全通用要求

边界防护	
应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络存在受保护的边界； （2）网络边界处部署了可提供访问控制功能的设备； （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。
访问控制	
a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	
办公网区域 外网边界区域	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备；

安全管理区域 服务器存储区域	（3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。
b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。
c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。
d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。
入侵防范	
应在关键网络节点处监视网络攻击行为。	
外网边界区域 服务器存储区域	（1）网络层部署支持对内部发起的攻击行为进行防范的设备； （2）现有的防范措施满足相应防护要求； （3）内部安全防范措施能检测相应攻击行为。
恶意代码和垃圾邮件防范	
应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	
外网边界区域 服务器存储区域	（1）在关键网络节点处部署合规的防恶意代码措施； （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试。
安全审计	
a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； （3）现有的审计措施满足相应的审计要求。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； （3）设备本地时间正常。
c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
办公网区域 外网边界区域 安全管理区域	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求；

服务器存储区域	（4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。

3.3.2 主要安全问题汇总分析

安全通用要求

（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为（如：办公网区域）。存在不能及时发现内部主机作为攻击跳板，或网络攻击行为而造成系统损坏/网络资源浪费的风险。中风险。

（2）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面（如：办公网区域）。无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。 中风险。

（3）缺乏对边界设备可信验证方面的安全设计要求。现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况（如：办公网区域）。缺乏对边界设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4 安全计算环境

3.4.1 网络设备

3.4.1.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
核心交换机 汇聚交换机	（1）设备对各登录模式均启用身份鉴别； （2）设备对登录管理的用户进行身份鉴别；

	（3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的全局密码策略； （6）设备配置加密的super认证。
b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
核心交换机 汇聚交换机	（1）设备配置合规的全局登录失败处理策略； （2）设备配置合规的操作超时退出措施。
c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
核心交换机 汇聚交换机	（1）设备配置合规的远程管理模式。
访问控制	
a）应对登录的用户分配账户和权限；	
核心交换机 汇聚交换机	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。
b）应重命名或删除默认账户，修改默认账户的默认口令；	
核心交换机 汇聚交换机	（1）设备不存在默认账户名； （2）设备账户口令设置合规。
c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
核心交换机 汇聚交换机	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。
d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	
核心交换机 汇聚交换机	（1）设备根据安全策略要求对特权用户进行分离； （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
核心交换机 汇聚交换机	（1）设备开启审计功能，审计进程正常； （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
核心交换机 汇聚交换机	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。
c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
核心交换机 汇聚交换机	（1）设备限制审计文件的访问控制权限，普通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效； （5）日志及审计记录保存大于6个月。

入侵防范	
a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	
核心交换机 汇聚交换机	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。
b) 应关闭不需要的系统服务、默认共享和高危端口；	
核心交换机 汇聚交换机	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。
c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
核心交换机 汇聚交换机	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
核心交换机 汇聚交换机	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
核心交换机 汇聚交换机	鉴别数据、重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； （2）设备对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
核心交换机 汇聚交换机	（1）设备定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。

3.4.1.2 主要安全问题汇总分析

安全通用要求

（1）设备不具备相关可信验证的技术措施（如：核心交换机）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.2 安全设备

3.4.2.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备对各登录模式均启用身份鉴别； （2）设备对登录管理的用户进行身份鉴别； （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备启用合规登录失败处理策略； （2）设备配置合规的操作超时退出措施。
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备配置合规的远程管理模式； （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。
访问控制	
a) 应对登录的用户分配账户和权限；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。
b) 应重命名或删除默认账户，修改默认账户的默认口令；	

WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备不存在默认账户名； (2) 设备账户口令设置合规。
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备不存在多余或过期账户； (2) 设备管理员用户与账户之间一一对应。
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备根据安全策略要求对特权用户进行分离； (2) 设备不存在多个管理级别高的特权用户； (3) 设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备开启审计功能，审计进程正常； (2)设备的日志审计级别满足要求,审计覆盖所有用户操作审计和记录。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备日期、时间正常； (2) 设备审计记录内容基本完整。
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
WEB应用防火墙 上网行为管理系统 基线核查系统	(1) 设备限制审计文件的访问控制权限，普通用户不可删除及修改； (2) 设备针对日志、审计记录具备充足的存储容量； (3) 对审计记录进行定期存档备份，其备份策略有效；

运维安全管理系统 防火墙-1 防火墙-2	（4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。
日志审计系统	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）日志及审计记录保存大于6个月。
入侵防范	
a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。
b）应关闭不需要的系统服务、默认共享和高危端口；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。
c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 防火墙-1 防火墙-2	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
运维安全管理系统	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制。
d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备管理具备数据有效性检验功能； （2）设备管理的校验接口范围较全面。
e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
WEB应用防火墙	（1）设备已根据需要不定期地对已发布的新固件版本进行更新；

上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。
恶意代码防范	
应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	
WEB应用防火墙 防火墙-1 防火墙-2	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	鉴别数据、重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； （2）设备对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a）应提供重要数据的本地数据备份与恢复功能；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。

3.4.2.2 主要安全问题汇总分析

安全通用要求

（1）设备不具备相关可信验证的技术措施（如：WEB应用防火墙）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.3 服务器和终端

3.4.3.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统对登录系统的用户进行身份鉴别； （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； （5）用户属性策略未勾选“密码永不过期”。
应用服务器-1 应用服务器-2 数据库服务器	（1）操作系统对登录系统的用户进行身份鉴别； （2）操作系统不存在空口令用户； （3）操作系统不存在默认信任的登录模式； （4）操作系统为登录用户设置的身份标识具有唯一性； （5）操作系统配置的一定的密码长度且定期更换； （6）操作系统配置一定的密码复杂度策略。
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统启用登录失败处理策略。 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略。
应用服务器-1 应用服务器-2 数据库服务器	（1）操作系统启用pam_tally2模块的合规登录失败处理策略； （2）操作系统配置合规的操作超时锁定； （3）操作系统启用SSH的合规登录超时策略。
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS的管理。
应用服务器-1 应用服务器-2 数据库服务器	（1）操作系统配置合规的远程管理模式； （2）操作系统远程端口使用情况合规； （3）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
访问控制	
a) 应对登录的用户分配账户和权限；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权

	限分配表情况一致。
应用服务器-1 应用服务器-2 数据库服务器	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在所有用户均属于root组的情况。
b）应重命名或删除默认账户，修改默认账户的默认口令；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统针对默认账户采用相应的安全策略配置； （2）操作系统账户不存在弱口令或空口令。
应用服务器-1 应用服务器-2 数据库服务器	（1）操作系统对多余帐户进行删除、锁定或禁止其登录； （2）操作系统账户口令设置合规。
c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
业务终端-1 业务终端-2 应用服务器-1 应用服务器-2 数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。
d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统根据安全策略要求对特权用户进行分离； （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
应用服务器-1 应用服务器-2 数据库服务器	（1）操作系统根据安全策略要求对特权用户进行分离； （2）操作系统不存在除root外的特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统开启审计策略，操作系统审计策略基本完整； （2）审计覆盖所有用户操作审计和记录。
应用服务器-1 应用服务器-2 数据库服务器	（1）操作系统开启审计功能，审计进程正常； （2）操作系统开启审计范围及策略满足要求，审计覆盖所有用户操作审计和记录。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
业务终端-1 业务终端-2 应用服务器-1	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。

应用服务器-2 数据库服务器 运维及管理终端-1 运维及管理终端-2	
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统采取对审计记录存储容量如下： 运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。
应用服务器-1 应用服务器-2 数据库服务器	(1)操作系统限制审计文件的访问控制权限,普通用户不可删除及修改; （2）操作系统针对日志、审计记录具备充足的存储容量； （3）操作系统采取合规的日志文件权限策略； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。
入侵防范	
a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。
应用服务器-1 应用服务器-2 数据库服务器	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。
b) 应关闭不需要的系统服务、默认共享和高危端口；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统不存在多余的默认共享及其它文件共享； （2）操作系统关闭不必要端口； （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。
应用服务器-1 应用服务器-2 数据库服务器	（1）操作系统关闭不必要端口； （2）操作系统禁用不必要服务； （3）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口； （4）漏洞扫描未发现高风险主机端口。
c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。

应用服务器-1 应用服务器-2 数据库服务器	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。
应用服务器-1 应用服务器-2 数据库服务器	（1）操作系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。
恶意代码防范	
应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。
应用服务器-1 应用服务器-2 数据库服务器	（1）操作系统安装深信服edr防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	鉴别数据、重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。
应用服务器-1 应用服务器-2 数据库服务器	鉴别数据: （1）系统在通信传输过程中对鉴别数据采取完整性保护措施。 重要配置数据: （1）系统在通信传输过程中对重要配置数据采取完整性保护措施。
数据备份恢复	
a）应提供重要数据的本地数据备份与恢复功能；	
业务终端-1 业务终端-2 应用服务器-1 应用服务器-2 数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。

剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施： 安全选项“不显示上次的用户名”->启用
应用服务器-1 应用服务器-2 数据库服务器	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统不保存过多终端历史记录。

3.4.3.2 主要安全问题汇总分析

安全通用要求

（1）缺乏对计算设备可信验证方面的安全设计要求。现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。现有的计算设备存在对系统运行过程中的可信检验不全面的情况。现有的可信验证存在部分告警、审计及联动措施不全面的情况(如：应用服务器-1）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.4 系统管理软件/平台

3.4.4.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
数据库服务器-Oracle	（1）数据库系统对登录系统的用户进行身份鉴别； （2）数据库系统不存在弱口令用户； （3）数据库系统为登录用户设置的身份标识具有唯一性； （4）数据库系统配置合规的密码长度及复杂度策略； （5）数据库系统配置合规的密码有效周期策略。
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
数据库服务器-Oracle	（1）数据库系统启用合规登录失败处理策略； （2）数据库系统执行合规的锁定策略。

c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
数据库服务器-Oracle	（1）数据库系统配置合规的远程管理模式。
访问控制	
a) 应对登录的用户分配账户和权限；	
应用服务器-1-Tomcat 应用服务器-2-Tomcat	（1）对应不同的账户均按需分配不同的用户权限，不存在中间件用户均属于管理级别、高权限的情况； （2）中间件配置可降权启动Tomcat的用户； （3）宿主系统针对中间件用户分别赋予相应的管理操作权限。
数据库服务器-Oracle	（1）登录数据库系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （2）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在多用户均与sys、DBA用户权限一致的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。
b) 应重命名或删除默认账户，修改默认账户的默认口令；	
应用服务器-1-Tomcat 应用服务器-2-Tomcat	（1）中间件不存在除如:Tomcat、admin、manager、role1等默认账户名； （2）中间件账户口令设置合规。
数据库服务器-Oracle	（1）数据库系统对多余帐户进行删除、锁定或禁止其登录； （2）数据库系统账户口令设置合规。
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
应用服务器-1-Tomcat 应用服务器-2-Tomcat	（1）中间件不存在多余或过期账户； （2）中间件管理员用户与账户之间一一对应； （3）中间件启用合规的管理用户名配置。
数据库服务器-Oracle	（1）数据库系统不存在多余或过期账户； （2）数据库系统管理员用户与账户之间一一对应。
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	
应用服务器-1-Tomcat 应用服务器-2-Tomcat	（1）中间件根据安全策略要求对特权用户及宿主管理用户进行分离； （2）中间件管理不存在多个管理级别高的特权用户； （3）中间件管理按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
数据库服务器-Oracle	（1）数据库系统根据安全策略要求对特权用户进行分离； （2）数据库系统用户权限合理，非管理员未设置过大权限； （3）数据库系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
应用服务器-1-Tomcat 应用服务器-2-Tomcat	（1）中间件开启审计功能，审计进程正常； （2）系统的日志审计级别满足要求。
数据库服务器-Oracle	（1）数据库系统开启审计功能，审计进程正常； （2）ORACLE数据库系统启动数据库日志模式和自动归档； （3）审计覆盖所有用户操作审计和记录。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
应用服务器-1-Tomcat 应用服务器-2-Tomcat	（1）中间件日期、时间正常； （2）中间件审计记录开启审核策略且日志级别正常。

数据库服务器-Oracle	（1）数据库宿主系统日期、时间正常； （2）数据库系统审计记录内容基本完整。
c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
应用服务器-1-Tomcat 应用服务器-2-Tomcat	（1）中间件限制审计文件的访问控制权限，普通用户不可删除及修改； （2）宿主系统针对中间件日志、审计记录具备充足的存储容量； （3）对中间件审计记录进行定期存档备份，其备份策略有效； （4）审计记录及日志保存大于6个月。
数据库服务器-Oracle	（1）数据库系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）数据库系统针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）日志及审计记录保存大于6个月。
入侵防范	
c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
数据库服务器-Oracle	（1）网络设备ACL策略有效限制访问本机的IP地址及管理模式。
d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	
应用服务器-1-Tomcat 应用服务器-2-Tomcat	（1）中间件管理具备数据有效性检验功能； （2）中间件管理的校验接口范围较全面。
e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
应用服务器-1-Tomcat 应用服务器-2-Tomcat	（1）中间件已根据需要不定期地对已发布的版本进行更新； （2）中间件更新安装前进行安全性和兼容性测试； （3）在系统上线或发生重大变更时测试并安装最新的中间件版本或更新补丁； （4）在不影响业务系统正常运行情况下，对发现的中间件漏洞在确保安全的情况下进行修补； （5）中间件进行扫描未发现存在可造成高风险的漏洞。
数据库服务器-Oracle	（1）数据库系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）数据库宿主系统不存在启用未加控制的高危端口； （3）MY_SQL分离默认安装的示例数据库； （4）数据库系统进行渗透及扫描未发现存在可造成高风险的漏洞。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
应用服务器-1-Tomcat 应用服务器-2-Tomcat	鉴别数据、重要配置数据: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。
数据库服务器-Oracle	鉴别数据、重要配置数据: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a）应提供重要数据的本地数据备份与恢复功能；	
应用服务器-1-Tomcat 应用服务器-2-Tomcat	（1）系统定义了相关需要备份的中间件重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）宿主系统定期完全依照备份策略，采用正确的配置进行本地备份；

	（4）中间件相关数据的备份周期合理：每天增量一次、每月全备一次； （5）中间件开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
数据库服务器-Oracle	（1）数据库系统定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）数据库系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	
应用服务器-1-Tomcat 应用服务器-2-Tomcat	（1）宿主系统具有清除用户鉴别信息的功能； （2）经测试，宿主系统退出后无法访问先前中间件登录过的页面； （3）经测试，宿主系统关闭后无残留的中间件用户鉴别信息。
数据库服务器-Oracle	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）数据库系统不保存终端历史记录。
个人信息保护	
a）应仅采集和保存业务必需的用户个人信息；	
数据库服务器-Oracle	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）数据库存储的用户个人信息均为业务应用必需的环节。
b）应禁止未授权访问和非法使用用户个人信息。	
数据库服务器-Oracle	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； （2）数据库具备控制措施禁止未授权访问用户个人信息表单； （3）数据库具备控制措施禁止非法使用用户个人信息表单。

3.4.4.2 主要安全问题汇总分析

安全通用要求

（1）未能提供中间件重要数据的异地定时数据备份功能（如：应用服务器-1-Tomcat）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

3.4.5 业务应用系统/平台

3.4.5.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
教学管理信息服务平台	（1）系统对各登录模式均启用身份鉴别； （2）系统对登录管理的用户进行身份鉴别； （3）系统登录用户设置的身份标识具有唯一性； （4）系统不存在空口令用户； （5）设备配置合规的密码策略。
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
教学管理信息服务平台	（1）系统启用合规登录失败处理策略； （2）系统配置合规的操作超时退出措施。
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
教学管理信息服务平台	(1)应用系统的用户鉴别数据采用SHA-512算法在可控网络环境中传输； （2）系统配置合规的远程管理模式。
访问控制	
a) 应对登录的用户分配账户和权限；	
教学管理信息服务平台	（1）可提供系统权限分配表； （2）登录系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需分配不同的用户权限，不存在所有用户均属于管理级别、高权限的情况。
b) 应重命名或删除默认账户，修改默认账户的默认口令；	
教学管理信息服务平台	（1）系统禁用默认账户名； （2）系统账户口令设置合规。
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
教学管理信息服务平台	（1）系统不存在多余或过期账户； （2）系统管理员用户与账户之间一一对应。
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	
教学管理信息服务平台	（1）系统不存在多个管理级别高的特权用户； （2）系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
教学管理信息服务平台	（1）系统开启审计功能，审计进程正常； (2)系统的日志审计级别满足要求,审计覆盖所有用户操作审计和记录。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
教学管理信息服务平台	（1）系统日期、时间正常； （2）系统审计记录内容基本完整。
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
教学管理信息服务平台	（1）系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）系统针对日志、审计记录具备充足的存储容量； （3）审计记录及日志保存大于6个月。

入侵防范	
c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
教学管理信息服务平台	（1）系统自身设定有效的终端访问策略，通过访问措施进行管理地址的限制。
d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	
教学管理信息服务平台	（1）系统具备数据有效性检验功能； （2）系统的校验接口范围较全面。
e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
教学管理信息服务平台	（1）系统已根据需要不定期地对已发布的版本进行更新； （2）在系统上线或发生重大变更时测试并安装最新的版本或更新补丁； （3）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
教学管理信息服务平台	鉴别数据、重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； （2）系统对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
教学管理信息服务平台	（1）系统定义了相关需要备份重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	
教学管理信息服务平台	（1）系统具有清除用户鉴别信息的功能； （2）经测试，系统退出后无法访问先前登录过的页面； （3）经测试，系统关闭后无残留的用户鉴别信息。
个人信息保护	
a) 应仅采集和保存业务必需的用户个人信息；	
教学管理信息服务平台	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息； （3）系统采集的用户个人信息均为业务应用必需的环节。
b) 应禁止未授权访问和非法使用用户个人信息。	
教学管理信息服务平台	（1）系统不采集和保存任何形式的用户个人信息； （2）系统对所有涉及个人信息的环节均有明确的授权同意过程； （3）系统具备控制措施禁止未授权访问用户个人信息； （4）系统具备控制措施禁止非法使用用户个人信息。

3.4.5.2 主要安全问题汇总分析

安全通用要求

（1）未能提供应用软件系统重要数据的异地定时数据备份功能（如：教学管理信息服务平台）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

3.4.6 数据资源

3.4.6.1 已有安全控制措施汇总分析

安全通用要求

数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
重要业务数据 重要个人信息	（1）系统在通信传输过程中对相关数据采取完整性保护措施； （2）系统对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
重要业务数据 重要个人信息	（1）系统定义了相关需要备份重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
个人信息保护	
a) 应仅采集和保存业务必需的用户个人信息；	
重要个人信息	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息； （3）系统采集的用户个人信息均为业务应用必需的环节。
b) 应禁止未授权访问和非法使用用户个人信息。	
重要个人信息	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； （2）系统具备控制措施禁止未授权访问用户个人信息； （3）系统具备控制措施禁止非法使用用户个人信息。

3.4.6.2 主要安全问题汇总分析

安全通用要求

重要业务数据

（1）未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要业务数据）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

重要个人信息

（1）未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要个人信息）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

3.4.7 其他系统或设备

3.4.7.1 已有安全控制措施汇总分析

安全通用要求

无其他系统或设备，不涉及相关测评

3.4.7.2 主要安全问题汇总分析

安全通用要求

无其他系统或设备，不涉及相关测评

3.5 安全管理中心

3.5.1 已有安全控制措施汇总分析

安全通用要求

系统管理	
a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；	
管理中心	（1）网络中部署运维安全管理系统实现集中的系统管理； （2）系统对登录用户进行身份鉴别；

	（3）系统用户标识具有唯一性； （4）系统可实现对账户的身份鉴别数据进行保密性和完整性保护； （5）系统管理操作模式具备控制措施； （6）系统具备相应的管理操作审计措施。
审计管理	
a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；	
管理中心	（1）网络中部署运维安全管理系统实现集中安全审计功能； （2）审计系统对审计管理员进行身份鉴别； （3）审计系统用户标识具有唯一性； （4）审计系统管理操作模式具备控制措施； （5）审计系统具备相应的管理操作审计措施。
b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	
管理中心	教学管理信息服务平台: （1）审计管理员定期对审计记录进行分析，对发现的安全可疑事件及时处理； （2）单位具有安全审计策略文件，规范审计记录的存储、管理和查询要求； （3）审计管理员按规范要求对审计记录进行管理。 重要审计数据: 日志审计系统、运维安全管理系统: （1）设备在通信传输过程中对相关数据采取完整性保护措施； （2）设备对重要数据在传输过程中采取必要的完整性保护措施。

3.5.2 主要安全问题汇总分析

安全通用要求

（1）系统管理的资源、运行及配置管理不够全面（如：管理中心）。系统的资源和运行缺少统一的管理，将导致系统可能无法按规划实现基于资源配置、 系统加载、异常处理、及备份/恢复等的安全控制措施。 低风险。

3.6 安全管理制度

3.6.1 已有安全控制措施汇总分析

安全通用要求

安全策略	
应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。	
制度文件、执行/记录文件	（1）单位具有网络安全工作的总体方针和安全策略文件； （2）制度内容包括明确的单位安全工作要求； （3）管理文件详见《信息安全总体策略》。
管理制度	
a) 应对安全管理活动中的主要管理内容建立安全管理制度；	
制度文件、执行/记录文件	（1）单位有针对安全管理活动中的各类管理内容建立安全管理制度； （2）现有制度已覆盖管理活动的主要的方面； （3）制度详见：《信息安全总体策略》、《网络安全管理规范》、《组织安全结构和人员职责制度》、《人员管理制度》、《员工考核管理制度》。
b) 应对管理人员或操作人员执行的日常管理操作建立操作规程。	
制度文件、执行/记录文件	（1）单位针对相关业务日常管理的操作建立规程类管理制度； （2）现有制度已覆盖重要管理方面的系统维护手册和用户操作规程等； （3）管理文件详见《设备及系统软件配置和操作手册》。
制定和发布	
a) 应指定或授权专门的部门或人员负责安全管理制度的制定；	
制度文件、执行/记录文件	（1）单位针对安全管理制度的制定，指定教育信息与网络中心部主要负责； （2）在已制定的相关制度中可查阅到被授权制定管理制度的部门/人员信息； （3）管理文件详见《安全管理组织规范》。
b) 安全管理制度应通过正式、有效的方式发布，并进行版本控制。	
制度文件、执行/记录文件	（1）单位针对制度的制定和发布要求，制定管理规范文件； （2）管理规范文件对文件制定及发布定义了规范要求； （3）安全管理制度的收发登记记录有效； （4）管理文件详见《制度制定、发布、评审和修订管理制度》、《收发文登记记录》。
评审和修订	
应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	
制度文件、执行/记录文件	（1）单位针对制度的合理性和适用性需进行论证和审定及修订的要求，制定管理规范文件； （2）管理规范文件对制度的评审及修订定义了规范要求； （3）单位具有安全管理制度的审定或论证的过程记录； （4）单位对做过修订的制度，具备有修订版本的安全管理过程记录； （5）管理文件详见《制度制定、发布、评审和修订管理制度》及 《安全管理制度评审记录》。

3.6.2 主要安全问题汇总分析

安全通用要求

教学管理信息服务平台针对安全管理制度层面的安全通用要求采取的安全措施比较完善，未发现不符合项。

3.7 安全管理机构

3.7.1 已有安全控制措施汇总分析

安全通用要求

岗位设置	
a) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；	
制度文件、执行/记录文件	（1）单位已明确网络安全管理工作的职能部门，并明确了各岗位职责； （2）单位各部门职责文档已明确网络安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备网络安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。
b) 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。	
制度文件、执行/记录文件	（1）单位已明确系统安全管理工作的职能部门，并明确了各岗位职责； （2）单位各部门职责文档已明确系统安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备系统安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。
人员配备	
应配备一定数量的系统管理员、审计管理员和安全管理员等。	
制度文件、执行/记录文件	（1）单位针对人员配备要求，制定了管理制度； （2）单位按要求配备一定数量的重要岗位管理人员； （3）单位针对各岗位人员，制定并维护人员档案； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。
授权和审批	
a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；	
制度文件、执行/记录文件	(1)单位在制度中用文字描述或在流程图中明确,对关键活动进行审批； （2）单位对审批过程明确审批权限，对各项信息系统的重要操作与变更

	明确审批部门和批准人； （3）管理文件详见《授权和审批管理规定》。
b) 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。	
制度文件、执行/记录文件	（1）单位针对各项业务操作及变更等建立了审批程序规定； （2）单位针对系统变更、系统接入、物理范围等事项已明确按审批程序执行，记录有批准人签字； （3）管理文件详见《授权和审批管理规定》。
沟通和合作	
a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；	
制度文件、执行/记录文件	（1）单位针对机构内部管理人员之间、部门之间的沟通与合作，制定了管理制度； （2）单位的管理制度规范了合作和沟通的方式和周期； （3）单位有组织机构内部人员联系表； （4）单位有定期召开信息安全会议，保存有会议纪要； （5）管理文件详见《安全教育和培训制度》、《技能培训记录》《外部联系表》。
b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；	
制度文件、执行/记录文件	（1）单位针对加强与外部单位的合作与沟通，制定了管理制度规定； （2）单位能按要求与相关单位保持沟通合作，并提供相关单位联系方式和交流会议纪要； （3）管理文件详见《安全教育和培训制度》、《技能培训记录》、《外部联系表》。
c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	
制度文件、执行/记录文件	（1）单位建立了完善的对外联单位的联系列表； （2）管理文件详见《外部联系表》。

3.7.2 主要安全问题汇总分析

安全通用要求

（1）单位开展的检查工作不够完善（如：制度文件、执行/记录文件）。检查工作开展不仔细，可能对存在或潜在的安全风险不能被及时发现并进行处理。 低风险。

3.8 安全管理人员

3.8.1 已有安全控制措施汇总分析

安全通用要求

人员录用

a) 应指定或授权专门的部门或人员负责人员录用；	
制度文件、执行/记录文件	（1）单位授权专门的部门负责人员录用工作，制定了管理制度规范； （2）由人力资源保障科负责人员录用工作； （3）管理文件详见《人员管理制度》。
b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查。	
制度文件、执行/记录文件	（1）单位针对人员录用过程，制定了明确要求，并形成人员安全管理制度； （2）单位现有管理制度明确说明录用人员应具备的条件； （3）单位按规定执行人员录用的相关审查过程； （4）管理文件详见《人员管理制度》、《人员入职考核记录》。
人员离岗	
应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。	
制度文件、执行/记录文件	（1）单位针对离岗人员权限终止及取回机构提供的各种设施的要求，制定了管理制度； （2）单位按规范开展对离岗人员的相关管理工作； （3）管理文件详见《人员管理度》、《人员离岗申请表》、《离场信息资料交接表》。
安全意识教育和培训	
应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。	
制度文件、执行/记录文件	（1）单位针对人员安全培训及责任和惩戒措施，制定了管理制度； （2）单位已开展安全意识教育及岗位技能培训。 （3）管理文件详见《安全教育和培训制度》。
外部人员访问管理	
a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；	
制度文件、执行/记录文件	（1）单位针对外部人员物理访问，制定了外部人员访问管理文档； （2）单位具备有效的外部人员访问重要区域的书面申请文档； （3）单位具备外部人员访问重要区域的登记记录； （4）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。
b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；	
制度文件、执行/记录文件	（1）单位针对外部接入受控网络访问系统，制定了管理制度； （2）单位具备外部人员接入受控网络前的申请审批流程； （3）单位具备外部人员接入及访问系统的书面申请文档； （4）单位具备外部人员接入及访问系统的登记记录； （5）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。

3.8.2 主要安全问题汇总分析

安全通用要求

（1）单位未完全按管理规范开展人员离场后的清理工作（如：制度文件、执行/记录文件）。人员离场后的清理工作开展不规范，可能导致遗留外部人员访问受控区域的记录，存在被二次非法利用，造成泄密。 低风险。

3.9 安全建设管理

3.9.1 已有安全控制措施汇总分析

安全通用要求

定级和备案	
a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；	
制度文件、执行/记录文件	（1）单位的被测系统于2022年4月已完成备案； （2）系统备案相关文档（定级报告）中明确等级划分方法和理由，SAG三个方面的级别描述清晰； （3）管理文件详见《定级备案》。
b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；	
制度文件、执行/记录文件	(1)单位针对系统定级结果的审批及评审工作等要求,制定了管理制度; （2）现有系统的定级已具备合理性和正确性审定； （3）管理文件详见《定级备案》。
c) 应保证定级结果经过相关部门的批准；	
制度文件、执行/记录文件	（1）单位针对系统定级结果的上级批准要求，制定了管理制度； （2）现有系统的定级获得了相关部门的批准； （3）管理文件详见《定级备案》。
d) 应将备案材料报主管部门和相应公安机关备案。	
制度文件、执行/记录文件	（1）单位对被测系统的等级备案表、定级报告等备案材料已经报相应公安机关备案； （2）单位具备公安机关出具的备案号； （3）管理文件详见《定级备案》。
产品采购和使用	
a) 应确保网络安全产品采购和使用符合国家的有关规定；	
制度文件、执行/记录文件	（1）单位已建立安全产品管理的相关管理规定； （2）单位具备安全产品采购流程及相关实施文档； （3）被测系统使用的安全产品具备销售许可资质； （4）安全产品具均为国内产品； （5）管理文件详见《设备安全管理制度》。
b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。	
制度文件、执行/记录文件	（1）单位已建立密码产品与服务管理的相关管理制度； （2）系统未使用密码产品；

	（3）管理文件详见《设备安全管理制度》。
外包软件开发	
b）应保证开发单位提供软件设计文档和使用指南。	
制度文件、执行/记录文件	（1）单位制定软件开发项目验收要求，明确开发单位的提交材料； （2）开发单位提供软件日常维护和使用所需的文档； （3）管理文件详见《外包开发软件管理规定》、《设备及系统软件配置和操作手册》。
工程实施	
a）应指定或授权专门的部门或人员负责工程实施过程的管理；	
制度文件、执行/记录文件	（1）单位针对专门的部门负责工程实施过程的管理要求，制定管理度； （2）单位由专岗负责系统建设的工程实施，且按照实施方案的要求对进度和质量进行控制； （3）管理文件详见《工程实施管理制度》。
b）应制定安全工程实施方案控制工程实施过程。	
制度文件、执行/记录文件	（1）单位制定了详细的工程实施方案； （2）工程实施单位严格按照方案执行，并有过程记录； （3）管理文件详见《测试及验收方案》、《工程项目实施方案》。
系统交付	
a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；	
制度文件、执行/记录文件	（1）单位具备系统交付清单； （2）系统交付清单内容较详细； （3）单位的清点工作较合规； （4）管理文件详见《系统交付管理》、《资产清单》。
b）应对负责运行维护的技术人员进行相应的技能培训；	
制度文件、执行/记录文件	（1）单位已对负责系统运行维护的技术人员进行了技能培训； （2）具备运维人员的培训记录； （3）管理文件详见《系统交付管理》、《资产清单》、《系统交付清单》、《技能培训记录》。
c）应提供建设过程文档和运行维护文档。	
制度文件、执行/记录文件	（1）单位提供了系统建设过程中的文档； （2）单位提供了指导用户进行系统运维的文档和系统培训手册； （3）管理文件详见《系统交付管理》、《系统交付清单》、《设备及系统软件配置和操作手册》。
等级测评	
a）应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；	
制度文件、执行/记录文件	（1）单位针对系统等级测评要求，制定管理制度； （2）系统按要求开展首次测评工作； （3）管理文件详见《系统安全管理制度》。
b）应在发生重大变更或级别发生变化时进行等级测评；	
制度文件、执行/记录文件	（1）管理制度中已规定在系统发生变更时及时对系统进行等级测评； （2）系统未发生过重大变更，系统等级未发生变化； （3）管理文件详见《系统安全管理制度》。
c）应确保测评机构的选择符合国家有关规定。	

制度文件、执行/记录文件	（1）已选择在“全国等级保护测评机构推荐目录”中的测评单位进行等级测评； （2）管理文件详见《系统安全管理制度》、《网络安全等级保护测评服务合同》。
服务供应商选择	
a) 应确保服务供应商的选择符合国家的有关规定；	
制度文件、执行/记录文件	（1）单位在管理制度内明确提出安全服务供应商选择的要求； （2）单位选择的安全服务商符合国家的有关规定，具备相应的安全服务资质； （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。
b) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。	
制度文件、执行/记录文件	（1）单位的管理制度中已规定，需与安全服务商签订安全相关的协议并明确整个服务供应链各方需履行的网络安全相关义务； （2）单位已按规定与选定的安全服务商签订合规的协议； （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。

3.9.2 主要安全问题汇总分析

安全通用要求

（1）单位未具备适用于被测系统的安全规划设计方案（如：制度文件、执行/记录文件）。规划设计需求不全面，可能导致安全方案设计不完善，信息系统存在安全缺陷。低风险。

（2）单位未具备完整的安全设计方案相关的文档。单位相关方案的设计的内容不够完善（如：制度文件、执行/记录文件）。相关合规的规划配套文件缺失，可能导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。 中风险。

（3）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定。单位未对相关论证过程及内容进行完整的记录（如：制度文件、执行/记录文件）。未开展规范的审批过程，可能存在安全整体规划缺乏合理性和可行性，导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。 低风险。

（4）单位未在软件开发过程中对所有软件安全性进行测试。单位未在软件安装之前按要求对所有软件开展恶意代码检测（如：制度文件、执行/记录文件）。软件交付前恶意代码检测不规范，可能在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。 低风险。

（5）单位未完全根据测试验收方案组织相关部门和人员开展验收工作（如：制度文件、执行/记录文件）。可能由于验收测试不严谨，造成测试过程缺乏计划性及操作性，无法保证经过测试验收的系统达到既定的安全性等目标。 低风险。

(6)针对系统上线前的安全性测试工作存在问题(如:制度文件、执行/记录文件)。未按规定开展上线前测试，安全隐患可能在系统上线运行前未被发现并作出相应处理。低风险。

3.10 安全运维管理

3.10.1 已有安全控制措施汇总分析

安全通用要求

环境管理	
a) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；	
制度文件、执行/记录文件	（1）单位建立机房安全方面的管理制度，对有关运维方面的管理作出规定； （2）单位具备完整的机房出入登记记录； （3）单位具备完整的机房基础设施的维护记录； （4）管理文件详见《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。
b) 应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；	
制度文件、执行/记录文件	（1）单位建立机房安全方面的管理制度； （2）单位现有机房管理记录与制度相符； （3）制度详见：《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。
c) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	

制度文件、执行/记录文件	（1）单位机房安全管理制度已明确来访人员的接待区域的要求； （2）单位按规范要求开展人员来访接待； （3）单位办公环境未发现有随意放置含有敏感信息介质的情况； （4）制度详见：《机房安全管理制度》、《物理安全管理规范》、《办公环境保密管理》。
资产管理	
应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。	
制度文件、执行/记录文件	（1）单位已建立有效的资产清单； （2）单位现有资产清单内容较全面； （3）制度详见：《设备安全管理制度》、《资产清单》。
介质管理	
a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；	
制度文件、执行/记录文件	（1）介质按管理要求放置于受控的环境中（如：机房）； （2）介质管理具备较全面的记录； （3）制度详见：《设备安全管理制度》、《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。
b) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。	
制度文件、执行/记录文件	（1）介质管理制度中对介质安全传输有明确规定； （2）存储重要信息的介质在物理传输过程，具备严格的环节控制，无重大环节疏漏； （3）对介质的归档和查询均具备记录； （4）制度详见：《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。
设备维护管理	
a) 应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	
制度文件、执行/记录文件	（1）单位人员岗位职责相关文档已明确设备维护管理的责任部门； （2）单位对各类设施、设备进行定期维护； （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。
b) 应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。	
制度文件、执行/记录文件	（1）单位建立了配套设施、软硬件维护管理方面的管理制度； （2）单位开展相关工作与制度相符，且保留记录； （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。
网络和系统安全管理	
a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；	
制度文件、执行/记录文件	（1）单位建立系统安全管理文档，对系统管理员的管理制定了要求； （2）单位对各类关键角色建立了相应的工作职责文档； （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网

	络安全管理制度》。
b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	
制度文件、执行/记录文件	（1）单位制定管理制度，对系统账号进行管理； （2）单位按管理规范开展账号管理工作； （3）账户管理记录内容较完整； （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。
c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	
制度文件、执行/记录文件	（1）单位建立了网络和系统安全管理制度； （2）网络和系统安全管理制度内容较全面； （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。
d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；	
制度文件、执行/记录文件	（1）单位对重要设备、系统的配置和操作建立配置手册； （2）现有操作配置手册已明确操作步骤、参数配置； （3）制度详见：《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。
e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。	
制度文件、执行/记录文件	（1）单位制定日常运维管理的相关制度规范； （2）单位按制度规范开展日常运维管理工作； （3）单位具备合规的运维记录； （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》、《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。
恶意代码防范管理	
a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	
制度文件、执行/记录文件	（1）单位制定恶意代码防范管理制度，明确对外来计算机或存储设备接入系统前进行恶意代码检查； （2）单位按外来计算机接入恶意代码检查规范开展工作； （3）单位制定培训管理制度，明确需通过培训提升员工的防恶意代码意识； （4）单位按培训管理要求开展工作； （5）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申请表》、《信息管理系统漏洞检查表》。
b) 应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；	
制度文件、执行/记录文件	（1）建立恶意代码防范管理文档； （2）管理制度中覆盖防恶意代码软件的授权使用、恶意代码库升级、定期查杀等内容； （3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》。
配置管理	
应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。	

制度文件、执行/记录文件	（1）单位制定了基本配置信息管理的制度要求； （2）管理文件详见：《主机安全管理规范》、《网络安全管理规范》、《应用安全管理规范》、《网络配置信息》。
变更管理	
应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。	
制度文件、执行/记录文件	（1）单位建立了关于系统变更管理的制度文件； （2）现有变更管理制度覆盖了变更管理的各方面要求； （3）制度详见：《变更控制管理制度》、《通用变更记录表》。
备份与恢复管理	
a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；	
制度文件、执行/记录文件	（1）单位根据业务重要程度，制定了需要定期备份的重要业务信息列表或清单。清单内需要定期备份的重要数据已经过用户方确认； （2）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。
b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等；	
制度文件、执行/记录文件	（1）单位建立了备份与恢复管理相关的安全管理制度； （2）备份与恢复管理的相关要求比较明确； （3）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。
c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	
制度文件、执行/记录文件	（1）单位现有管理制度，明确了数据备份策略和数据恢复策略，以及备份程序和恢复程序； （2）单位可按策略要求实现重要数据的定期备份与恢复性测试； （3）单位现有的备份的数据均经过恢复性测试，可确保备份的数据可用； （4）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。
安全事件处置	
a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件；	
制度文件、执行/记录文件	（1）单位已在安全培训及宣传过程中告知用户在发现安全弱点和可疑事件时及时向安全管理部门报告； （2）单位在系统运维过程中对发现的安全弱点和可疑事件均编制了对应的报告或相关文档； （3）单位现有安全弱点和可疑事件报告文档内容较详实； （4）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。
b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；	
制度文件、执行/记录文件	（1）单位制定了安全事件报告和处置管理制度； （2）现有安全事件管理制度内容较完整； （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。
c) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。	
制度文件、执行/记录文件	（1）单位具备对安全事件的分析、处理、总结、防范等的报告／过程文档；

	（2）单位提供的安全事件报告和响应处置记录内容较完整； （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。
应急预案管理	
a）应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；	
制度文件、执行/记录文件	（1）单位制定重要事件的应急预案； （2）单位现有应急预案涉及的类型范围较全面； （3）单位现有应急预案的内容较完整； （4）制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。
b）应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。	
制度文件、执行/记录文件	（1）单位定期对相关人员进行应急预案培训； （2）单位根据不同的应急预案，按要求进行应急演练； （3）单位具备近期应急预案工作开展的相关记录； （4）单位提供的应急预案培训记录比较完整； （5）单位提供的应急预案演练记录比较完整； （6）经检查单位目前一旦出现应急事件，可参照预案合理有序的进行应急事件处置过程； （7）制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。

3.10.2 主要安全问题汇总分析

安全通用要求

（1）单位未严格按规范开展漏洞及安全隐患检测工作（如：制度文件、执行/记录文件）。漏洞检测、修补工作不到位，可能存在未授权人员利用漏洞攻击信息系统的风险。 低风险。

（2）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作（如：制度文件、执行/记录文件）。可能导致系统恶意代码检测管理不到位，存在信息系统感染恶意代码，从而导致严重的信息安全风险。 低风险。

（3）单位不了解现有密码相关的国家标准和行业标准。单位缺乏密码管理要求的制度文档（如：制度文件、执行/记录文件）。密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不到位，存在违反国家政策的风险。 中风险。

3.11 其他安全要求指标

3.11.1 已有安全控制措施汇总分析

本次测评未涉及其他安全要求指标。

3.11.2 主要安全问题汇总分析

本次测评未涉及其他安全要求指标。

3.12 验证测试

验证测试包括漏洞扫描，渗透测试等，验证测试发现的安全问题对应到相应的测评项的结果记录中。详细验证测试报告见报告附录。

3.12.1 漏洞扫描

3.12.1.1 漏洞扫描结果统计

本次测评主要使用了[绿盟远程安全评估系统]对系统的设备进行了安全扫描，其所涉及的系统版本为：[V6.0R04F01SP06]，规则库版本为：[V6.0R02F01.2900]。扫描结果如下：

经分析统计，共发现各接入点存在2类漏洞，其中0类危险程度为高的漏洞，0类危害程度为中的漏洞，2类危害程度为低的漏洞。

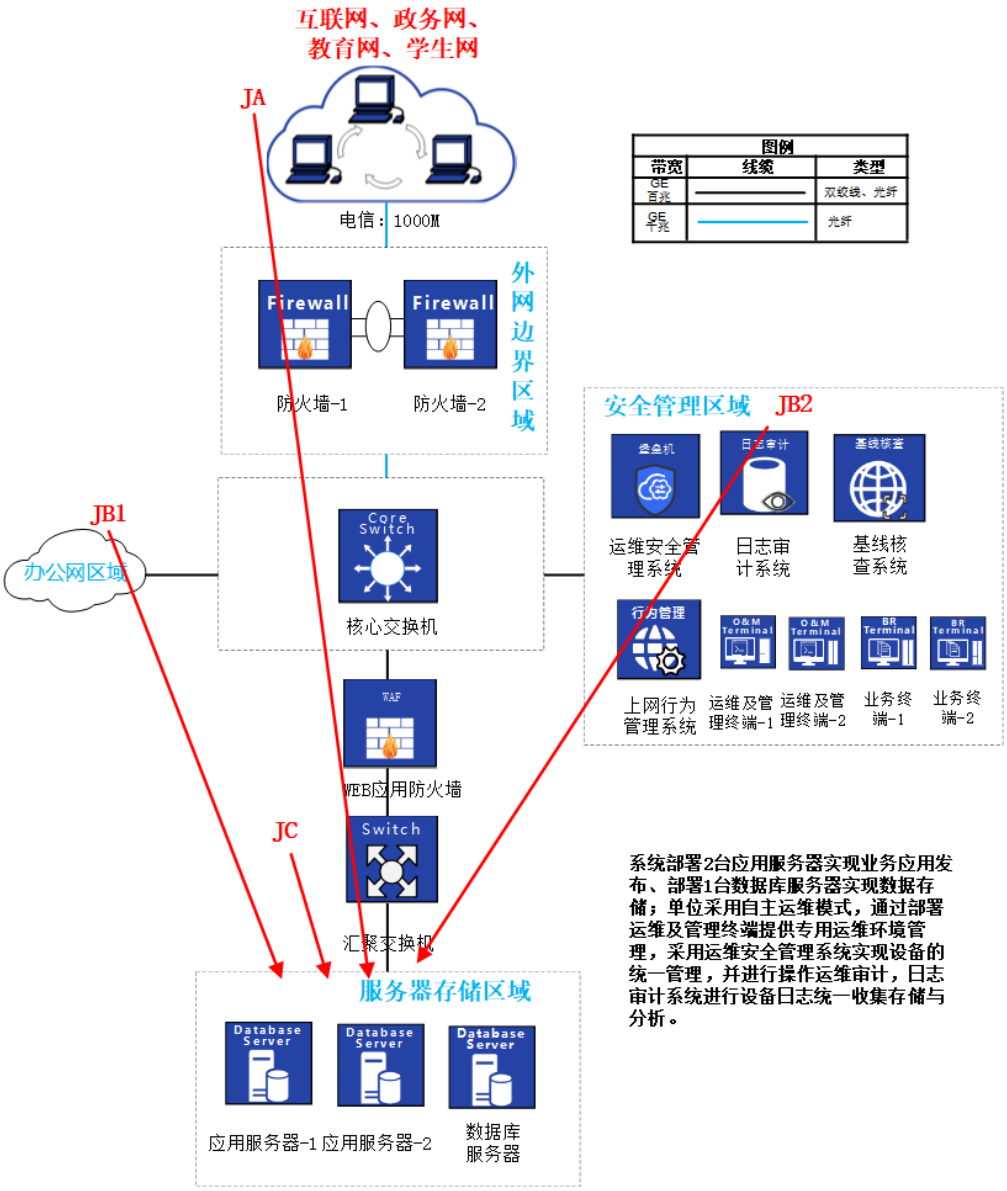


图 3-1 漏洞扫描工具接入测试示意图

接入点JA：在防火墙外侧接入，开展扫描/渗透主要目的是，探测对外服务功能区上各服务器、应用系统对外部网络边界暴露的安全漏洞情况，并根据漏洞扫描的结果接入渗透测试工具集，试图利用服务器、应用的安全漏洞入侵网络的行为。

接入点JB：在办公网区域VLAN段、安全管理区域VLAN段接入，开展扫描/渗透主要目的是，模拟外联单位/内部恶意用户发现操作系统、数据库、Web应用、第三方产品等安全漏洞的过程，并尝试利用以上漏洞实施诸如获取系统控制权（GetShell）、获得大量敏感信息（DragLibrary）等模拟攻击行为。

接入点JC：在系统所在VLAN的交换机接入，开展扫描/渗透主要目的是，直接测试对服务功能区上各服务器在最小化防御的基础上，对网络暴露的安全漏洞情况。

（1）接入点A漏洞扫描结果统计

根据在接入点A对16台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-1 接入点 A 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	0	0	0	0
2	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	0	0	0	0
3	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	0	0	0	0
4	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	0	0	0	0
5	172.16.1.14/上网行为管理系统	(安全设备)深信服 AC12.0.26	0	0	0	0
6	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	0	0	0	0
7	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	0	0	0	0
8	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	0	0	0	0
9	192.168.33.11/业务终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
10	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
11	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
12	192.168.33.10/业务终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
13	10.2.2.16/数据库服务器	(服务器存储设备)CentOS 7.7	0	0	0	0
14	10.2.2.17/应用服务器-1	(服务器存储设备)CentOS 7.7	0	0	0	0
15	10.2.2.18/应用服务器-2	(服务器存储设备)CentOS 7.7	0	0	0	0
16	https://jwc.mmpt.edu.cn/教学管理信息服务平台	(业务应用软件平台) V6.0	0	0	0	0

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
安全漏洞数量小计			0	0	0	0

（2）接入点B漏洞扫描结果统计

根据在接入点B对16台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-2 接入点 B 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	1	0	0	1
2	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	1	0	0	1
3	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	1	0	0	1
4	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	2	0	0	2
5	172.16.1.14/上网行为管理系统	(安全设备)深信服AC12.0.26	1	0	0	1
6	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	1	0	0	1
7	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	1	0	0	1
8	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	1	0	0	1
9	192.168.33.11/业务终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
10	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
11	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
12	192.168.33.10/业务终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
13	10.2.2.16/数据库服务器	(服务器存储设备)CentOS 7.7	1	0	0	1
14	10.2.2.17/应用服务器-1	(服务器存储设备)CentOS 7.7	1	0	0	1
15	10.2.2.18/应用服务器-2	(服务器存储设备)CentOS 7.7	1	0	0	1

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
16	https://jwc.mmpt.edu.cn/教学管理信息服务平台	(业务应用软件平台) V6.0	0	0	0	0
安全漏洞数量小计			12	0	0	12

(3) 接入点C漏洞扫描结果统计

根据在接入点C对16台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-3 接入点 C 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	1	0	0	1
2	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	1	0	0	1
3	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	1	0	0	1
4	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	2	0	0	2
5	172.16.1.14/上网行为管理系统	(安全设备)深信服AC12.0.26	1	0	0	1
6	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	1	0	0	1
7	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	1	0	0	1
8	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	1	0	0	1
9	192.168.33.11/业务终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
10	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
11	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
12	192.168.33.10/业务终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
13	10.2.2.16/数据库服务器	(服务器存储设备)CentOS 7.7	1	0	0	1
14	10.2.2.17/应用服务器-1	(服务器存储设备)CentOS 7.7	1	0	0	1

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
15	10.2.2.18/应用服务器-2	(服务器存储设备)CentOS 7.7	1	0	0	1
16	https://jwc.mmpt.edu.cn/教学管理信息服务平台	(业务应用软件平台) V6.0	0	0	0	0
安全漏洞数量小计			12	0	0	12

3.12.1.2 漏洞扫描问题描述

通过对漏洞扫描结果进行分析,教学管理信息服务平台存在的主要安全漏洞汇总如下表所示

表 3-4 主要安全漏洞汇总表

序号	安全漏洞名称	关联资产/域名	严重程度
1	允许Traceroute探测 此类漏洞涉及网络设备、安全设备、服务器存储设备。	10.2.2.16/数据库服务器 10.2.2.17/应用服务器-1 10.2.2.18/应用服务器-2 10.2.1.4/运维安全管理系统 10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/上网行为管理系统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/汇聚交换机 172.16.1.2/核心交换机	低
2	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161) 此类漏洞涉及网络设备。	172.16.1.2/核心交换机	低

3.12.2 渗透测试

经分析统计，共发现各接入点存在1类漏洞，其中0类危险程度为高的漏洞，0类危害程度为中的漏洞，1类危害程度为低的漏洞。

3.12.2.1 渗透测试过程说明

方案制定：

在得到委托单位的书面授权许可后，才进行渗透测试的实施。并且将实施范围、方法、时间、人员等具体的方案委托单位进行交流，并得到委托单位的认同。在测试实施之前，会做到让委托单位对渗透测试过程和风险的知晓，使随后的正式测试流程都在委托单位的管控下。

信息收集：

此阶段中，渗透测试人员对目标信息系统进行必要的信息收集，如操作系统类型、开放的端口和服务、中间件信息、后台数据库类型、web开发语言等，即收集有利于漏洞挖掘的相关信息，为渗透测试做准备。

漏洞挖掘方法：

此阶段中，渗透测试人员对目标信息系统开始进行渗透测试，利用已知信息和现有条件及技术进行漏洞挖掘，尽可能发现目标信息系统中存在的所有安全风险，并进行记录。

漏洞利用：

此阶段中，渗透测试人员对目标信息系统对上一阶段漏洞挖掘中发现的漏洞进行必要的利用以证明其危害性，再对渗透测试过程所产生的测试数据进行清除。

输出报告：

此阶段中，渗透测试人员把渗透测试记录、截图等相关信息进行整理，然后撰写渗透测试报告，最终提交给委托单位。

漏洞修复：

此阶段中，委托单位依据收到的渗透测试报告对其中所提出的漏洞进行整改，可参考报告中所提出的修复建议，整改完成后联系本单位相关人员准备回归测试。

回归测试：

此阶段中，渗透测试人员对整改后的目标信息系统进行复测，以确定报告中提出的漏洞是否已被修复，若已被修复，则进入下一阶段；否则，返回上一阶段。

测试工具：

序号	工具	工具用途
1	Burpsuite Pro	用于攻击Web应用程序的集成软件
2	Sqlmap	开源的自动化SQL注入工具
3	Nmap	开源的网络发现和安全审计工具
4	OWASP ZAP	自动化Web应用漏洞扫描工具
5	其他测试工具	根据信息系统的类别选择不同的工具（如自写脚本、目录扫描器、木马扫描器、其它开源工具等）

3.12.2.2 渗透测试问题描述

通过渗透测试发现，教学管理信息服务平台存在的安全问题汇总如下表所示。

表 3-5 渗透测试结果汇总表

序号	安全问题	关联资产/域名	严重程度
1	缺少“Content-Security-Policy”响应头 此类漏洞涉及业务应用软件平台。	https://jwc.mmpt.edu.cn/ 教学管理信息服务平台	低

3.13 单项测评小结

3.13.1 控制点符合情况汇总

根据单项测评结果汇总控制点符合情况如下表所示。（表格以不同颜色对测评结果进行区分，不符合的安全控制点采用红色标识，部分符合的采用黄色标识，不适用的采用蓝色标识且不做勾选。）

表 3-6 控制点符合情况汇总表

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
1	安全通用要求	安全物理环境	物理位置选择	√		
2			物理访问控制		√	
3			防盗窃和防破坏	√		
4			防雷击	√		
5			防火		√	
6			防水和防潮	√		
7			防静电			√
8			温湿度控制	√		
9			电力供应	√		
10			电磁防护	√		
11	安全通用要求	安全通信网络	网络架构		√	
12			通信传输	√		
13			可信验证			√
14	安全通用要求	安全区域边界	边界防护	√		
15			访问控制	√		
16			入侵防范		√	
17			恶意代码和垃圾邮件防范		√	
18			安全审计	√		
19			可信验证			√

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
20	安全通用要求	安全计算环境	身份鉴别	√		
21			访问控制	√		
22			安全审计	√		
23			入侵防范	√		
24			恶意代码防范	√		
25			可信验证			√
26			数据完整性	√		
27			数据备份恢复		√	
28			剩余信息保护	√		
29			个人信息保护	√		
30	安全通用要求	安全管理中心	系统管理		√	
31			审计管理	√		
32	安全通用要求	安全管理制度	安全策略	√		
33			管理制度	√		
34			制定和发布	√		
35			评审和修订	√		
36	安全通用要求	安全管理机构	岗位设置	√		
37			人员配备	√		
38			授权和审批	√		
39			沟通和合作	√		

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
40			审核和检查		√	
41	安全通用要求	安全管理人员	人员录用	√		
42			人员离岗	√		
43			安全意识教育和培训	√		
44			外部人员访问管理		√	
45	安全通用要求	安全建设管理	定级和备案	√		
46			安全方案设计			√
47			产品采购和使用	√		
48			自行软件开发			
49			外包软件开发		√	
50			工程实施	√		
51			测试验收		√	
52			系统交付	√		
53			等级测评	√		
54			服务供应商选择	√		
55	安全通用要求	安全运维管理	环境管理	√		
56			资产管理	√		
57			介质管理	√		
58			设备维护管理	√		
59			漏洞和风险管理			√

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
60			网络和系统安全管理	√		
61			恶意代码防范管理		√	
62			配置管理	√		
63			密码管理			√
64			变更管理	√		
65			备份与恢复管理	√		
66			安全事件处置	√		
67			应急预案管理	√		
68			外包运维管理			
安全通用要求控制点符合情况数量统计				47	12	7
控制点符合情况数量统计				47	12	7

3.13.2 安全问题汇总

针对单项测评结果中存在的部分符合和不符合项进行汇总，形成了安全问题如下表所示。

表 3-7 安全问题汇总表

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T1	（1）机房出入口未配置电子门禁系统。	信息化机房	安全通用要求	安全物理环境	物理访问控制	机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。
T2	（1）机房建设未完全采用符合耐火等级的建筑材料； （2）机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级。	信息化机房	安全通用要求	安全物理环境	防火	b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T3	（1）机房内缺乏防静电措施（如防静电地板或铺设防静电地毯 ）。	信息化机房	安全通用要求	安全物理环境	防静电	应采用防静电地板或地面并采用必要的接地防静电措施。
T4	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	安全通用要求	安全通信网络	网络架构	a）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
T5	（1）缺乏对通信设备可信验证方面的安全设计要求； （2）现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况。	安全通信网络	安全通用要求	安全通信网络	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T6	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	安全通用要求	安全区域边界	入侵防范	应在关键网络节点处监视网络攻击行为。
T7	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	安全通用要求	安全区域边界	恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。
T8	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	办公网区域 外网边界区域 安全管理区域 服务器存储区域	安全通用要求	安全区域边界	可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T9	（1）设备不具备相关可信验证的技术措施。	WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统	安全通用要求	安全计算环境	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
		核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2				警，并将验证结果形成审计记录送至安全管理中心。
T10	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。	业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	安全通用要求	安全计算环境	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T11	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况； （3）现有的计算设备存在对系统运行过程中的可信检验不全面的情况； （4）现有的可信验证存在部分告警、审计及联动措施不全面的情况。	应用服务器-1 应用服务器-2 数据库服务器	安全通用要求	安全计算环境	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T12	（1）未能提供中间件重要数据的异地定时数据备份功能。	应用服务器-1-Tomcat 应用服务器-2-Tomcat	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T13	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	教学管理信息服务平台	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T14	（1）未能提供数据库系统重要数据的异地定时数据备份功能。	数据库服务器-Oracle	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T15	（1）未能提供应用软件系统重要数据的异地定时数	重要业务数据 重要个人信息	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
	据备份功能。					将重要数据定时批量传送至备用场地。
T16	（1）系统管理的资源、运行及配置管理不够全面。	管理中心	安全通用要求	安全管理中心	系统管理	b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
T17	（1）单位开展的检查工作不够完善。	制度文件、执行/记录文件	安全通用要求	安全管理机构	审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。
T18	（1）单位未完全按管理规范开展人员离场后的清理工作。	制度文件、执行/记录文件	安全通用要求	安全管理人员	外部人员访问管理	c）外部人员离场后应及时清除其所有的访问权限。
T19	（1）单位未具备适用于被测系统的安全规划设计方案。	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
T20	（1）单位未具备完整的安全设计方案相关的文档； （2）单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	b）应根据保护对象的安全保护等级进行安全方案设计；
T21	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； （2）单位未对相关论证过程及内容进行完整的记录。	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	c）应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。
T22	（1）单位未在软件开发过程中对所有软件安全性进行测试； （2）单位未在软件安装之前按要求对所有软件开展恶意代码检测。	制度文件、执行/记录文件	安全通用要求	安全建设管理	外包软件开发	a）应在软件交付前检测其中可能存在的恶意代码；
T23	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	安全通用要求	安全建设管理	测试验收	a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T24	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	安全通用要求	安全建设管理	测试验收	b）应进行上线前的安全性测试，并出具安全测试报告。
T25	（1）单位未严格按规范开展漏洞及安全隐患检测工作。	制度文件、执行/记录文件	安全通用要求	安全运维管理	漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。
T26	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	安全通用要求	安全运维管理	恶意代码防范管理	c）应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。
T27	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	制度文件、执行/记录文件	安全通用要求	安全运维管理	密码管理	a）应遵循密码相关国家标准和行业标准；

4 整体测评

从安全控制间、区域间和验证测试等方面对单元测评的结果进行验证、分析和整体评价。

具体内容参见《GB/T 28448-2019信息安全技术 网络安全等级保护测评要求》。

4.1 安全控制点间安全测评

安全控制间的安全测评主要考虑同一区域内、同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用。安全功能上的增强和补充可以使两个不同强度、不同等级的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。

4.1.1 安全建设管理

4.1.1.1 安全通用要求

（T23）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。

单位未具备适用于被测系统的安全规划设计方案。安全方案设计不完善，导致规划设计需求不全面，信息系统存在安全缺陷。可升高单位未完全根据测试验收方案组织相关部门和人员开展验收工作的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

（T24）针对系统上线前的安全性测试工作存在问题。

单位未在软件交付之前按要求对所有软件开展恶意代码检测，导致在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。可升高针对系统上线前的安全性测试工作存在问题的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

4.1.2 安全运维管理

4.1.2.1 安全通用要求

（T26）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。

单位未严格按规范开展漏洞及安全隐患检测工作，漏洞检测工作不到位，导致存在未授权人员利用漏洞攻击信息系统的风险。可升高单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

4.2 区域间安全测评

区域间的安全测评主要考虑互连互通（包括物理上和逻辑上的互连互通等）的不同区域之间存在的安全功能增强、补充和削弱等关联作用，特别是有数据交换的两个不同区域。

4.2.1 安全物理环境

4.2.1.1 安全通用要求

（T1）机房出入口未配置电子门禁系统。

机房所在位置处于内部受控区域，非授权人员无法随意通过现有控制措施（如机械锁）进出机房，且具备相对完善的机房出入管理要求（具备《机房安全管理制度》），并实际执行措施效果良好（具备《机房出入登记表》），可降低机房出入口访问控制措施缺失的问题严重程度（如信息化机房）。根据整体测评分析，问题严重程度变化为降低。

4.2.2 安全通信网络

4.2.2.1 安全通用要求

（T4）关键的应用服务和数据库服务网段未独立进行子网划分的情况。

单位有完整的IP地址规范，对IP地址的使用、回收均有记录《资产清单》，且系统具备相对完善的设备自身访问控制策略管理要求（具备《网络安全管理规范》、《设备及系统软件配置和操作手册》），措施效果良好，有助于部分补充未划分子网的安全功能不足（如安全通信网络）。根据整体测评分析，问题严重程度变化为降低。

4.2.3 安全区域边界

4.2.3.1 安全通用要求

（T6）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。

网络环境划分了相应的安全区域，区域间具备有效的访问控制措施，区域内各主机设备部署深信服EDR单机版，策略库、规则库更新及时，能够对攻击行为进行检测、阻断或限制，实际措施效果良好，且系统具备相对完善的策略库、规则库更新/校准管理

要求，管理措施效果良好且及时检查更新有效性（具备《漏洞检测报告》、《主机安全管理规范》），可降低外部网络攻击防御措施缺失的问题严重程度（如办公网区域、安全管理区域）。根据整体测评分析，问题严重程度变化为降低。

（T7）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。

系统部署于可控的网络环境内（具备有效的访问控制、入侵防护措施）限制相关主机对象访问非受控网络，操作系统层面配置防御策略（具备本地防火墙策略、核心交换机地址限制策略、部署深信服EDR单机版），恶意代码入侵的可能性相对较低，可降低恶意代码防范措施缺失的问题严重程度（如办公网区域、安全管理区域）。根据整体测评分析，问题严重程度变化为降低。

4.3 整体测评结果汇总

经整体测评后安全问题严重程度变化情况如下表所示

表 4-1 整体测评结果汇总表

问题编号	安全问题描述	测评对象	整体测评描述	严重程度变化
T1	（1）机房出入口未配置电子门禁系统。	信息化机房	（1）机房所在位置处于内部受控区域，非授权人员无法随意通过现有控制措施（如机械锁）进出机房，且具备相对完善的机房出入管理要求（具备《机房安全管理制度》），并实际执行措施效果良好（具备《机房出入登记表》），可降低机房出入口访问控制措施缺失的问题严重程度。	□升高 ☑降低
T4	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	（1）单位有完整的IP地址规范，对IP地址的使用、回收均有记录《资产清单》，且系统具备相对完善的设备自身访问控制策略管理要求（具备《网络安全管理规范》、《设备及系统软件配置和操作手册》），措施效果良好，有助于部分补充未划分子网的安全功能不足。	□升高 ☑降低

问题编号	安全问题描述	测评对象	整体测评描述	严重程度变化
T6	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	（1）网络环境划分了相应的安全区域，区域间具备有效的访问控制措施，区域内各主机设备部署深信服EDR单机版，策略库、规则库更新及时，能够对攻击行为进行检测、阻断或限制，实际措施效果良好，且系统具备相对完善的策略库、规则库更新/校准管理要求，管理措施效果良好且及时检查更新有效性（具备《漏洞检测报告》、《主机安全管理规范》），可降低外部网络攻击防御措施缺失的问题严重程度。	□升高 ☑降低
T7	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	（1）系统部署于可控的网络环境内（具备有效的访问控制、入侵防护措施）限制相关主机对象访问非受控网络，操作系统层面配置防御策略（具备本地防火墙策略、核心交换机地址限制策略、部署深信服EDR单机版），恶意代码入侵的可能性相对较低，可降低恶意代码防范措施缺失的问题严重程度。	□升高 ☑降低
T23	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	（1）单位未具备适用于被测系统的安全规划设计方案。安全方案设计不完善，导致规划设计需求不全面，信息系统存在安全缺陷。可升高单位未完全根据测试验收方案组织相关部门和人员开展验收工作的问题严重程度。	☑升高 □降低
T24	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	（1）单位未在软件交付之前按要求对所有软件开展恶意代码检测，导致在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。可升高针对系统上线前的安全性测试工作存在问题的问题严重程度。	☑升高 □降低
T26	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	（1）单位未严格按规范开展漏洞及安全隐患检测工作，漏洞检测工作不到位，导致存在未授权人员利用漏洞攻击信息系统的风险。可升高单位未严格按规范要求，针对防范	☑升高 □降低

问题编号	安全问题描述	测评对象	整体测评描述	严重程度变化
			恶意代码攻击的技术措施的有效性验证，开展工作的问题严重程度。	

5 安全问题风险分析

针对等级测评结果中存在的所有安全问题,结合关联资产和威胁分别分析安全问题可能产生的危害结果,找出可能对系统、单位、社会及国家造成的最大安全危害(损失),并根据最大安全危害(损失)的严重程度进一步确定安全问题的风险等级,结果为“高”、“中”或“低”。最大安全危害（损失）结果应结合安全问题所影响业务的重要程度、相关系统组件的重要程度、安全问题严重程度以及安全事件影响范围等进行综合分析。

表 5-1 安全问题风险分析

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
1	安全物理环境	（1）机房出入口未配置电子门禁系统。	信息化机房	物理攻击	（1）上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域，可能对系统的平稳运行造成影响。	中风险
2	安全物理环境	（1）机房建设未完全采用符合耐火等级的建筑材料; （2）机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级。	信息化机房	物理环境影响	（1）存在发生火情时助燃火灾的风险。	低风险
3	安全物理环境	（1）机房内缺乏防静电措施(如防静电地板或铺设防静电地毯 ）。	信息化机房	软硬件故障	（1）存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。	中风险
4	安全通信网络	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	恶意攻击	（1）上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变得更为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰	中风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
					难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。	
5	安全通信网络	（1）缺乏对通信设备可信验证方面的安全设计要求； （2）现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况。	安全通信网络	恶意攻击	（1）缺乏对系统可执行程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致计算资源被干扰和破坏造成损失。	低风险
6	安全区域边界	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	恶意攻击	（1）存在不能及时发现内部主机作为攻击跳板，或网络攻击行为而造成系统损坏/网络资源浪费的风险。	中风险
7	安全区域边界	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	恶意攻击	（1）无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。	中风险
8	安全区域边界	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	办公网区域 外网边界区域 安全管理区域 服务器存储区域	恶意攻击	（1）缺乏对边界设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险
9	安全计算环境	（1）设备不具备相关可信验证的技术措施。	WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2	恶意攻击	（1）缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险
10	安全计算环境	（1）缺乏对计算设备可信验证方面的安全设计要求；	业务终端-1 业务终端-2 运维及管理终端-1	恶意攻击	（1）缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可	低风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
		（2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。	运维及管理终端-2		信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	
11	安全计算环境	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况； （3）现有的计算设备存在对系统运行过程中的可信检验不全面的情况； （4）现有的可信验证存在部分告警、审计及联动措施不全面的情况。	应用服务器-1 应用服务器-2 数据库服务器	恶意攻击	（1）缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险
12	安全计算环境	（1）未能提供中间件重要数据的异地定时数据备份功能。	应用服务器-1-Tomcat 应用服务器-2-Tomcat	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。	中风险
13	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	教学管理信息服务平台	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。	中风险
14	安全计算环境	（1）未能提供数据库系统重要数据的异地定时数据备份功能。	数据库服务器-Oracle	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供，使企业的经济利益或声誉受到损害。	中风险
15	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	重要业务数据 重要个人信息	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。	中风险
16	安全管理中心	（1）系统管理的资源、运行及配置管理不够全面。	管理中心	恶意攻击	（1）系统的资源和运行缺少统一的管理，将导致系统可能无法按规划实现基	低风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
					于资源配置、 系统加载、异常处理、及备份/恢复等的安全控制措施。	
17	安全管理机构	（1）单位开展的检查工作不够完善。	制度文件、执行/记录文件	管理不到位	（1）检查工作开展不仔细，可能对存在或潜在的安全风险不能被及时发现并进行处理。	低风险
18	安全管理人员	（1）单位未完全按管理规范开展人员离场后的清理工作。	制度文件、执行/记录文件	管理不到位	（1）人员离场后的清理工作开展不规范，可能导致遗留外部人员访问受控区域的记录，存在被二次非法利用，造成泄密。	低风险
19	安全建设管理	（1）单位未具备适用于被测系统的安全规划设计方案。	制度文件、执行/记录文件	管理不到位	（1）规划设计需求不全面，可能导致安全方案设计不完善，信息系统存在安全缺陷。	低风险
20	安全建设管理	（1）单位未具备完整的安全设计方案相关的文档； （2）单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	管理不到位	（1）相关合规的规划配套文件缺失，可能导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。	中风险
21	安全建设管理	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； （2）单位未对相关论证过程及内容进行完整的记录。	制度文件、执行/记录文件	管理不到位	（1）未开展规范的审批过程，可能存在安全整体规划缺乏合理性和可行性，导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。	低风险
22	安全建设管理	（1）单位未在软件开发过程中对所有软件安全性进行测试； （2）单位未在软件安装之前按要求对所有软件开展恶意代码检测。	制度文件、执行/记录文件	管理不到位	（1）软件交付前恶意代码检测不规范，可能在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。	低风险
23	安全建设管理	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	管理不到位	（1）可能由于验收测试不严谨，造成测试过程缺乏计划性及操作性，无法保证经过测试验收的系统达到既定的安全性等目标。	低风险
24	安全建设管理	（1）针对系统上线前的安全性测试工作存在问	制度文件、执行/记录文件	管理不到	（1）未按规定开展上线前测试，安全隐患可能在系	低风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
		题。		位	统上线运行前未被发现并作出相应处理。	
25	安全运维管理	（1）单位未严格按规范开展漏洞及安全隐患检测工作。	制度文件、执行/记录文件	管理不到位	（1）漏洞检测、修补工作不到位，可能存在未授权人员利用漏洞攻击信息系统的风险。	低风险
26	安全运维管理	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	管理不到位	（1）可能导致系统恶意代码检测管理不到位，存在信息系统感染恶意代码，从而导致严重的信息安全风险。	低风险
27	安全运维管理	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	制度文件、执行/记录文件	管理不到位	（1）密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不到位，存在违反国家政策的风险。	中风险

6 等级测评结论

等级测评结论由安全问题风险分析结果和综合得分共同确定，判定依据如下表所示。

表 6-1 等级测评结论判别依据

测评结论	判别依据
优	被测对象中存在安全问题，但不会导致被测对象面临中、高等级安全风险，且系统综合得分 90 分以上（含90 分）。
良	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分 80分以上（含 80分）。
中	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分 70分以上（含 70分）
差	被测对象中存在安全问题，而且会导致被测对象面临高等级安全风险，或被测对象综合得分低于 70 分。

综合得分计算方法如下：

设M为被测对象的综合得分，$M = V_t + V_m$，V_t和V_m根据下列公式计算。

$$V_t=\begin{cases}100\cdot y-\sum_{k=1}^{t} f(\omega_k)\cdot(1-x_k)\cdot S, & V_t>0\\ 0, & V_t\le 0\end{cases}$$

$$V_m=\begin{cases}100\cdot(1-y)-\sum_{k=1}^{m} f(\omega_k)\cdot(1-x_k)\cdot S, & V_m>0\\ 0, & V_m\le 0\end{cases}$$

$$0\le x_k\le 1,\ S=100\cdot\frac{1}{n},\ f(\omega_k)=\begin{cases}1, & \omega_k=\text{一般}\\ 2, & \omega_k=\text{重要}\\ 3, & \omega_k=\text{关键}\end{cases}$$

其中，y为关注系数，取值在0至1之间，由等级保护工作管理部门给出，默认值为0.5。n为被测对象涉及的总测评项数（不含不适用项，下同），t为技术方面对应的总测评项数，V_t为技术方面的得分，m为管理方面对应的总测评项数，V_m为管理方面的得分，ω_k为测评项k的重要程度（分为一般、重要和关键），x_k为测评项k的得分，如果测评项k涉及多测评项对象，则x_k取值为多测评对象得分的算术平均值。

x_k的得分计算如下：

测评项k涉及对象 / 测评项k定性判定	只涉及单个对象	涉及多个对象
符合	1	1
部分符合	0.5	计算测评对象平均分，取值在0至1之间
不符合	0	0

注：当测评项k涉及多个对象时，针对每个对象的得分取值为1、0.5和0。

根据第5章安全问题风险分析结果统计高、中、低风险安全问题的数量，利用综合得分计算公式计算出被测对象的综合得分，并将相关结果填入下表。

表 6-2 安全问题统计和综合得分

被测对象名称	安全问题数量			综合得分
	高风险	中风险	低风险	
教学管理信息服务平台	0	11	16	73.85

依据 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》和GB/T 28448—2019《信息安全技术 网络安全等级保护测评要求》的第二级要求，经对教学管理信息服务平台的安全保护状况进行综合分析评价，等级测评结论如下：

教学管理信息服务平台本次等级测评的综合得分为73.85，且不存在高等级安全风险，等级测评结论为中。

7 安全问题整改建议

表 7-1 安全问题整改建议

序号	安全类	安全问题	关联资产	整改建议
1	安全物理环境	(1)机房出入口未配置电子门禁系统。	信息化机房	(1) 采用电子门禁系统严格控制机房其他出入口的进出，或安排专人值守； (2) 采用电子门禁系统，对机房所有人员出入进行登记记录，并保存。
2	安全物理环境	(1)机房建设未完全采用符合耐火等级的建筑材料； (2)机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级。	信息化机房	(1) 机房及相关的工作房间和辅助房采用具有耐火等级的建筑材料； (2) 机房建设采用符合相关耐火等级（二级）的建筑材料。（内外墙壁均应采用具有防火涂料、隔热板、铝板、钢板等阻燃或不燃的材料）； (3) 机房耐火等级建筑材料有相关合格证，并留存机房验收文档。
3	安全物理环境	(1)机房内缺乏防静电措施（如防静电地板或铺设防静电地毯）。	信息化机房	(1) 机房铺设防静电地板或铺设防静电地毯； (2) 机房房静电设计可依据GB50174-2008和GB50314-2006相关规定进行机房设计和验收。
4	安全通信网络	(1)关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	(1) 建议独立划分出应用服务器网段、数据库服务器网段。
5	安全通信	(1)缺乏对通信设备可信验	安全通信网络	(1) 建议在管理规范文档内对通信设

序号	安全类	安全问题	关联资产	整改建议
	网络	证方面的安全设计要求； (2)现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况。		备可信验证方面的安全设计提出要求； （2）建议系统实现对所有可执行环节进行可信验证，包括： 运行过程中的可信检验： ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■通信应用连接过程。
6	安全区域边界	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	（1）建议网络层部署的防火墙配置对内部发起的攻击行为实现防范功能策略，实现检测、防止或限制从内部发起的网络攻击行为； （2）内部安全防范措施能检测以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、碎片攻击、网络蠕虫攻击、应用漏洞攻击。
7	安全区域边界	(1)现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	（1）建议现有部署的恶意代码防范措施网络边界覆盖全面，及时对恶意代码及逆行检测和清除。
8	安全区域边界	(1)缺乏对边界设备可信验证方面的安全设计要求； (2)现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）建议对边界设备系统程序的可信验证设计并保存设计文件； （2）建议系统实现对所有可执行环节进行可信验证。
9	安全计算环境	(1)设备不具备相关可信验证的技术措施。	WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2	（1）建议通过设备的启动过程和运行过程中对预装软件（包括系统引导程序、系统程序、相关应用程序和重要配置参数）的完整性验证或检测，确保对系统引导程序、系统程序、重要配置参数和关键应用程序可信根验证； （2）建议设备启用在检测到其可信性受到破坏后进行报警的相关功能。
10	安全计算环境	(1)缺乏对计算设备可信验证方面的安全设计要求； (2)现有的计算设备存在对系统运行过程中的可信检验	业务终端-1 业务终端-2 运维及管理终端-1	（1）建议对计算设备系统程序的可信验证设计并保存设计文件； （2）建议系统实现对所有可执行环节进行可信验证。

序号	安全类	安全问题	关联资产	整改建议
		完全缺失的情况。	运维及管理终端-2	
11	安全计算环境	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况； （3）现有的计算设备存在对系统运行过程中的可信检验不全面的情况； （4）现有的可信验证存在部分告警、审计及联动措施不全面的情况。	应用服务器-1 应用服务器-2 数据库服务器	（1）建议对计算设备系统程序的可信验证设计并保存设计文件； （2）建议系统实现对所有可执行环节进行可信验证。
12	安全计算环境	（1）未能提供中间件重要数据的异地定时数据备份功能。	应用服务器-1-Tomcat 应用服务器-2-Tomcat	（1）建议设置异地灾备机房，并利用通信网络将中间件重要数据定时备份至备份场地； （2）异地备份的中间件数据范围（不限于）包括系统的： ■配置数据 ■重要日志数据。
13	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	教学管理信息服务平台	（1）建议设置异地灾备机房，并利用通信网络将应用软件系统重要数据定时备份至备份场地； （2）异地备份的应用软件系统数据范围（不限于）包括系统的：配置数据、重要日志数据，业务数据。
14	安全计算环境	（1）未能提供数据库系统重要数据的异地定时数据备份功能。	数据库服务器-Oracle	（1）建议设置异地灾备机房，并利用通信网络将重要数据定时备份至备份场地； （2）异地备份的数据范围（不限于）包括系统的： ■配置数据 ■重要业务数据。
15	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	重要业务数据 重要个人信息	（1）建议设置异地灾备机房，并利用通信网络将应用软件系统重要数据定时备份至备份场地。
16	安全管理中心	（1）系统管理的资源、运行及配置管理不够全面。	管理中心	（1）需实现系统包括对可信证书管理、可信基准库的管理。
17	安全管理机构	（1）单位开展的检查工作不够完善。	制度文件、执行/记录文件	（1）建议单位按要求提供安全检查报告。
18	安全管理	（1）单位未完全按管理规范	制度文件、执行	（1）建议单位按管理规范开展人员离

序号	安全类	安全问题	关联资产	整改建议
	人员	开展人员离场后的清理工作。	/记录文件	场后的清理工作。至少包括：保留清理记录、及时清除离场后的所有访问权限、记录访问权限清除时间。
19	安全建设管理	(1)单位未具备适用于被测系统的安全规划设计方案。	制度文件、执行/记录文件	（1）建议单位根据等保要求进行过全面的自查或对比，根据系统的安全级别选择基本安全措施； （2）建议规划方案需根据风险分析结果对系统安全措施进行补充和整，并在系统建设\\整改方案中有详细描述。
20	安全建设管理	(1)单位未具备完整的安全设计方案相关的文档； (2)单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	（1）建议单位根据信息系统的等级划分情况，准备安全设计方案、安全管理策略、安全建设规划文档等； （2）建议相关文档内容应完善，包括统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、密码技术要求、总体建设规划和详细设计方案，并形成一致性的配套文件。
21	安全建设管理	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； (2)单位未对相关论证过程及内容进行完整的记录。	制度文件、执行/记录文件	（1）建议单位组织相关部门和安全技术专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定； （2）保存论证和审定记录，记录包括批准时间、批准人员签字； （3）文件经过批准后，才能正式实施。
22	安全建设管理	(1)单位未在软件开发过程中对所有软件安全性进行测试； (2)单位未在软件安装之前按要求对所有软件开展恶意代码检测。	制度文件、执行/记录文件	（1）建议开发商提供软件源代码，软件安装前检测软件中的恶意代码； （2）输出检测报告（或提供第三方检测报告），内容包括测试时间、测试地点、测试对象、测试结论、测试人员。
23	安全建设管理	(1)单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	（1）建议根据测试验收过程记录与结果，形成测试验收报告。
24	安全建设管理	(1)针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	（1）建议系统建设完成后，委托第三方测试单位对系统进行安全性测试，并出具安全性测试报告； (2)测试报告内容至少包括测试时间、测试地点、测试人、测试对象、测试方法、测试过程、测试发现的安全问题、整改建议、测试结论，并有第三方测试机构的签字盖章。
25	安全运维	(1)单位未严格按规范开展	制度文件、执行	（1）建议单位定期开展漏洞扫描，对

序号	安全类	安全问题	关联资产	整改建议
	管理	漏洞及安全隐患检测工作。	/记录文件	发现的安全漏洞和隐患进行及时修补评估； （2）对必需修补的安全漏洞和隐患进行加固测试，测试无误后，备份系统数据，再从生产环境进行修补； （3）对于剩余安全漏洞和隐患进行残余风险分析，明确安全风险整改原则。
26	安全运维管理	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	（1）建议单位按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。包括;定期对相关产品的恶意代码库进行升级；对相关设备升级情况进行记录；对各类防病毒产品上截获的恶意代码进行分析并汇总上报； （2）单位需保留完整的恶意代码检测/升级的记录。至少具备：执行人、升级结果/检测结果、处理方式、负责人签字 。
27	安全运维管理	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	制度文件、执行/记录文件	（1）建议单位学习现有密码相关的国家标准和行业标准。建立密码管理要求的制度文档。

漏洞安全问题整改建议

序号	安全类	安全问题	关联资产	整改建议
1	安全计算环境	允许Traceroute探测 此类漏洞涉及网络设备、安全设备、服务器存储设备。	10.2.2.16/数据库服务器 10.2.2.17/应用服务器-1 10.2.2.18/应用服务器-2 10.2.1.4/运维安全管理系统 10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/上网行为管理系	在防火墙出站规则中禁用echo-reply（type 0）、time-exceeded（type 11）、destination-unreachable（type 3）类型的ICMP包。

序号	安全类	安全问题	关联资产	整改建议
			统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/ 汇聚交换机 172.16.1.2/核心交换机	
2	安全计算环境	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161) 此类漏洞涉及网络设备。	172.16.1.2/核心交换机	临时解决方法：* 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://downloads.ssh.com/ 对于具体Linux发行版中使用的版本，可以参考如下链接,确认系统是否受该漏洞影响: Redhat ------- https://rhn.redhat.com/errata/RHSA-2009-1287.html Suse ------- http://support.novell.com/security/cve/CVE-2008-5161.html Ubuntu ------- http://people.canonical.com/~ubuntu-security/cve/2008/CVE-2008-5161.html
3	安全计算环境	缺少“Content-Security-Policy”响应头 此类漏洞涉及业务应用软件平台。	https://jwc.mmpt.edu.cn/ 教学管理信息服务平台	在服务器中配置Content-Security-Policy响应头为“default-src 'self’”。

【正文结束】

附录A 被测对象资产

A.1 物理机房

附录A 表- 1物理机房

序号	机房名称	物理位置	重要程度
1	信息化机房	茂名市茂南区文明北路232号大院大楼	关键

A.2 网络设备

附录A 表- 2网络设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度	备注
1	核心交换机	否	H3C version 7.1.070, Release 7585P07	H3C S7500E-X	核心数据交换、访问控制	关键	
2	汇聚交换机	否	H3C version 7.1.070, Release 6126P20	H3C S5560X-30C-EI	数据交换	重要	

A.3 安全设备

附录A 表- 3安全设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度	备注
1	WEB应用防火墙	否	深信服AF 8.0.9	深信服WAF-2000-H642	应用防护、入侵防范、病毒防护	重要	
2	防火墙-2	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键	
3	上网行为管理系统	否	深信服AC12.0.26	深信服AC-1000-D600-PT	上网行为管理及终端准入控制	重要	
4	基线核查系统	否	深信服V3.0.3	深信服AC-1000-D602-PT	漏洞扫描	重要	
5	日志审计系统	否	深信服LAS 3.0.5	深信服AC-1000-D601-PT	日志审计	重要	
6	运维安全管理系统	否	深信服V3.0.6	深信服AC-1000-D603-PT	运维审计	重要	
7	防火墙-1	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键	

A.4 服务器

附录A 表-4服务器

序号	设备名称	所属业务应用系统/平台名称	是否虚拟设备	操作系统及版本	数据库管理系统及版本	中间件及版本	重要程度	备注
1	应用服务器-1	教学管理信息服务平台	否	CentOS 7.7	/	Tomcat 8.5	关键	
2	应用服务器-2	教学管理信息服务平台	否	CentOS 7.7	/	Tomcat 8.5	关键	
3	数据库服务器	教学管理信息服务平台	否	CentOS 7.7	Oracle 11.2.0.1.0	/	关键	

A.5 终端设备

附录A 表-5终端设备

序号	设备名称	是否虚拟设备	操作系统/控制软件及版本	用途	重要程度	备注
1	运维及管理终端-2	否	Windows 10（版本21H2（内部版本19044.1889））	运维管理、系统管理	一般	
2	业务终端-1	否	Windows 10（版本20H2（内部版本19044.1889）	业务管理	一般	
3	业务终端-2	否	Windows 10（版本20H2（内部版本19044.1889）	业务管理	一般	
4	运维及管理终端-1	否	Windows 10（版本20H2（内部版本19044.1889）	运维管理、系统管理	一般	

A.6 其他系统或设备

附录A 表-6其他系统或设备

序号	设备名称	是否虚拟设备	操作系统/控制软件及版本	用途	重要程度	备注
/	/	/	/	/	/	/

注释：本次测评对象中不涉及专用移动互联终端等，不开展抽测。

A.7 系统管理软件/平台

附录A 表-7系统管理软件/平台

序号	系统管理软件/平台名称	所在设备名称	版本	主要功能	重要程度	备注
1	应用服务器-2-Tomcat	应用服务器-2	8.0.37	页面发布	关键	
2	数据库服务器-Oracle	数据库服务器	11.2.0.1.0	数据生产、存储	关键	
3	应用服务器-1-Tomcat	应用服务器-1	8.0.37	页面发布	关键	

A.8 业务应用软件/平台

附录A 表-8业务应用系统/平台

序号	业务应用系统/平台名称	主要功能	业务应用软件及版本	开发厂商	重要程度
1	教学管理信息服务平台	教学管理信息服务平台主要实现教务管理服务，系统包括系统管理、学籍管理、师资管理、教学计划、排课管理、选课管理、成绩管理、考试管理、毕业管理、教学评价等功能模块。教学管理信息服务平台以培养、运行、保障、监控为主线，实现教务工作事务性管理和战略性管理的相互叠加，实现学校培养过程管理、教学质量检查、教学工作管理等日常教学事务管理。	V6.0	正方软件股份有限公司	关键

A.9 数据资源

附录A 表-9数据资源

序号	数据类别	所属业务应用	安全防护需求	重要程度
1	重要个人信息	教学管理信息服务平台	完整性、保密性	关键
2	重要业务数据	教学管理信息服务平台	完整性、保密性	关键
3	鉴别数据	教学管理信息服务平台(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性、保密性	关键
4	重要审计数据	教学管理信息服务平台（安全管理中心）	完整性	重要

序号	数据类别	所属业务应用	安全防护需求	重要程度
5	重要配置数据	教学管理信息服务平台(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性	关键

注释：网络设备、安全设备、服务器、终端、系统管理软件/平台和业务应用系统等所涉及的鉴别数据和重要配置数据分别在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。重要审计数据在安全管理中心进行汇总测评证据，包括数据完整性。重要业务数据和重要个人信息分别在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。

A.10 密码产品

附录A 表- 10密码产品

序号	产品/模块名称	生成厂商	商密型号	密码算法	用途	重要程度
/	/	/	/	/	/	/

注释：本次测评不存在加密机等密码产品。

A.11 安全相关人员

附录A 表- 11安全相关人员

序号	姓名	岗位/角色	联系方式	所属单位
1	叶永利	安全管理员	0668-2920122	茂名职业技术学院
2	吴国华	系统管理员	0668-2920122	茂名职业技术学院
3	杨云	审计管理员	0668-2920122	茂名职业技术学院
4	吴国华	机房管理员	0668-2920122	茂名职业技术学院
5	龙恒	网络管理员	13377766618	茂名职业技术学院
6	龙恒	数据管理员	13377766618	茂名职业技术学院
7	龙恒	应用管理员	13377766618	茂名职业技术学院
8	杨云	资产管理员	0668-2920122	茂名职业技术学院

A.12 安全管理文档

附录A 表-12安全管理文档

序号	文档名称	主要内容
1	制度类文档-办公环境保密管理	关于单位办公环境管理制度文档
2	制度类文档-信息安全漏洞扫描规范	关于单位安全漏洞工作规范制度文档
3	制度类文档-安全漏洞管理制度	关于单位安全漏洞管理工作制度文档
4	制度类文档-恶意代码防范管理制度	关于单位恶意代码防范工作制度文档
5	制度类文档-安全事件报告和处置	关于单位网络安全事件管理、处置、流程等报告制度文档
6	制度类文档-外部服务人员管理规范	关于单位针对外部人员工作管理规范制度文档
7	制度类文档-测试及验收方案	关于单位测试验收方案文档
8	制度类文档-办公环境管理制度	关于单位办公环境管理制度文档
9	制度类文档-组织安全结构和人员职责制度	关于单位安全结构、人员职责
10	制度类文档-员工考核管理制度	关于单位人员考核工作管理制度文档
11	制度类文档-工程测试验收管理	关于单位工程测试工作管理制度文档
12	制度类文档-恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
13	制度类文档-服务供应商选择安全管理制度	关于单位安全服务供应商管理规定制度文档
14	制度类文档-安全审查和检查管理规范	关于单位安全检查、审查工作规范制度文档
15	制度类文档-信息系统恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
16	制度类文档-工程实施管理制度	关于单位工程实施工作管理制度文档
17	制度类文档-系统交付管理	关于单位交付工作管理制度文档
18	制度类文档-介质管理制度	关于单位介质安全管理工制度文档
19	制度类文档-物理安全管理规范	关于加强单位办公区域及电子计算机机房的管理和设备运行安全，规范办公区域及机房建设，使人员办公高效及机房设备安全、稳定运行的制度文档
20	制度类文档-外包开发	关于单位外包项目管理工作制度文档

序号	文档名称	主要内容
	软件管理规定	
21	制度类文档-信息安全总体策略	关于单位网络安全方针、策略制度文档
22	制度类文档-岗位安排及岗位职责	关于单位岗位职责、岗位安排制度文档
23	制度类文档-组织安全结构和人员职责制度	关于单位组织结构、人员安排、人员职责制度文档
24	制度类文档-信息安全奖惩办法	关于单位人员奖惩制度文档
25	制度类文档-应用安全管理规范	关于规定单位应用安全管理要求及规范的制度文档
26	制度类文档-授权和审批管理规定	关于单位授权审批、审批流程规范制度文档
27	制度类文档-网络安全管理制度	关于单位网络安全工作管理制度文档
28	制度类文档-网络与信息系统安全设计规范	关于单位网络与信息化安全设计制度文档
29	制度类文档-信息系统外包运维管理制度	关于单位外包运维工作管理制度文档
30	制度类文档-系统安全管理制度	关于单位系统安全管理、安全服务管理制度文档
31	制度类文档-外部人员访问管理制度	关于单位针对外来人员访问管控制度文档
32	制度类文档-安全教育和培训制度	关于单位安全培训、安全交流工作制度文档
33	制度类文档-制度制定、发布、评审和修订管理制度	关于单位制度制定、发布、评审和修订等管理文档
34	制度类文档-应用系统业务用户密码设置规定	关于单位用户密码管理制度文档
35	制度类文档-备份与恢复管理制度	关于单位数据备份、恢复管理制度文档
36	制度类文档-机房安全管理制度	关于单位机房安全管理工作制度文档
37	制度类文档-安全管理组织规范	关于单位组织结构管理规范制度文档
38	制度类文档-主机安全管理规范	关于规定单位主机系统安全管理要求规范，指导业务平台主机的安全配置和维护的制度文档
39	制度类文档-设备安全管理制度	关于单位设备安全管理制度文档
40	制度类文档-数据安全管理规范	关于保障关键数据安全，从数据库本身、数据加密、数据备份恢复三个方面对数据安全进行规范的制度文档

序号	文档名称	主要内容
41	制度类文档-变更控制管理制度	关于单位变更流程、控制管理制度文档
42	制度类文档-系统及应用数据备份管理规范	关于单位数据备份、恢复管理制度文档
43	制度类文档-网络安全事件报告制度	关于单位网络安全事件管理报告文档
44	制度类文档-离岗人员工作交接规范	关于单位离岗交接工作规范制度文档
45	制度类文档-网络安全管理规范	关于保障单位网络系统的安全稳定运行，抵御内部和外部各种形式的网络攻击或威胁制定的管理文档
46	制度类文档-网络安全事件应急预案	关于单位网络安全事件应急处理、流程、培训等管理制度文档
47	制度类文档-外部接入受控网络访问系统管理规范	关于单位针对外部人员工作接入规范制度文档
48	制度类文档-人员管理制度	关于单位人员录用、调岗、离岗管理制度文档
49	操作类文档-设备操作规程	关于单位相关设备操作指导文档
50	操作类文档-软硬件日常维护管理规程	关于单位计算机网络系统使用、管理、信息安全、资源共享有所遵循,规范上网操作流程,提高网络系统安全性的指导文档
51	操作类文档-数据备份策略	关于单位数据备份策略文件
52	操作类文档-设备及系统软件配置和操作手册	关于单位安全设备操作、Linux服务器配置手册、主机运维操作手册、软件操作手册、防火墙配置和操作手册、数据库日常运维操作手册等指导文档
53	记录类文档-人员入职考核记录	关于人员录用、考核工作记录
54	记录类文档-离场信息资料交接表	关于人员离岗交接工作记录
55	记录类文档-安全管理制度评审记录	关于单位制度审计记录
56	记录类文档-设备维修申请表	关于单位设备维护工作申请记录
57	记录类文档-设备操作维护记录	关于单位设备维护工作记录
58	记录类文档-人员培训及考核记录表	关于人员培训、考核等工作记录
59	记录类文档-设备出入登记记录表	关于设备进出机房登记工作记录
60	记录类文档-接入受控网络申请表	关于外来人员接入工作记录
61	记录类文档-信息系统	关于备份介质销毁申请工作记录

序号	文档名称	主要内容
	存储介质销毁申请表	
62	记录类文档-漏洞检测报告	关于单位安全漏洞检测报告文档
63	记录类文档-备份工作汇总表	关于单位数据备份工作总结表
64	记录类文档-收发文登记记录	关于单位文档签发记录
65	记录类文档-应急预案培训记录表	关于单位应急预案培训工作记录
66	记录类文档-技能培训记录	关于单位系统培训工作、考核工作记录
67	记录类文档-离职员工物品交回登记表	关于人员离岗工物交接工作记录
68	记录类文档-外部人员访问记录表	关于外来人员访问登记工作记录
69	记录类文档-网络信息安全事件记录表	关于单位网络安全事件工作记录
70	记录类文档-网络配置信息	关于单位配置信息登记工作记录
71	记录类文档-机房设备维修记录表	关于单位机房设备维修工作记录
72	记录类文档-机房巡检记录表	关于单位机房环境巡检记录
73	记录类文档-系统交付清单	关于单位交付工作记录
74	记录类文档-信息管理系统漏洞检查表	关于单位安全漏洞工作检测记录表
75	记录类文档-访问记录表	关于人员访问工作记录
76	记录类文档-安全建设方案评审纪录	关于单位网络与信息化安全设计方案评审工作记录
77	记录类文档-关键岗位人员考核记录	关于关键岗位考核工作记录
78	记录类文档-信息安全检查记录表	关于单位安全检查工作记录
79	记录类文档-信息系统存储介质使用清单	关于备份介质存储使用清单
80	记录类文档-外部人员访问申请表	关于外来人员访问申请流程工作记录
81	记录类文档-信息安全会议记录	关于单位安全培训、安全交流会议记录
82	记录类文档-机房设备维护记录表	关于设备维护登记工作记录

序号	文档名称	主要内容
83	记录类文档-评审和修订记录	关于单位变更评审、修订工作记录
84	记录类文档-人员离岗申请表	关于人员离岗申请记录
85	记录类文档-数据备份记录表	关于单位数据备份工作记录
86	记录类文档-数据恢复申请表	关于单位数据恢复工作申请表
87	记录类文档-存储介质目录清单	关于备份介质存储工作清单
88	记录类文档-机房维护日志	关于机房维护工作记录
89	记录类文档-通用变更记录表	关于单位变更工作记录
90	记录类文档-专家论证记录表	关于单位网络方案论证记录
91	记录类文档-外部会议文件和记录	关于单位外部联系、交流及会议工作记录
92	记录类文档-软件交付清单	关于单位交付工作记录
93	记录类文档-监理审批表	关于单位监理审核工作记录
94	记录类文档-重要操作审批表	关于单位审批工作记录
95	记录类文档-备份介质使用记录	关于备份介质使用登记工作记录
96	记录类文档-机房出入登记表	关于人员进出机房登记工作记录
97	证据类文档-定级备案	关于单位系统定级报告、备案证文件
98	证据类文档-深信服安全采购合同	关于单位与安全厂家服务采购、产品选择合同文件
99	证据类文档-资产清单	关于单位信息系统资产清单统计表
100	证据类文档-网络安全系统设计方案	关于单位网络与信息化安全设计方案文档
101	证据类文档-外部联系表	关于单位内部联系及外部联系名单
102	证据类文档-网络安全等级保护工作小组名单	关于单位网络安全等级保护工作小组人员名单文件
103	证据类文档-网络安全等级保护测评服务合同	关于单位与安全服务商签定的安全服务合同文件
104	证据类文档-信息安全	关于单位安全事件分析报告

序号	文档名称	主要内容
	事件分析报告表	
105	证据类文档-工程项目实施方案	关于单位工程实施方案文档
106	证据类文档-安全职位人员	关于单位人员岗位安排名单

附录B 上次测评问题整改情况说明

此次为教学管理信息服务平台初次等级测评，之前未实施过等级保护测评工作。

附录B 表- 1上次测评问题整改情况

序号	主要安全问题	整改情况	情况说明
/	/	□已整改 □未整改	/

附录C 单项测评结果汇总

C.1 安全物理环境

附录 C 表-1 安全物理环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			物理位置选择	物理访问控制	防盗窃和防破坏	防雷击	防火	防水和防潮	防静电	温湿度控制	电力供应	电磁防护
1	信息化机房	符合	2	0	2	1	1	2	0	1	2	1
		部分符合	0	1	0	0	0	0	0	0	0	0
		不符合	0	0	0	0	1	0	1	0	0	0
		不适用	0	0	0	0	0	0	0	0	0	0

附录 C 表-2 安全物理环境单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.2 安全通信网络

附录 C 表-3 安全通信网络单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求		
			网络架构	通信传输	可信验证
1	安全通信网络	符合	1	1	0
		部分符合	1	0	0
		不符合	0	0	1
		不适用	0	0	0

附录 C 表-4 安全通信网络单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.3 安全区域边界

附录 C 表-5 安全区域边界单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求					
			边界防护	访问控制	入侵防范	恶意代码和垃圾邮件防范	安全审计	可信验证
1	外网边界区域	符合	1	4	1	1	3	0
		部分符合	0	0	0	0	0	0
		不符合	0	0	0	0	0	1
		不适用	0	0	0	0	0	0
2	安全管理区域	符合	1	4	0	0	3	0
		部分符合	0	0	0	1	0	0
		不符合	0	0	1	0	0	1
		不适用	0	0	0	0	0	0
3	服务器存储区域	符合	1	4	1	1	3	0
		部分符合	0	0	0	0	0	0
		不符合	0	0	0	0	0	1
		不适用	0	0	0	0	0	0
4	办公网区域	符合	1	4	0	0	3	0
		部分符合	0	0	0	1	0	0
		不符合	0	0	1	0	0	1
		不适用	0	0	0	0	0	0

附录 C 表-6 安全区域边界单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.4 安全计算环境

C.4.1 网络设备

附录 C 表-7 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	汇聚交换机	符合	3	4	3	4	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	1	0	0	1	1	--
2	核心交换机	符合	3	4	3	4	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	1	0	0	1	1	--

C.4.2 安全设备

附录 C 表-8 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	基线核查系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
2	上网行为管理系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
3	WEB应用防火墙	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
4	防火墙-1	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
5	防火墙-2	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
6	日志	符合	3	4	3	5	0	0	1	1	0	--

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
	审计系统	部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
7	运维安全管理系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--

C.4.3 服务器和终端

附录 C 表-9 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	应用服务器-1	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
2	数据库服务器	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
3	应用服务器-2	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
4	业务终端-2	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
5	业务终端-1	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
		不适用	0	0	0	1	0	0	0	1	0	--
6	运维及管理终端-2	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
7	运维及管理终端-1	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--

C.4.4 系统管理软件/平台

附录 C 表-10 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	应用服务器-1-Tomcat	符合	0	4	3	2	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	3	0	0	3	1	1	0	0	0	--
2	应用服务器-2-Tomcat	符合	0	4	3	2	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	3	0	0	3	1	1	0	0	0	--
3	数据库服务器-Oracle	符合	3	4	3	2	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	0	0	0	3	1	1	0	0	0	--

C.4.5 业务应用系统/平台

附录 C 表-11 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	教学管理信息服务平台	符合	3	4	3	3	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	0	0	0	2	1	1	0	0	0	--

C.4.6 数据资源

附录 C 表-12 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	重要个人信息	符合	--	--	--	--	--	--	1	1	0	2
		部分符合	--	--	--	--	--	--	0	0	0	0
		不符合	--	--	--	--	--	--	0	1	0	0
		不适用	--	--	--	--	--	--	0	0	1	0
2	重要业务数据	符合	--	--	--	--	--	--	1	1	0	0
		部分符合	--	--	--	--	--	--	0	0	0	0
		不符合	--	--	--	--	--	--	0	1	0	0
		不适用	--	--	--	--	--	--	0	0	1	2

C.4.7 其他系统或设备

附录 C 表-13 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	--	符合	--	--	--	--	--	--	--	--	--	--
		部分符合	--	--	--	--	--	--	--	--	--	--
		不符合	--	--	--	--	--	--	--	--	--	--
		不适用	--	--	--	--	--	--	--	--	--	--

C.5 安全管理中心

附录 C 表-14 安全管理中心单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求	
			系统管理	审计管理
1	管理中心	符合	1	2
		部分符合	0	0
		不符合	1	0
		不适用	0	0

附录 C 表-15 安全管理中心单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.6 安全管理制度

附录 C 表-16 安全管理制度单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求			
			安全策略	管理制度	制定和发布	评审和修订
1	制度文件、执行/记录文件	符合	1	2	2	1
		部分符合	0	0	0	0
		不符合	0	0	0	0
		不适用	0	0	0	0

C.7 安全管理机构

附录 C 表-17 安全管理机构单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求				
			岗位设置	人员配备	授权和审批	沟通和合作	审核和检查
1	制度文件、执行/记录文件	符合	2	1	2	3	0
		部分符合	0	0	0	0	1
		不符合	0	0	0	0	0
		不适用	0	0	0	0	0

C.8 安全管理人员

附录 C 表-18 安全管理人员单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求			
			人员录用	人员离岗	安全意识教育和培训	外部人员访问管理
1	制度文件、执行/记录文件	符合	2	1	1	2
		部分符合	0	0	0	0
		不符合	0	0	0	1
		不适用	0	0	0	0

C.9 安全建设管理

附录 C 表-19 安全建设管理单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			定级和备案	安全方案设计	产品采购和使用	自行软件开发	外包软件开发	工程实施	测试验收	系统交付	等级测评	服务供应商选择
1	制度文件、执行/记录文件	符合	4	0	2	0	1	2	0	3	3	2
		部分符合	0	0	0	0	0	0	1	0	0	0
		不符合	0	3	0	0	1	0	1	0	0	0
		不适用	0	0	0	2	0	0	0	0	0	0

附录 C 表-20 安全建设管理单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.10 安全运维管理

附录 C 表-21 安全运维管理单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求												
			环境管理	资产管理	介质管理	设备维护管理	漏洞和风险管理	网络和系统安全管理	恶意代码防范管理	配置管理	密码管理	变更管理	备份与恢复管理	安全事件处置	应急预案管理	外包运维管理
1	制度文件、执行/记录文件	符合	3	1	2	2	0	5	2	1	0	1	3	3	2	0
		部分符合	0	0	0	0	0	0	1	0	0	0	0	0	0	0
		不符合	0	0	0	0	1	0	0	0	1	0	0	0	0	0
		不适用	0	0	0	0	0	0	0	0	1	0	0	0	0	2

附录 C 表-22 安全运维管理单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.11 其他安全要求指标

附录 C 表-23 其他指标单项测评结果汇总表

序号	测评对象	符合情况
本报告不涉及		

附录D 单项测评结果记录

D.1 安全物理环境

D.1.1 安全通用要求

D.1.1.1 信息化机房

安全控制点	测评指标	结果结论	符合程度
物理位置选择	a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；	（1）机房和办公场地场所在建筑物具有建筑验收文档，包含对防震、防风和防雨能力的说明； ■机房建设地址为：茂名市茂南区文明北路232号大院大楼 （2）机房和办公场地未出严重的问题。 ■无雨水渗透痕迹 ■无因风导致的较严重尘土 ■无屋顶、墙体、地面等破损开裂	符合
	b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	（1）机房未部署在易发生问题的位置； （2）机房对于空调设备的排水管等部位采取密封防漏处理； （3）机房对于楼板进行了防护措施。	符合
物理访问控制	机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。	（1）制定了《机房安全管理制度》，内容包含机房出入方面的管理规定； （2）对未配置电子门禁系统的出入口指定专人7*24小时负责机房出入，对出入的人员进行身份鉴别和登记，可查出入记录，且出入有专人陪同； (3)机房存在未配置门禁系统的开放出入口。	部分符合
防盗窃和防破坏	a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识；	（1）机房设备或主要部件都固定在机架上； （2）机房内对主要部件已绑定相应不易除去的标签； ■包括网络设备 ■包括安全设备 ■包括服务器 ■包括网络线缆	符合

安全控制点	测评指标	结果结论	符合程度
		（3）重要机柜已进行上锁处理。	
	b）应将通信线缆铺设在隐蔽安全处。	（1）通信线缆铺设在下走线槽隐蔽处中； （2）通信线缆设有明显的源目的标识； （3）通信线缆均铺设整齐、规范。	符合
防雷击	应将各类机柜、设施和设备等通过接地系统安全接地。	（1）机房设置专用地线； （2）机房内机柜、设施和设备等进行接地处理； （3）交流电源接地验收检测结果符合要求。	符合
防火	a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；	（1）机房采用经消防检测部门检测合格并在有效期内的（如 七氟丙烷）气体自动灭火设备，火灾自动报警类型为烟感+红外； （2）自动消防系统工作状态正常，有定期巡检和维护记录《机房巡检记录表》； （3）建立机房消防的管理制度相关文档《机房安全管理制度》，按管理要求机房无人情况下气体灭火配置为自动模式，进入机房调整为手动模式，机房报警有7*24小时值班人员进行监控。	符合
	b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。	（1）机房及相关的工作房间和辅助房没有采用具有耐火等级的建筑材料； （2）缺乏机房防火设计文档； （3）缺乏机房防火验收文档。	不符合
防水和防潮	a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	（1）机房不存在雨水渗透、破损等不合规情况； （2）机房不位于建筑的顶层、边缘区域。	符合
	b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。	（1）机房区域范围已部署1台科华品牌（精密）空调，机房内分别配置1组温湿度传感器监控； （2）机房内空调下方已铺设安装好挡水和排水设施； （3）机房墙壁或楼板的管道采取必要的防渗防漏等防水保护措施； （4）机房安装检测设备（如：漏水检测绳）检测地下积水，及时处理机房水蒸气结露和地下积水的转移与渗透； （5）目前防水\防潮检测未发现异常情况，并且有防水防潮的运维记录《机房维护日志》。	符合
防静电	应采用防静电地板或地面并采用必要的接地防静电措施。	（1）对机房内设备（可导电金属线槽）采用了接地静电泄放措施； （2）机房未采用防静电地板或铺设防静电地毯。	不符合
温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围	（1）机房范围已部署1组科华品牌精密空调进行温湿度调节； （2）机房范围已部署空调及加湿机进行温湿	符合

安全控制点	测评指标	结果结论	符合程度
	之内。	度调节； （3）温湿度自动调节设施运作正常，有运行和维护记录《机房维护日志》； （4）机房温度能保持在24摄氏度到28摄氏度之间； （5）机房湿度能保持在40%到65%之间。	
电力供应	a）应在机房供电线路上配置稳压器和过电压防护设备；	（1）机房配备了稳压器和过电压防护设备； （2）稳压器和过电压防护设备正常工作； （3）机房具备电力供应安全设计，并在其中标明配备稳压器、过电压防护设备等要求。	符合
	b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。	（1）机房配备了1组科华品牌UPS； （2）UPS正常工作，可满足主要设备断电情况下的至少1小时正常运行要求； （3）UPS有定期（至少每年）检查和维护，有运行和维护记录《机房巡检记录表》。	符合
电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。	（1）通信线缆铺设采用独立的具有电磁屏蔽作用线槽； （2）电源线缆铺设采用独立的具有电磁屏蔽作用线槽； （3）弱电线缆隔离铺设，没有干扰。	符合

D.2 安全通信网络

D.2.1 安全通用要求

D.2.1.1 安全通信网络

安全控制点	测评指标	结果结论	符合程度
网络架构	a）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；	（1）已对网络地址划分，且便于管理和控制； （2）网络地址划分采用核心交换机实现外网边界区域、服务器存储区域等的划分； （3）重要核心网络区域与非重要网络在同一网段； （4）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	部分符合
	b）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	（1）网络内重要网段未部署在网络边界处，且未直接连接外部信息系统； （2）系统通过防火墙对重要网段采取访问控制策略； （3）各安全域（子网）的出口唯一。	符合
通信传输	应采用校验技术保证通信过程中数据的完整性。	（1）网络系统中未涉及完整性保障设备，但在安全计算环境方面网络设备采用SSH协议、安全设备采用HTTPS协议、操作系统采用SSH协议、应用系统采用HTTPS协议来保证通信过程中数据的完整性。	符合

安全控制点	测评指标	结果结论	符合程度
可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对通信设备可信验证方面的安全设计要求； （2）现有的通信设备存在未能实现操作系统到上层应用的信任链的情况，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■通信应用连接过程	不符合

D.3 安全区域边界

D.3.1 安全通用要求

D.3.1.1 办公网区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■办公网区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	符合
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是	符合

安全控制点	测评指标	结果结论	符合程度
		拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	
	d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制,能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略,无法检测、防止或限制从内部发起的网络攻击行为。	不符合
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试； （4）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	部分符合
安全审计	a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间	符合

安全控制点	测评指标	结果结论	符合程度
	他与审计相关的信息；	■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.3.1.2 外网边界区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■外网边界区域 （2）网络边界处部署了可提供访问控制功能的设备； ■防火墙 ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	符合
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■防火墙 ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条	符合

安全控制点	测评指标	结果结论	符合程度
		显示禁止所有通信网络。	
	b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署支持对内部发起的攻击行为进行防范的设备； ■防火墙(带入侵防御模块) ■WEB应用防火墙 （2）现有的防范措施满足相应防护要求； ■所有关键网络边界均有检测措施 ■设备的规则库及时更新 ■检测(模块)符合国家相关产品检测要求 ■其安全策略有效 (3)内部安全防范措施能检测相应攻击行为。 ■端口扫描 ■强力攻击 ■木马后门攻击 ■拒绝服务攻击 ■缓冲区溢出攻击 ■碎片攻击 ■网络蠕虫攻击	符合

安全控制点	测评指标	结果结论	符合程度
		■应用漏洞攻击	
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试。	符合
安全审计	a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数	不符合

安全控制点	测评指标	结果结论	符合程度
	录送至安全管理中心。	■边界防护应用程序	

D.3.1.3 安全管理区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■安全管理区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	符合
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■防火墙（状态检测防火墙）	符合

安全控制点	测评指标	结果结论	符合程度
		（3）访问控制设备支持并启用基于连接状态的检测机制,能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略,无法检测、防止或限制从内部发起的网络攻击行为。	不符合
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试； （4）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	部分符合
安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个	符合

安全控制点	测评指标	结果结论	符合程度
		月； （5）定期收集日志记录并定期备份。	
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.3.1.4 服务器存储区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■服务器存储区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	符合
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址	符合

安全控制点	测评指标	结果结论	符合程度
		■目的地址 ■源端口 ■目的端口 ■协议	
	d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■WEB应用防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制,能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署支持对内部发起的攻击行为进行防范的设备； ■WEB应用防火墙 （2）现有的防范措施满足相应防护要求； ■所有关键网络边界均有检测措施 ■设备的规则库及时更新 ■检测(模块)符合国家相关产品检测要求 ■其安全策略有效 (3)内部安全防范措施能检测相应攻击行为。 ■端口扫描 ■强力攻击 ■木马后门攻击 ■拒绝服务攻击 ■缓冲区溢出攻击 ■碎片攻击 ■网络蠕虫攻击 ■应用漏洞攻击	符合
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■WEB应用防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试。	符合
安全审计	a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■WEB应用防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块)	符合

安全控制点	测评指标	结果结论	符合程度
		■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.4 安全计算环境

D.4.1 安全通用要求

D.4.1.1 网络设备

D.4.1.1.1 核心交换机

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括VTY认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有	符合

安全控制点	测评指标	结果结论	符合程度
		唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的全局密码策略； ■Password control:Enabled ■Password aging:Enabled (180 days) ■Password length:Enabled (8 characters) ■Password composition:Enabled (4 types, 1 characters per type) （6）设备配置加密的super认证。	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备配置合规的全局登录失败处理策略； ■Password control: Enabled ■Maximum login attempts: 5 ■Action for exceeding login attempts: Lock user for 5 minutes （2）设备配置合规的操作超时退出措施。 ■VTY配置idle-timeout 15 0	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式。 ■未启用TELNET ■启用SSH	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般	符合

安全控制点	测评指标	结果结论	符合程度
		用户管理员权限,不赋予用户不必要的操作权限。	
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； ■Information Center: Enabled ■Console: Enabled ■Monitor: Enabled ■Log host: Enabled 10.2.1.2 ■Security log file: Enabled （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制； ■对ssh 登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合

安全控制点	测评指标	结果结论	符合程度
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）网络层相关设备不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的交换功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规	符合

安全控制点	测评指标	结果结论	符合程度
		范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.1.2 汇聚交换机

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括VTY认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的全局密码策略； ■Password control:Enabled ■Password aging:Enabled (180 days) ■Password length:Enabled (8 characters) ■Password composition:Enabled (4 types, 1 characters per type) （6）设备配置加密的super认证。	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备配置合规的全局登录失败处理策略； ■Password control: Enabled ■Maximum login attempts: 5 ■Action for exceeding login attempts: Lock user for 5 minutes （2）设备配置合规的操作超时退出措施。	符合

安全控制点	测评指标	结果结论	符合程度
		■VTY配置idle-timeout 15 0	
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式。 ■未启用TELNET ■启用SSH	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； ■Information Center: Enabled ■Console: Enabled ■Monitor: Enabled ■Log host: Enabled 10.2.1.2 ■Security log file: Enabled （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型	符合

安全控制点	测评指标	结果结论	符合程度
		■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制； ■对ssh 登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）网络层相关设备不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的交换功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备	（1）设备不具备相关可信验证的技术措施；	不符合

安全控制点	测评指标	结果结论	符合程度
	的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2 安全设备

D.4.1.2.1 WEB应用防火墙

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； (2)登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令	符合

安全控制点	测评指标	结果结论	符合程度
		■未设置空口令	
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合

安全控制点	测评指标	结果结论	符合程度
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据	符合

安全控制点	测评指标	结果结论	符合程度
		（2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.2 上网行为管理系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b）应具有登录失败处理功	（1）设备启用合规登录失败处理策略；	符合

安全控制点	测评指标	结果结论	符合程度
	能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间	符合

安全控制点	测评指标	结果结论	符合程度
		■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备	（1）设备不具备相关可信验证的技术措施；	不符合

安全控制点	测评指标	结果结论	符合程度
	的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.3 基线核查系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合

安全控制点	测评指标	结果结论	符合程度
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方	（1）设备通过核心交换机的访问控制策略，	符合

安全控制点	测评指标	结果结论	符合程度
	式或网络地址范围对通过网络进行管理的管理终端进行限制；	通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的基线核查功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合

安全控制点	测评指标	结果结论	符合程度
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.4 日志审计系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟	符合

安全控制点	测评指标	结果结论	符合程度
	等相关措施；	（2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识	符合

安全控制点	测评指标	结果结论	符合程度
		■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。	不符合

安全控制点	测评指标	结果结论	符合程度
	结果形成审计记录送至安全管理中心。	■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施; ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施; ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能;	（1）设备定义了相关重要数据; ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范; （3）设备定期完全依照备份策略，采用正确的配置进行本地备份; （4）设备的备份周期为：每月一次; （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息;	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.5 运维安全管理系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员	符合

安全控制点	测评指标	结果结论	符合程度
		■系统操作员 (2)设备不存在多个管理级别高的特权用户； (3) 设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	(1) 设备开启审计功能，审计进程正常； (2) 设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	(1) 设备日期、时间正常； (2) 设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	(1) 设备限制审计文件的访问控制权限，普通用户不可删除及修改； (2) 设备针对日志、审计记录具备充足的存储容量； (3) 对审计记录进行定期存档备份，其备份策略有效； (4) 部署日志审计系统实时对日志进行统一收集存储； (5) 日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	(1) 设备在全局模式下禁用部分不必要的服务； (2) 设备在部分接口模式下禁用部分不必要的服务； (3) 漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	(1) 设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； (3) 漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	(1) 设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制。 ■对Web登录配置管理地址，限制登录范围	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要	(1) 设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 (2) 设备管理的校验接口范围较全面。	符合

安全控制点	测评指标	结果结论	符合程度
	求；	■包括人机接口校验 ■包括通信接口校验	
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份；	符合

安全控制点	测评指标	结果结论	符合程度
		（4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.6 防火墙-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合

安全控制点	测评指标	结果结论	符合程度
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效；	符合

安全控制点	测评指标	结果结论	符合程度
		（4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.7 防火墙-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证	符合

安全控制点	测评指标	结果结论	符合程度
	具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验	符合

安全控制点	测评指标	结果结论	符合程度
		■包括通信接口校验	
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确	符合

安全控制点	测评指标	结果结论	符合程度
		的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.3 服务器和终端

D.4.1.3.1 应用服务器-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）操作系统不存在空口令用户； ■etc/passwd文件中各用户的第二字段处不为空 ■/etc/shadow文件中各用户密码字段处不为空 （3）操作系统不存在默认信任的登录模式； （4）操作系统为登录用户设置的身份标识具有唯一性； ■UID具有唯一性 ■UID=0只能root用户 （5）操作系统配置的一定的密码长度且定期更换； ■PASS_MAX_DAYS 180 ■PASS_MIN_DAYS 1 ■PASS_MIN_LEN 8 ■PASS_WARN_AGE 28 （6）操作系统配置一定的密码复杂度策略。 ■minlen=8	符合

安全控制点	测评指标	结果结论	符合程度
		■ucredit=-2 ■lcredit=-1 ■dcredit=-4 ■ocredit=-1	
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用pam_tally2模块的合规登录失败处理策略； auth required /lib/security/pam_tally.so onerr=fail no_magic_root和 account required /lib/security/pam_tally.so deny=10 no_magic_root reset （2）操作系统配置合规的操作超时锁定； ■配置具备以下措施： /etc/profile设置TMOUT=300 （3）操作系统启用SSH的合规登录超时策略。 ■配置具备以下措施： /sshd_config设置 ClientAliveInterval 60 ClientAliveCountMax 3	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）操作系统配置合规的远程管理模式； ■启用SSH （2）操作系统远程端口使用情况合规； ■21（FTP）未启用 ■23（Telnet）未启用 （3）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在所有用户均属于root组的情况。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统对多余帐户进行删除、锁定或禁止其登录； （2）操作系统账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户	（1）操作系统根据安全策略要求对特权用户进行分离；	符合

安全控制点	测评指标	结果结论	符合程度
	的权限分离。	（2）操作系统不存在除root外的特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计功能，审计进程正常； ■rsyslog：loaded ■auditctl：enabled=1 （2）操作系统开启审计范围及策略满足要求，审计覆盖所有用户操作审计和记录。 ■rsyslog：*.info;mail.none;news.none;authpriv.none;cron.none /var/log/messages ■auditctl： 关键目录、文件的审计行为采用 perm=rwxa	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）操作系统针对日志、审计记录具备充足的存储容量； （3）操作系统采取合规的日志文件权限策略； ■/var/log/messages：640 ■/var/log/secure：640 ■/var/log/audit/audit.log：640 对审计记录进行定期存档备份,其备份策略有效 （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统关闭不必要端口； （2）操作系统禁用不必要服务；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口； （4）漏洞扫描未发现高风险主机端口。	
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服edr防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证； ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序 （3）现有的可信验证缺乏以下措施。 ■对可信性破坏报警 ■将可信性验证结果形成审计记录 ■对可信性审计的动态关联感知	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对鉴别数据采取完整性保护措施。	符合

安全控制点	测评指标	结果结论	符合程度
		■使用SSH加密协议进行传输 重要配置数据: （1）系统在通信传输过程中对重要配置数据采取完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为服务器设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统不保存过多终端历史记录。 ■通过echo $HISTSIZE查看history保留数目为30	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）本设备不存在此部分的控制需求，故此项不适用	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）本设备不存在此部分的控制需求，故此项不适用	不适用

D.4.1.3.2 应用服务器-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）操作系统不存在空口令用户； ■etc/passwd文件中各用户的第二字段处不为空 ■/etc/shadow文件中各用户密码字段处不为	符合

安全控制点	测评指标	结果结论	符合程度
		空 （3）操作系统不存在默认信任的登录模式； （4）操作系统为登录用户设置的身份标识具有唯一性； ■UID具有唯一性 ■UID=0只能root用户 （5）操作系统配置的一定的密码长度且定期更换； ■PASS_MAX_DAYS 180 ■PASS_MIN_DAYS 1 ■PASS_MIN_LEN 8 ■PASS_WARN_AGE 28 （6）操作系统配置一定的密码复杂度策略。 ■minlen=8 ■ucredit=-2 ■lcredit=-1 ■dcredit=-4 ■ocredit=-1	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用pam_tally2模块的合规登录失败处理策略； auth required /lib/security/pam_tally.so onerr=fail no_magic_root和 account required /lib/security/pam_tally.so deny=10 no_magic_root reset （2）操作系统配置合规的操作超时锁定； ■配置具备以下措施： /etc/profile设置TMOUT=300 （3）操作系统启用SSH的合规登录超时策略。 ■配置具备以下措施： /sshd_config设置 ClientAliveInterval 60 ClientAliveCountMax 3	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）操作系统配置合规的远程管理模式； ■启用SSH （2）操作系统远程端口使用情况合规； ■21（FTP）未启用 ■23（Telnet）未启用 （3）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需求分配不同的用	符合

安全控制点	测评指标	结果结论	符合程度
		户组及对应的权限，不存在所有用户均属于root组的情况。	
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统对多余帐户进行删除、锁定或禁止其登录； （2）操作系统账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； （2）操作系统不存在除root外的特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计功能，审计进程正常； ■rsyslog：loaded ■auditctl：enabled=1 （2）操作系统开启审计范围及策略满足要求，审计覆盖所有用户操作审计和记录。 ■rsyslog：*.info;mail.none;news.none;authpriv.none;cron.none /var/log/messages ■auditctl： 关键目录、文件的审计行为采用 perm=rwxa	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）操作系统针对日志、审计记录具备充足的存储容量； （3）操作系统采取合规的日志文件权限策略； ■/var/log/messages：640	符合

安全控制点	测评指标	结果结论	符合程度
		■/var/log/secure：640 ■/var/log/audit/audit.log：640 对审计记录进行定期存档备份,其备份策略有效 （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统关闭不必要端口； （2）操作系统禁用不必要服务； （3）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口； （4）漏洞扫描未发现高风险主机端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补；（3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服edr防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备	（1）缺乏对计算设备可信验证方面的安全设	不符合

安全控制点	测评指标	结果结论	符合程度
	的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	计要求； （2）系统未实现对所有可执行环节进行可信验证； ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序 （3）现有的可信验证缺乏以下措施。 ■对可信性破坏报警 ■将可信性验证结果形成审计记录 ■对可信性审计的动态关联感知	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对鉴别数据采取完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）系统在通信传输过程中对重要配置数据采取完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为服务器设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统不保存过多终端历史记录。 ■通过echo $HISTSIZE查看history保留数目为30	符合
个人信息保护	a）应仅采集和保存业务必	（1）本设备不存在此部分的控制需求，故此	不适用

安全控制点	测评指标	结果结论	符合程度
	需的用户个人信息； b）应禁止未授权访问和非法使用用户个人信息。	项不适用 （1）本设备不存在此部分的控制需求，故此项不适用	 不适用

D.4.1.3.3 数据库服务器

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）操作系统不存在空口令用户； ■etc/passwd文件中各用户的第二字段处不为空 ■/etc/shadow文件中各用户密码字段处不为空 （3）操作系统不存在默认信任的登录模式； （4）操作系统为登录用户设置的身份标识具有唯一性； ■UID具有唯一性 ■UID=0只能root用户 （5）操作系统配置的一定的密码长度且定期更换； ■PASS_MAX_DAYS 180 ■PASS_MIN_DAYS 1 ■PASS_MIN_LEN 8 ■PASS_WARN_AGE 28 （6）操作系统配置一定的密码复杂度策略。 ■minlen=8 ■ucredit=-2 ■lcredit=-1 ■dcredit=-4 ■ocredit=-1	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用pam_tally2模块的合规登录失败处理策略； auth required /lib/security/pam_tally.so onerr=fail no_magic_root和 account required /lib/security/pam_tally.so deny=10 no_magic_root reset （2）操作系统配置合规的操作超时锁定； ■配置具备以下措施： /etc/profile设置TMOUT=300 （3）操作系统启用SSH的合规登录超时策略。 ■配置具备以下措施：	符合

安全控制点	测评指标	结果结论	符合程度
		/sshd_config设置 ClientAliveInterval 60 ClientAliveCountMax 3	
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）操作系统配置合规的远程管理模式； ■启用SSH （2）操作系统远程端口使用情况合规； ■21（FTP）未启用 ■23（Telnet）未启用 （3）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在所有用户均属于root组的情况。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统对多余帐户进行删除、锁定或禁止其登录； （2）操作系统账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； （2）操作系统不存在除root外的特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计功能，审计进程正常； ■rsyslog：loaded ■auditctl：enabled=1 （2）操作系统开启审计范围及策略满足要求，审计覆盖所有用户操作审计和记录。 ■rsyslog： *.info;mail.none;news.none;authpriv.none;cron.none /var/log/messages ■auditctl： 关键目录、文件的审计行为采用 perm=rwxa	符合
	b) 审计记录应包括事件的	（1）操作系统日期、时间正常；	符合

安全控制点	测评指标	结果结论	符合程度
	日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）操作系统针对日志、审计记录具备充足的存储容量； （3）操作系统采取合规的日志文件权限策略； ■/var/log/messages：640 ■/var/log/secure：640 ■/var/log/audit/audit.log：640 对审计记录进行定期存档备份，其备份策略有效 （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统关闭不必要端口； （2）操作系统禁用不必要服务； （3）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口； （4）漏洞扫描未发现高风险主机端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）在不影响业务系统正常运行情况下，对	符合

安全控制点	测评指标	结果结论	符合程度
		发现的系统漏洞在确保安全的情况下进行修补； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服edr防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证； ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序 （3）现有的可信验证缺乏以下措施。 ■对可信性破坏报警 ■将可信性验证结果形成审计记录 ■对可信性审计的动态关联感知	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对鉴别数据采取完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）系统在通信传输过程中对重要配置数据采取完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备；	符合

安全控制点	测评指标	结果结论	符合程度
		（5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为服务器设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统不保存过多终端历史记录。 ■通过echo $HISTSIZE查看history保留数目为30	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）本设备不存在此部分的控制需求，故此项不适用	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）本设备不存在此部分的控制需求，故此项不适用	不适用

D.4.1.3.4 业务终端-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败	符合

安全控制点	测评指标	结果结论	符合程度
		■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下：运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口	（1）操作系统不存在此部分的控制需求，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	输入或通过通信接口输入的内容符合系统设定要求；		
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输	符合

安全控制点	测评指标	结果结论	符合程度
		（3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.5 业务终端-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施；	符合

安全控制点	测评指标	结果结论	符合程度
		■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 (5)用户属性策略未勾选“密码永不过期”。	
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员	符合

安全控制点	测评指标	结果结论	符合程度
		（2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下:运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b）应关闭不需要的系统服	（1）操作系统不存在多余的默认共享及其它	符合

安全控制点	测评指标	结果结论	符合程度
	务、默认共享和高危端口；	文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必	符合

安全控制点	测评指标	结果结论	符合程度
		要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.6 运维及管理终端-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户	符合

安全控制点	测评指标	结果结论	符合程度
		■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	(1)操作系统采取对审计记录存储容量如下:运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限；	符合

安全控制点	测评指标	结果结论	符合程度
		（4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程	（1）缺乏对计算设备可信验证方面的安全设计要求；	不符合

安全控制点	测评指标	结果结论	符合程度
	序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理	不适用

安全控制点	测评指标	结果结论	符合程度
	数据定时批量传送至备用场地。	要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施： 安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.7 运维及管理终端-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式；	符合

安全控制点	测评指标	结果结论	符合程度
	息在网络传输过程中被窃听。	（2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期	符合

安全控制点	测评指标	结果结论	符合程度
	他与审计相关的信息；	■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下:运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G; （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据	符合

安全控制点	测评指标	结果结论	符合程度
		■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.4 系统管理软件/平台

D.4.1.4.1 应用服务器-1-Tomcat

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）Tomcat中间件关闭web管理控制台，其身份鉴别功能由宿主操作系统实现，不适用。	不适用
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）Tomcat中间件关闭web管理控制台，其身份鉴别功能由宿主操作系统实现，不适用。	不适用
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）Tomcat中间件关闭web管理控制台，其身份鉴别功能由宿主操作系统实现，不适用。	不适用
访问控制	a）应对登录的用户分配账	（1）对应不同的账户均按需分配不同的用户	符合

安全控制点	测评指标	结果结论	符合程度
	户和权限；	权限，不存在中间件用户均属于管理级别、高权限的情况； （2）中间件配置可降权启动Tomcat的用户； （3）宿主系统针对中间件用户分别赋予相应的管理操作权限。 ■包括审计权限 ■包括操作权限	
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）中间件不存在除如:Tomcat、admin、manager、role1等默认账户名； （2）中间件账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）中间件不存在多余或过期账户； （2）中间件管理员用户与账户之间一一对应； （3）中间件启用合规的管理用户名配置。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）中间件根据安全策略要求对特权用户及宿主管理用户进行分离； （2）中间件管理不存在多个管理级别高的特权用户； （3）中间件管理按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）中间件开启审计功能，审计进程正常； ■开启Cataline引擎的日志文件 catalina.org.apache.juli.FileHandler.level = FINE ■开启内部代码丢出的日志 localhost.org.apache.juli.FileHandler.level = FINE ■开启manager应用日志 manager.org.apache.juli.FileHandler.level = FINE ■开启控制台输出的日志 java.util.logging.ConsoleHandler.level = FINE ■开启Access访问日志。 server.xml文件配置正常，未被注释标记<!-- -->； （2）系统的日志审计级别满足要求。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）中间件日期、时间正常； （2）中间件审计记录开启审核策略且日志级别正常。 ■日志级别不低于“FINE” ■日志配置pattern值设为common ■日志配置pattern值为自定义格式，至少包	符合

安全控制点	测评指标	结果结论	符合程度
		含：%h %l %u %t %s	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）中间件限制审计文件的访问控制权限，普通用户不可删除及修改； ■localhost.log 644 ■catalina.log 644 ■host-manager.log 644 ■manager.log 644 （2）宿主系统针对中间件日志、审计记录具备充足的存储容量； ■日志存储在/log/tomcat/目录下 ■日志创建计划为每天/每周/每月 ■不限制最大日志文件大小 （3）对中间件审计记录进行定期存档备份，其备份策略有效； （4）审计记录及日志保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）中间件系统不存在此部分的安装控制需求，不适用。	不适用
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）Tomcat中间件的管理地址限制功能由宿主操作系统实现，故该项不适用。	不适用
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）中间件管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）中间件管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）中间件已根据需要不定期地对已发布的版本进行更新； （2）中间件更新安装前进行安全性和兼容性测试； （3）在系统上线或发生重大变更时测试并安装最新的中间件版本或更新补丁； （4）在不影响业务系统正常运行情况下，对发现的中间件漏洞在确保安全的情况下进行修补； （5）中间件进行扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软	（1）中间件系统不存在此部分的控制需求，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	件，并定期进行升级和更新防恶意代码库。		
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输 重要配置数据: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份的中间件重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）宿主系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）中间件相关数据的备份周期合理：每天增量一次、每月全备一次； （5）中间件开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存	(1)宿主系统具有清除用户鉴别信息的功能；	符合

安全控制点	测评指标	结果结论	符合程度
	储空间被释放或重新分配前得到完全清除。	（2）经测试，宿主系统退出后无法访问先前中间件登录过的页面； （3）经测试，宿主系统关闭后无残留的中间件用户鉴别信息。	
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用

D.4.1.4.2 应用服务器-2-Tomcat

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）Tomcat中间件关闭web管理控制台，其身份鉴别功能由宿主操作系统实现，不适用。	不适用
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）Tomcat中间件关闭web管理控制台，其身份鉴别功能由宿主操作系统实现，不适用。	不适用
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）Tomcat中间件关闭web管理控制台，其身份鉴别功能由宿主操作系统实现，不适用。	不适用
访问控制	a）应对登录的用户分配账户和权限；	（1）对应不同的账户均按需分配不同的用户权限，不存在中间件用户均属于管理级别、高权限的情况； （2）中间件配置可降权启动Tomcat的用户； （3）宿主系统针对中间件用户分别赋予相应的管理操作权限。 ■包括审计权限 ■包括操作权限	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）中间件不存在除如:Tomcat、admin、manager、role1等默认账户名； （2）中间件账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）中间件不存在多余或过期账户； （2）中间件管理员用户与账户之间一一对应； （3）中间件启用合规的管理用户名配置。	符合

安全控制点	测评指标	结果结论	符合程度
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）中间件根据安全策略要求对特权用户及宿主管理用户进行分离； （2）中间件管理不存在多个管理级别高的特权用户； （3）中间件管理按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）中间件开启审计功能，审计进程正常； ■开启Cataline引擎的日志文件 catalina.org.apache.juli.FileHandler.level = FINE ■开启内部代码丢出的日志 localhost.org.apache.juli.FileHandler.level = FINE ■开启manager应用日志 manager.org.apache.juli.FileHandler.level = FINE ■开启控制台输出的日志 java.util.logging.ConsoleHandler.level = FINE ■开启Access访问日志。 server.xml文件配置正常，未被注释标记<!-- -->； （2）系统的日志审计级别满足要求。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）中间件日期、时间正常； （2）中间件审计记录开启审核策略且日志级别正常。 ■日志级别不低于“FINE” ■日志配置pattern值设为common ■日志配置pattern值为自定义格式，至少包含：%h %l %u %t %s	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）中间件限制审计文件的访问控制权限，普通用户不可删除及修改； ■localhost.log 644 ■catalina.log 644 ■host-manager.log 644 ■manager.log 644 （2）宿主系统针对中间件日志、审计记录具备充足的存储容量； ■日志存储在/log/tomcat/目录下 ■日志创建计划为每天/每周/每月 ■不限制最大日志文件大小 （3）对中间件审计记录进行定期存档备份，其备份策略有效； （4）审计记录及日志保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和	（1）中间件系统不存在此部分的安装控制需求，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	应用程序；		
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）Tomcat中间件的管理地址限制功能由宿主操作系统实现，故该项不适用。	不适用
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）中间件管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）中间件管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）中间件已根据需要不定期地对已发布的版本进行更新； （2）中间件更新安装前进行安全性和兼容性测试； （3）在系统上线或发生重大变更时测试并安装最新的中间件版本或更新补丁； （4）在不影响业务系统正常运行情况下，对发现的中间件漏洞在确保安全的情况下进行修补； （5）中间件进行扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输	符合

安全控制点	测评指标	结果结论	符合程度
		重要配置数据: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份的中间件重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）宿主系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）中间件相关数据的备份周期合理：每天增量一次、每月全备一次； （5）中间件开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）宿主系统具有清除用户鉴别信息的功能； （2）经测试，宿主系统退出后无法访问先前中间件登录过的页面； （3）经测试，宿主系统关闭后无残留的中间件用户鉴别信息。	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用

D.4.1.4.3 数据库服务器-Oracle

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）数据库系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）数据库系统不存在弱口令用户； ■ORACLE数据库已修改默认口令	符合

安全控制点	测评指标	结果结论	符合程度
		■ORACLE数据库不存在空口令用户 （3）数据库系统为登录用户设置的身份标识具有唯一性； （4）数据库系统配置合规的密码长度及复杂度策略； ■PASSWORD_VERIFY_FUNCTION ，LIMIT=VERIFY_FUNCTION ■IF LENGTH(password) 值为8 ■PASSWORD_REUSE_MAX值为5 （5）数据库系统配置合规的密码有效周期策略。 ■PASSWORD_LIFE_TIME值为 180	
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）数据库系统启用合规登录失败处理策略； ■ORACLE 数据库系统FAILED_LOGIN_ATTEMPTS= 10 （2）数据库系统执行合规的锁定策略。 ■PASSWORD_LOCK_TIME=1	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）数据库系统配置合规的远程管理模式。 ■ORACLE 数据库系统sqlnet.encryption为true ■ORACLE 数据库系统采用sqlplus连接数据库，客户端与服务器端之间通信是加密的	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）登录数据库系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （2）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在多用户均与sys、DBA用户权限一致的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）数据库系统对多余帐户进行删除、锁定或禁止其登录； ■数据库系统账户禁用不常用的默认用户 （2）数据库系统账户口令设置合规。 ■数据库系统各用户未使用空口令 ■数据库系统未使用弱口令或默认与用户名相同的口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）数据库系统不存在多余或过期账户； （2）数据库系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）数据库系统根据安全策略要求对特权用户进行分离； ■配置系统管理员	符合

安全控制点	测评指标	结果结论	符合程度
		■配置安全审计员 ■配置系统操作员 （2）数据库系统用户权限合理，非管理员未设置过大权限； ■具备DBA角色的用户仅为 SYS、SYSTEM （3）数据库系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）数据库系统开启审计功能，审计进程正常； ■ORACLE 数据库系统audit_sys_operations=TRUE ■ORACLE 数据库系统audit_trail=DB （2）ORACLE数据库系统启动数据库日志模式和自动归档； ■Automatic archival=Enabled （3）审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）数据库宿主系统日期、时间正常； （2）数据库系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括重要用户行为 ■包括系统资源的异常使用情况 ■包括重要系统命令的使用 ■包括重要的安全相关事件	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）数据库系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）数据库系统针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）日志及审计记录保存大于6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）网络设备ACL策略有效限制访问本机的IP地址及管理模式。	符合
	d）应提供数据有效性检验	（1）数据库系统不存在此部分的控制需求，	不适用

安全控制点	测评指标	结果结论	符合程度
	功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	不适用。	
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）数据库系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）数据库宿主系统不存在启用未加控制的高危端口； （3）MY_SQL分离默认安装的示例数据库； （4）数据库系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■SQLNET.ENCRYPTION_SERVER = REQUIRED ■SQLNET.ENCRYPTION_TYPES_SERVER = RC4_256 ■SQLNET.CRYPTO_CHECKSUM_SERVER = REQUIRED 重要配置数据: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■SQLNET.ENCRYPTION_SERVER = REQUIRED	符合

安全控制点	测评指标	结果结论	符合程度
		■SQLNET.ENCRYPTION_TYPES_SERVER = RC4_256 ■SQLNET.CRYPTO_CHECKSUM_SERVER = REQUIRED	
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）数据库系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）数据库系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）数据库系统未能提供异地数据备份功能。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）数据库系统不保存终端历史记录。	符合
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）数据库存储的用户个人信息均为业务应用必需的环节。	符合
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； ■包括信息采集 ■包括信息保存 ■包括信息访问 ■包括信息使用 （2）数据库具备控制措施禁止未授权访问用户个人信息表单； （3）数据库具备控制措施禁止非法使用用户个人信息表单。	符合

D.4.1.5 业务应用系统/平台

D.4.1.5.1 教学管理信息服务平台

安全控制点	测评指标	结果结论	符合程度

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）系统对各登录模式均启用身份鉴别； ■包括管理后台认证 （2）系统对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）系统登录用户设置的身份标识具有唯一性； （4）系统不存在空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）系统启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）系统配置合规的操作超时退出措施。 ■管理后台配置超时15分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）应用系统的用户鉴别数据采用SHA-512算法在可控网络环境中传输； （2）系统配置合规的远程管理模式。 ■启用HTTPS	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供系统权限分配表； （2）登录系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需分配不同的用户权限，不存在所有用户均属于管理级别、高权限的情况。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）系统禁用默认账户名； （2）系统账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）系统不存在多余或过期账户； （2）系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）系统不存在多个管理级别高的特权用户； （2）系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对	（1）系统开启审计功能，审计进程正常； （2）系统的日志审计级别满足要求，审计覆	符合

安全控制点	测评指标	结果结论	符合程度
	重要的用户行为和重要安全事件进行审计；	盖所有用户操作审计和记录。	
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）系统日期、时间正常； （2）系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）系统针对日志、审计记录具备充足的存储容量； （3）审计记录及日志保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）应用软件系统不存在此部分的安装控制需求，不适用。	不适用
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）应用软件系统不存在此部分的控制需求，不适用。	不适用
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）系统自身设定有效的终端访问策略，通过访问措施进行管理地址的限制。 ■系统管理页面仅能内网登录	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）系统具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）系统的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）系统已根据需要不定期地对已发布的版本进行更新； （2）在系统上线或发生重大变更时测试并安装最新的版本或更新补丁； （3）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）应用软件系统不存在此部分的控制需求，不适用。	不适用
可信验证	可基于可信根对计算设备	（1）应用软件系统不存在此部分的控制需求，	不适用

安全控制点	测评指标	结果结论	符合程度
	的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	不适用。	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）系统具有清除用户鉴别信息的功能； （2）经测试，系统退出后无法访问先前登录过的页面； （3）经测试，系统关闭后无残留的用户鉴别信息。	符合

安全控制点	测评指标	结果结论	符合程度
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息； （3）系统采集的用户个人信息均为业务应用必需的环节。	符合
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）系统不采集和保存任何形式的用户个人信息； （2）系统对所有涉及个人信息的环节均有明确的授权同意过程； ■包括信息采集 ■包括信息保存 ■包括信息访问 ■包括信息使用 （3）系统具备控制措施禁止未授权访问用户个人信息； （4）系统具备控制措施禁止非法使用用户个人信息。	符合

D.4.1.6 数据资源

D.4.1.6.1 重要业务数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	（1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要业务数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份重要数据； ■包括重要业务数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用	（1）单位未能提供异地数据备份措施。	不符合

安全控制点	测评指标	结果结论	符合程度
	场地。		
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）该测评项测评对象鉴别数据，已在安全计算环境层面其他对象判定，此项不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）该测评项测评对象为重要个人信息的内容，已在安全计算环境层面其他对象判定，该项不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）该测评项测评对象为重要个人信息的内容，已在安全计算环境层面其他对象判定，该项不适用。	不适用

D.4.1.6.2 重要个人信息

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	（1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要个人信息 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份重要数据； ■包括重要个人信息 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）该测评项测评对象鉴别数据，已在安全计算环境层面其他对象判定，此项不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息； （3）系统采集的用户个人信息均为业务应用	符合

安全控制点	测评指标	结果结论	符合程度
		必需的环节。	
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； ■包括信息采集 ■包括信息保存 ■包括信息访问 ■包括信息使用 （2）系统具备控制措施禁止未授权访问用户个人信息； （3）系统具备控制措施禁止非法使用用户个人信息。	符合

D.4.1.6.3 鉴别数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	数据库服务器-Oracle: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■SQLNET.ENCRYPTION_SERVER = REQUIRED ■SQLNET.ENCRYPTION_TYPES_SERVER = RC4_256 ■SQLNET.CRYPTO_CHECKSUM_SERVER = REQUIRED 应用服务器-1-Tomcat、应用服务器-2-Tomcat: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输 业务终端-1、业务终端-2、运维及管理终端-1、运维及管理终端-2: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。	符合

安全控制点	测评指标	结果结论	符合程度
		■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 教学管理信息服务平台: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输 应用服务器-1、应用服务器-2、数据库服务器: （1）系统在通信传输过程中对鉴别数据采取完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	该测评项在各系统及设备已做判定,数据资源针对鉴别数据不做判定	不适用
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	该测评项在各系统及设备已做判定,数据资源针对鉴别数据不做判定，不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	应用服务器-1-Tomcat、应用服务器-2-Tomcat: （1）宿主系统具有清除用户鉴别信息的功能； （2）经测试，宿主系统退出后无法访问先前中间件登录过的页面； （3）经测试，宿主系统关闭后无残留的中间件用户鉴别信息。 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）网络层设备不适用。 业务终端-1、业务终端-2、运维及管理终端-1、运维及管理终端-2: （1）身份鉴别信息释放或清除机制正常且满	符合

安全控制点	测评指标	结果结论	符合程度
		足要求； （2）操作系统用户的鉴别信息释放措施： 安全选项“不显示上次的用户名”->启用 应用服务器-1、应用服务器-2、数据库服务器: （1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统不保存过多终端历史记录。 ■通过echo $HISTSIZE查看history保留数目为30 教学管理信息服务平台: （1）系统具有清除用户鉴别信息的功能； （2）经测试，系统退出后无法访问先前登录过的页面； （3）经测试，系统关闭后无残留的用户鉴别信息。 数据库服务器-Oracle: （1）身份鉴别信息释放或清除机制正常且满足要求； （2）数据库系统不保存终端历史记录。	
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	鉴别数据不存在此部分的控制需求,故此项不适用	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	鉴别数据不存在此部分的控制需求,故此项不适用	不适用

D.4.1.6.4 重要配置数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	教学管理信息服务平台: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输 数据库服务器-Oracle: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■SQLNET.ENCRYPTION_SERVER = REQUIRED ■SQLNET.ENCRYPTION_TYPES_SERVER = RC4_256	符合

安全控制点	测评指标	结果结论	符合程度
		■SQLNET.CRYPTO_CHECKSUM_SERVER = REQUIRED 应用服务器-1-Tomcat、应用服务器-2-Tomcat: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 业务终端-1、业务终端-2、运维及管理终端-1、运维及管理终端-2: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 应用服务器-1、应用服务器-2、数据库服务器: （1）系统在通信传输过程中对重要配置数据采取完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）设备定义了相关重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 应用服务器-1-Tomcat、应用服务器-2-Tomcat: （1）系统定义了相关需要备份的中间件重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）宿主系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）中间件相关数据的备份周期合理：每天增量一次、每月全备一次； （5）中间件开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 业务终端-1、业务终端-2、应用服务器-1、应用服务器-2、数据库服务器、运维及管理终端-1、运维及管理终端-2: （1）操作系统定义了相关重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 教学管理信息服务平台: （1）系统定义了相关需要备份重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进	

安全控制点	测评指标	结果结论	符合程度
		行正常的数据恢复的测试记录《数据恢复申请表》。 数据库服务器-Oracle: （1）数据库系统定义了相关重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）数据库系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、运维安全管理系统、防火墙-1、防火墙-2: （1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 数据库服务器-Oracle: （1）数据库系统未能提供异地数据备份功能。 应用服务器-1-Tomcat、应用服务器-2-Tomcat、教学管理信息服务平台: （1）单位未能提供异地数据备份措施。 业务终端-1、业务终端-2、运维及管理终端-1、运维及管理终端-2: （1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 应用服务器-1、应用服务器-2、数据库服务器: （1）设备为服务器设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 核心交换机、汇聚交换机: （1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要	不符合

安全控制点	测评指标	结果结论	符合程度
		求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	重要配置数据不存在此部分的控制需求,故此项不适用	不适用
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	重要配置数据不存在此部分的控制需求,故此项不适用	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	重要配置数据不存在此部分的控制需求,故此项不适用	不适用

D.4.1.7 其他系统或设备

无

D.5 安全管理中心

D.5.1 安全通用要求

D.5.1.1 管理中心

安全控制点	测评指标	结果结论	符合程度
系统管理	a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；	（1）网络中部署运维安全管理系统实现集中的系统管理； （2）系统对登录用户进行身份鉴别； ■包括合规的用户名 ■包括合规的口令策略 （3）系统用户标识具有唯一性； ■不存在多人共享 ■增加、删除用户或权限变更需经过审批 （4）系统可实现对账户的身份鉴别数据进行保密性和完整性保护； （5）系统管理操作模式具备控制措施； ■只允许系统管理员登录 ■具备特定的登录命令 ■具备特定的登录操作界面 （6）系统具备相应的管理操作审计措施。 ■可实现对系统管理操作进行审计 ■审计范围覆盖所有用户 ■操作审计不可被删除	符合
	b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。	（1）系统管理员对系统的资源和运行进行配置、控制和管理； ■包括用户身份管理 ■包括资源配置管理 ■包括系统加载和启动管理 ■包括系统运行的异常处理管理 ■包括数据和设备的备份与恢复管理	不符合

安全控制点	测评指标	结果结论	符合程度
		（2）系统的资源、运行及配置管理不够全面。 ■缺乏可信证书管理 ■缺乏可信基准库管理	
审计管理	a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；	（1）网络中部署运维安全管理系统实现集中安全审计功能； （2）审计系统对审计管理员进行身份鉴别； ■包括合规的用户名 ■包括合规的口令策略 （3）审计系统用户标识具有唯一性； ■不存在多人共享 ■增加、删除用户或权限变更需经过审批 （4）审计系统管理操作模式具备控制措施； ■只允许审计管理员登录 ■具备特定的登录命令 ■具备特定的登录操作界面 （5）审计系统具备相应的管理操作审计措施。 ■可实现对安全审计操作进行审计 ■审计范围覆盖所有审计管理用户 ■操作审计不可被删除	符合
	b）应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	教学管理信息服务平台： （1）审计管理员定期对审计记录进行分析，对发现的安全可疑事件及时处理； （2）单位具有安全审计策略文件，规范审计记录的存储、管理和查询要求； （3）审计管理员按规范要求对审计记录进行管理。 ■审计记录不可随意删除/修改 ■定期备份、存储审计记录 ■审计记录存储周期满足6个月要求 重要审计数据： 日志审计系统、运维安全管理系统： （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要审计数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■网络设备、安全设备使用rsyslog协议进行传输 ■Linux操作系统使用rsyslog协议进行传输 ■Windows操作系统使用插件+SSL协议进行传输	符合

D.6 安全管理制度

D.6.1 安全通用要求

D.6.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。	（1）单位具有网络安全工作的总体方针和安全策略文件； ■具备独立的网络安全总体方针文件 ■具备涵盖网络安全总体方针策略要求的相关管理文件 ■具备安全策略文件 （2）制度内容包括明确的单位安全工作要求； ■安全目标 ■安全范围 ■安全原则 ■安全框架 ■各类安全策略 （3）管理文件详见《信息安全总体策略》。	符合
管理制度	a）应对安全管理活动中的主要管理内容建立安全管理制度；	（1）单位有针对安全管理活动中的各类管理内容建立安全管理制度； （2）现有制度已覆盖管理活动的主要的方面； ■具备文件控制管理 ■具备安全检查管理 ■具备人力资源及培训 ■具备设备管理 ■具备软件开发/外包开发项目管理 ■具备机房安全管理 ■具备信息分类及管理 ■具备网络安全管理 ■具备系统安全管理 ■具备恶意代码管理 ■具备变更控制 ■具备备份及介质管理 ■具备事件管理 ■具备应急预案 （3）制度详见：《信息安全总体策略》、《网络安全管理规范》、《组织安全结构和人员职责制度》、《人员管理制度》、《员工考核管理制度》。	符合
	b）应对管理人员或操作人员执行的日常管理操作建立操作规程。	（1）单位针对相关业务日常管理的操作建立规程类管理制度； （2）现有制度已覆盖重要管理方面的系统维护手册和用户操作规程等； ■具备网络/安全管理 ■具备服务器管理 ■具备数据库管理	符合

安全控制点	测评指标	结果结论	符合程度
		■具备机房硬件设施管理 ■具备业务应用管理 （3）管理文件详见《设备及系统软件配置和操作手册》。	
制定和发布	a）应指定或授权专门的部门或人员负责安全管理制度的制定；	（1）单位针对安全管理制度的制定，指定教育信息与网络中心部主要负责； （2）在已制定的相关制度中可查阅到被授权制定管理制度的部门/人员信息； （3）管理文件详见《安全管理组织规范》。	符合
	b）安全管理制度应通过正式、有效的方式发布，并进行版本控制。	（1）单位针对制度的制定和发布要求，制定管理规范文件； （2）管理规范文件对文件制定及发布定义了规范要求； ■包括安全管理制度的制定和发布程序 ■包括格式要求 ■包括版本编号要求 （3）安全管理制度的收发登记记录有效； ■具备通过正式、有效的方式收发 ■具备正式发文 ■具备领导签署、单位盖章等 （4）管理文件详见《制度制定、发布、评审和修订管理制度》、《收发文登记记录》。	符合
评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	（1）单位针对制度的合理性和适用性需进行论证和审定及修订的要求，制定管理规范文件； （2）管理规范文件对制度的评审及修订定义了规范要求； （3）单位具有安全管理制度的审定或论证的过程记录； （4）单位对做过修订的制度，具备有修订版本的安全管理过程记录； （5）管理文件详见《制度制定、发布、评审和修订管理制度》及 《安全管理制度评审记录》。	符合

D.7 安全管理机构

D.7.1 安全通用要求

D.7.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
岗位设置	a）应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面	（1）单位已明确网络安全管理工作的职能部门，并明确了各岗位职责； ■已设置机房管理员	符合

安全控制点	测评指标	结果结论	符合程度
	的负责人岗位，并定义各负责人的职责；	■已设置网络管理员 ■已设置安全管理员 （2）单位各部门职责文档已明确网络安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备网络安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	
	b）应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。	（1）单位已明确系统安全管理工作的职能部门，并明确了各岗位职责； ■已设置系统管理员 ■已设置数据管理员 ■已设置审计管理员 ■已设置应用管理员 （2）单位各部门职责文档已明确系统安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备系统安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	符合
人员配备	应配备一定数量的系统管理员、审计管理员和安全管理员等。	（1）单位针对人员配备要求，制定了管理制度； （2）单位按要求配备一定数量的重要岗位管理人员； （3）单位针对各岗位人员，制定并维护人员档案； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	符合
授权和审批	a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；	（1）单位在制度中用文字描述或在流程图中明确，对关键活动进行审批； ■具备部门职责文档明确各部门审批事项 ■具备岗位职责文档明确各岗位审批事项 （2）单位对审批过程明确审批权限，对各项信息系统的重要操作与变更明确审批部门和批准人； （3）管理文件详见《授权和审批管理规定》。	符合
	b）应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。	（1）单位针对各项业务操作及变更等建立了审批程序规定； ■包括系统变更 ■包括重要操作 ■包括物理访问 ■包括系统接入 （2）单位针对系统变更、系统接入、物理范	符合

安全控制点	测评指标	结果结论	符合程度
		围等事项已明确按审批程序执行,记录有批准人签字; （3）管理文件详见《授权和审批管理规定》。	
沟通和合作	a）应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；	（1）单位针对机构内部管理人员之间、部门之间的沟通与合作，制定了管理制度； （2）单位的管理制度规范了合作和沟通的方式和周期； （3）单位有组织机构内部人员联系表； （4）单位有定期召开信息安全会议，保存有会议纪要； （5）管理文件详见《安全教育和培训制度》、《技能培训记录》《外部联系表》。	符合
	b）应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；	（1）单位针对加强与外部单位的合作与沟通,制定了管理制度规定; ■包括公安机关 ■包括网络安全职能部门 ■包括职能监管机构 ■包括各类供应商 ■包括业界专家 ■包括安全组织 （2）单位能按要求与相关单位保持沟通合作,并提供相关单位联系方式和交流会议纪要; （3）管理文件详见《安全教育和培训制度》、《技能培训记录》、《外部联系表》。	符合
	c）应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	（1）单位建立了完善的对外联单位的联系列表; ■记录单位名称 ■记录合作内容 ■记录联系人 ■记录联系方式 （2）管理文件详见《外部联系表》。	符合
审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。	（1）单位针对定期开展常规安全检查，制定了管理制度; （2）单位对检查工作的范围、过程、要求等管理的比较完善; ■系统日常运行 ■系统漏洞 ■数据备份 ■包括敏感系统检查人员 （3）单位已按要求由安全管理员定期检查,检查内容需覆盖系统运行相关的管理活动,并能提供安全检查报告; （4）管理文件详见《安全审查和检查管理规	部分符合

安全控制点	测评指标	结果结论	符合程度
		范》； （5）单位开展的检查工作不够完善。 ■未定期检查	

D.8 安全管理人员

D.8.1 安全通用要求

D.8.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
人员录用	a）应指定或授权专门的部门或人员负责人员录用；	（1）单位授权专门的部门负责人员录用工作，制定了管理制度规范； （2）由人力资源保障科负责人员录用工作； （3）管理文件详见《人员管理制度》。	符合
	b）应对被录用人员的身份、安全背景、专业资格或资质等进行审查。	（1）单位针对人员录用过程，制定了明确要求，并形成人员安全管理制度； （2）单位现有管理制度明确说明录用人员应具备的条件； ■包括学历/学位要求 ■包括技术人员的专业技术要求 ■包括管理人员的安全管理要求 （3）单位按规定执行人员录用的相关审查过程； ■包括录用人身份 ■包括安全背景 ■包括专业资格 ■包括资质 （4）管理文件详见《人员管理制度》、《人员入职考核记录》。	符合
人员离岗	应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。	（1）单位针对离岗人员权限终止及取回机构提供的各种设施的要求，制定了管理制度； （2）单位按规范开展对离岗人员的相关管理工作； ■明确负责部门 ■及时终止其访问权限 ■交还身份证件 ■交还软硬件设备 （3）管理文件详见《人员管理度》、《人员离岗申请表》、《离场信息资料交接表》。	符合
安全意识教育和培训	应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。	（1）单位针对人员安全培训及责任和惩戒措施，制定了管理制度； （2）单位已开展安全意识教育及岗位技能培训 ■具备明确培训周期	符合

安全控制点	测评指标	结果结论	符合程度
		■具备有效的培训方式 ■具备清晰的培训内容 ■具备考核要求 （3）管理文件详见《安全教育和培训制度》。	
外部人员访问管理	a）应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；	（1）单位针对外部人员物理访问，制定了外部人员访问管理文档； ■明确允许外部人员访问的范围 ■明确外部人员进入的条件 ■明确外部人员进入的访问控制措施 （2）单位具备有效的外部人员访问重要区域的书面申请文档； ■具有申请人 ■具有申请原因 ■具有范围 ■具有日期 ■具有批准人签字 （3）单位具备外部人员访问重要区域的登记记录； ■记录进入时间、 ■记录离开时间 ■记录访问区域 ■记录陪同人信息 （4）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。	符合
	b）应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；	（1）单位针对外部接入受控网络访问系统，制定了管理制度； （2）单位具备外部人员接入受控网络前的申请审批流程； （3）单位具备外部人员接入及访问系统的书面申请文档； ■具有申请人 ■具有申请原因 ■具有访问权限 ■具有日期 ■具有批准人签字 （4）单位具备外部人员接入及访问系统的登记记录； ■记录访问权限 ■记录访问时限 ■记录账户 （5）管理文件详见《外部人员访问管理制度》、	符合

安全控制点	测评指标	结果结论	符合程度
		《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。	
	c) 外部人员离场后应及时清除其所有的访问权限。	（1）单位针对人员离场后的清理工作，制定了管理制度； （2）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》； （3）单位未完全按管理规范开展人员离场后的清理工作。 ■缺乏清理记录 ■未及时清除离场后的所有访问权限 ■未记录访问权限清除时间	不符合

D.9 安全建设管理

D.9.1 安全通用要求

D.9.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
定级和备案	a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；	（1）单位的被测系统于2022年4月已完成备案； （2）系统备案相关文档（定级报告）中明确等级划分方法和理由，SAG三个方面的级别描述清晰； （3）管理文件详见《定级备案》。	符合
	b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；	（1）单位针对系统定级结果的审批及评审工作等要求，制定了管理制度； （2）现有系统的定级已具备合理性和正确性审定； ■具备单位部门审定 （3）管理文件详见《定级备案》。	符合
	c) 应保证定级结果经过相关部门的批准；	（1）单位针对系统定级结果的上级批准要求，制定了管理制度； （2）现有系统的定级获得了相关部门的批准； （3）管理文件详见《定级备案》。	符合
	d) 应将备案材料报主管部门和相应公安机关备案。	（1）单位对被测系统的等级备案表、定级报告等备案材料已经报相应公安机关备案； （2）单位具备公安机关出具的备案号； （3）管理文件详见《定级备案》。	符合
安全方案设计	a) 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整	（1）单位未具备适用于被测系统的安全规划设计方案； （2）现有方案文档未能完全按照规范要求选	不符合

安全控制点	测评指标	结果结论	符合程度
	安全措施；	择安全措施。 ■缺乏安全保护等级的要求 ■缺乏风险分析结果的要求 ■缺乏实际安全需求	
	b) 应根据保护对象的安全保护等级进行安全方案设计；	（1）单位未具备完整的安全设计方案相关的文档。 ■缺乏总体规划 ■缺乏安全设计方案 ■缺乏相关配套文件 ■缺乏保护对象的安全保护等级要求	不符合
	c) 应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； ■缺乏安全整体规划 ■缺乏安全设计方案 ■缺乏安全配套文件 （2）单位未对相关论证过程及内容进行完整的记录。	不符合
产品采购和使用	a) 应确保网络安全产品采购和使用符合国家的有关规定；	（1）单位已建立安全产品管理的相关管理规定； ■包括采购要求 ■包括使用要求 （2）单位具备安全产品采购流程及相关实施文档； （3）被测系统使用的安全产品具备销售许可资质； （4）安全产品具均为国内产品； （5）管理文件详见《设备安全管理制度》。	符合
	b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。	（1）单位已建立密码产品与服务管理的相关管理制度； ■包括采购要求 ■包括使用要求 （2）系统未使用密码产品； （3）管理文件详见《设备安全管理制度》。	符合
自行软件开发	a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。	不适用
	b) 应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。	不适用
外包软件开发	a) 应在软件交付前检测其中可能存在的恶意代码；	（1）单位针对软件交付前测试恶意代码的要求，制定了管理制度； （2）管理文件详见《外包开发软件管理规定》；	不符合

安全控制点	测评指标	结果结论	符合程度
		（3）单位未在软件交付之前按要求对所有软件开展恶意代码检测。 ■缺乏恶意代码检测报告	
	b）应保证开发单位提供软件设计文档和使用指南。	（1）单位制定软件开发项目验收要求，明确开发单位的提交材料； （2）开发单位提供软件日常维护和使用所需的文档； ■包括需求分析说明书 ■包括软件设计说明书 ■包括软件操作手册 （3）管理文件详见《外包开发软件管理规定》、《设备及系统软件配置和操作手册》。	符合
工程实施	a）应指定或授权专门的部门或人员负责工程实施过程的管理；	（1）单位针对专门的部门负责工程实施过程的管理要求，制定管理度； （2）单位由专岗负责系统建设的工程实施，且按照实施方案的要求对进度和质量进行控制； （3）管理文件详见《工程实施管理制度》。	符合
	b）应制定安全工程实施方案控制工程实施过程。	（1）单位制定了详细的工程实施方案； ■包括工程时间限制 ■包括进度控制 ■包括质量控制 （2）工程实施单位严格按照方案执行，并有过程记录； （3）管理文件详见《测试及验收方案》、《工程项目实施方案》。	符合
测试验收	a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；	（1）单位可提供被测系统的合规测试验收方案； ■包括测试人员 ■包括测试验收内容 ■包括现场操作过程 （2）管理文件详见《测试及验收方案》、《工程项目实施方案》； （3）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。 ■缺乏验收报告 ■缺乏报告审定意见	部分符合
	b）应进行上线前的安全性测试，并出具安全测试报告。	（1）单位对系统上线前需开展安全性测试的要求，制定管理制度； （2）管理文件详见《外包开发软件管理规定》、《系统交付管理》； （3）针对系统上线前的安全性测试工作存在问题。	不符合

安全控制点	测评指标	结果结论	符合程度
		■缺乏测试报告	
系统交付	a) 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；	（1）单位具备系统交付清单； （2）系统交付清单内容较详细； ■包括设备 ■包括软件 ■包括文档 （3）单位的清点工作较合规； ■已依据交付清单开展清点工作 （4）管理文件详见《系统交付管理》、《资产清单》。	符合
	b) 应对负责运行维护的技术人员进行相应的技能培训；	（1）单位已对负责系统运行维护的技术人员进行了技能培训； （2）具备运维人员的培训记录； ■包括培训时间 ■包括培训地点 ■包括培训对象 ■包括培训内容 ■包括培训参与人员签字 （3）管理文件详见《系统交付管理》、《资产清单》、《系统交付清单》、《技能培训记录》。	符合
	c) 应提供建设过程文档和运行维护文档。	（1）单位提供了系统建设过程中的文档； （2）单位提供了指导用户进行系统运维的文档和系统培训手册； （3）管理文件详见《系统交付管理》、《系统交付清单》、《设备及系统软件配置和操作手册》。	符合
等级测评	a) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；	（1）单位针对系统等级测评要求，制定管理制度； （2）系统按要求开展首次测评工作； （3）管理文件详见《系统安全管理制度》。	符合
	b) 应在发生重大变更或级别发生变化时进行等级测评；	（1）管理制度中已规定在系统发生变更时及时对系统进行等级测评； （2）系统未发生过重大变更，系统等级未发生变化； （3）管理文件详见《系统安全管理制度》。	符合
	c) 应确保测评机构的选择符合国家有关规定。	（1）已选择在“全国等级保护测评机构推荐目录”中的测评单位进行等级测评； （2）管理文件详见《系统安全管理制度》、《网络安全等级保护测评服务合同》。	符合
服务供应商选择	a) 应确保服务供应商的选择符合国家的有关规定；	（1）单位在管理制度内明确提出安全服务供应商选择的要求； （2）单位选择的安全服务商符合国家的有关	符合

安全控制点	测评指标	结果结论	符合程度
		规定，具备相应的安全服务资质； （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。	
	b）应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。	（1）单位的管理制度中已规定，需与安全服务商签订安全相关的协议并明确整个服务供应链各方需履行的网络安全相关义务； （2）单位已按规定与选定的安全服务商签订合规的协议； ■明确整个服务供应链各方需履行的网络安全相关义务 ■包括保密范围 ■包括安全责任 ■包括违约责任 ■包括协议的有效期限 ■包括责任人签字 （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。	符合

D.10 安全运维管理

D.10.1 安全通用要求

D.10.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
环境管理	a）应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；	（1）单位建立机房安全方面的管理制度，对有关运维方面的管理作出规定； ■指定教育信息与网络中心部门负责管理 ■包括出入管理要求 ■包括定期维护要求 ■包括空调要求 ■包括供配电设备要求 ■包括消防设施要求 ■包括温湿度控制要求 （2）单位具备完整的机房出入登记记录； ■记录来访人员 ■记录来访时间 ■记录离开时间 ■记录携带物品 （3）单位具备完整的机房基础设施的维护记录； ■记录维护日期 ■记录维护人 ■记录维护设备 ■记录故障原因 ■记录维护结果	符合

安全控制点	测评指标	结果结论	符合程度
		（4）管理文件详见《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。	
	b）应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；	（1）单位建立机房安全方面的管理制度； ■包括物理访问管理 ■包括物品进出管理 ■包括环境安全管理 （2）单位现有机房管理记录与制度相符； ■具备物理访问记录 ■具备物品进出记录 ■具备环境安全相关记录 （3）制度详见：《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。	符合
	c）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	（1）单位机房安全管理制度已明确来访人员的接待区域的要求； （2）单位按规范要求开展人员来访接待； ■划分来访人员的接待区域 ■记录来访人员的情况 （3）单位办公环境未发现有随意放置含有敏感信息介质的情况； ■无纸档文件 ■无移动介质 （4）制度详见：《机房安全管理制度》、《物理安全管理规范》、《办公环境保密管理》。	符合
资产管理	应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。	（1）单位已建立有效的资产清单； （2）单位现有资产清单内容较全面； ■包括设备设施类别 ■包括软件类别 ■包括文档类别 ■包括资产责任人 ■包括所属级别 ■包括所处位置 ■包括所处部门 （3）制度详见：《设备安全管理制度》、《资产清单》。	符合
介质管理	a）应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘	（1）介质按管理要求放置于受控的环境中（如：机房）； （2）介质管理具备较全面的记录； ■包括介质归档 ■包括使用情况	符合

安全控制点	测评指标	结果结论	符合程度
	点；	■包括定期盘点记录 （3）制度详见：《设备安全管理制度》、《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。	
	b）应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。	（1）介质管理制度中对介质安全传输有明确规定； ■包括人员选择 ■包括打包要求 ■包括交付要求 （2）存储重要信息的介质在物理传输过程，具备严格的环节控制，无重大环节疏漏； （3）对介质的归档和查询均具备记录； （4）制度详见：《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。	符合
设备维护管理	a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	（1）单位人员岗位职责相关文档已明确设备维护管理的责任部门； （2）单位对各类设施、设备进行定期维护； （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。	符合
	b）应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。	（1）单位建立了配套设施、软硬件维护管理方面的管理制度； ■包括维护人员的责任 ■包括维修和服务的审批 ■包括维修过程的监督控制 （2）单位开展相关工作与制度相符，且保留记录； ■包括维修和服务审批 ■包括维修过程记录 （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。	符合
漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。	（1）单位制定管理制度，规范对安全漏洞和隐患的检测、识别及评估修补要求； （2）制度详见：《恶意代码防范管理制度》； （3）单位未严格按规范开展漏洞及安全隐患检测工作。 ■未定期开展漏洞扫描	不符合
网络和系统安全管理	a）应划分不同的管理员角色进行网络和系统的运维	（1）单位建立系统安全管理文档，对系统管理员的管理制定了要求；	符合

安全控制点	测评指标	结果结论	符合程度
	管理，明确各个角色的责任和权限；	■包括角色划分 ■包括角色的责任 ■包括角色权限 （2）单位对各类关键角色建立了相应的工作职责文档； ■包括安全管理员 ■包括网络管理员 ■包括系统管理员 ■包括数据管理员 ■包括审计管理员 （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	
	b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	（1）单位制定管理制度，对系统账号进行管理； ■指定专人 ■包括申请账户管理 ■包括建立账户管理 ■包括删除账户管理 （2）单位按管理规范开展账号管理工作； ■具备相关审批流程 ■具备相关审批记录 ■具备管理登记记录 （3）账户管理记录内容较完整； ■包括变更日期 ■包括变更时间 ■包括变更人 ■包括变更设备/系统 ■包括变更结果 （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	符合
	c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	（1）单位建立了网络和系统安全管理制度； （2）网络和系统安全管理制度内容较全面； ■包括安全策略要求 ■包括账户管理 ■包括配置文件的生成及备份 ■包括变更审批管理 ■包括授权访问 ■包括最小服务控制 ■包括升级与打补丁管理 ■包括审计日志管理 ■包括口令管理 （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	符合

安全控制点	测评指标	结果结论	符合程度
	d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；	（1）单位对重要设备、系统的配置和操作建立配置手册； ■包括操作系统 ■包括数据库 ■包括网络设备 ■包括安全设备 ■包括应用和组件 （2）现有操作配置手册已明确操作步骤、参数配置； （3）制度详见：《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。	符合
	e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。	（1）单位制定日常运维管理的相关制度规范； （2）单位按制度规范开展日常运维管理工作； （3）单位具备合规的运维记录； ■包括日常巡检记录 ■包括运行维护记录 ■包括参数的设置记录 ■包括参数的修改记录 （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》、《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。	符合
恶意代码防范管理	a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	（1）单位制定恶意代码防范管理制度，明确对外来计算机或存储设备接入系统前进行恶意代码检查； （2）单位按外来计算机接入恶意代码检查规范开展工作； ■对外来计算机接入进行恶意代码检查 ■具备合规的检测记录 （3）单位制定培训管理制度，明确需通过培训提升员工的防恶意代码意识； （4）单位按培训管理要求开展工作； ■定期对员工开展防恶意代码意识培训 ■具备合规的培训记录 （5）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申请表》、《信息管理系统漏洞检查表》。	符合
	b) 应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；	（1）建立恶意代码防范管理文档； （2）管理制度中覆盖防恶意代码软件的授权使用、恶意代码库升级、定期查杀等内容； （3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》。	符合
	c) 应定期检查恶意代码库	（1）单位指定专门的部门负责定期验证防范	部分符合

安全控制点	测评指标	结果结论	符合程度
	的升级情况，对截获的恶意代码进行及时分析处理。	恶意代码攻击的技术措施的有效性； （2）单位近期未发生过严重的恶意代码攻击事件； （3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申请表》、《信息管理系统漏洞检查表》； （4）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。 ■未定期对相关产品的恶意代码库进行升级 ■未对所有防病毒产品上截获的恶意代码进行分析并汇总上报	
配置管理	应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。	（1）单位制定了基本配置信息管理的制度要求； ■包括网络拓扑结构 ■包括设备安装的软件组件 ■包括软件组件的版本 （2）管理文件详见：《主机安全管理规范》、《网络安全管理规范》、《应用安全管理规范》、《网络配置信息》。	符合
密码管理	a）应遵循密码相关国家标准和行业标准；	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	不符合
	b）应使用国家密码管理主管部门认证核准的密码技术和产品。	（1）单位未采购涉及密码技术的产品，不适用。	不适用
变更管理	应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。	（1）单位建立了关于系统变更管理的制度文件； （2）现有变更管理制度覆盖了变更管理的各方面要求； ■包括变更管理要求 ■包括整体变更管理流程 ■包括变更内容分析与论证 ■包括变更方案审批流程 ■包括变更后通报 （3）制度详见：《变更控制管理制度》、《通用变更记录表》。	符合
备份与恢复管理	a）应识别需要定期备份的重要业务信息、系统数据及软件系统等；	（1）单位根据业务重要程度，制定了需要定期备份的重要业务信息列表或清单。清单内需要定期备份的重要数据已经过用户方确认； （2）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管	符合

安全控制点	测评指标	结果结论	符合程度
		理规范》。	
	b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等；	（1）单位建立了备份与恢复管理相关的安全管理制度； （2）备份与恢复管理的相关要求比较明确； ■规定备份方式 ■规定备份频度 ■规定存储介质 ■规定保存期 （3）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。	符合
	c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	（1）单位现有管理制度，明确了数据备份策略和数据恢复策略，以及备份程序和恢复程序； （2）单位可按策略要求实现重要数据的定期备份与恢复性测试； （3）单位现有的备份的数据均经过恢复性测试，可确保备份的数据可用； （4）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。	符合
安全事件处置	a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件；	（1）单位已在安全培训及宣传过程中告知用户在发现安全弱点和可疑事件时及时向安全管理部门报告； （2）单位在系统运维过程中对发现的安全弱点和可疑事件均编制了对应的报告或相关文档； （3）单位现有安全弱点和可疑事件报告文档内容较详实； （4）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	符合
	b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；	（1）单位制定了安全事件报告和处置管理制度； （2）现有安全事件管理制度内容较完整； ■包括安全事件类型分类 ■包括安全事件有关的工作职责 ■包括安全事件的报告 ■包括安全事件的处置 ■包括安全事件的响应流程 （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	符合

安全控制点	测评指标	结果结论	符合程度
	c) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。	（1）单位具备对安全事件的分析、处理、总结、防范等的报告／过程文档； （2）单位提供的安全事件报告和响应处置记录内容较完整； ■记录引发安全事件的原因 ■记录事件的证据 ■记录处置过程 ■包括经验教训 ■提出补救措施 （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	符合
应急预案管理	a) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；	（1）单位制定重要事件的应急预案； （2）单位现有应急预案涉及的类型范围较全面； ■包括针对机房的预案 ■包括针对网络传输的预案 ■包括针对网络设备的预案 ■包括针对操作系统的预案 ■包括针对数据库的预案 ■包括针对安全漏洞攻击的预案 ■包括针对恶意代码的预案 ■包括针对数据泄露的预案 （3）单位现有应急预案的内容较完整； ■明确重要事件的应急处理流程 ■明确系统恢复流程等内容 （4）制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。	符合
	b) 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。	(1)单位定期对相关人员进行应急预案培训； （2）单位根据不同的应急预案，按要求进行应急演练； （3）单位具备近期应急预案工作开展的相关记录； ■具备培训记录 ■具备演练记录 (4)单位提供的应急预案培训记录比较完整； ■明确培训对象 ■明确培训内容 ■明确培训结果 (5)单位提供的应急预案演练记录比较完整； ■记录演练时间 ■记录主要操作内容 ■记录演练结果 （6）经检查单位目前一旦出现应急事件，可	符合

安全控制点	测评指标	结果结论	符合程度
		参照预案合理有序的进行应急事件处置过程；(7) 制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。	
外包运维管理	a) 应确保外包运维服务商的选择符合国家的有关规定；	(1)单位目前未涉及任何外包运维服务情况，不适用。	不适用
	b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。	(1)单位目前未涉及任何外包运维服务情况，不适用。	不适用

D.11 其他安全要求

本次测评不涉及其他安全要求指标。

附录E 漏洞扫描结果记录

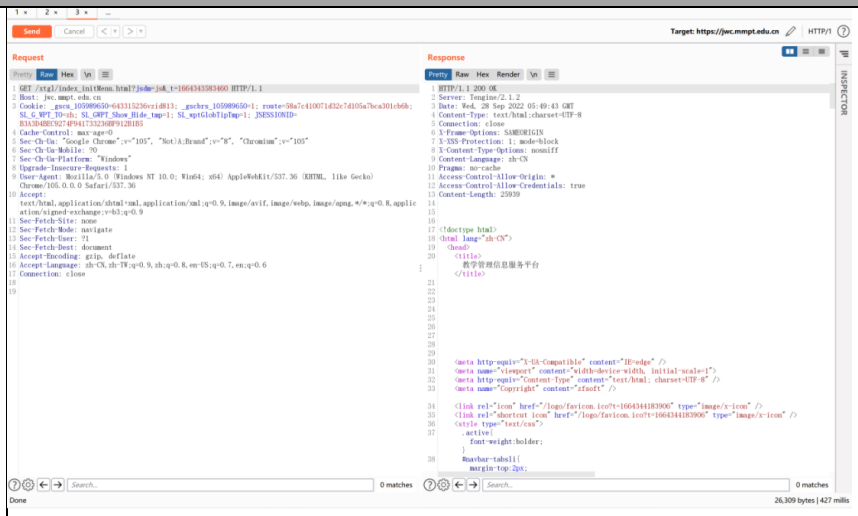
附录E表-1漏洞扫描主要安全漏洞

序号	危险程度	漏洞名称	影响IP
1	低	允许Traceroute探测 此类漏洞涉及网络设备、安全设备、服务器存储设备。	10.2.2.16/数据库服务器 10.2.2.17/应用服务器-1 10.2.2.18/应用服务器-2 10.2.1.4/运维安全管理系统 10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/上网行为管理系统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/汇聚交换机 172.16.1.2/核心交换机
2	低	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161) 此类漏洞涉及网络设备。	172.16.1.2/核心交换机

附录F 渗透测试结果记录

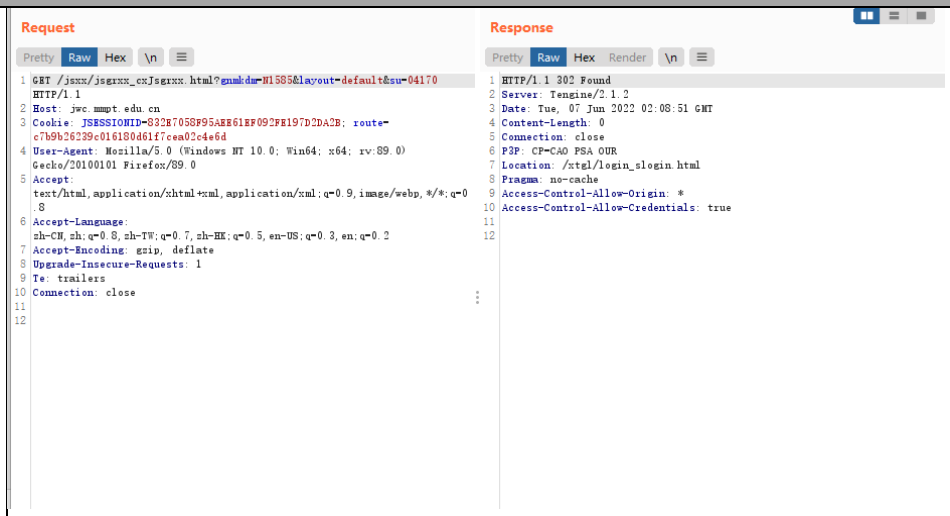
F.1 业务应用软件平台 缺少“Content-Security-Policy”响应头

缺少“Content-Security-Policy”响应头	
危险程度	低
渗透位置	JB,JC
影响URL实体	https://jwc.mmpt.edu.cn/xtgl/index_initMenu.html?jsdm=js&_t=1664343583460
渗透详情	渗透方法：使用burp suite进行抓包检测 采用的工具：Burp suite 测试过程：使用BurpSuite抓包查看响应头未包含Content-Security-Policy字段

缺少“Content-Security-Policy”响应头


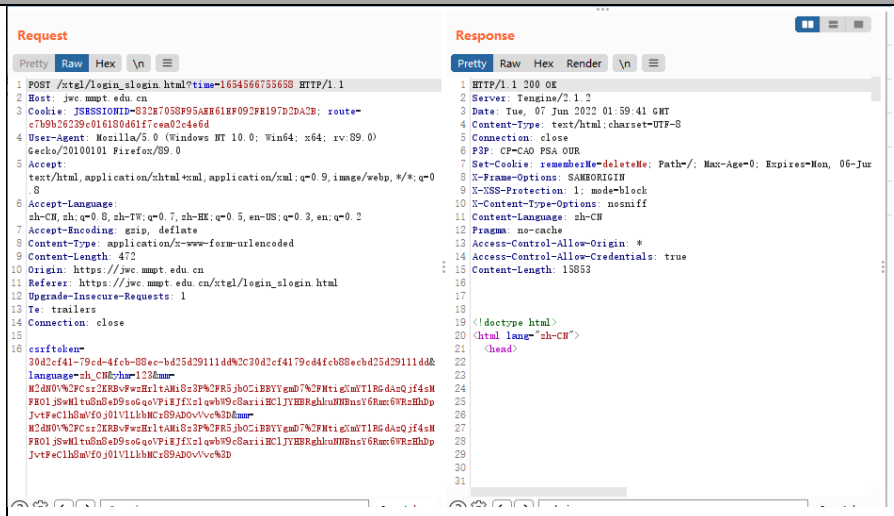
F.2 业务应用软件平台 未授权访问

未授权访问	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：在未登录的情况下无法访问用户管理信息。 采用的工具：BurpSuite 测试过程：在未登录的情况下无法访问用户管理信息。 

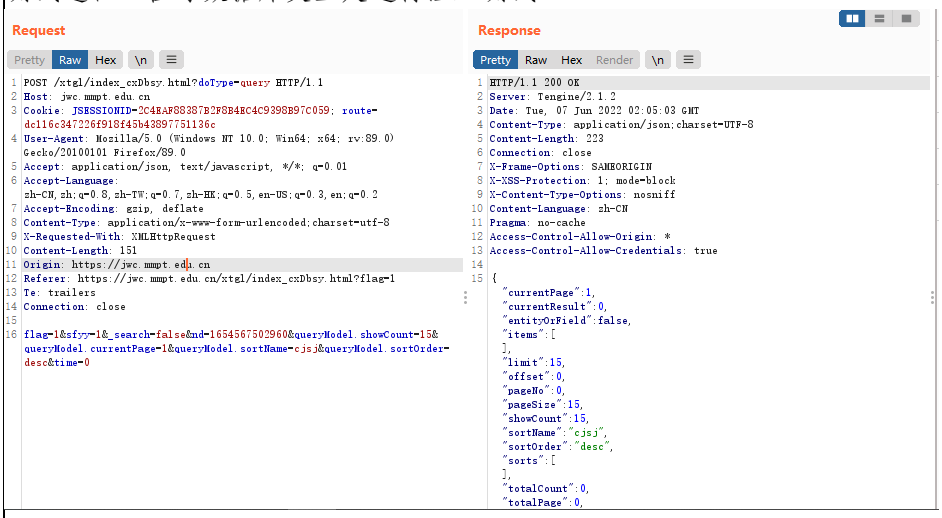
未授权访问	
	

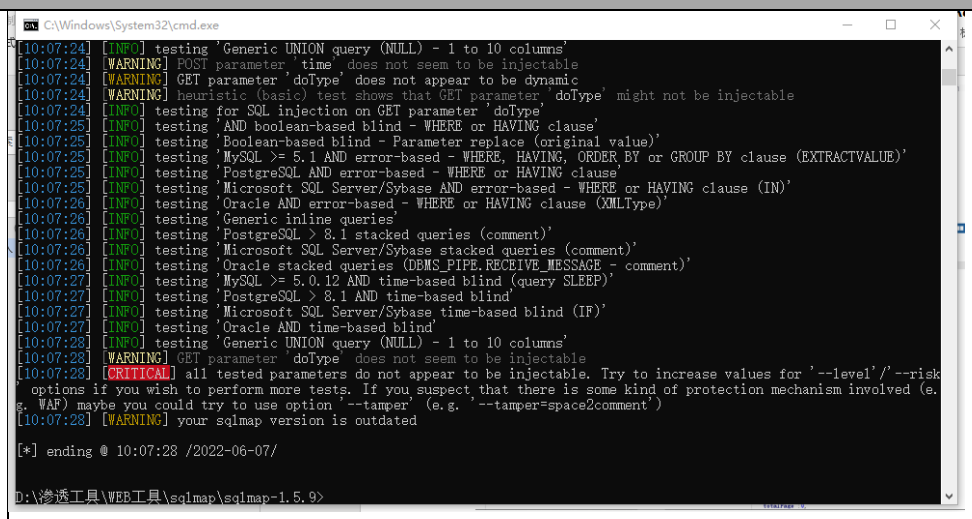
F.3 业务应用软件平台　已解密的登录请求

已解密的登录请求	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：测试是否所有登录请求都以加密方式发送到服务器 采用的工具：Burpsuite 测试过程：模拟登录请求，发现口令加密传输 

已解密的登录请求	
	

F.4 业务应用软件平台　　SQL注入漏洞

SQL注入漏洞	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：通过手工或工具检测系统在执行SQL语句时是否存在注入 采用的工具：Burpsuite、Sqlmap 测试过程：在与数据库交互处进行注入测试 

SQL注入漏洞


附录G 威胁列表

附录G 表- 1威胁列表

序号	威胁列表	描述
1	恶意攻击	利用工具和技术对信息系统进行攻击和入侵。威胁行为包括：恶意代码、邮件勒索、网络攻击等。
2	软硬件故障	对业务实施或系统运行产生影响的设备硬件故障、通讯链路中断、系统本身或软件缺陷造等问题。威胁行为包括：设备故障、软件故障等。
3	管理不到位	由于制度缺失、不完善等原因导致安全管理无法落实或者不到位。威胁行为包括：管理不到位、媒体负面报道等。
4	无作为或操作失误	应该执行而没有执行相应的操作，或者无意执行了错误的操作。威胁行为包括：操作失误、维护错误等。
5	敏感信息泄漏	敏感信息泄露给不应了解的他人。威胁行为包括：内部信息泄露、外部信息泄露等。
6	物理环境影响	对信息系统正常运行造成影响的物理环境问题和自然灾害。威胁行为包括：物理损害等。
7	越权或滥用	越权访问本来无权访问的资源，或者滥用自己的权限破坏信息系统。威胁行为包括：未授权的设备使用、权限滥用、权限伪造等。
8	物理攻击	通过物理的接触造成对软件、硬件和数据的破坏。威胁行为包括：设备失效等。
9	篡改	非法修改信息，破坏信息的完整性使系统的安全性降低或信息不可用。威胁行为包括：硬件篡改、数据篡改等。
10	抵赖	否认所做的操作。威胁行为包括：行为否认（抵赖）、媒体负面报道等。

报告编号：44090243008-00005-22-0163-01

网络安全等级保护
科研创新信息化管理系统等级测评报告

委托单位：茂名职业技术学院

测评单位：广东南方信息安全研究院

报告时间：2022年10月30日

网络安全等级测评基本信息表

被测对象				
被测对象名称	科研创新信息化管理系统		安全保护等级	第二级（S2A2）
备案证明编号	44090243008-00005			
被测单位				
单位名称	茂名职业技术学院			
单位地址	广东省茂名市茂南区文明北路232号大院		邮政编码	525000
联系人	姓名	龙恒	职务/职称	教师
	所属部门	教育信息与网络中心	办公电话	0668-2920122
	移动电话	13377766618	电子邮件	372383968@qq.com
测评单位				
单位名称	广东南方信息安全研究院		机构代码	SC202127130010163
单位地址	广州市科学城彩频路9号B座12楼1202		邮政编码	510663
联系人	姓名	谢若雨	职务/职称	助理
	所属部门	办公室	办公电话	020-32290702
	移动电话	18819149895	电子邮件	office@cybersec-gd.cn
审核批准	编制人	林炳良	编制日期	2022.10.30
	审核人	李	审核日期	2022.10.30
	批准人	陈林彩	批准日期	2022.10.30

声明

本报告是科研创新信息化管理系统的等级测评报告。

本报告测评结论的有效性建立在被测评单位提供相关证据的真实性基础之上。

本报告中给出的测评结论仅对被测对象当时的安全状态有效。当测评工作完成后，由于被测对象发生变更而涉及到的系统构成组件（或子系统）本报告不再适用。

本报告中给出的测评结论不能作为对被测对象内部部署的相关系统构成组件（或产品）的测评结论。

在任何情况下，若需引用本报告中的测评结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。

单位名称：广东南方信息安全研究院

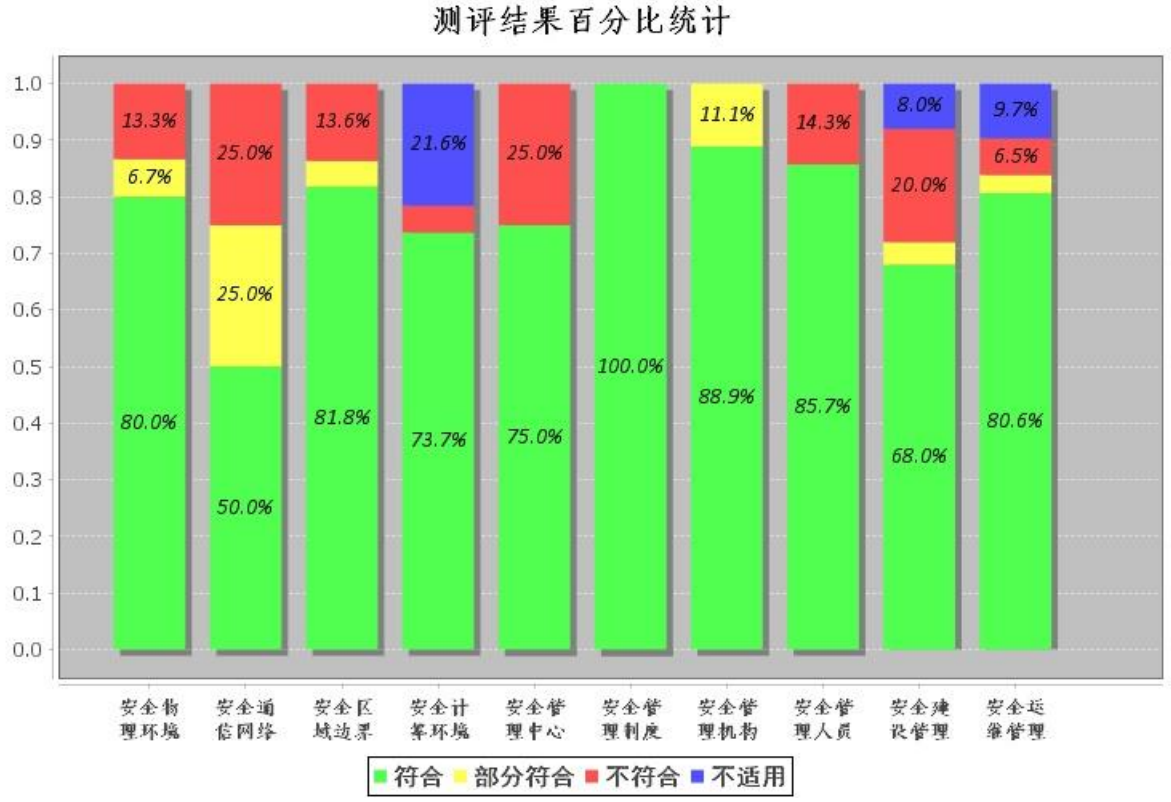
2022年10月30日

等级测评结论

测评结论和综合得分			
被测对象名称	科研创新信息化管理系统	安全保护等级	第二级（S2A2）
扩展要求应用情况	□云计算 □移动互联 □物联网 □工业控制系统 □大数据		
被测对象描述	科研创新信息化管理系统是由茂名职业技术学院统一组织规划建设，由北京易普拉格科技股份有限公司负责开发，于2019年11月正式投入运行，由教育信息与网络中心负责运行维护。茂名职业技术学院是该信息系统的业务主管部门，茂名职业技术学院为该信息系统定级的责任单位。 科研创新信息化管理系统网络主要分为4个区域，分别为外网边界区域、安全管理区域、服务器存储区域、办公网区域，主要由网络设备、安全设备组成，对互联网提供业务访问。科研创新信息化管理系统为B/S结构，主要由Windows平台的操作系统，MSSQL平台的数据库系统，及Tomcat中间件系统组成。单位采用自主运维模式，通过部署运维及管理终端提供专用运维环境管理，采用运维安全管理系统实现设备的统一管理，并进行操作运维审计，日志审计系统进行设备日志统一收集存储与分析。 科研创新信息化管理系统用于科研管理信息化建设，系统主要功能包括项目管理，经费管理，论文、著作、专利、艺术作品等成果管理，科研人员，科研机构管理。根据学校科教研管理的分工，提供不同的解决方案，让科研管理变得更简单。		
安全状况描述	科研创新信息化管理系统通信传输具备一定的保护措施，安全区域边界较清晰，网络层具备访问控制、安全审计的相应技术措施。各设备在身份鉴别、访问控制、安全审计、入侵防范方面具备控制措施。重要数据在数据完整性、个人信息保护方面具备保护措施。在安全管理制度层面较为完善。在网络架构不够完整，网络层在入侵防范、恶意代码和垃圾邮件防范的技术措施存在不足。重要数据在数据备份恢复方面存在不足。 科研创新信息化管理系统在本次测评中总共出现25类问题，其中0类高风险问题,10类中风险问题，15类低风险问题。在本次测评通过扫描及渗透发现3类漏洞问题，其中0类危险程度为高的漏洞，0类危险程度为中的漏洞，3类危险程度为低的漏洞。 科研创新信息化管理系统本次等级测评的综合得分为73.85，且不存在高等级安全风险，等级测评结论为中。		
等级测评结论	中	综合得分	73.85

总体评价

通过对信息系统基本安全保护状态的分析，茂名职业技术学院针对科研创新信息化管理系统面临的主要安全威胁采取了相应的安全机制，基本达到保护信息系统重要资产的作用。科研创新信息化管理系统在本次测评中采用了GB/T 22239-2019，其中安全通用要求135项，不适用5项。



在安全物理环境方面，针对安全通用要求，基础设施在防雷击、电磁防护、防水和防潮、物理位置选择、电力供应、防盗窃和防破坏、温湿度控制等方面较为完善（如：信息化机房）。在物理访问控制、防静电等方面还不够完善（如：信息化机房），机房出入口未配置电子门禁系统，机房内缺乏防静电措施（如防静电地板或铺设防静电地毯）。

在安全通信网络方面,针对安全通用要求,网络环境在通信传输等方面较为完善(如:安全通信网络）。在网络架构等方面还不够完善（如：安全通信网络），关键的应用服务和数据库服务网段未独立进行子网划分的情况。

在安全区域边界方面，针对安全通用要求，网络环境在边界防护、安全审计、访问控制等方面较为完善（如：外网边界区域，安全管理区域，服务器存储区域等）。在入侵防范、恶意代码和垃圾邮件防范等方面还不够完善(如:安全管理区域,办公网区域),网络层部署防火墙,防火墙未配置对内部发起的攻击行为实现防范功能策略,无法检测、防止或限制从内部发起的网络攻击行为,现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。

在安全计算环境方面，针对安全通用要求，计算环境在个人信息保护、安全审计、数据完整性、访问控制、入侵防范、恶意代码防范、身份鉴别、剩余信息保护等方面较为完善。在主机方面，在可信验证等方面还不够完善（如：业务终端-2，业务终端-1，应用/数据库服务器等），缺乏对计算设备可信验证方面的安全设计要求，现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。在应用方面，在数据备份恢复等方面还不够完善（如：应用/数据库服务器-MSSQL），未能提供数据库系统重要数据的异地定时数据备份功能。在网络及安全设备方面,在可信验证等方面还不够完善(如:基线核查系统，上网行为管理系统，WEB应用防火墙等），设备不具备相关可信验证的技术措施。在数据保护方面,在数据备份恢复等方面还不够完善(如:重要个人信息,重要业务数据），未能提供应用软件系统重要数据的异地定时数据备份功能。

在安全管理中心方面，针对安全通用要求，安全控制措施在审计管理等方面较为完善（如：管理中心）。在系统管理等方面还不够完善（如：管理中心），系统管理的资源、运行及配置管理不够全面。

在安全管理制度方面,针对安全通用要求,管理制度体系在制定和发布、安全策略、管理制度、评审和修订等方面较为完善（如：制度文件、执行/记录文件）。

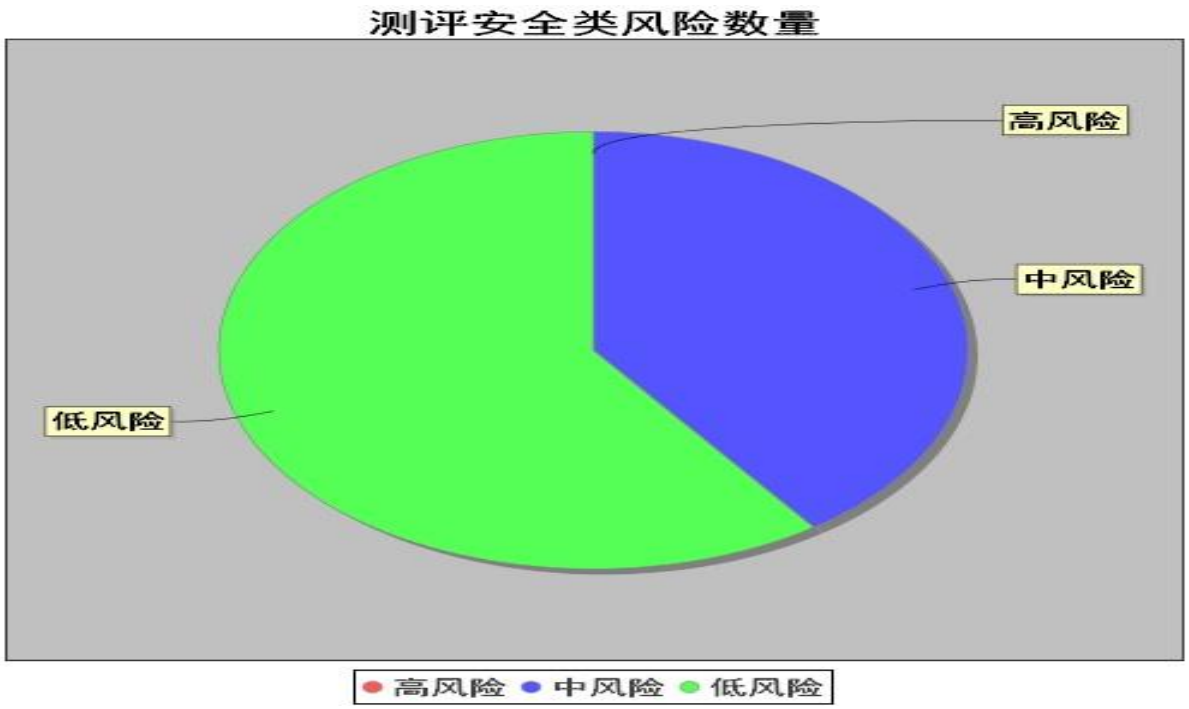
在安全管理机构方面，针对安全通用要求，机构建设在人员配备、沟通和合作、授权和审批、岗位设置等方面较为完善（如：制度文件、执行/记录文件）。在审核和检查等方面还不够完善（如：制度文件、执行/记录文件），单位开展的检查工作不够完善。

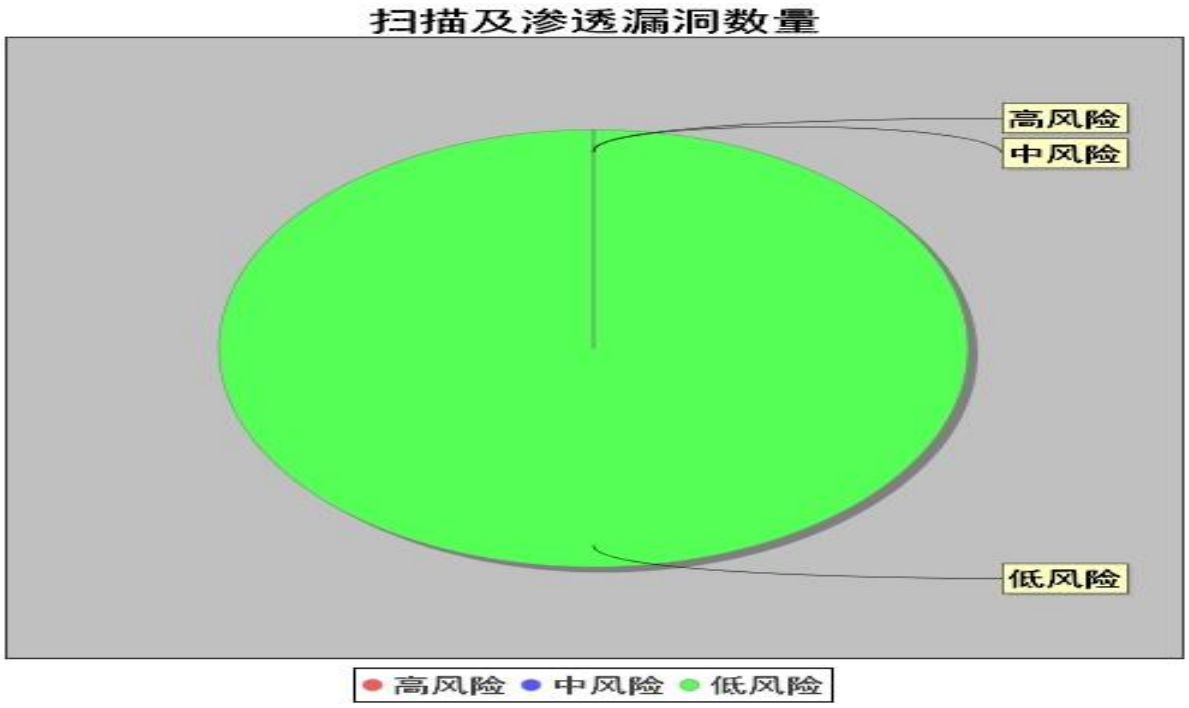
在安全管理人员方面,针对安全通用要求,人员在人员录用、安全意识教育和培训、人员离岗等方面较为完善（如：制度文件、执行/记录文件）。在外部人员访问管理等方面还不够完善（如：制度文件、执行/记录文件），单位未完全按管理规范开展人员离场后的清理工作。

在安全建设管理方面，针对安全通用要求，系统建设在定级和备案、工程实施、等级测评、产品采购和使用、服务供应商选择、系统交付等方面较为完善(如:制度文件、执行/记录文件)。在安全方案设计等方面还不够完善(如:制度文件、执行/记录文件)，单位未具备完整的安全设计方案相关的文档，单位相关方案的设计的内容不够完善。

在安全运维管理方面，针对安全通用要求，系统运维在介质管理、设备维护管理、网络和系统安全管理、备份与恢复管理、资产管理、应急预案管理、环境管理、配置管理、安全事件处置、变更管理等方面较为完善（如：制度文件、执行/记录文件）。在密码管理等方面还不够完善（如：制度文件、执行/记录文件），单位不了解现有密码相关的国家标准和行业标准，单位缺乏密码管理要求的制度文档。

科研创新信息化管理系统在本次测评中总共出现25类问题，其中0类高风险问题,10类中风险问题，15类低风险问题。在本次测评通过扫描及渗透发现3类漏洞问题，其中0类危险程度为高的漏洞，0类危险程度为中的漏洞，3类危险程度为低的漏洞。





科研创新信息化管理系统本次等级测评的综合得分为73.85，且不存在高等级安全风险，等级测评结论为中。

主要安全问题及整改建议

一、安全物理环境

安全通用要求

(1)中风险 机房出入口未配置电子门禁系统（如：信息化机房）。 上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域,可能对系统的平稳运行造成影响。

建议安排专人7*24小时负责机房出入，对出入的人员进行身份鉴别和登记，且出入有专人陪同或在机房出入口配置电子门禁系统，控制、鉴别和记录进入的人员。

(2)中风险 机房内缺乏防静电措施（如防静电地板或铺设防静电地毯 ）（如：信息化机房）。 存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。

建议采用防静电地板或地面并采用必要的接地防静电措施。

二、安全通信网络

安全通用要求

(1)中风险 关键的应用服务和数据库服务网段未独立进行子网划分的情况（如：安全通信网络）。 上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变得更为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。

建议独立划分出应用服务器网段、数据库服务器网段。

三、安全区域边界

安全通用要求

(1)中风险 网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为（如：办公网区域）。 存在不

能及时发现内部主机作为攻击跳板，或网络攻击行为而造成系统损坏/网络资源浪费的风险。

建议网络层部署的防火墙配置对内部发起的攻击行为实现防范功能策略，实现检测、防止或限制从内部发起的网络攻击行为。

(2)中风险 现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面（如：办公网区域）。 无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。

建议现有部署的恶意代码防范措施网络边界覆盖全面，及时对恶意代码及逆行检测和清除。

四、安全计算环境

1、网络设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

2、安全设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

3、服务器和终端

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

4、系统管理软件/平台

安全通用要求

(1)中风险 未能提供数据库系统重要数据的异地定时数据备份功能（如：应用/数据库

服务器-MSSQL）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供，使企业的经济利益或声誉受到损害。

建议数据库系统利用通信网络将关键数据定时批量传送至备用场地，实现异地数据异地备份。

5、业务应用系统/平台

安全通用要求

(1)中风险 未能提供应用软件系统重要数据的异地定时数据备份功能（如：科研创新信息化管理系统）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。

建议设置异地灾备机房，并利用通信网络将应用软件系统重要数据定时备份至备份场地。

6、数据资源

安全通用要求

重要业务数据

(1)中风险 未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要业务数据）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。

建议利用通信网络将应用软件系统关键数据定时批量传送至备用场地，实现异地数据异地备份。

重要个人信息

(1)中风险 未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要个人信息）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会

影响到业务服务的持续提供。

建议利用通信网络将应用软件系统关键数据定时批量传送至备用场地，实现异地数据异地备份。

7、其他系统或设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

五、安全管理中心

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

六、安全管理制度

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

七、安全管理机构

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

八、安全管理人员

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

九、安全建设管理

安全通用要求

(1)中风险 单位未具备完整的安全设计方案相关的文档。单位相关方案的设计的内容不够完善（如：制度文件、执行/记录文件）。 相关合规的规划配套文件缺失，可能导

致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。

建议根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件。

十、安全运维管理

安全通用要求

(1)中风险 **单位不了解现有密码相关的国家标准和行业标准。单位缺乏密码管理要求的制度文档（如：制度文件、执行/记录文件）。 密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不到位，存在违反国家政策的风险。**

建议单位学习现有密码相关的国家标准和行业标准。建立密码管理要求的制度文档。

目录

网络安全等级测评基本信息表 I
声明 II
等级测评结论 III
总体评价 IV
主要安全问题及整改建议 VIII
一、安全物理环境 VIII
安全通用要求 VIII
二、安全通信网络 VIII
安全通用要求 VIII
三、安全区域边界 VIII
安全通用要求 VIII
四、安全计算环境 IX
1、网络设备 IX
安全通用要求 IX
2、安全设备 IX
安全通用要求 IX
3、服务器和终端 IX
安全通用要求 IX
4、系统管理软件/平台 IX
安全通用要求 IX
5、业务应用系统/平台 X
安全通用要求 X
6、数据资源 X
安全通用要求 X
7、其他系统或设备 XI
安全通用要求 XI
五、安全管理中心 XI
安全通用要求 XI
六、安全管理制度 XI
安全通用要求 XI
七、安全管理机构 XI
安全通用要求 XI
八、安全管理人员 XI
安全通用要求 XI
九、安全建设管理 XI
安全通用要求 XI
十、安全运维管理 XII
安全通用要求 XII

目录.....XIII
1 测评项目概述.....1
1.1 测评目的.....1
1.2 测评依据.....1
1.3 测评过程.....2
1.4 报告分发范围.....5
2 被测对象描述.....5
2.1 被测对象概述.....5
2.1.1 定级结果.....5
2.1.2 业务和采用的技术.....5
2.1.3 网络结构.....5
2.2 测评指标.....7
2.2.1 安全通用要求指标.....7
2.2.2 安全扩展要求指标.....9
2.2.3 其他安全要求指标.....10
2.2.4 不适用安全要求指标.....10
2.3 测评对象.....10
2.3.1 测评对象选择方法.....10
2.3.2 测评对象选择结果.....11
2.3.2.1 物理机房.....12
2.3.2.2 网络设备.....12
2.3.2.3 安全设备.....12
2.3.2.4 服务器.....13
2.3.2.5 终端设备.....13
2.3.2.6 其他系统或设备.....13
2.3.2.7 系统管理软件/平台.....14
2.3.2.8 业务应用软件/平台.....14
2.3.2.9 数据资源.....15
2.3.2.10 安全相关人员.....15
2.3.2.11 安全管理文档.....16
3 单项测评结果分析.....21
3.1 安全物理环境.....21
3.1.1 已有安全控制措施汇总分析.....21
3.1.2 主要安全问题汇总分析.....22
3.2 安全通信网络.....23
3.2.1 已有安全控制措施汇总分析.....23
3.2.2 主要安全问题汇总分析.....23
3.3 安全区域边界.....24
3.3.1 已有安全控制措施汇总分析.....24
3.3.2 主要安全问题汇总分析.....25
3.4 安全计算环境.....26
3.4.1 网络设备.....26

3.4.1.1 已有安全控制措施汇总分析 26
3.4.1.2 主要安全问题汇总分析 28
3.4.2 安全设备 28
3.4.2.1 已有安全控制措施汇总分析 28
3.4.2.2 主要安全问题汇总分析 32
3.4.3 服务器和终端 32
3.4.3.1 已有安全控制措施汇总分析 32
3.4.3.2 主要安全问题汇总分析 35
3.4.4 系统管理软件/平台 36
3.4.4.1 已有安全控制措施汇总分析 36
3.4.4.2 主要安全问题汇总分析 39
3.4.5 业务应用系统/平台 39
3.4.5.1 已有安全控制措施汇总分析 39
3.4.5.2 主要安全问题汇总分析 41
3.4.6 数据资源 42
3.4.6.1 已有安全控制措施汇总分析 42
3.4.6.2 主要安全问题汇总分析 42
3.4.7 其他系统或设备 43
3.4.7.1 已有安全控制措施汇总分析 43
3.4.7.2 主要安全问题汇总分析 43
3.5 安全管理中心 43
3.5.1 已有安全控制措施汇总分析 43
3.5.2 主要安全问题汇总分析 44
3.6 安全管理制度 44
3.6.1 已有安全控制措施汇总分析 44
3.6.2 主要安全问题汇总分析 45
3.7 安全管理机构 46
3.7.1 已有安全控制措施汇总分析 46
3.7.2 主要安全问题汇总分析 47
3.8 安全管理人员 47
3.8.1 已有安全控制措施汇总分析 47
3.8.2 主要安全问题汇总分析 48
3.9 安全建设管理 49
3.9.1 已有安全控制措施汇总分析 49
3.9.2 主要安全问题汇总分析 51
3.10 安全运维管理 52
3.10.1 已有安全控制措施汇总分析 52
3.10.2 主要安全问题汇总分析 56
3.11 其他安全要求指标 56
3.11.1 已有安全控制措施汇总分析 56
3.11.2 主要安全问题汇总分析 56
3.12 验证测试 57
3.12.1 漏洞扫描 57
3.12.1.1 漏洞扫描结果统计 57

3.12.1.2 漏洞扫描问题描述 61
3.12.2 渗透测试 62
3.12.2.1 渗透测试过程说明 62
3.12.2.2 渗透测试问题描述 64
3.13 单项测评小结 64
3.13.1 控制点符合情况汇总 64
3.13.2 安全问题汇总 68
4 整体测评 71
4.1 安全控制点间安全测评 71
4.1.1 安全建设管理 72
4.1.1.1 安全通用要求 72
4.1.2 安全运维管理 72
4.1.2.1 安全通用要求 72
4.2 区域间安全测评 73
4.2.1 安全物理环境 73
4.2.1.1 安全通用要求 73
4.2.2 安全通信网络 73
4.2.2.1 安全通用要求 73
4.2.3 安全区域边界 73
4.2.3.1 安全通用要求 74
4.3 整体测评结果汇总 74
5 安全问题风险分析 76
6 等级测评结论 80
7 安全问题整改建议 82
附录A 被测对象资产 88
A.1 物理机房 88
A.2 网络设备 88
A.3 安全设备 88
A.4 服务器 89
A.5 终端设备 89
A.6 其他系统或设备 89
A.7 系统管理软件/平台 89
A.8 业务应用软件/平台 90
A.9 数据资源 90
A.10 密码产品 91
A.11 安全相关人员 91
A.12 安全管理文档 91
附录B 上次测评问题整改情况说明 96
附录C 单项测评结果汇总 97
C.1 安全物理环境 97

C.2 安全通信网络.....97
C.3 安全区域边界.....97
C.4 安全计算环境.....98
C.4.1 网络设备.....98
C.4.2 安全设备.....99
C.4.3 服务器和终端.....100
C.4.4 系统管理软件/平台.....100
C.4.5 业务应用系统/平台.....101
C.4.6 数据资源.....101
C.4.7 其他系统或设备.....102
C.5 安全管理中心.....102
C.6 安全管理制度.....102
C.7 安全管理机构.....103
C.8 安全管理人员.....103
C.9 安全建设管理.....103
C.10 安全运维管理.....103
C.11 其他安全要求指标.....104
附录D 单项测评结果记录.....104
D.1 安全物理环境.....104
D.1.1 安全通用要求.....104
D.1.1.1 信息化机房.....104
D.2 安全通信网络.....107
D.2.1 安全通用要求.....107
D.2.1.1 安全通信网络.....107
D.3 安全区域边界.....107
D.3.1 安全通用要求.....107
D.3.1.1 办公网区域.....107
D.3.1.2 外网边界区域.....110
D.3.1.3 安全管理区域.....112
D.3.1.4 服务器存储区域.....114
D.4 安全计算环境.....117
D.4.1 安全通用要求.....117
D.4.1.1 网络设备.....117
D.4.1.2 安全设备.....124
D.4.1.3 服务器和终端.....148
D.4.1.4 系统管理软件/平台.....170
D.4.1.5 业务应用系统/平台.....178
D.4.1.6 数据资源.....181
D.4.1.7 其他系统或设备.....189
D.5 安全管理中心.....189
D.5.1 安全通用要求.....189
D.5.1.1 管理中心.....189
D.6 安全管理制度.....190
D.6.1 安全通用要求.....190

D.6.1.1 制度文件、执行/记录文件 190
D.7 安全管理机构 192
D.7.1 安全通用要求 192
D.7.1.1 制度文件、执行/记录文件 192
D.8 安全管理人员 195
D.8.1 安全通用要求 195
D.8.1.1 制度文件、执行/记录文件 195
D.9 安全建设管理 197
D.9.1 安全通用要求 197
D.9.1.1 制度文件、执行/记录文件 197
D.10 安全运维管理 201
D.10.1 安全通用要求 201
D.10.1.1 制度文件、执行/记录文件 201
D.11 其他安全要求 209
附录E 漏洞扫描结果记录 209
附录F 渗透测试结果记录 209
附录G 威胁列表 211

1 测评项目概述

1.1 测评目的

安全等级测评的目标是通过对目标系统在安全技术及管理方面的测评,对目标系统的安全技术状态及安全管理状况做出初步判断,给出目标系统在安全技术及安全管理方面与其相应安全等级保护要求之间的差距。测评结论作为委托方进一步完善系统安全策略及安全技术防护措施依据。

项目背景是为进一步提高信息系统的保障能力,根据《信息安全等级保护管理办法》（公通字2007【43】号）的精神，茂名职业技术学院委托广东南方信息安全研究院（SC202127130010163）对科研创新信息化管理系统实施等级测评，以期发现信息系统和等级保护标准的差距以及存在的安全隐患，为后续的安全整改工作提供参考依据。

1.2 测评依据

测评过程中主要依据的标准:

测评标准

（1）GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》

（2）GB/T 28448-2019 《信息安全技术 网络安全等级保护测评要求》

测评参考标准

（1）GB 17859-1999 《计算机信息系统 安全保护等级划分准则》

（2）GB/T 28449-2018 《信息安全技术 网络安全等级保护测评过程指南》

（3）GB/T 20984-2007 《信息安全技术 信息安全风险评估规范》

（4）GB/T 25058-2019 《信息安全技术 网络安全等级保护实施指南》

测评参考法律法规

（1）《中华人民共和国网络安全法》

（2）《中华人民共和国密码法》

（3）《中华人民共和国数据安全法》

1.3 测评过程

本次等级测评分为四个过程：测评准备活动、方案编制活动、测评实施活动、报告编制活动。具体如图 1-1 所示。其中，各阶段的时间安排如下：

⑴ 测评准备活动

测评准备活动的目标是顺利启动测评项目,收集定级对象相关资料,准备测评所需资料,为编制测评方案打下良好的基础。测评准备活动包括工作启动、信息收集和分析、工具和表单准备三项主要任务。

（2）方案编制活动

方案编制活动的目标是整理测评准备活动中获取的定级对象相关资料,为现场测评活动提供最基本的文档和指导方案。方案编制活动包括测评对象确定、测评指标确定、测评内容确定、工具测试方法确定、测评指导书开发及测评方案编制六项主要任务。

（3）现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调,为现场测评的顺利开展打下良好基础,依据测评方案实施现场测评工作,将测评方案和测评方法等内容具体落实到现场测评活动中。现场测评工作应取得报告编制活动所需的、足够的证据和资料。现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

（4）报告编制活动

在现场测评工作结束后,测评机构应对现场测评获得的测评结果(或称测评证据)进行汇总分析,形成等级测评结论,并编制测评报告。测评人员在初步判定单项测评结果后,还需进行单元测评结果判定、整体测评、系统安全保障评估,经过整体测评后,有的单项

测评结果可能会有所变化,需进一步修订单项测评结果,而后针对安全问题进行风险评估,形成等级测评结论。分析与报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、系统安全保障评估、安全问题风险评估、等级测评结论形成及测评报告编制七项主要任务。

各阶段完成的关键任务：

序号	阶段	任务	对象	开始日期	结束日期
1	测评准备活动	工作启动	项目甲乙双方	2022年8月15日	2022年8月19日
2		信息收集与分析	调研表	2022年8月22日	2022年8月25日
3		工具和表单准备	测评工具、测评授权书、文档交接单	2022年8月25日	2022年8月30日
4	方案编制活动	测评对象确认	测评方案-对象列表	2022年8月31日	2022年8月31日
5		测评指标确认	测评方案-指标列表	2022年8月31日	2022年8月31日
6		测评内容确认	测评方案-内容列表	2022年9月1日	2022年9月1日
7		工具测试方法确认	测评方案-工具测试方法列表	2022年9月1日	2022年9月1日
8		测评指导书开发	测评作业指导书	2022年9月2日	2022年9月2日
9		测评方案编制	测评方案	2022年9月5日	2022年9月5日
10	现场测评活动	现场测评准备	工具、人员、表单准备	2022年9月28日	2022年9月28日
11		现场测评和结果记录	安全管理访谈	2022年9月28日	2022年9月28日
12			安全管理文档检查	2022年9月28日	2022年9月28日
13			安全物理环境测评	2022年9月28日	2022年9月28日
14			安全通信网络	2022年9月28日	2022年9月29日
15			安全区域边界	2022年9月28日	2022年9月29日
16			安全计算环境	2022年9月28日	2022年9月29日
17			工具测试	2022年9月29日	2022年10月9日
18		结果确认和资料归还	检测人员出入场确认单、测评现场服务评价单	2022年10月8日	2022年10月9日
19	报告编制活动	单项测评结果	测评报告	2022年10月9日	2022年10月12日

序号	阶段	任务	对象	开始日期	结束日期
		判定			
20		单元测评结果判定		2022年10月9日	2022年10月17日
21		整体测评		2022年10月9日	2022年10月17日
22		系统安全保障评估		2022年10月9日	2022年10月17日
23		安全问题风险分析		2022年10月9日	2022年10月17日
24		等级测评结论形成		2022年10月17日	2022年10月30日
25		测评报告编制		2022年10月17日	2022年10月30日

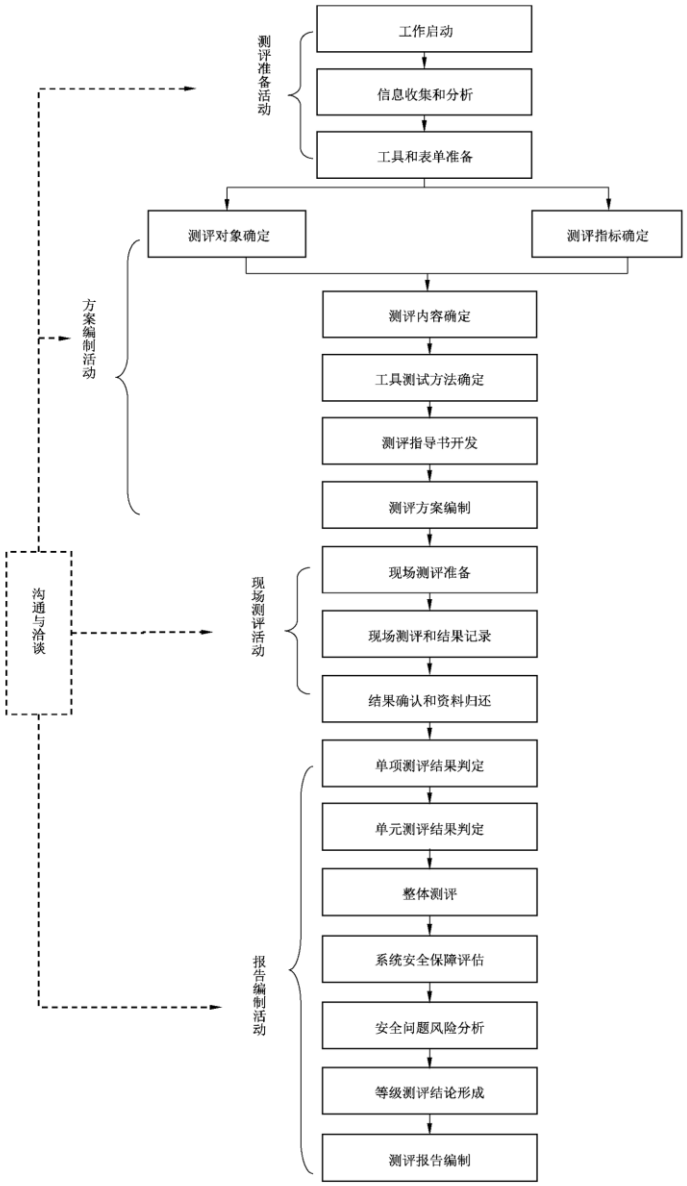


图 1-1 等级保护测评工作流程图

其中，于项目前期召开了项目启动会议，确定了工作方案及项目人员名单；于现场测评完成后召开了项目末次会议，确认了测评发现的问题；于2022年10月30日在对系统的整改情况进行了复核确认后，完成报告编制。

1.4 报告分发范围

等级测评报告正本一式3份，其中茂名职业技术学院1份，广东南方信息安全研究院1份，受理备案的公安机关1份。

2 被测对象描述

2.1 被测对象概述

2.1.1 定级结果

表 2-1定级结果

被测对象名称	安全保护等级	业务信息安全等级	系统服务安全等级
科研创新信息化管理系统	2	2	2

2.1.2 业务和采用的技术

科研创新信息化管理系统用于科研管理信息化建设，系统主要功能包括项目管理，经费管理，论文、著作、专利、艺术作品等成果管理，科研人员，科研机构管理。根据学校科教研管理的分工，提供不同的解决方案，让科研管理变得更简单。

被测对象未采用云计算/移动互联/物联网/工业控制/大数据等技术情况。

2.1.3 网络结构

科研创新信息化管理系统主要是对互联网提供服务,相关设备部署在信息化机房当中,其简要拓扑如下:

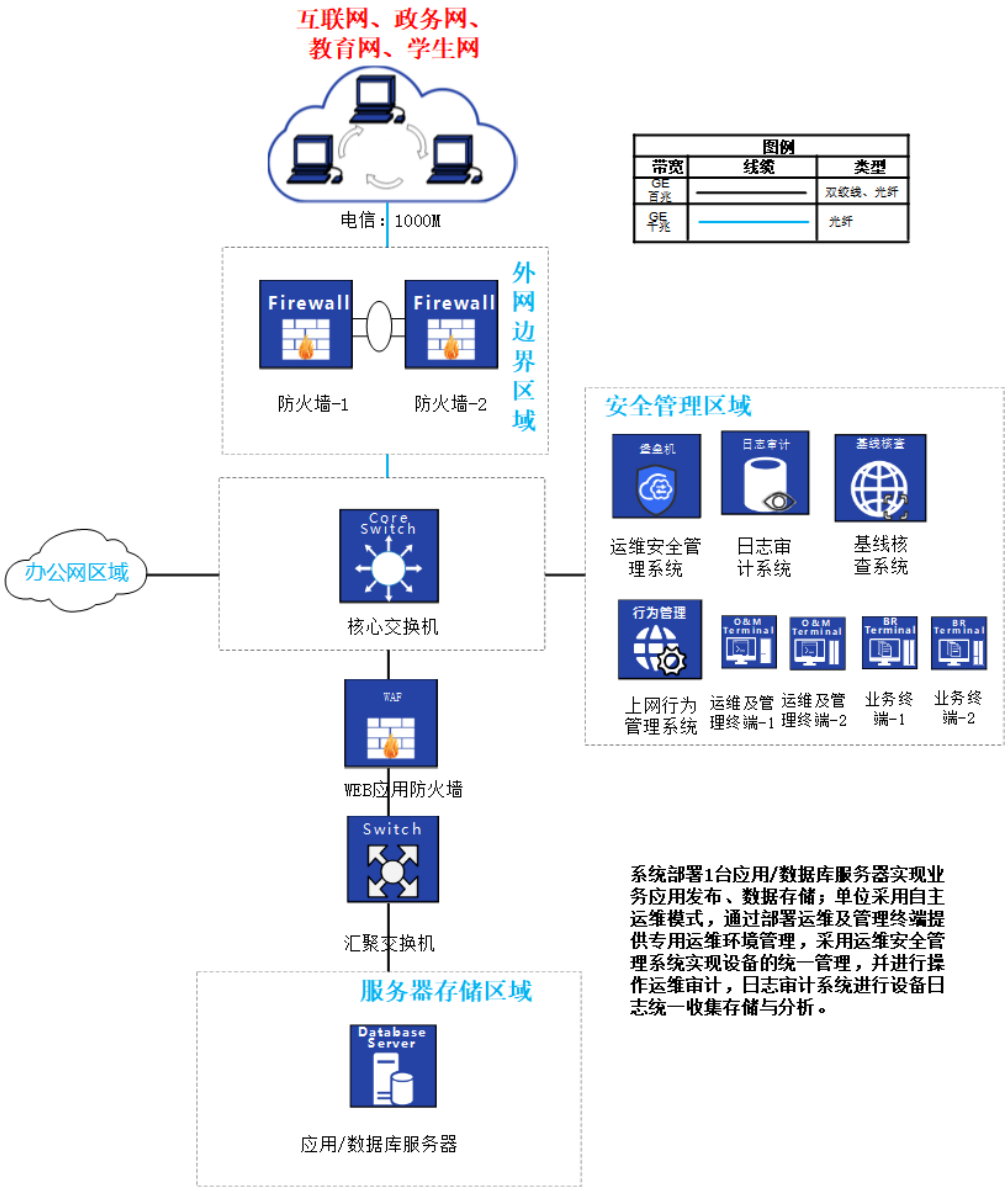


图 2-1 科研创新信息化管理系统网络拓扑图

如图2-1科研创新信息化管理系统网络拓扑图所示，科研创新信息化管理系统网络安全域划分为4个，分别为外网边界区域、安全管理区域、服务器存储区域、办公网区域。

1、外网边界区域：

外网边界区域网络主要包括科研创新信息化管理系统的业务服务和信息交换应用，是安全管理区域、服务器存储区域、办公网区域的出口边界；其链路接入为光纤线，带宽为1000mb。通过部署核心交换机、防火墙等设备实施网络访问控制，防火墙（入侵

防御模块）实现网络入侵攻击行为防御。

2、办公网区域：

办公网区域网络主要包括科研创新信息化管理系统与办公区域的信息交换应用，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、防火墙、上网行为管理系统等设备实施网络访问控制、防火墙（入侵防御模块）实现网络入侵攻击行为防御。

3、安全管理区域：

安全管理区域网络主要包括日志审计系统、运维安全管理系统、上网行为管理系统，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、上网行为管理系统等设备实施网络访问控制。

4、服务器存储区域：

服务器存储区域网络主要包括科研创新信息化管理系统的应用服务器、数据库服务器，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、上网行为管理系统等设备实现一定的网络访问控制。

5、服务器部署情况：

科研创新信息化管理系统由1台应用/数据库服务器实现应用发布、数据处理、存储、维护。

6、灾备及冗余

科研创新信息化管理系统无异地备份机房，未实现异地备份数据定时传输功能。系统重要数据根据需求采用每天增量、每月全备到本地信息化机房。

科研创新信息化管理系统未实现冗余措施。

2.2 测评指标

2.2.1 安全通用要求指标

表 2-2 安全通用要求指标

安全类	安全控制点	测评项数
安全物理环境	物理位置选择	2
	物理访问控制	1
	防盗窃和防破坏	2
	防雷击	1
	防火	2
	防水和防潮	2
	防静电	1
	温湿度控制	1
	电力供应	2
	电磁防护	1
安全通信网络	网络架构	2
	通信传输	1
	可信验证	1
安全区域边界	边界防护	1
	访问控制	4
	入侵防范	1
	恶意代码和垃圾邮件防范	1
	安全审计	3
	可信验证	1
安全计算环境	身份鉴别	3
	访问控制	4
	安全审计	3
	入侵防范	5
	恶意代码防范	1
	可信验证	1
	数据完整性	1
	数据备份恢复	2
	剩余信息保护	1
	个人信息保护	2
安全管理中心	系统管理	2
	审计管理	2
安全管理制度	安全策略	1
	管理制度	2
	制定和发布	2
	评审和修订	1
安全管理机构	岗位设置	2
	人员配备	1
	授权和审批	2
	沟通和合作	3

安全类	安全控制点	测评项数
	审核和检查	1
安全管理人员	人员录用	2
	人员离岗	1
	安全意识教育和培训	1
	外部人员访问管理	3
安全建设管理	定级和备案	4
	安全方案设计	3
	产品采购和使用	2
	自行软件开发	2
	外包软件开发	2
	工程实施	2
	测试验收	2
	系统交付	3
	等级测评	3
	服务供应商选择	2
安全运维管理	环境管理	3
	资产管理	1
	介质管理	2
	设备维护管理	2
	漏洞和风险管理	1
	网络和系统安全管理	5
	恶意代码防范管理	3
	配置管理	1
	密码管理	2
	变更管理	1
	备份与恢复管理	3
	安全事件处置	3
	应急预案管理	2
	外包运维管理	2
安全通用要求指标数量统计		135

2.2.2 安全扩展要求指标

表 2-3 安全扩展要求指标

扩展类型	安全类	安全控制点	测评项数
本次测评不涉及安全扩展要求指标			

2.2.3 其他安全要求指标

表 2-4 其他安全要求指标

安全类	安全控制点	测评项数
本次测评不涉及其他安全要求指标		

2.2.4 不适用安全要求指标

表 2-5-1 不适用安全要求指标

安全类	安全控制点	不适用项	不适用原因
安全建设管理	自行软件开发	a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。
安全建设管理	自行软件开发	b) 应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。
安全运维管理	密码管理	b) 应使用国家密码管理主管部门认证核准的密码技术和产品。	（1）单位未采购涉及密码技术的产品，不适用。
安全运维管理	外包运维管理	a) 应确保外包运维服务商的选择符合国家的有关规定；	（1）单位目前未涉及任何外包运维服务情况，不适用。
安全运维管理	外包运维管理	b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。	（1）单位目前未涉及任何外包运维服务情况，不适用。

表 2-5-2 其他不适用安全要求指标

安全类	安全控制点	不适用项	不适用原因
本次测评不涉及其他安全要求指标			

2.3 测评对象

2.3.1 测评对象选择方法

科研创新信息化管理系统等级测评的测评对象种类上基本覆盖、数量进行抽样，重点抽查主要的设备、设施、人员和文档等。结合科研创新信息化管理系统的网络拓扑结构和业务情况，本次等级测评的测评对象在抽样时主要考虑以下几个方面：

（1） 主机房（包括其环境、设备和设施等）和灾备机房；

（2） 存储被测系统重要数据的介质的存放环境；

（3） 办公场地；

（4） 整个系统的网络拓扑结构；

（5） 安全设备，包括防火墙等；

（6） 边界网络设备，包括路由器、楼层交换机等；

（7） 对整个信息系统或其局部的安全性起作用的网络互联设备，如核心交换机、路由器等；

（8） 承载业务处理系统主要业务或数据的服务器（包括其操作系统和数据库）；

（9） 管理终端和主要应用系统终端；

（10） 能够完成系统不同业务使命的业务应用系统；

（11） 业务备份系统；

（12） 信息安全主管人员、各方面的负责人员、具体负责安全管理的当事人、业务负责人；

（13） 涉及到信息系统安全的所有管理制度和记录。

抽样原则：在等级测评时，业务处理系统中配置相同的安全设备、边界网络设备、网络互联设备、服务器、终端以及备份设备，每类至少抽查两台作为测评对象。

2.3.2 测评对象选择结果

2.3.2.1 物理机房

表 2-6 物理机房

序号	机房名称	物理位置	重要程度
1	信息化机房	茂名市茂南区文明北路232号大院大楼	关键

2.3.2.2 网络设备

表 2-7 网络设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度
1	汇聚交换机	否	H3C version 7.1.070, Release 6126P20	H3C S5560X-30C-EI	数据交换	重要
2	核心交换机	否	H3C version 7.1.070, Release 7585P07	H3C S7500E-X	核心数据交换、访问控制	关键

2.3.2.3 安全设备

表 2-8 安全设备

序号	设备名称	是否虚拟设备	系统及版本	品牌型号	用途	重要程度
1	基线核查系统	否	深信服V3.0.3	深信服AC-1000-D602-PT	漏洞扫描	重要
2	防火墙-1	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键
3	WEB应用防火墙	否	深信服AF 8.0.9	深信服WAF-2000-H642	应用防护、入侵防范、病毒防护	重要
4	上网行为管理系统	否	深信服AC12.0.26	深信服AC-1000-D600-PT	上网行为管理及终端准入控制	重要
5	防火墙-2	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键
6	日志审计系统	否	深信服LAS 3.0.5	深信服AC-1000-D601-	日志审计	重要

序号	设备名称	是否虚拟设备	系统及版本	品牌型号	用途	重要程度
				PT		
7	运维安全管理系统	否	深信服V3.0.6	深信服AC-1000-D603-PT	运维审计	重要

2.3.2.4 服务器

表 2-9 服务器

序号	设备名称	所属业务应用系统/平台	是否虚拟设备	操作系统及版本	数据库管理系统及版本	中间件及版本	重要程度
1	应用/数据库服务器	科研创新信息化管理系统	否	Windows Server 2012 R2	MSSQL 2008 R2	Tomcat 8.5	关键

2.3.2.5 终端设备

表 2-10 终端设备

序号	设备名称	是否虚拟设备	操作系统及版本	用途	重要程度
1	业务终端-2	否	Windows 10 （版本 20H2（内部版本 19044.1889）	业务管理	一般
2	运维及管理终端-1	否	Windows 10 （版本 20H2（内部版本 19044.1889）	运维管理、系统管理	一般
3	业务终端-1	否	Windows 10 （版本 20H2（内部版本 19044.1889）	业务管理	一般
4	运维及管理终端-2	否	Windows 10 （版本 21H2（内部版本 19044.1889））	运维管理、系统管理	一般

2.3.2.6 其他系统或设备

表 2-11 其他系统或设备

序号	设备名称	是否虚拟设备	系统及版本	用途	重要程度
/	/	/	/	/	/

注释：本次测评对象中不涉及专用移动互联终端等，不开展抽测。

2.3.2.7 系统管理软件/平台

表 2-12 系统管理软件/平台

序号	系统管理软件/平台名称	主要功能	版本	所在设备名称	重要程度
1	应用/数据库服务器-Tomcat	页面发布	8.5	应用/数据库服务器	关键
2	应用/数据库服务器-MSSQL	数据生产、存储	2008 R2	应用/数据库服务器	关键

2.3.2.8 业务应用软件/平台

表 2-13 业务应用系统/平台

序号	业务应用软件/平台名称	主要功能	业务应用软件及版本	开发厂商	重要程度
1	科研创新信息化管理系统	科研创新信息化管理系统用于科研管理信息化建设，系统主要功能包括项目管理，经费管理，论文、著作、专利、艺术作品等成果管理，科研人员，科研机构管理。根据学校科教研管理的分工，提供不同的解决方案，让科研管理变得更简单。	V6.0	北京易普拉格科技股份有限公司	关键

2.3.2.9 数据资源

表 2-14 数据资源

序号	数据类别	所属业务应用	安全防护需求	重要程度
1	重要个人信息	科研创新信息化管理系统	完整性、保密性	关键
2	重要业务数据	科研创新信息化管理系统	完整性、保密性	关键
3	鉴别数据	科研创新信息化管理系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性、保密性	关键
4	重要审计数据	科研创新信息化管理系统（安全管理中心)	完整性	重要
5	重要配置数据	科研创新信息化管理系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性	关键

注释：网络设备、安全设备、服务器、终端、系统管理软件/平台和业务应用系统等所涉及的鉴别数据和重要配置数据分别在各自测评对象中汇总测评证据后集中体现,包括数据完整性、数据保密性和备份恢复。重要审计数据在安全管理中心进行汇总测评证据，包括数据完整性。重要业务数据和重要个人信息分别在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。

2.3.2.10 安全相关人员

表 2-15 安全相关人员

序号	姓名	岗位/角色	联系方式	所属单位
1	杨云	资产管理员	0668-2920122	茂名职业技术学院
2	龙恒	网络管理员	13377766618	茂名职业技术学院
3	龙恒	数据管理员	13377766618	茂名职业技术学院
4	龙恒	应用管理员	13377766618	茂名职业技术学院
5	杨云	审计管理员	0668-2920122	茂名职业技术学院
6	吴国华	机房管理员	0668-2920122	茂名职业技术

序号	姓名	岗位/角色	联系方式	所属单位
				学院
7	叶永利	安全管理员	0668-2920122	茂名职业技术学院
8	吴国华	系统管理员	0668-2920122	茂名职业技术学院

2.3.2.11 安全管理文档

表 2-16 安全管理文档

序号	文档名称	主要内容
1	制度类文档-安全事件报告和处置	关于单位网络安全事件管理、处置、流程等报告制度文档
2	制度类文档-组织安全结构和人员职责制度	关于单位组织结构、人员安排、人员职责制度文档
3	制度类文档-介质管理制度	关于单位介质安全管理工制度文档
4	制度类文档-安全管理组织规范	关于单位组织结构管理规范制度文档
5	制度类文档-主机安全管理规范	关于规定单位主机系统安全管理要求规范，指导业务平台主机的安全配置和维护的制度文档
6	制度类文档-应用安全管理规范	关于规定单位应用安全管理要求及规范的制度文档
7	制度类文档-外部服务人员管理规范	关于单位针对外部人员工作管理规范制度文档
8	制度类文档-备份与恢复管理制度	关于单位数据备份、恢复管理制度文档
9	制度类文档-组织安全结构和人员职责制度	关于单位安全结构、人员职责
10	制度类文档-离岗人员工作交接规范	关于单位离岗交接工作规范制度文档
11	制度类文档-机房安全管理制度	关于单位机房安全管理工作制度文档
12	制度类文档-信息系统外包运维管理制度	关于单位外包运维工作管理制度文档
13	制度类文档-信息系统恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
14	制度类文档-信息安全漏洞扫描规范	关于单位安全漏洞工作规范制度文档
15	制度类文档-员工考核管理制度	关于单位人员考核工作管理制度文档
16	制度类文档-物理安全管理	关于加强单位办公区域及电子计算机机房的管理和设备运行安

序号	文档名称	主要内容
	规范	全，规范办公区域及机房建设，使人员办公高效及机房设备安全、稳定运行的制度文档
17	制度类文档-系统交付管理	关于单位交付工作管理制度文档
18	制度类文档-信息安全奖惩办法	关于单位人员奖惩制度文档
19	制度类文档-办公环境管理制度	关于单位办公环境管理制度文档
20	制度类文档-网络安全管理制度	关于单位网络安全工作管理制度文档
21	制度类文档-安全漏洞管理制度	关于单位安全漏洞管理工作制度文档
22	制度类文档-变更控制管理制度	关于单位变更流程、控制管理制度文档
23	制度类文档-测试及验收方案	关于单位测试验收方案文档
24	制度类文档-工程测试验收管理	关于单位工程测试工作管理制度文档
25	制度类文档-安全审查和检查管理规范	关于单位安全检查、审查工作规范制度文档
26	制度类文档-外部人员访问管理制度	关于单位针对外来人员访问管控制度文档
27	制度类文档-安全教育和培训制度	关于单位安全培训、安全交流工作制度文档
28	制度类文档-网络安全事件应急预案	关于单位网络安全事件应急处理、流程、培训等管理制度文档
29	制度类文档-应用系统业务用户密码设置规定	关于单位用户密码管理制度文档
30	制度类文档-系统安全管理制度	关于单位系统安全管理、安全服务管理制度文档
31	制度类文档-工程实施管理制度	关于单位工程实施工作管理制度文档
32	制度类文档-人员管理制度	关于单位人员录用、调岗、离岗管理制度文档
33	制度类文档-设备安全管理制度	关于单位设备安全管理制度文档
34	制度类文档-恶意代码防范管理制度	关于单位恶意代码防范工作制度文档
35	制度类文档-信息安全总体策略	关于单位网络安全方针、策略制度文档
36	制度类文档-网络安全管理规范	关于保障单位网络系统的安全稳定运行，抵御内部和外部各种形式的网络攻击或威胁制定的管理文档
37	制度类文档-恶意代码防范管理制度	关于单位恶意代码工作管理制度文档

序号	文档名称	主要内容
38	制度类文档-网络安全事件报告制度	关于单位网络安全事件管理报告文档
39	制度类文档-办公环境保密管理	关于单位办公环境管理制度文档
40	制度类文档-服务供应商选择安全管理制度	关于单位安全服务供应商管理规定制度文档
41	制度类文档-岗位安排及岗位职责	关于单位岗位职责、岗位安排制度文档
42	制度类文档-外部接入受控网络访问系统管理规范	关于单位针对外部人员工作接入规范制度文档
43	制度类文档-外包开发软件管理规定	关于单位外包项目管理工作制度文档
44	制度类文档-数据安全管理规范	关于保障关键数据安全，从数据库本身、数据加密、数据备份恢复三个方面对数据安全进行规范的制度文档
45	制度类文档-授权和审批管理规定	关于单位授权审批、审批流程规范制度文档
46	制度类文档-制度制定、发布、评审和修订管理制度	关于单位制度制定、发布、评审和修订等管理文档
47	制度类文档-网络与信息系统安全设计规范	关于单位网络与信息化安全设计制度文档
48	制度类文档-系统及应用数据备份管理规范	关于单位数据备份、恢复管理制度文档
49	操作类文档-设备操作规程	关于单位相关设备操作指导文档
50	操作类文档-设备及系统软件配置和操作手册	关于单位安全设备操作、Linux服务器配置手册、主机运维操作手册、软件操作手册、防火墙配置和操作手册、数据库日常运维操作手册等指导文档
51	操作类文档-数据备份策略	关于单位数据备份策略文件
52	操作类文档-软硬件日常维护管理规程	关于单位计算机网络系统使用、管理、信息安全、资源共享有所遵循,规范上网操作流程,提高网络系统安全性的指导文档
53	记录类文档-收发文登记记录	关于单位文档签发记录
54	记录类文档-人员入职考核记录	关于人员录用、考核工作记录
55	记录类文档-机房维护日志	关于机房维护工作记录
56	记录类文档-设备维修申请表	关于单位设备维护工作申请记录
57	记录类文档-技能培训记录	关于单位系统培训工作、考核工作记录
58	记录类文档-信息系统存储介质销毁申请表	关于备份介质销毁申请工作记录
59	记录类文档-设备操作维护记录	关于单位设备维护工作记录
60	记录类文档-评审和修订记	关于单位变更评审、修订工作记录

序号	文档名称	主要内容
	录	
61	记录类文档-重要操作审批表	关于单位审批工作记录
62	记录类文档-监理审批表	关于单位监理审核工作记录
63	记录类文档-离场信息资料交接表	关于人员离岗交接工作记录
64	记录类文档-通用变更记录表	关于单位变更工作记录
65	记录类文档-设备出入登记记录表	关于设备进出机房登记工作记录
66	记录类文档-软件交付清单	关于单位交付工作记录
67	记录类文档-网络配置信息	关于单位配置信息登记工作记录
68	记录类文档-人员培训及考核记录表	关于人员培训、考核等工作记录
69	记录类文档-安全建设方案评审纪录	关于单位网络与信息化安全设计方案评审工作记录
70	记录类文档-信息管理系统漏洞检查表	关于单位安全漏洞工作检测记录表
71	记录类文档-信息安全检查记录表	关于单位安全检查工作记录
72	记录类文档-机房出入登记表	关于人员进出机房登记工作记录
73	记录类文档-备份介质使用记录	关于备份介质使用登记工作记录
74	记录类文档-访问记录表	关于人员访问工作记录
75	记录类文档-信息系统存储介质使用清单	关于备份介质存储使用清单
76	记录类文档-接入受控网络申请表	关于外来人员接入工作记录
77	记录类文档-离职员工物品交回登记表	关于人员离岗工物交接工作记录
78	记录类文档-数据恢复申请表	关于单位数据恢复工作申请表
79	记录类文档-网络信息安全事件记录表	关于单位网络安全事件工作记录
80	记录类文档-数据备份记录表	关于单位数据备份工作记录
81	记录类文档-机房设备维修记录表	关于单位机房设备维修工作记录
82	记录类文档-外部会议文件和记录	关于单位外部联系、交流及会议工作记录
83	记录类文档-人员离岗申请	关于人员离岗申请记录

序号	文档名称	主要内容
	表	
84	记录类文档-安全管理制度评审记录	关于单位制度审计记录
85	记录类文档-关键岗位人员考核记录	关于关键岗位考核工作记录
86	记录类文档-机房巡检记录表	关于单位机房环境巡检记录
87	记录类文档-存储介质目录清单	关于备份介质存储工作清单
88	记录类文档-外部人员访问记录表	关于外来人员访问登记工作记录
89	记录类文档-外部人员访问申请表	关于外来人员访问申请流程工作记录
90	记录类文档-系统交付清单	关于单位交付工作记录
91	记录类文档-应急预案培训记录表	关于单位应急预案培训工作记录
92	记录类文档-漏洞检测报告	关于单位安全漏洞检测报告文档
93	记录类文档-机房设备维护记录表	关于设备维护登记工作记录
94	记录类文档-专家论证记录表	关于单位网络方案论证记录
95	记录类文档-信息安全会议记录	关于单位安全培训、安全交流会议记录
96	记录类文档-备份工作汇总表	关于单位数据备份工作总结表
97	证据类文档-信息安全事件分析报告表	关于单位安全事件分析报告
98	证据类文档-网络安全系统设计方案	关于单位网络与信息化安全设计方案文档
99	证据类文档-资产清单	关于单位信息系统资产清单统计表
100	证据类文档-网络安全等级保护工作小组名单	关于单位网络安全等级保护工作小组人员名单文件
101	证据类文档-安全职位人员	关于单位人员岗位安排名单
102	证据类文档-外部联系表	关于单位内部联系及外部联系名单
103	证据类文档-网络安全等级保护测评服务合同	关于单位与安全服务商签定的安全服务合同文件
104	证据类文档-定级备案	关于单位系统定级报告、备案证文件
105	证据类文档-深信服安全采购合同	关于单位与安全厂家服务采购、产品选择合同文件
106	证据类文档-工程项目实施方案	关于单位工程实施方案文档

3 单项测评结果分析

3.1 安全物理环境

3.1.1 已有安全控制措施汇总分析

安全通用要求

物理位置选择	
a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；	
信息化机房	（1）机房和办公场地场所在建筑物具有建筑验收文档，包含对防震、防风和防雨能力的说明； （2）机房和办公场地未出严重的问题。
b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	
信息化机房	（1）机房未部署在易发生问题的位置； （2）机房对于空调设备的排水管等部位采取密封防漏处理； （3）机房对于楼板进行了防护措施。
防盗窃和防破坏	
a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识；	
信息化机房	（1）机房设备或主要部件都固定在机架上； （2）机房内对主要部件已绑定相应不易除去的标签； （3）重要机柜已进行上锁处理。
b) 应将通信线缆铺设在隐蔽安全处。	
信息化机房	（1）通信线缆铺设在下走线槽隐蔽处中； （2）通信线缆设有明显的源目的标识； （3）通信线缆均铺设整齐、规范。
防雷击	
应将各类机柜、设施和设备等通过接地系统安全接地。	
信息化机房	（1）机房设置专用地线； （2）机房内机柜、设施和设备等进行接地处理； （3）交流电源接地验收检测结果符合要求。
防火	
a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；	
信息化机房	（1）机房采用经消防检测部门检测合格并在有效期内的（如 七氟丙烷）气体自动灭火设备，火灾自动报警类型为烟感+红外； （2）自动消防系统工作状态正常，有定期巡检和维护记录《机房巡检记录表》； （3）建立机房消防的管理制度相关文档《机房安全管理制度》，按管理要求机房无人情况下气体灭火配置为自动模式，进入机房调整为手动模式，机房报警有7*24小时值班人员进行监控。
防水和防潮	

a) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	
信息化机房	（1）机房不存在雨水渗透、破损等不合规情况； （2）机房不位于建筑的顶层、边缘区域。
b) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。	
信息化机房	（1）机房区域范围已部署1台科华品牌（精密）空调，机房内分别配置1组温湿度传感器监控； （2）机房内空调下方已铺设安装好挡水和排水设施； （3）机房墙壁或楼板的管道采取必要的防渗防漏等防水保护措施； （4）机房安装检测设备（如：漏水检测绳）检测地下积水，及时处理机房水蒸气结露和地下积水的转移与渗透； （5）目前防水\防潮检测未发现异常情况，并且有防水防潮的运维记录《机房维护日志》。
温湿度控制	
应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。	
信息化机房	（1）机房范围已部署1组科华品牌精密空调进行温湿度调节； （2）机房范围已部署空调及加湿机进行温湿度调节； (3)温湿度自动调节设施运作正常,有运行和维护记录《机房维护日志》; （4）机房温度能保持在24摄氏度到28摄氏度之间； （5）机房湿度能保持在40%到65%之间。
电力供应	
a) 应在机房供电线路上配置稳压器和过电压防护设备；	
信息化机房	（1）机房配备了稳压器和过电压防护设备； （2）稳压器和过电压防护设备正常工作； （3）机房具备电力供应安全设计，并在其中标明配备稳压器、过电压防护设备等要求。
b) 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。	
信息化机房	（1）机房配备了1组科华品牌UPS； （2）UPS正常工作，可满足主要设备断电情况下的至少1小时正常运行要求； （3）UPS有定期（至少每年）检查和维护，有运行和维护记录《机房巡检记录表》。
电磁防护	
电源线和通信线缆应隔离铺设，避免互相干扰。	
信息化机房	（1）通信线缆铺设采用独立的具有电磁屏蔽作用线槽； （2）电源线缆铺设采用独立的具有电磁屏蔽作用线槽； （3）弱电线缆隔离铺设，没有干扰。

3.1.2 主要安全问题汇总分析

安全通用要求

（1）机房出入口未配置电子门禁系统（如：信息化机房）。上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域,可能对系统的平稳运行造成影响。中风险。

（2）机房建设未完全采用符合耐火等级的建筑材料。机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级（如：信息化机房）。存在发生火情时助燃火灾的风险。 低风险。

（3）机房内缺乏防静电措施（如防静电地板或铺设防静电地毯 ）（如：信息化机房）。存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。 中风险。

3.2 安全通信网络

3.2.1 已有安全控制措施汇总分析

安全通用要求

网络架构	
b) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	
安全通信网络	(1)网络内重要网段未部署在网络边界处,且未直接连接外部信息系统; (2) 系统通过防火墙对重要网段采取访问控制策略; (3) 各安全域（子网）的出口唯一。
通信传输	
应采用校验技术保证通信过程中数据的完整性。	
安全通信网络	(1) 网络系统中未涉及完整性保障设备，但在安全计算环境方面网络设备采用SSH协议、安全设备采用HTTPS协议、操作系统采用SSH协议、应用系统采用HTTPS协议来保证通信过程中数据的完整性。

3.2.2 主要安全问题汇总分析

安全通用要求

（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况（如：安全通信网络）。上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变得更

为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。 中风险。

（2）缺乏对通信设备可信验证方面的安全设计要求。现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况（如：安全通信网络）。缺乏对系统可执行程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致计算资源被干扰和破坏造成损失。 低风险。

3.3 安全区域边界

3.3.1 已有安全控制措施汇总分析

安全通用要求

边界防护	
应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络存在受保护的边界； （2）网络边界处部署了可提供访问控制功能的设备； （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。
访问控制	
a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。
b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。
c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	
办公网区域 外网边界区域 安全管理区域	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数

服务器存储区域	据包是被接收还是拒绝通过特定指示条件来决定。
d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	(1) 网络内支持状态检测和会话机制检测的区域及边界； (2) 网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； (3) 访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。
入侵防范	
应在关键网络节点处监视网络攻击行为。	
外网边界区域 服务器存储区域	(1) 网络层部署支持对内部发起的攻击行为进行防范的设备； (2) 现有的防范措施满足相应防护要求； (3) 内部安全防范措施能检测相应攻击行为。
恶意代码和垃圾邮件防范	
应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	
外网边界区域 服务器存储区域	(1) 在关键网络节点处部署合规的防恶意代码措施； (2) 恶意代码防护机制的代码库运作正常，定期更新恶意代码库； (3) 有对恶意代码库更新前的安全性及兼容性进行测试。
安全审计	
a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	(1) 网络层相关设备均开启本地审计功能； (2) 网络内部署审计措施对网络边界、重要网络节点进行安全审计； (3) 现有的审计措施满足相应的审计要求。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	(1) 设备均开启日志记录功能； (2) 现有环境内日志信息较全面； (3) 设备本地时间正常。
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	(1) 网络层部署日志审计系统，统一接收及保存相关设备的审计记录； (2) 相关网络及安全设备的本地日志文件不可删除修改； (3) 审计记录的备份机制符合信息安全管理要求； (4) 日志及审计记录的保存能力可超过6个月； (5) 定期收集日志记录并定期备份。

3.3.2 主要安全问题汇总分析

安全通用要求

(1)网络层部署防火墙,防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为（如：办公网区域）。存在不能及时发现内部主机作为攻击跳板，或网络攻击行为而造成系统损坏/网络资源浪费的风险。中风险。

(2)现有部署的恶意代码防范措施存在不合规的问题,网络边界覆盖不全面(如：办公网区域）。无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。 中风险。

(3) 缺乏对边界设备可信验证方面的安全设计要求。现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况（如：办公网区域）。缺乏对边界设备的相关程序的可信性验证,无法保证系统始终运行于可信环境中,运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4 安全计算环境

3.4.1 网络设备

3.4.1.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
核心交换机 汇聚交换机	(1) 设备对各登录模式均启用身份鉴别； (2) 设备对登录管理的用户进行身份鉴别； (3) 设备名及登录用户设置的身份标识具有唯一性； (4) 设备不存在明文或空口令用户； (5) 设备配置合规的全局密码策略； (6) 设备配置加密的super认证。
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
核心交换机 汇聚交换机	(1) 设备配置合规的全局登录失败处理策略； (2) 设备配置合规的操作超时退出措施。

c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
核心交换机 汇聚交换机	（1）设备配置合规的远程管理模式。
访问控制	
a) 应对登录的用户分配账户和权限；	
核心交换机 汇聚交换机	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。
b) 应重命名或删除默认账户，修改默认账户的默认口令；	
核心交换机 汇聚交换机	（1）设备不存在默认账户名； （2）设备账户口令设置合规。
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
核心交换机 汇聚交换机	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	
核心交换机 汇聚交换机	（1）设备根据安全策略要求对特权用户进行分离； （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
核心交换机 汇聚交换机	（1）设备开启审计功能，审计进程正常； （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
核心交换机 汇聚交换机	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
核心交换机 汇聚交换机	（1）设备限制审计文件的访问控制权限，普通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效； （5）日志及审计记录保存大于6个月。
入侵防范	
a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	
核心交换机 汇聚交换机	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。
b) 应关闭不需要的系统服务、默认共享和高危端口；	
核心交换机	（1）设备采用安全策略限制部分高危端口；

汇聚交换机	（2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。
c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
核心交换机 汇聚交换机	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
核心交换机 汇聚交换机	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
核心交换机 汇聚交换机	鉴别数据、重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； （2）设备对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a）应提供重要数据的本地数据备份与恢复功能；	
核心交换机 汇聚交换机	（1）设备定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。

3.4.1.2 主要安全问题汇总分析

安全通用要求

（1）设备不具备相关可信验证的技术措施（如：核心交换机）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.2 安全设备

3.4.2.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别

a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备对各登录模式均启用身份鉴别； （2）设备对登录管理的用户进行身份鉴别； （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备启用合规登录失败处理策略； （2）设备配置合规的操作超时退出措施。
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备配置合规的远程管理模式； （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。
访问控制	
a) 应对登录的用户分配账户和权限；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。
b) 应重命名或删除默认账户，修改默认账户的默认口令；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备不存在默认账户名； （2）设备账户口令设置合规。
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	

WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备不存在多余或过期账户； (2) 设备管理员用户与账户之间一一对应。
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备根据安全策略要求对特权用户进行分离； (2) 设备不存在多个管理级别高的特权用户； (3) 设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备开启审计功能，审计进程正常； (2)设备的日志审计级别满足要求,审计覆盖所有用户操作审计和记录。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备日期、时间正常； (2) 设备审计记录内容基本完整。
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
WEB应用防火墙 上网行为管理系统 基线核查系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备限制审计文件的访问控制权限，普通用户不可删除及修改； (2) 设备针对日志、审计记录具备充足的存储容量； (3) 对审计记录进行定期存档备份，其备份策略有效； (4) 部署日志审计系统实时对日志进行统一收集存储； (5) 日志及审计记录保存大于6个月。
日志审计系统	(1) 设备限制审计文件的访问控制权限，普通用户不可删除及修改； (2) 设备针对日志、审计记录具备充足的存储容量； (3) 对审计记录进行定期存档备份，其备份策略有效； (4) 日志及审计记录保存大于6个月。
入侵防范	

a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。
b) 应关闭不需要的系统服务、默认共享和高危端口；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。
c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 防火墙-1 防火墙-2	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
运维安全管理系统	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制。
d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备管理具备数据有效性检验功能； （2）设备管理的校验接口范围较全面。
e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。
恶意代码防范	
应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	

WEB应用防火墙 防火墙-1 防火墙-2	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	鉴别数据、重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； （2）设备对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a）应提供重要数据的本地数据备份与恢复功能；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。

3.4.2.2 主要安全问题汇总分析

安全通用要求

（1）设备不具备相关可信验证的技术措施（如：WEB应用防火墙）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.3 服务器和终端

3.4.3.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别
a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统对登录系统的用户进行身份鉴别； （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； （5）用户属性策略未勾选“密码永不过期”。
b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统启用登录失败处理策略。 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略。
c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS的管理。
应用/数据库服务器	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用‘RDP安全层’参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS的管理。
访问控制	
a）应对登录的用户分配账户和权限；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。
b）应重命名或删除默认账户，修改默认账户的默认口令；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统针对默认账户采用相应的安全策略配置； （2）操作系统账户不存在弱口令或空口令。
c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。
d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	
业务终端-1 业务终端-2	（1）操作系统根据安全策略要求对特权用户进行分离； （2）操作系统不存在特权用户；

应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（3）操作系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统开启审计策略，操作系统审计策略基本完整； （2）审计覆盖所有用户操作审计和记录。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。
c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统采取对审计记录存储容量如下： 运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。
入侵防范	
a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。
b）应关闭不需要的系统服务、默认共享和高危端口；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统不存在多余的默认共享及其它文件共享； （2）操作系统关闭不必要端口； （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。
c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。

e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。
恶意代码防范	
应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	鉴别数据、重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施: 安全选项“不显示上次的用户名”->启用

3.4.3.2 主要安全问题汇总分析

安全通用要求

（1）缺乏对计算设备可信验证方面的安全设计要求。现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况（如：业务终端-1）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.4 系统管理软件/平台

3.4.4.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
应用/数据库服务器-MSSQL	（1）数据库系统对登录系统的用户进行身份鉴别； （2）数据库系统不存在弱口令用户； （3）数据库系统不存在默认信任的登录模式； （4）数据库系统为登录用户设置的身份标识具有唯一性； （5）数据库系统配置合规的密码长度及复杂度策略； （6）数据库系统配置合规的密码有效周期策略。
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
应用/数据库服务器-MSSQL	（1）数据库系统启用合规登录失败处理策略； （2）数据库系统执行合规的锁定策略； （3）数据库系统配置合规的操作超时锁定。
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
应用/数据库服务器-MSSQL	（1）宿主操作系统配置合规的远程管理模式； （2）使用运维安全管理系统统一管理操作系统远程登录，运维安全管理系统采用了HTTPS 的管理。
访问控制	
a) 应对登录的用户分配账户和权限；	
应用/数据库服务器-MSSQL	（1）可提供数据库系统权限表； （2）登录数据库系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在所有用户均属于sysadmin的情况； （4）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。
应用/数据库服务器-Tomcat	（1）对应不同的账户均按需分配不同的用户权限，不存在中间件用户均属于管理级别、高权限的情况；

	（2）中间件配置可降权启动Tomcat的用户； （3）宿主系统针对中间件用户分别赋予相应的管理操作权限。
b）应重命名或删除默认账户，修改默认账户的默认口令；	
应用/数据库服务器-MSSQL	（1）数据库系统对多余帐户进行删除、锁定或禁止其登录； （2）数据库系统账户口令设置合规。
应用/数据库服务器-Tomcat	（1）中间件不存在除如:Tomcat、admin、manager、role1等默认账户名； （2）中间件账户口令设置合规。
c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
应用/数据库服务器-MSSQL	（1）数据库系统不存在多余或过期账户； （2）数据库系统管理员用户与账户之间一一对应。
应用/数据库服务器-Tomcat	（1）中间件不存在多余或过期账户； （2）中间件管理员用户与账户之间一一对应； （3）中间件启用合规的管理用户名配置。
d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	
应用/数据库服务器-MSSQL	（1）数据库系统根据安全策略要求对特权用户进行分离； （2）数据库系统不存除sa外的特权用户； （3）数据库系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
应用/数据库服务器-Tomcat	（1）中间件根据安全策略要求对特权用户及宿主管理用户进行分离； （2）中间件管理不存在多个管理级别高的特权用户； （3）中间件管理按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
应用/数据库服务器-MSSQL	（1）数据库系统开启审计功能，审计进程正常； （2）审计覆盖所有用户操作审计和记录。
应用/数据库服务器-Tomcat	（1）中间件开启审计功能，审计进程正常； （2）系统的日志审计级别满足要求。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
应用/数据库服务器-MSSQL	（1）数据库宿主系统日期、时间正常； （2）数据库系统审计记录内容基本完整。
应用/数据库服务器-Tomcat	（1）中间件日期、时间正常； （2）中间件审计记录开启审核策略且日志级别正常。
c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
应用/数据库服务器-MSSQL	（1）数据库系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）数据库系统针对日志、审计记录具备充足的存储容量； （3）MS_SQL数据库系统日志文件安装路径下的log文件（\SQL Server\MSSQLMSSQLSERVER\MSSQL\Log\ERRORLOG）everyone用户没有写权限； （4）日志及审计记录保存大于6个月。
应用/数据库服务器-Tomcat	（1）中间件限制审计文件的访问控制权限，普通用户不可删除及修改； （2）宿主系统针对中间件日志、审计记录具备充足的存储容量； （3）对中间件审计记录进行定期存档备份，其备份策略有效；

	（4）审计记录及日志保存大于6个月。
入侵防范	
c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
应用/数据库服务器-MSSQL	（1）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	
应用/数据库服务器-Tomcat	（1）中间件管理具备数据有效性检验功能； （2）中间件管理的校验接口范围较全面。
e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
应用/数据库服务器-MSSQL	（1）数据库系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）补丁安装前进行安全性和兼容性测试； （3）在系统上线或发生重大变更时测试并安装数据库安全补丁； （4）MS_SQL分离默认安装的示例数据库； （5）数据库系统进行渗透及扫描未发现存在可造成高风险的漏洞。
应用/数据库服务器-Tomcat	（1）中间件已根据需要不定期地对已发布的版本进行更新； （2）中间件更新安装前进行安全性和兼容性测试； （3）在系统上线或发生重大变更时测试并安装最新的中间件版本或更新补丁； （4）在不影响业务系统正常运行情况下，对发现的中间件漏洞在确保安全的情况下进行修补； （5）中间件进行扫描未发现存在可造成高风险的漏洞。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
应用/数据库服务器-MSSQL	鉴别数据、重要配置数据： （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。
应用/数据库服务器-Tomcat	鉴别数据、重要配置数据： （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a）应提供重要数据的本地数据备份与恢复功能；	
应用/数据库服务器-MSSQL	（1）数据库系统定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）数据库系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
应用/数据库服务器-Tomcat	（1）中间件系统定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）中间件系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）中间件系统的备份周期为：每天一次增量、每月一次全备； （5）中间件系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。

剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	
应用/数据库服务器-MSSQL	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）数据库系统不保存终端历史记录； （3）MS_SQL引用产品测试结果，信息删除后可法保证完全清除。
应用/数据库服务器-Tomcat	（1）宿主系统具有清除用户鉴别信息的功能； （2）经测试，宿主系统退出后无法访问先前中间件登录过的页面； （3）经测试，宿主系统关闭后无残留的中间件用户鉴别信息。
个人信息保护	
a）应仅采集和保存业务必需的用户个人信息；	
应用/数据库服务器-MSSQL	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）数据库存储的用户个人信息均为业务应用必需的环节。
b）应禁止未授权访问和非法使用用户个人信息。	
应用/数据库服务器-MSSQL	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； （2）数据库具备控制措施禁止未授权访问用户个人信息表单； （3）数据库具备控制措施禁止非法使用用户个人信息表单。

3.4.4.2 主要安全问题汇总分析

安全通用要求

（1）未能提供数据库系统重要数据的异地定时数据备份功能（如：应用/数据库服务器-MSSQL）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供，使企业的经济利益或声誉受到损害。 中风险。

3.4.5 业务应用系统/平台

3.4.5.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
科研创新信息化管理系统	（1）系统对各登录模式均启用身份鉴别； （2）系统对登录管理的用户进行身份鉴别； （3）系统登录用户设置的身份标识具有唯一性； （4）系统不存在空口令用户； （5）设备配置合规的密码策略。

b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
科研创新信息化管理系统	（1）系统启用合规登录失败处理策略； （2）系统配置合规的操作超时退出措施。
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
科研创新信息化管理系统	(1)应用系统的用户鉴别数据采用SHA-512算法在可控网络环境中传输; （2）系统配置合规的远程管理模式。
访问控制	
a) 应对登录的用户分配账户和权限；	
科研创新信息化管理系统	（1）可提供系统权限分配表； （2）登录系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需分配不同的用户权限，不存在所有用户均属于管理级别、高权限的情况。
b) 应重命名或删除默认账户，修改默认账户的默认口令；	
科研创新信息化管理系统	（1）系统禁用默认账户名； （2）系统账户口令设置合规。
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
科研创新信息化管理系统	（1）系统不存在多余或过期账户； （2）系统管理员用户与账户之间一一对应。
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	
科研创新信息化管理系统	（1）系统不存在多个管理级别高的特权用户； （2）系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
科研创新信息化管理系统	（1）系统开启审计功能，审计进程正常； (2)系统的日志审计级别满足要求,审计覆盖所有用户操作审计和记录。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
科研创新信息化管理系统	（1）系统日期、时间正常； （2）系统审计记录内容基本完整。
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
科研创新信息化管理系统	（1）系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）系统针对日志、审计记录具备充足的存储容量； （3）审计记录及日志保存大于6个月。
入侵防范	
c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
科研创新信息化管理系统	（1）系统自身设定有效的终端访问策略，通过访问措施进行管理地址的限制。
d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	
科研创新信息化管理系统	（1）系统具备数据有效性检验功能； （2）系统的校验接口范围较全面。

e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
科研创新信息化管理系统	(1) 系统已根据需要不定期地对已发布的版本进行更新； (2) 在系统上线或发生重大变更时测试并安装最新的版本或更新补丁； (3) 在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
科研创新信息化管理系统	鉴别数据、重要配置数据: (1) 系统在通信传输过程中对相关数据采取完整性保护措施； (2) 系统对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
科研创新信息化管理系统	(1) 系统定义了相关需要备份重要数据； (2) 单位具备合理的重要数据的备份策略规范； (3) 系统定期完全依照备份策略，采用正确的配置进行本地备份； (4) 系统的备份周期合理：每天增量一次、每月全备一次； (5) 系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	
科研创新信息化管理系统	(1) 系统具有清除用户鉴别信息的功能； (2) 经测试，系统退出后无法访问先前登录过的页面； (3) 经测试，系统关闭后无残留的用户鉴别信息。
个人信息保护	
a) 应仅采集和保存业务必需的用户个人信息；	
科研创新信息化管理系统	(1) 单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； (2) 系统按管理规范，仅最小化采集必需的用户个人信息； (3) 系统采集的用户个人信息均为业务应用必需的环节。
b) 应禁止未授权访问和非法使用用户个人信息。	
科研创新信息化管理系统	(1) 系统不采集和保存任何形式的用户个人信息； (2) 系统对所有涉及个人信息的环节均有明确的授权同意过程； (3) 系统具备控制措施禁止未授权访问用户个人信息； (4) 系统具备控制措施禁止非法使用用户个人信息。

3.4.5.2 主要安全问题汇总分析

安全通用要求

（1）未能提供应用软件系统重要数据的异地定时数据备份功能（如：科研创新信息化管理系统）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

3.4.6 数据资源

3.4.6.1 已有安全控制措施汇总分析

安全通用要求

数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
重要业务数据 重要个人信息	（1）系统在通信传输过程中对相关数据采取完整性保护措施； （2）系统对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
重要业务数据 重要个人信息	（1）系统定义了相关需要备份重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
个人信息保护	
a) 应仅采集和保存业务必需的用户个人信息；	
重要个人信息	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息； （3）系统采集的用户个人信息均为业务应用必需的环节。
b) 应禁止未授权访问和非法使用用户个人信息。	
重要个人信息	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； （2）系统具备控制措施禁止未授权访问用户个人信息； （3）系统具备控制措施禁止非法使用用户个人信息。

3.4.6.2 主要安全问题汇总分析

安全通用要求

重要业务数据

（1）未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要业务数据）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

重要个人信息

（1）未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要个人信息）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

3.4.7 其他系统或设备

3.4.7.1 已有安全控制措施汇总分析

安全通用要求

无其他系统或设备，不涉及相关测评

3.4.7.2 主要安全问题汇总分析

安全通用要求

无其他系统或设备，不涉及相关测评

3.5 安全管理中心

3.5.1 已有安全控制措施汇总分析

安全通用要求

系统管理	
a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；	
管理中心	（1）网络中部署运维安全管理系统实现集中的系统管理； （2）系统对登录用户进行身份鉴别； （3）系统用户标识具有唯一性； （4）系统可实现对账户的身份鉴别数据进行保密性和完整性保护； （5）系统管理操作模式具备控制措施； （6）系统具备相应的管理操作审计措施。

审计管理	
a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；	
管理中心	（1）网络中部署运维安全管理系统实现集中安全审计功能； （2）审计系统对审计管理员进行身份鉴别； （3）审计系统用户标识具有唯一性； （4）审计系统管理操作模式具备控制措施； （5）审计系统具备相应的管理操作审计措施。
b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	
管理中心	科研创新信息化管理系统: （1）审计管理员定期对审计记录进行分析，对发现的安全可疑事件及时处理； （2）单位具有安全审计策略文件，规范审计记录的存储、管理和查询要求； （3）审计管理员按规范要求对审计记录进行管理。 重要审计数据: 日志审计系统、运维安全管理系统: （1）设备在通信传输过程中对相关数据采取完整性保护措施； （2）设备对重要数据在传输过程中采取必要的完整性保护措施。

3.5.2 主要安全问题汇总分析

安全通用要求

（1）系统管理的资源、运行及配置管理不够全面（如：管理中心）。系统的资源和运行缺少统一的管理，将导致系统可能无法按规划实现基于资源配置、 系统加载、异常处理、及备份/恢复等的安全控制措施。 低风险。

3.6 安全管理制度

3.6.1 已有安全控制措施汇总分析

安全通用要求

安全策略
应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。

制度文件、执行/记录文件	（1）单位具有网络安全工作的总体方针和安全策略文件； （2）制度内容包括明确的单位安全工作要求； （3）管理文件详见《信息安全总体策略》。
管理制度	
a）应对安全管理活动中的主要管理内容建立安全管理制度；	
制度文件、执行/记录文件	（1）单位有针对安全管理活动中的各类管理内容建立安全管理制度； （2）现有制度已覆盖管理活动的主要的方面； （3）制度详见：《信息安全总体策略》、《网络安全管理规范》、《组织安全结构和人员职责制度》、《人员管理制度》、《员工考核管理制度》。
b）应对管理人员或操作人员执行的日常管理操作建立操作规程。	
制度文件、执行/记录文件	（1）单位针对相关业务日常管理的操作建立规程类管理制度； （2）现有制度已覆盖重要管理方面的系统维护手册和用户操作规程等； （3）管理文件详见《设备及系统软件配置和操作手册》。
制定和发布	
a）应指定或授权专门的部门或人员负责安全管理制度的制定；	
制度文件、执行/记录文件	（1）单位针对安全管理制度的制定，指定教育信息与网络中心部主要负责； （2）在已制定的相关制度中可查阅到被授权制定管理制度的部门/人员信息； （3）管理文件详见《安全管理组织规范》。
b）安全管理制度应通过正式、有效的方式发布，并进行版本控制。	
制度文件、执行/记录文件	（1）单位针对制度的制定和发布要求，制定管理规范文件； （2）管理规范文件对文件制定及发布定义了规范要求； （3）安全管理制度的收发登记记录有效； （4）管理文件详见《制度制定、发布、评审和修订管理制度》、《收发文登记记录》。
评审和修订	
应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	
制度文件、执行/记录文件	（1）单位针对制度的合理性和适用性需进行论证和审定及修订的要求，制定管理规范文件； （2）管理规范文件对制度的评审及修订定义了规范要求； （3）单位具有安全管理制度的审定或论证的过程记录； （4）单位对做过修订的制度，具备有修订版本的安全管理过程记录； （5）管理文件详见《制度制定、发布、评审和修订管理制度》及 《安全管理制度评审记录》。

3.6.2 主要安全问题汇总分析

安全通用要求

科研创新信息化管理系统针对安全管理制度层面的安全通用要求采取的安全措施比较完善，未发现不符合项。

3.7 安全管理机构

3.7.1 已有安全控制措施汇总分析

安全通用要求

岗位设置	
a) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；	
制度文件、执行/记录文件	（1）单位已明确网络安全管理工作的职能部门，并明确了各岗位职责； （2）单位各部门职责文档已明确网络安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备网络安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。
b) 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。	
制度文件、执行/记录文件	（1）单位已明确系统安全管理工作的职能部门，并明确了各岗位职责； （2）单位各部门职责文档已明确系统安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备系统安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。
人员配备	
应配备一定数量的系统管理员、审计管理员和安全管理员等。	
制度文件、执行/记录文件	（1）单位针对人员配备要求，制定了管理制度； （2）单位按要求配备一定数量的重要岗位管理人员； （3）单位针对各岗位人员，制定并维护人员档案； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。
授权和审批	
a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；	
制度文件、执行/记录文件	(1)单位在制度中用文字描述或在流程图中明确,对关键活动进行审批； （2）单位对审批过程明确审批权限，对各项信息系统的重要操作与变更明确审批部门和批准人； （3）管理文件详见《授权和审批管理规定》。
b) 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。	
制度文件、执行/记录文件	（1）单位针对各项业务操作及变更等建立了审批程序规定；

	（2）单位针对系统变更、系统接入、物理范围等事项已明确按审批程序执行，记录有批准人签字； （3）管理文件详见《授权和审批管理规定》。
沟通和合作	
a）应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；	
制度文件、执行/记录文件	（1）单位针对机构内部管理人员之间、部门之间的沟通与合作，制定了管理制度； （2）单位的管理制度规范了合作和沟通的方式和周期； （3）单位有组织机构内部人员联系表； （4）单位有定期召开信息安全会议，保存有会议纪要； （5）管理文件详见《安全教育和培训制度》、《技能培训记录》《外部联系表》。
b）应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；	
制度文件、执行/记录文件	（1）单位针对加强与外部单位的合作与沟通，制定了管理制度规定； （2）单位能按要求与相关单位保持沟通合作，并提供相关单位联系方式和交流会议纪要； （3）管理文件详见《安全教育和培训制度》、《技能培训记录》、《外部联系表》。
c）应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	
制度文件、执行/记录文件	（1）单位建立了完善的对外联单位的联系列表； （2）管理文件详见《外部联系表》。

3.7.2 主要安全问题汇总分析

安全通用要求

（1）单位开展的检查工作不够完善（如：制度文件、执行/记录文件）。检查工作开展不仔细，可能对存在或潜在的安全风险不能被及时发现并进行处理。 低风险。

3.8 安全管理人员

3.8.1 已有安全控制措施汇总分析

安全通用要求

人员录用	
a）应指定或授权专门的部门或人员负责人员录用；	
制度文件、执行/记录文件	（1）单位授权专门的部门负责人员录用工作，制定了管理制度规范； （2）由人力资源保障科负责人员录用工作； （3）管理文件详见《人员管理制度》。

b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查。	
制度文件、执行/记录文件	(1) 单位针对人员录用过程，制定了明确要求，并形成人员安全管理制度； (2) 单位现有管理制度明确说明录用人员应具备的条件； (3) 单位按规定执行人员录用的相关审查过程； (4) 管理文件详见《人员管理制度》、《人员入职考核记录》。
人员离岗	
应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。	
制度文件、执行/记录文件	(1) 单位针对离岗人员权限终止及取回机构提供的各种设施的要求，制定了管理制度； (2) 单位按规范开展对离岗人员的相关管理工作； (3) 管理文件详见《人员管理度》、《人员离岗申请表》、《离场信息资料交接表》。
安全意识教育和培训	
应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。	
制度文件、执行/记录文件	(1) 单位针对人员安全培训及责任和惩戒措施，制定了管理制度； (2) 单位已开展安全意识教育及岗位技能培训。 (3) 管理文件详见《安全教育和培训制度》。
外部人员访问管理	
a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；	
制度文件、执行/记录文件	(1) 单位针对外部人员物理访问，制定了外部人员访问管理文档； (2) 单位具备有效的外部人员访问重要区域的书面申请文档； (3) 单位具备外部人员访问重要区域的登记记录； (4) 管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。
b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；	
制度文件、执行/记录文件	(1) 单位针对外部接入受控网络访问系统，制定了管理制度； (2) 单位具备外部人员接入受控网络前的申请审批流程； (3) 单位具备外部人员接入及访问系统的书面申请文档； (4) 单位具备外部人员接入及访问系统的登记记录； (5) 管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。

3.8.2 主要安全问题汇总分析

安全通用要求

（1）单位未完全按管理规范开展人员离场后的清理工作（如：制度文件、执行/记录文件）。人员离场后的清理工作开展不规范，可能导致遗留外部人员访问受控区域的记录，存在被二次非法利用，造成泄密。 低风险。

3.9 安全建设管理

3.9.1 已有安全控制措施汇总分析

安全通用要求

定级和备案	
a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；	
制度文件、执行/记录文件	（1）单位的被测系统于2022年4月已完成备案； （2）系统备案相关文档（定级报告）中明确等级划分方法和理由，SAG三个方面的级别描述清晰； （3）管理文件详见《定级备案》。
b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；	
制度文件、执行/记录文件	(1)单位针对系统定级结果的审批及评审工作等要求,制定了管理制度; （2）现有系统的定级已具备合理性和正确性审定； （3）管理文件详见《定级备案》。
c) 应保证定级结果经过相关部门的批准；	
制度文件、执行/记录文件	（1）单位针对系统定级结果的上级批准要求，制定了管理制度； （2）现有系统的定级获得了相关部门的批准； （3）管理文件详见《定级备案》。
d) 应将备案材料报主管部门和相应公安机关备案。	
制度文件、执行/记录文件	（1）单位对被测系统的等级备案表、定级报告等备案材料已经报相应公安机关备案； （2）单位具备公安机关出具的备案号； （3）管理文件详见《定级备案》。
产品采购和使用	
a) 应确保网络安全产品采购和使用符合国家的有关规定；	
制度文件、执行/记录文件	（1）单位已建立安全产品管理的相关管理规定； （2）单位具备安全产品采购流程及相关实施文档； （3）被测系统使用的安全产品具备销售许可资质； （4）安全产品具均为国内产品； （5）管理文件详见《设备安全管理制度》。
b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。	
制度文件、执行/记录文件	（1）单位已建立密码产品与服务管理的相关管理制度； （2）系统未使用密码产品； （3）管理文件详见《设备安全管理制度》。
外包软件开发	

b) 应保证开发单位提供软件设计文档和使用指南。	
制度文件、执行/记录文件	(1) 单位制定软件开发项目验收要求，明确开发单位的提交材料； (2) 开发单位提供软件日常维护和使用所需的文档； (3) 管理文件详见《外包开发软件管理规定》、《设备及系统软件配置和操作手册》。
工程实施	
a) 应指定或授权专门的部门或人员负责工程实施过程的管理；	
制度文件、执行/记录文件	(1) 单位针对专门的部门负责工程实施过程的管理要求，制定管理度； (2) 单位由专岗负责系统建设的工程实施，且按照实施方案的要求对进度和质量进行控制； (3) 管理文件详见《工程实施管理制度》。
b) 应制定安全工程实施方案控制工程实施过程。	
制度文件、执行/记录文件	(1) 单位制定了详细的工程实施方案； (2) 工程实施单位严格按照方案执行，并有过程记录； (3) 管理文件详见《测试及验收方案》、《工程项目实施方案》。
系统交付	
a) 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；	
制度文件、执行/记录文件	(1) 单位具备系统交付清单； (2) 系统交付清单内容较详细； (3) 单位的清点工作较合规； (4) 管理文件详见《系统交付管理》、《资产清单》。
b) 应对负责运行维护的技术人员进行相应的技能培训；	
制度文件、执行/记录文件	(1) 单位已对负责系统运行维护的技术人员进行了技能培训； (2) 具备运维人员的培训记录； (3) 管理文件详见《系统交付管理》、《资产清单》、《系统交付清单》、《技能培训记录》。
c) 应提供建设过程文档和运行维护文档。	
制度文件、执行/记录文件	(1) 单位提供了系统建设过程中的文档； (2) 单位提供了指导用户进行系统运维的文档和系统培训手册； (3) 管理文件详见《系统交付管理》、《系统交付清单》、《设备及系统软件配置和操作手册》。
等级测评	
a) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；	
制度文件、执行/记录文件	(1) 单位针对系统等级测评要求，制定管理制度； (2) 系统按要求开展首次测评工作； (3) 管理文件详见《系统安全管理制度》。
b) 应在发生重大变更或级别发生变化时进行等级测评；	
制度文件、执行/记录文件	(1) 管理制度中已规定在系统发生变更时及时对系统进行等级测评； (2) 系统未发生过重大变更，系统等级未发生变化； (3) 管理文件详见《系统安全管理制度》。
c) 应确保测评机构的选择符合国家有关规定。	
制度文件、执行/记录文件	(1) 已选择在“全国等级保护测评机构推荐目录”中的测评单位进行等级测评； (2) 管理文件详见《系统安全管理制度》、《网络安全等级保护测评服

	务合同》。
服务供应商选择	
a) 应确保服务供应商的选择符合国家的有关规定；	
制度文件、执行/记录文件	（1）单位在管理制度内明确提出安全服务供应商选择的要求； （2）单位选择的安全服务商符合国家的有关规定，具备相应的安全服务资质； （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。
b) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。	
制度文件、执行/记录文件	（1）单位的管理制度中已规定，需与安全服务商签订安全相关的协议并明确整个服务供应链各方需履行的网络安全相关义务； （2）单位已按规定与选定的安全服务商签订合规的协议； （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。

3.9.2 主要安全问题汇总分析

安全通用要求

（1）单位未具备适用于被测系统的安全规划设计方案（如：制度文件、执行/记录文件）。规划设计需求不全面，可能导致安全方案设计不完善，信息系统存在安全缺陷。低风险。

（2）单位未具备完整的安全设计方案相关的文档。单位相关方案的设计的内容不够完善（如：制度文件、执行/记录文件）。相关合规的规划配套文件缺失，可能导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。 中风险。

（3）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定。单位未对相关论证过程及内容进行完整的记录（如：制度文件、执行/记录文件）。未开展规范的审批过程，可能存在安全整体规划缺乏合理性和可行性，导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。 低风险。

（4）单位未在软件开发过程中对所有软件安全性进行测试。单位未在软件安装之前按要求对所有软件开展恶意代码检测（如：制度文件、执行/记录文件）。软件交付

前恶意代码检测不规范，可能在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。 低风险。

（5）单位未完全根据测试验收方案组织相关部门和人员开展验收工作（如：制度文件、执行/记录文件）。可能由于验收测试不严谨，造成测试过程缺乏计划性及操作性，无法保证经过测试验收的系统达到既定的安全性等目标。 低风险。

(6)针对系统上线前的安全性测试工作存在问题(如:制度文件、执行/记录文件)。未按规定开展上线前测试，安全隐患可能在系统上线运行前未被发现并作出相应处理。低风险。

3.10 安全运维管理

3.10.1 已有安全控制措施汇总分析

安全通用要求

环境管理	
a) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；	
制度文件、执行/记录文件	（1）单位建立机房安全方面的管理制度，对有关运维方面的管理作出规定； （2）单位具备完整的机房出入登记记录； （3）单位具备完整的机房基础设施的维护记录； （4）管理文件详见《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。
b) 应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；	
制度文件、执行/记录文件	（1）单位建立机房安全方面的管理制度； （2）单位现有机房管理记录与制度相符； （3）制度详见：《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。
c) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	
制度文件、执行/记录文件	（1）单位机房安全管理制度已明确来访人员的接待区域的要求； （2）单位按规范要求开展人员来访接待； （3）单位办公环境未发现有随意放置含有敏感信息介质的情况； （4）制度详见：《机房安全管理制度》、《物理安全管理规范》、《办

	公环境保密管理》。
资产管理	
应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。	
制度文件、执行/记录文件	（1）单位已建立有效的资产清单； （2）单位现有资产清单内容较全面； （3）制度详见：《设备安全管理制度》、《资产清单》。
介质管理	
a）应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；	
制度文件、执行/记录文件	（1）介质按管理要求放置于受控的环境中（如：机房）； （2）介质管理具备较全面的记录； （3）制度详见：《设备安全管理制度》、《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。
b）应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。	
制度文件、执行/记录文件	（1）介质管理制度中对介质安全传输有明确规定； （2）存储重要信息的介质在物理传输过程，具备严格的环节控制，无重大环节疏漏； （3）对介质的归档和查询均具备记录； （4）制度详见：《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。
设备维护管理	
a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	
制度文件、执行/记录文件	（1）单位人员岗位职责相关文档已明确设备维护管理的责任部门； （2）单位对各类设施、设备进行定期维护； （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。
b）应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。	
制度文件、执行/记录文件	（1）单位建立了配套设施、软硬件维护管理方面的管理制度； （2）单位开展相关工作与制度相符，且保留记录； （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。
网络和系统安全管理	
a）应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；	
制度文件、执行/记录文件	（1）单位建立系统安全管理文档，对系统管理员的管理制定了要求； （2）单位对各类关键角色建立了相应的工作职责文档； （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。
b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	
制度文件、执行/记录文件	（1）单位制定管理制度，对系统账号进行管理； （2）单位按管理规范开展账号管理工作；

	（3）账户管理记录内容较完整； （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。
c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	
制度文件、执行/记录文件	（1）单位建立了网络和系统安全管理制度； （2）网络和系统安全管理制度内容较全面； （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。
d）应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；	
制度文件、执行/记录文件	（1）单位对重要设备、系统的配置和操作建立配置手册； （2）现有操作配置手册已明确操作步骤、参数配置； （3）制度详见：《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。
e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。	
制度文件、执行/记录文件	（1）单位制定日常运维管理的相关制度规范； （2）单位按制度规范开展日常运维管理工作； （3）单位具备合规的运维记录； （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》、《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。
恶意代码防范管理	
a）应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	
制度文件、执行/记录文件	（1）单位制定恶意代码防范管理制度，明确对外来计算机或存储设备接入系统前进行恶意代码检查； （2）单位按外来计算机接入恶意代码检查规范开展工作； （3）单位制定培训管理制度，明确需通过培训提升员工的防恶意代码意识； （4）单位按培训管理要求开展工作； （5）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申请表》、《信息管理系统漏洞检查表》。
b）应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；	
制度文件、执行/记录文件	（1）建立恶意代码防范管理文档； （2）管理制度中覆盖防恶意代码软件的授权使用、恶意代码库升级、定期查杀等内容； （3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》。
配置管理	
应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。	
制度文件、执行/记录文件	（1）单位制定了基本配置信息管理的制度要求； （2）管理文件详见：《主机安全管理规范》、《网络安全管理规范》、《应用安全管理规范》、《网络配置信息》。
变更管理	

应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。	
制度文件、执行/记录文件	（1）单位建立了关于系统变更管理的制度文件； （2）现有变更管理制度覆盖了变更管理的各方面要求； （3）制度详见：《变更控制管理制度》、《通用变更记录表》。
备份与恢复管理	
a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；	
制度文件、执行/记录文件	（1）单位根据业务重要程度，制定了需要定期备份的重要业务信息列表或清单。清单内需要定期备份的重要数据已经过用户方确认； （2）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。
b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等；	
制度文件、执行/记录文件	（1）单位建立了备份与恢复管理相关的安全管理制度； （2）备份与恢复管理的相关要求比较明确； （3）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。
c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	
制度文件、执行/记录文件	（1）单位现有管理制度，明确了数据备份策略和数据恢复策略，以及备份程序和恢复程序； （2）单位可按策略要求实现重要数据的定期备份与恢复性测试； （3）单位现有的备份的数据均经过恢复性测试，可确保备份的数据可用； （4）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。
安全事件处置	
a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件；	
制度文件、执行/记录文件	（1）单位已在安全培训及宣传过程中告知用户在发现安全弱点和可疑事件时及时向安全管理部门报告； （2）单位在系统运维过程中对发现的安全弱点和可疑事件均编制了对应的报告或相关文档； （3）单位现有安全弱点和可疑事件报告文档内容较详实； （4）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。
b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；	
制度文件、执行/记录文件	（1）单位制定了安全事件报告和处置管理制度； （2）现有安全事件管理制度内容较完整； （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。
c) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。	
制度文件、执行/记录文件	（1）单位具备对安全事件的分析、处理、总结、防范等的报告／过程文档； （2）单位提供的安全事件报告和响应处置记录内容较完整； （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。
应急预案管理	
a) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；	

制度文件、执行/记录文件	（1）单位制定重要事件的应急预案； （2）单位现有应急预案涉及的类型范围较全面； （3）单位现有应急预案的内容较完整； （4）制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。
b）应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。	
制度文件、执行/记录文件	（1）单位定期对相关人员进行应急预案培训； （2）单位根据不同的应急预案，按要求进行应急演练； （3）单位具备近期应急预案工作开展的相关记录； （4）单位提供的应急预案培训记录比较完整； （5）单位提供的应急预案演练记录比较完整； （6）经检查单位目前一旦出现应急事件，可参照预案合理有序的进行应急事件处置过程； （7）制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。

3.10.2 主要安全问题汇总分析

安全通用要求

（1）单位未严格按规范开展漏洞及安全隐患检测工作（如：制度文件、执行/记录文件）。漏洞检测、修补工作不到位，可能存在未授权人员利用漏洞攻击信息系统的风险。 低风险。

（2）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作（如：制度文件、执行/记录文件）。可能导致系统恶意代码检测管理不到位，存在信息系统感染恶意代码，从而导致严重的信息安全风险。 低风险。

（3）单位不了解现有密码相关的国家标准和行业标准。单位缺乏密码管理要求的制度文档（如：制度文件、执行/记录文件）。密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不到位，存在违反国家政策的风险。 中风险。

3.11 其他安全要求指标

3.11.1 已有安全控制措施汇总分析

本次测评未涉及其他安全要求指标。

3.11.2 主要安全问题汇总分析

本次测评未涉及其他安全要求指标。

3.12 验证测试

验证测试包括漏洞扫描，渗透测试等，验证测试发现的安全问题对应到相应的测评项的结果记录中。详细验证测试报告见报告附录。

3.12.1 漏洞扫描

3.12.1.1 漏洞扫描结果统计

本次测评主要使用了[绿盟远程安全评估系统]对系统的设备进行了安全扫描，其所涉及的系统版本为：[V6.0R04F01SP06]，规则库版本为：[V6.0R02F01.2900]。扫描结果如下：

经分析统计，共发现各接入点存在2类漏洞，其中0类危险程度为高的漏洞，0类危害程度为中的漏洞，2类危害程度为低的漏洞。

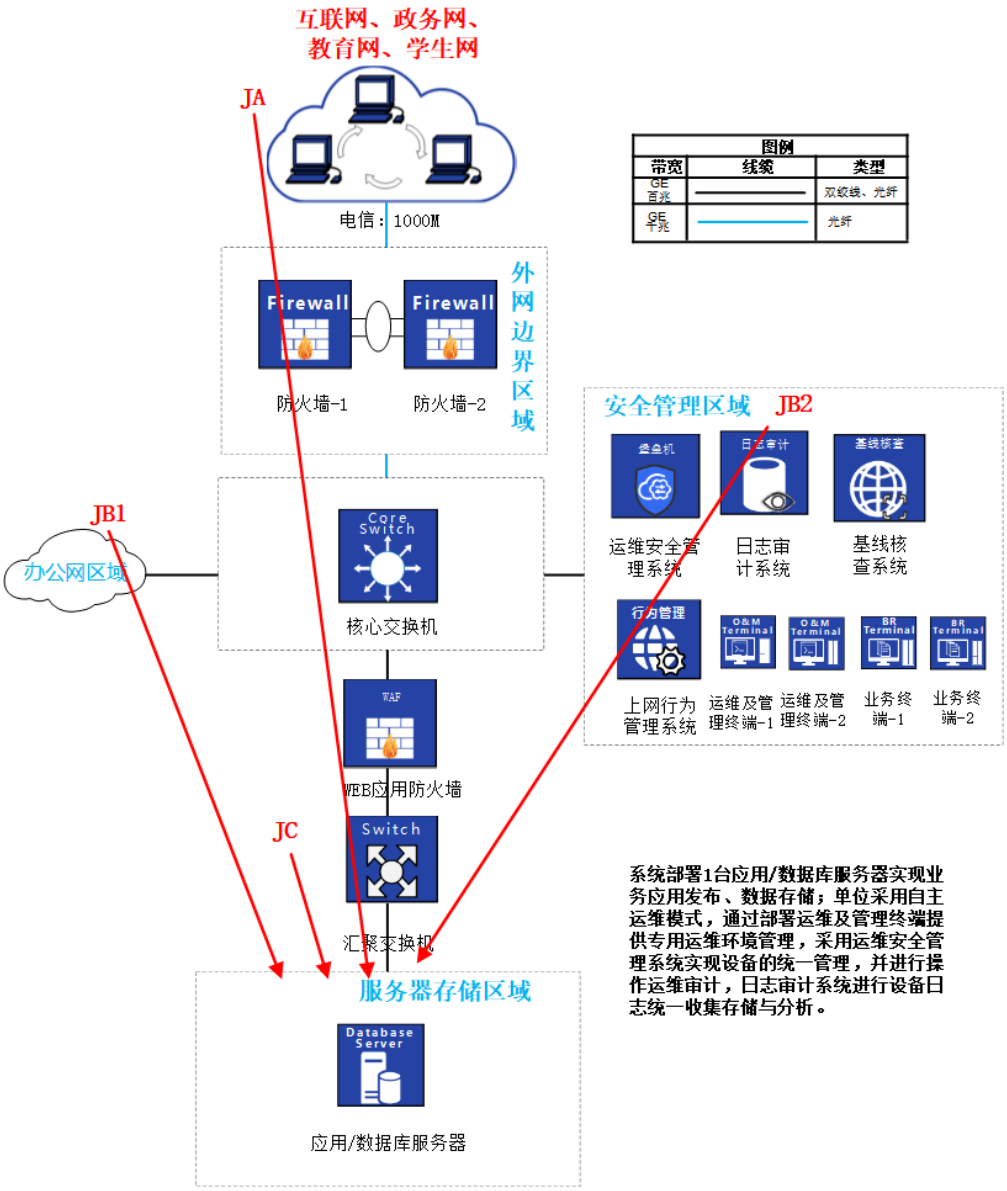


图 3-1 漏洞扫描工具接入测试示意图

接入点JA：在防火墙外侧接入，开展扫描/渗透主要目的是，探测对外服务功能区上各服务器、应用系统对外部网络边界暴露的安全漏洞情况，并根据漏洞扫描的结果接入渗透测试工具集，试图利用服务器、应用的安全漏洞入侵网络的行为。

接入点JB：在办公网区域VLAN段、安全管理区域VLAN段接入，开展扫描/渗透主要目的是，模拟外联单位/内部恶意用户发现操作系统、数据库、Web应用、第三方产品等安全漏洞的过程，并尝试利用以上漏洞实施诸如获取系统控制权（GetShell）、获得大量敏感信息（DragLibrary）等模拟攻击行为。

接入点JC：在系统所在VLAN的交换机接入，开展扫描/渗透主要目的是，直接测试对服务功能区上各服务器在最小化防御的基础上，对网络暴露的安全漏洞情况。

（1）接入点A漏洞扫描结果统计

根据在接入点A对14台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-1 接入点 A 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	0	0	0	0
2	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	0	0	0	0
3	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	0	0	0	0
4	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	0	0	0	0
5	172.16.1.14/上网行为管理系统	(安全设备)深信服 AC12.0.26	0	0	0	0
6	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	0	0	0	0
7	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	0	0	0	0
8	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	0	0	0	0
9	192.168.33.11/业务终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
10	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
11	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
12	192.168.33.10/业务终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
13	10.2.4.10/应用/数据库服务器	(服务器存储设备)Windows Server 2012 R2	0	0	0	0
14	https://ky.mmpt.edu.cn/科研创新信息化管理系统	(业务应用软件平台) V6.0	0	0	0	0
安全漏洞数量小计			10	0	0	10

（2）接入点B漏洞扫描结果统计

根据在接入点B对14台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-2 接入点 B 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	1	0	0	1
2	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	1	0	0	1
3	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	1	0	0	1
4	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	2	0	0	2
5	172.16.1.14/上网行为管理系统	(安全设备)深信服 AC12.0.26	1	0	0	1
6	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	1	0	0	1
7	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	1	0	0	1
8	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	1	0	0	1
9	192.168.33.11/业务终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
10	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
11	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
12	192.168.33.10/业务终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
13	10.2.4.10/应用/数据库服务器	(服务器存储设备)Windows Server 2012 R2	1	0	0	1
14	https://ky.mmpt.edu.cn/科研创新信息化管理系统	(业务应用软件平台) V6.0	0	0	0	0
安全漏洞数量小计			10	0	0	10

（3）接入点C漏洞扫描结果统计

根据在接入点C对14台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-3 接入点 C 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	1	0	0	1
2	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	1	0	0	1
3	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	1	0	0	1
4	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	2	0	0	2
5	172.16.1.14/上网行为管理系统	(安全设备)深信服 AC12.0.26	1	0	0	1
6	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	1	0	0	1
7	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	1	0	0	1
8	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	1	0	0	1
9	192.168.33.11/业务终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
10	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
11	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
12	192.168.33.10/业务终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
13	10.2.4.10/应用/数据库服务器	(服务器存储设备)Windows Server 2012 R2	1	0	0	1
14	https://ky.mmpt.edu.cn/科研创新信息化管理系统	(业务应用软件平台) V6.0	0	0	0	0
安全漏洞数量小计			10	0	0	10

3.12.1.2 漏洞扫描问题描述

通过对漏洞扫描结果进行分析,科研创新信息化管理系统存在的主要安全漏洞汇总如下表所示

表 3-4 主要安全漏洞汇总表

序号	安全漏洞名称	关联资产/域名	严重程度
1	允许Traceroute探测 此类漏洞涉及网络设备、安全设备、服务器存储设备。	10.2.4.10/应用/数据库服务器 10.2.1.4/运维安全管理系统 10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/上网行为管理系统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/汇聚交换机 172.16.1.2/核心交换机	低
2	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161) 此类漏洞涉及网络设备。	172.16.1.2/核心交换机	低

3.12.2 渗透测试

经分析统计，共发现各接入点存在1类漏洞，其中0类危险程度为高的漏洞，0类危害程度为中的漏洞，1类危害程度为低的漏洞。

3.12.2.1 渗透测试过程说明

方案制定：

在得到委托单位的书面授权许可后，才进行渗透测试的实施。并且将实施范围、方法、时间、人员等具体的方案委托单位进行交流，并得到委托单位的认同。在测试实施之前，会做到让委托单位对渗透测试过程和风险的知晓，使随后的正式测试流程都在委托单位的管控下。

信息收集：

此阶段中，渗透测试人员对目标信息系统进行必要的信息收集，如操作系统类型、开放的端口和服务、中间件信息、后台数据库类型、web开发语言等，即收集有利于漏洞挖掘的相关信息，为渗透测试做准备。

漏洞挖掘方法：

此阶段中，渗透测试人员对目标信息系统开始进行渗透测试，利用已知信息和现有条件及技术进行漏洞挖掘，尽可能发现目标信息系统中存在的所有安全风险，并进行记录。

漏洞利用：

此阶段中，渗透测试人员对目标信息系统对上一阶段漏洞挖掘中发现的漏洞进行必要的利用以证明其危害性，再对渗透测试过程所产生的测试数据进行清除。

输出报告：

此阶段中，渗透测试人员把渗透测试记录、截图等相关信息进行整理，然后撰写渗透测试报告，最终提交给委托单位。

漏洞修复：

此阶段中，委托单位依据收到的渗透测试报告对其中所提出的漏洞进行整改，可参考报告中所提出的修复建议，整改完成后联系本单位相关人员准备回归测试。

回归测试：

此阶段中，渗透测试人员对整改后的目标信息系统进行复测，以确定报告中提出的漏洞是否已被修复，若已被修复，则进入下一阶段；否则，返回上一阶段。

测试工具：

序号	工具	工具用途
1	Burpsuite Pro	用于攻击Web应用程序的集成软件
2	Sqlmap	开源的自动化SQL注入工具

序号	工具	工具用途
3	Nmap	开源的网络发现和安全审计工具
4	OWASP ZAP	自动化Web应用漏洞扫描工具
5	其他测试工具	根据信息系统的类别选择不同的工具（如自写脚本、目录扫描器、木马扫描器、其它开源工具等）

3.12.2.2 渗透测试问题描述

通过渗透测试发现，科研创新信息化管理系统存在的安全问题汇总如下表所示。

表 3-5 渗透测试结果汇总表

序号	安全问题	关联资产/域名	严重程度
1	缺少“X-Content-Type-Options”响应头 此类漏洞涉及业务应用软件平台。	https://ky.mmpt.edu.cn/ 科研创新信息化管理系统	低

3.13 单项测评小结

3.13.1 控制点符合情况汇总

根据单项测评结果汇总控制点符合情况如下表所示。（表格以不同颜色对测评结果进行区分，不符合的安全控制点采用红色标识，部分符合的采用黄色标识，不适用的采用蓝色标识且不做勾选。）

表 3-6 控制点符合情况汇总表

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
1	安全通用要求	安全物理环境	物理位置选择	√		
2			物理访问控制		√	
3			防盗窃和防破坏	√		
4			防雷击	√		
5			防火		√	
6			防水和防潮	√		

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
7			防静电			√
8			温湿度控制	√		
9			电力供应	√		
10			电磁防护	√		
11	安全通用要求	安全通信网络	网络架构		√	
12			通信传输	√		
13			可信验证			√
14	安全通用要求	安全区域边界	边界防护	√		
15			访问控制	√		
16			入侵防范		√	
17			恶意代码和垃圾邮件防范		√	
18			安全审计	√		
19			可信验证			√
20	安全通用要求	安全计算环境	身份鉴别	√		
21			访问控制	√		
22			安全审计	√		
23			入侵防范	√		
24			恶意代码防范	√		
25			可信验证			√
26			数据完整性	√		

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
27			数据备份恢复		√	
28			剩余信息保护	√		
29			个人信息保护	√		
30	安全通用要求	安全管理中心	系统管理		√	
31			审计管理	√		
32	安全通用要求	安全管理制度	安全策略	√		
33			管理制度	√		
34			制定和发布	√		
35			评审和修订	√		
36	安全通用要求	安全管理机构	岗位设置	√		
37			人员配备	√		
38			授权和审批	√		
39			沟通和合作	√		
40			审核和检查		√	
41	安全通用要求	安全管理人员	人员录用	√		
42			人员离岗	√		
43			安全意识教育和培训	√		
44			外部人员访问管理		√	
45	安全通用要求	安全建设管理	定级和备案	√		
46			安全方案设计			√

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
47			产品采购和使用	√		
48			自行软件开发			
49			外包软件开发		√	
50			工程实施	√		
51			测试验收		√	
52			系统交付	√		
53			等级测评	√		
54			服务供应商选择	√		
55	安全通用要求	安全运维管理	环境管理	√		
56			资产管理	√		
57			介质管理	√		
58			设备维护管理	√		
59			漏洞和风险管理			√
60			网络和系统安全管理	√		
61			恶意代码防范管理		√	
62			配置管理	√		
63			密码管理			√
64			变更管理	√		
65			备份与恢复管理	√		
66			安全事件处置	√		

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
67			应急预案管理	√		
68			外包运维管理			
安全通用要求控制点符合情况数量统计				47	12	7
控制点符合情况数量统计				47	12	7

3.13.2 安全问题汇总

针对单项测评结果中存在的部分符合和不符合项进行汇总，形成了安全问题如下表所示。

表 3-7 安全问题汇总表

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T1	（1）机房出入口未配置电子门禁系统。	信息化机房	安全通用要求	安全物理环境	物理访问控制	机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。
T2	（1）机房建设未完全采用符合耐火等级的建筑材料； （2）机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级。	信息化机房	安全通用要求	安全物理环境	防火	b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。
T3	（1）机房内缺乏防静电措施（如防静电地板或铺设防静电地毯）。	信息化机房	安全通用要求	安全物理环境	防静电	应采用防静电地板或地面并采用必要的接地防静电措施。
T4	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	安全通用要求	安全通信网络	网络架构	a）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
T5	（1）缺乏对通信设备可信验证方面的安全设计要求； （2）现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况。	安全通信网络	安全通用要求	安全通信网络	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
						形成审计记录送至安全管理中心。
T6	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	安全通用要求	安全区域边界	入侵防范	应在关键网络节点处监视网络攻击行为。
T7	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	安全通用要求	安全区域边界	恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。
T8	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	办公网区域 外网边界区域 安全管理区域 服务器存储区域	安全通用要求	安全区域边界	可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T9	（1）设备不具备相关可信验证的技术措施。	WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2	安全通用要求	安全计算环境	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T10	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。	业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	安全通用要求	安全计算环境	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
						中心。
T11	（1）未能提供数据库系统重要数据的异地定时数据备份功能。	应用/数据库服务器-MSSQL	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T12	（1）未能提供中间件重要数据的异地定时数据备份功能。	应用/数据库服务器-Tomcat	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T13	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	科研创新信息化管理系统 重要业务数据 重要个人信息	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T14	（1）系统管理的资源、运行及配置管理不够全面。	管理中心	安全通用要求	安全管理中心	系统管理	b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
T15	（1）单位开展的检查工作不够完善。	制度文件、执行/记录文件	安全通用要求	安全管理机构	审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。
T16	（1）单位未完全按管理规范开展人员离场后的清理工作。	制度文件、执行/记录文件	安全通用要求	安全管理人员	外部人员访问管理	c）外部人员离场后应及时清除其所有的访问权限。
T17	（1）单位未具备适用于被测系统的安全规划设计方案。	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
T18	（1）单位未具备完整的安全设计方案相关的文档； （2）单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	b）应根据保护对象的安全保护等级进行安全方案设计；
T19	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； （2）单位未对相关论证过程及内容进行完整的记	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	c）应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
	录。					
T20	（1）单位未在软件开发过程中对所有软件安全性进行测试； （2）单位未在软件安装之前按要求对所有软件开展恶意代码检测。	制度文件、执行/记录文件	安全通用要求	安全建设管理	外包软件开发	a）应在软件交付前检测其中可能存在的恶意代码；
T21	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	安全通用要求	安全建设管理	测试验收	a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；
T22	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	安全通用要求	安全建设管理	测试验收	b）应进行上线前的安全性测试，并出具安全测试报告。
T23	（1）单位未严格按规范开展漏洞及安全隐患检测工作。	制度文件、执行/记录文件	安全通用要求	安全运维管理	漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。
T24	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	安全通用要求	安全运维管理	恶意代码防范管理	c）应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。
T25	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	制度文件、执行/记录文件	安全通用要求	安全运维管理	密码管理	a）应遵循密码相关国家标准和行业标准；

4 整体测评

从安全控制间、区域间和验证测试等方面对单元测评的结果进行验证、分析和整体评价。

具体内容参见《GB/T 28448-2019信息安全技术 网络安全等级保护测评要求》。

4.1 安全控制点间安全测评

安全控制间的安全测评主要考虑同一区域内、同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用。安全功能上的增强和补充可以使两个不同强度、不同等级的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。

4.1.1 安全建设管理

4.1.1.1 安全通用要求

（T21）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。

单位未具备适用于被测系统的安全规划设计方案。安全方案设计不完善，导致规划设计需求不全面，信息系统存在安全缺陷。可升高单位未完全根据测试验收方案组织相关部门和人员开展验收工作的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

（T22）针对系统上线前的安全性测试工作存在问题。

单位未在软件交付之前按要求对所有软件开展恶意代码检测，导致在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。可升高针对系统上线前的安全性测试工作存在问题的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

4.1.2 安全运维管理

4.1.2.1 安全通用要求

（T24）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。

单位未严格按规范开展漏洞及安全隐患检测工作，漏洞检测工作不到位，导致存在未授权人员利用漏洞攻击信息系统的风险。可升高单位未严格按规范要求，针对防范恶

意代码攻击的技术措施的有效性验证，开展工作的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

4.2 区域间安全测评

区域间的安全测评主要考虑互连互通（包括物理上和逻辑上的互连互通等）的不同区域之间存在的安全功能增强、补充和削弱等关联作用，特别是有数据交换的两个不同区域。

4.2.1 安全物理环境

4.2.1.1 安全通用要求

（T1）机房出入口未配置电子门禁系统。

机房所在位置处于内部受控区域，非授权人员无法随意通过现有控制措施（如机械锁）进出机房，且具备相对完善的机房出入管理要求（具备《机房安全管理制度》），并实际执行措施效果良好（具备《机房出入登记表》），可降低机房出入口访问控制措施缺失的问题严重程度（如信息化机房）。根据整体测评分析，问题严重程度变化为降低。

4.2.2 安全通信网络

4.2.2.1 安全通用要求

（T4）关键的应用服务和数据库服务网段未独立进行子网划分的情况。

单位有完整的IP地址规范，对IP地址的使用、回收均有记录《资产清单》，且系统具备相对完善的设备自身访问控制策略管理要求（具备《网络安全管理规范》、《设备及系统软件配置和操作手册》），措施效果良好，有助于部分补充未划分子网的安全功能不足（如安全通信网络）。根据整体测评分析，问题严重程度变化为降低。

4.2.3 安全区域边界

4.2.3.1 安全通用要求

（T6）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。

网络环境划分了相应的安全区域，区域间具备有效的访问控制措施，区域内各主机设备部署深信服EDR单机版，策略库、规则库更新及时，能够对攻击行为进行检测、阻断或限制，实际措施效果良好，且系统具备相对完善的策略库、规则库更新/校准管理要求，管理措施效果良好且及时检查更新有效性（具备《漏洞检测报告》、《主机安全管理规范》），可降低外部网络攻击防御措施缺失的问题严重程度（如办公网区域、安全管理区域）。根据整体测评分析，问题严重程度变化为降低。

（T7）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。

系统部署于可控的网络环境内（具备有效的访问控制、入侵防护措施）限制相关主机对象访问非受控网络，操作系统层面配置防御策略（具备本地防火墙策略、核心交换机地址限制策略、部署深信服EDR单机版），恶意代码入侵的可能性相对较低，可降低恶意代码防范措施缺失的问题严重程度（如办公网区域、安全管理区域）。根据整体测评分析，问题严重程度变化为降低。

4.3 整体测评结果汇总

经整体测评后安全问题严重程度变化情况如下表所示

表 4-1 整体测评结果汇总表

问题编号	安全问题描述	测评对象	整体测评描述	严重程度变化
T1	（1）机房出入口未配置电子门禁系统。	信息化机房	（1）机房所在位置处于内部受控区域，非授权人员无法随意通过现有控制措施（如机械锁）进出机房，且具备相对完善的机房出入管理要求（具备《机房安全管理制度》），	□升高 ☑降低

问题编号	安全问题描述	测评对象	整体测评描述	严重程度变化
			并实际执行措施效果良好（具备《机房出入登记表》），可降低机房出入口访问控制措施缺失的问题严重程度。	
T4	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	（1）单位有完整的IP地址规范，对IP地址的使用、回收均有记录《资产清单》，且系统具备相对完善的设备自身访问控制策略管理要求（具备《网络安全管理规范》、《设备及系统软件配置和操作手册》），措施效果良好，有助于部分补充未划分子网的安全功能不足。	□升高 ☑降低
T6	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	（1）网络环境划分了相应的安全区域，区域间具备有效的访问控制措施，区域内各主机设备部署深信服EDR单机版，策略库、规则库更新及时，能够对攻击行为进行检测、阻断或限制，实际措施效果良好，且系统具备相对完善的策略库、规则库更新/校准管理要求，管理措施效果良好且及时检查更新有效性（具备《漏洞检测报告》、《主机安全管理规范》），可降低外部网络攻击防御措施缺失的问题严重程度。	□升高 ☑降低
T7	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	（1）系统部署于可控的网络环境内（具备有效的访问控制、入侵防护措施）限制相关主机对象访问非受控网络，操作系统层面配置防御策略（具备本地防火墙策略、核心交换机地址限制策略、部署深信服EDR单机版），恶意代码入侵的可能性相对较低，可降低恶意代码防范措施缺失的问题严重程度。	□升高 ☑降低
T21	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	（1）单位未具备适用于被测系统的安全规划设计方案。安全方案设计不完善，导致规划设计需求不全面，信息系统存在安全缺陷。可升高单位未完全根据测试验收方案组织相关部门和人员开展验收工作的问题严重程度。	☑升高 □降低

问题编号	安全问题描述	测评对象	整体测评描述	严重程度变化
T22	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	（1）单位未在软件交付之前按要求对所有软件开展恶意代码检测，导致在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。可升高针对系统上线前的安全性测试工作存在问题的问题严重程度。	☑升高 □降低
T24	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	（1）单位未严格按规范开展漏洞及安全隐患检测工作，漏洞检测工作不到位，导致存在未授权人员利用漏洞攻击信息系统的风险。可升高单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作的问题严重程度。	☑升高 □降低

5 安全问题风险分析

针对等级测评结果中存在的所有安全问题，结合关联资产和威胁分别分析安全问题可能产生的危害结果，找出可能对系统、单位、社会及国家造成的最大安全危害（损失），并根据最大安全危害（损失）的严重程度进一步确定安全问题的风险等级，结果为“高”、“中”或“低”。最大安全危害（损失）结果应结合安全问题所影响业务的重要程度、相关系统组件的重要程度、安全问题严重程度以及安全事件影响范围等进行综合分析。

表 5-1 安全问题风险分析

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
1	安全物理环境	（1）机房出入口未配置电子门禁系统。	信息化机房	物理攻击	（1）上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域，可能对系统的平稳运行造成影响。	中风险
2	安全物理环境	（1）机房建设未完全采用符合耐火等级的建筑材料； （2）机房建设不具备防	信息化机房	物理环境影响	（1）存在发生火情时助燃火灾的风险。	低风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
		火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级。				
3	安全物理环境	（1）机房内缺乏防静电措施（如防静电地板或铺设防静电地毯）。	信息化机房	软硬件故障	（1）存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。	中风险
4	安全通信网络	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	恶意攻击	（1）上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变得更为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。	中风险
5	安全通信网络	（1）缺乏对通信设备可信验证方面的安全设计要求； （2）现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况。	安全通信网络	恶意攻击	（1）缺乏对系统可执行程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致计算资源被干扰和破坏造成损失。	低风险
6	安全区域边界	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	恶意攻击	（1）存在不能及时发现内部主机作为攻击跳板，或网络攻击行为而造成系统损坏/网络资源浪费的风险。	中风险
7	安全区域边界	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	恶意攻击	（1）无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。	中风险
8	安全区域边界	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	办公网区域 外网边界区域 安全管理区域 服务器存储区域	恶意攻击	（1）缺乏对边界设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
9	安全计算环境	（1）设备不具备相关可信验证的技术措施。	WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2	恶意攻击	（1）缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险
10	安全计算环境	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。	业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	恶意攻击	（1）缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险
11	安全计算环境	（1）未能提供数据库系统重要数据的异地定时数据备份功能。	应用/数据库服务器-MSSQL	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供，使企业的经济利益或声誉受到损害。	中风险
12	安全计算环境	（1）未能提供中间件重要数据的异地定时数据备份功能。	应用/数据库服务器-Tomcat	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。	中风险
13	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	科研创新信息化管理系统 重要业务数据 重要个人信息	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。	中风险
14	安全管理中心	（1）系统管理的资源、运行及配置管理不够全面。	管理中心	恶意攻击	（1）系统的资源和运行缺少统一的管理，将导致系统可能无法按规划实现基于资源配置、 系统加载、异常处理、及备份/恢复等的安全控制措施。	低风险
15	安全管理机构	（1）单位开展的检查工作不够完善。	制度文件、执行/记录文件	管理不到位	（1）检查工作开展不仔细，可能对存在或潜在的安全风险不能被及时发现	低风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
					并进行处理。	
16	安全管理人员	（1）单位未完全按管理规范开展人员离场后的清理工作。	制度文件、执行/记录文件	管理不到位	（1）人员离场后的清理工作开展不规范，可能导致遗留外部人员访问受控区域的记录，存在被二次非法利用，造成泄密。	低风险
17	安全建设管理	（1）单位未具备适用于被测系统的安全规划设计方案。	制度文件、执行/记录文件	管理不到位	（1）规划设计需求不全面，可能导致安全方案设计不完善，信息系统存在安全缺陷。	低风险
18	安全建设管理	（1）单位未具备完整的安全设计方案相关的文档； （2）单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	管理不到位	（1）相关合规的规划配套文件缺失，可能导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。	中风险
19	安全建设管理	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； （2）单位未对相关论证过程及内容进行完整的记录。	制度文件、执行/记录文件	管理不到位	（1）未开展规范的审批过程，可能存在安全整体规划缺乏合理性和可行性，导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。	低风险
20	安全建设管理	（1）单位未在软件开发过程中对所有软件安全性进行测试； （2）单位未在软件安装之前按要求对所有软件开展恶意代码检测。	制度文件、执行/记录文件	管理不到位	（1）软件交付前恶意代码检测不规范，可能在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。	低风险
21	安全建设管理	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	管理不到位	（1）可能由于验收测试不严谨，造成测试过程缺乏计划性及操作性，无法保证经过测试验收的系统达到既定的安全性等目标。	低风险
22	安全建设管理	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	管理不到位	（1）未按规定开展上线前测试，安全隐患可能在系统上线运行前未被发现并作出相应处理。	低风险
23	安全运维管理	（1）单位未严格按规范开展漏洞及安全隐患检测工作。	制度文件、执行/记录文件	管理不到位	（1）漏洞检测、修补工作不到位，可能存在未授权人员利用漏洞攻击信息系统的风险。	低风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
24	安全运维管理	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	管理不到位	（1）可能导致系统恶意代码检测管理不到位，存在信息系统感染恶意代码，从而导致严重的信息安全风险。	低风险
25	安全运维管理	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	制度文件、执行/记录文件	管理不到位	（1）密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不到位，存在违反国家政策的风险。	中风险

6 等级测评结论

等级测评结论由安全问题风险分析结果和综合得分共同确定，判定依据如下表所示。

表 6-1 等级测评结论判别依据

测评结论	判别依据
优	被测对象中存在安全问题，但不会导致被测对象面临中、高等级安全风险，且系统综合得分 90 分以上（含90 分）。
良	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分 80分以上（含 80分）。
中	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分 70分以上（含 70分）
差	被测对象中存在安全问题，而且会导致被测对象面临高等级安全风险，或被测对象综合得分低于 70 分。

综合得分计算方法如下：

设M为被测对象的综合得分，$M = V_t + V_m$，V_t和V_m根据下列公式计算。

$$V_t = \begin{cases} 100 \cdot y - \sum_{k=1}^{t} f(\omega_k) \cdot (1 - x_k) \cdot S, & V_t > 0 \\ 0, & V_t \leq 0 \end{cases}$$

$$V_m = \begin{cases} 100 \cdot (1-y) - \sum_{k=1}^{m} f(\omega_k) \cdot (1-x_k) \cdot S, & V_m > 0 \\ 0, & V_m \le 0 \end{cases}$$

$$0 \le x_k \le 1,\ S = 100 \cdot \frac{1}{n},\ f(\omega_k) = \begin{cases} 1, & \omega_k = \text{一般} \\ 2, & \omega_k = \text{重要} \\ 3, & \omega_k = \text{关键} \end{cases}$$

其中，y为关注系数，取值在0至1之间，由等级保护工作管理部门给出，默认值为0.5。n为被测对象涉及的总测评项数（不含不适用项，下同），t为技术方面对应的总测评项数，V_t为技术方面的得分，m为管理方面对应的总测评项数，V_m为管理方面的得分，ω_k为测评项k的重要程度（分为一般、重要和关键），x_k为测评项k的得分，如果测评项k涉及多测评项对象，则x_k取值为多测评对象得分的算术平均值。

x_k的得分计算如下：

测评项k涉及对象 / 测评项k定性判定	只涉及单个对象	涉及多个对象
符合	1	1
部分符合	0.5	计算测评对象平均分，取值在0至1之间
不符合	0	0

注：当测评项k涉及多个对象时，针对每个对象的得分取值为1、0.5和0。

根据第5章安全问题风险分析结果统计高、中、低风险安全问题的数量，利用综合得分计算公式计算出被测对象的综合得分，并将相关结果填入下表。

表 6-2 安全问题统计和综合得分

被测对象名称	安全问题数量			综合得分
	高风险	中风险	低风险	
科研创新信息化管理系统	0	10	15	73.85

依据 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》和GB/T 28448—2019《信息安全技术 网络安全等级保护测评要求》的第二级要求，经对科研创新信息化管理系统的安全保护状况进行综合分析评价，等级测评结论如下：

科研创新信息化管理系统本次等级测评的综合得分为73.85，且不存在高等级安全风险，等级测评结论为中。

7 安全问题整改建议

表 7-1 安全问题整改建议

序号	安全类	安全问题	关联资产	整改建议
1	安全物理环境	(1)机房出入口未配置电子门禁系统。	信息化机房	(1) 采用电子门禁系统严格控制机房其他出入口的进出，或安排专人值守； (2) 采用电子门禁系统，对机房所有人员出入进行登记记录，并保存。
2	安全物理环境	(1)机房建设未完全采用符合耐火等级的建筑材料； (2)机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级。	信息化机房	(1) 机房及相关的工作房间和辅助房采用具有耐火等级的建筑材料； (2) 机房建设采用符合相关耐火等级（二级）的建筑材料。（内外墙壁均应采用具有防火涂料、隔热板、铝板、钢板等阻燃或不燃的材料）； (3) 机房耐火等级建筑材料有相关合格证，并留存机房验收文档。
3	安全物理环境	(1)机房内缺乏防静电措施（如防静电地板或铺设防静电地毯）。	信息化机房	(1) 机房铺设防静电地板或铺设防静电地毯； (2) 机房房静电设计可依据GB50174-2008和GB50314-2006相关规定进行机房设计和验收。
4	安全通信网络	(1)关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	(1) 建议独立划分出应用服务器网段、数据库服务器网段。
5	安全通信	(1)缺乏对通信设备可信验	安全通信网络	(1) 建议在管理规范文档内对通信设

序号	安全类	安全问题	关联资产	整改建议
	网络	证方面的安全设计要求； (2)现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况。		备可信验证方面的安全设计提出要求； （2）建议系统实现对所有可执行环节进行可信验证，包括： 运行过程中的可信检验： ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■通信应用连接过程。
6	安全区域边界	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	（1）建议网络层部署的防火墙配置对内部发起的攻击行为实现防范功能策略，实现检测、防止或限制从内部发起的网络攻击行为； （2）内部安全防范措施能检测以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、碎片攻击、网络蠕虫攻击、应用漏洞攻击。
7	安全区域边界	(1)现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	（1）建议现有部署的恶意代码防范措施网络边界覆盖全面，及时对恶意代码及逆行检测和清除。
8	安全区域边界	(1)缺乏对边界设备可信验证方面的安全设计要求； (2)现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）建议对边界设备系统程序的可信验证设计并保存设计文件； （2）建议系统实现对所有可执行环节进行可信验证。
9	安全计算环境	(1)设备不具备相关可信验证的技术措施。	WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2	（1）建议通过设备的启动过程和运行过程中对预装软件（包括系统引导程序、系统程序、相关应用程序和重要配置参数）的完整性验证或检测，确保对系统引导程序、系统程序、重要配置参数和关键应用程序可信根验证； （2）建议设备启用在检测到其可信性受到破坏后进行报警的相关功能。
10	安全计算环境	(1)缺乏对计算设备可信验证方面的安全设计要求； (2)现有的计算设备存在对系统运行过程中的可信检验	业务终端-1 业务终端-2 应用/数据库服务器	（1）建议对计算设备系统程序的可信验证设计并保存设计文件； （2）建议系统实现对所有可执行环节进行可信验证。

序号	安全类	安全问题	关联资产	整改建议
		完全缺失的情况。	运维及管理终端-1 运维及管理终端-2	
11	安全计算环境	（1）未能提供数据库系统重要数据的异地定时数据备份功能。	应用/数据库服务器-MSSQL	（1）建议设置异地灾备机房，并利用通信网络将重要数据定时备份至备份场地； （2）异地备份的数据范围（不限于）包括系统的： ■配置数据 ■重要业务数据。
12	安全计算环境	（1）未能提供中间件重要数据的异地定时数据备份功能。	应用/数据库服务器-Tomcat	（1）建议设置异地灾备机房，并利用通信网络将中间件重要数据定时备份至备份场地； （2）异地备份的中间件数据范围（不限于）包括系统的： ■配置数据 ■重要日志数据。
13	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	重要业务数据 重要个人信息	（1）建议设置异地灾备机房，并利用通信网络将应用软件系统重要数据定时备份至备份场地。
			科研创新信息化管理系统	（1）建议设置异地灾备机房，并利用通信网络将应用软件系统重要数据定时备份至备份场地； （2）异地备份的应用软件系统数据范围（不限于）包括系统的：配置数据、重要日志数据，业务数据。
14	安全管理中心	（1）系统管理的资源、运行及配置管理不够全面。	管理中心	（1）需实现系统包括对可信证书管理、可信基准库的管理。
15	安全管理机构	（1）单位开展的检查工作不够完善。	制度文件、执行/记录文件	（1）建议单位按要求提供安全检查报告。
16	安全管理人员	（1）单位未完全按管理规范开展人员离场后的清理工作。	制度文件、执行/记录文件	（1）建议单位按管理规范开展人员离场后的清理工作。至少包括：保留清理记录、及时清除离场后的所有访问权限、记录访问权限清除时间。
17	安全建设管理	（1）单位未具备适用于被测系统的安全规划设计方案。	制度文件、执行/记录文件	（1）建议单位根据等保要求进行过全面的自查或对比，根据系统的安全级别选择基本安全措施； （2）建议规划方案需根据风险分析结果对系统安全措施进行补充和整，并在系统建设\\整改方案中有详细描述。

序号	安全类	安全问题	关联资产	整改建议
18	安全建设管理	(1)单位未具备完整的安全设计方案相关的文档； (2)单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	(1) 建议单位根据信息系统的等级划分情况，准备安全设计方案、安全管理策略、安全建设规划文档等； (2) 建议相关文档内容应完善，包括统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、密码技术要求、总体建设规划和详细设计方案，并形成一致性的配套文件。
19	安全建设管理	(1) 单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； (2)单位未对相关论证过程及内容进行完整的记录。	制度文件、执行/记录文件	(1) 建议单位组织相关部门和安全技术专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定； (2) 保存论证和审定记录，记录包括批准时间、批准人员签字； (3) 文件经过批准后，才能正式实施。
20	安全建设管理	(1)单位未在软件开发过程中对所有软件安全性进行测试； (2)单位未在软件安装之前按要求对所有软件开展恶意代码检测。	制度文件、执行/记录文件	(1) 建议开发商提供软件源代码，软件安装前检测软件中的恶意代码； (2) 输出检测报告（或提供第三方检测报告），内容包括测试时间、测试地点、测试对象、测试结论、测试人员。
21	安全建设管理	(1)单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	(1) 建议根据测试验收过程记录与结果，形成测试验收报告。
22	安全建设管理	(1)针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	(1) 建议系统建设完成后，委托第三方测试单位对系统进行安全性测试，并出具安全性测试报告； (2) 测试报告内容至少包括测试时间、测试地点、测试人、测试对象、测试方法、测试过程、测试发现的安全问题、整改建议、测试结论，并有第三方测试机构的签字盖章。
23	安全运维管理	(1)单位未严格按规范开展漏洞及安全隐患检测工作。	制度文件、执行/记录文件	(1) 建议单位定期开展漏洞扫描，对发现的安全漏洞和隐患进行及时修补评估； (2) 对必需修补的安全漏洞和隐患进行加固测试，测试无误后，备份系统数据，再从生产环境进行修补； (3) 对于剩余安全漏洞和隐患进行残余风险分析，明确安全风险整改原则。
24	安全运维管理	(1) 单位未严格按规范要求，针对防范恶意代码攻击	制度文件、执行/记录文件	(1) 建议单位按规范要求，针对防范恶意代码攻击的技术措施的有效性验

序号	安全类	安全问题	关联资产	整改建议
		的技术措施的有效性验证，开展工作。		证，开展工作。包括;定期对相关产品的恶意代码库进行升级；对相关设备升级情况进行记录；对各类防病毒产品上截获的恶意代码进行分析并汇总上报； （2）单位需保留完整的恶意代码检测/升级的记录。至少具备：执行人、升级结果/检测结果、处理方式、负责人签字 。
25	安全运维管理	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	制度文件、执行/记录文件	（1）建议单位学习现有密码相关的国家标准和行业标准。建立密码管理要求的制度文档。

漏洞安全问题整改建议

序号	安全类	安全问题	关联资产	整改建议
1	安全计算环境	允许Traceroute探测 此类漏洞涉及网络设备、安全设备、服务器存储设备。	10.2.4.10/应用/数据库服务器 10.2.1.4/运维安全管理系统 10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/ 上网行为管理系统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/ 汇聚交换机 172.16.1.2/核心交换机	在防火墙出站规则中禁用echo-reply（type 0）、time-exceeded（type 11）、destination-unreachable（type 3）类型的ICMP包。
2	安全计算环境	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161) 此类漏洞涉及网络设备。	172.16.1.2/核心交换机	临时解决方法：* 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问

序号	安全类	安全问题	关联资产	整改建议
				题，请到厂商的主页下载：https://downloads.ssh.com/ 对于具体Linux发行版中使用的版本，可以参考如下链接,确认系统是否受该漏洞影响:Redhat -------https://rhn.redhat.com/errata/RHSA-2009-1287.html Suse -------http://support.novell.com/security/cve/CVE-2008-5161.html Ubuntu -------http://people.canonical.com/~ubuntu-security/cve/2008/CVE-2008-5161.html
3	安全计算环境	缺少“X-Content-Type-Options”响应头 此类漏洞涉及业务应用软件平台。	https://ky.mmpt.edu.cn/科研创新信息化管理系统	在服务器中配置X-Content-Type-Options响应头为“nosniff”。

【正文结束】

附录A 被测对象资产

A.1 物理机房

附录A 表- 1物理机房

序号	机房名称	物理位置	重要程度
1	信息化机房	茂名市茂南区文明北路232号大院大楼	关键

A.2 网络设备

附录A 表- 2网络设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度	备注
1	汇聚交换机	否	H3C version 7.1.070, Release 6126P20	H3C S5560X-30C-EI	数据交换	重要	
2	核心交换机	否	H3C version 7.1.070, Release 7585P07	H3C S7500E-X	核心数据交换、访问控制	关键	

A.3 安全设备

附录A 表- 3安全设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度	备注
1	基线核查系统	否	深信服V3.0.3	深信服AC-1000-D602-PT	漏洞扫描	重要	
2	防火墙-1	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键	
3	WEB应用防火墙	否	深信服AF 8.0.9	深信服WAF-2000-H642	应用防护、入侵防范、病毒防护	重要	
4	上网行为管理系统	否	深信服AC12.0.26	深信服AC-1000-D600-PT	上网行为管理及终端准入控制	重要	
5	防火墙-2	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键	
6	日志审计系统	否	深信服LAS 3.0.5	深信服AC-1000-D601-PT	日志审计	重要	
7	运维安全管理系统	否	深信服V3.0.6	深信服AC-1000-D603-PT	运维审计	重要	

A.4 服务器

附录A 表-4服务器

序号	设备名称	所属业务应用系统/平台名称	是否虚拟设备	操作系统及版本	数据库管理系统及版本	中间件及版本	重要程度	备注
1	应用/数据库服务器	科研创新信息化管理系统	否	Windows Server 2012 R2	MSSQL 2008 R2	Tomcat 8.5	关键	

A.5 终端设备

附录A 表-5终端设备

序号	设备名称	是否虚拟设备	操作系统/控制软件及版本	用途	重要程度	备注
1	业务终端-2	否	Windows 10 （版本20H2 （内部版本19044.1889）	业务管理	一般	
2	运维及管理终端-1	否	Windows 10 （版本20H2 （内部版本19044.1889）	运维管理、系统管理	一般	
3	业务终端-1	否	Windows 10 （版本20H2 （内部版本19044.1889）	业务管理	一般	
4	运维及管理终端-2	否	Windows 10 （版本21H2 （内部版本19044.1889））	运维管理、系统管理	一般	

A.6 其他系统或设备

附录A 表-6其他系统或设备

序号	设备名称	是否虚拟设备	操作系统/控制软件及版本	用途	重要程度	备注
/	/	/	/	/	/	/

注释：本次测评对象中不涉及专用移动互联终端等，不开展抽测。

A.7 系统管理软件/平台

附录A 表-7系统管理软件/平台

序号	系统管理软件/平台名称	所在设备名称	版本	主要功能	重要程度	备注
1	应用/数据库服务器-Tomcat	应用/数据库服务器	8.5	页面发布	关键	

序号	系统管理软件/平台名称	所在设备名称	版本	主要功能	重要程度	备注
2	应用/数据库服务器-MSSQL	应用/数据库服务器	2008 R2	数据生产、存储	关键	

A.8 业务应用软件/平台

附录A 表-8业务应用系统/平台

序号	业务应用系统/平台名称	主要功能	业务应用软件及版本	开发厂商	重要程度
1	科研创新信息化管理系统	科研创新信息化管理系统用于科研管理信息化建设，系统主要功能包括项目管理，经费管理，论文、著作、专利、艺术作品等成果管理，科研人员，科研机构管理。根据学校科教研管理的分工，提供不同的解决方案，让科研管理变得更简单。	V6.0	北京易普拉格科技股份有限公司	关键

A.9 数据资源

附录A 表-9数据资源

序号	数据类别	所属业务应用	安全防护需求	重要程度
1	重要个人信息	科研创新信息化管理系统	完整性、保密性	关键
2	重要业务数据	科研创新信息化管理系统	完整性、保密性	关键
3	鉴别数据	科研创新信息化管理系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性、保密性	关键
4	重要审计数据	科研创新信息化管理系统（安全管理中心）	完整性	重要
5	重要配置数据	科研创新信息化管理系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性	关键

注释：网络设备、安全设备、服务器、终端、系统管理软件/平台和业务应用系统等所涉及的鉴别数据和重要配置数据分别在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。重要审计数据在安全管理中心进行汇总测评证据，

包括数据完整性。重要业务数据和重要个人信息分别在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。

A.10 密码产品

附录A 表-10密码产品

序号	产品/模块名称	生成厂商	商密型号	密码算法	用途	重要程度
/	/	/	/	/	/	/

注释：本次测评不存在加密机等密码产品。

A.11 安全相关人员

附录A 表-11安全相关人员

序号	姓名	岗位/角色	联系方式	所属单位
1	杨云	资产管理员	0668-2920122	茂名职业技术学院
2	龙恒	网络管理员	13377766618	茂名职业技术学院
3	龙恒	数据管理员	13377766618	茂名职业技术学院
4	龙恒	应用管理员	13377766618	茂名职业技术学院
5	杨云	审计管理员	0668-2920122	茂名职业技术学院
6	吴国华	机房管理员	0668-2920122	茂名职业技术学院
7	叶永利	安全管理员	0668-2920122	茂名职业技术学院
8	吴国华	系统管理员	0668-2920122	茂名职业技术学院

A.12 安全管理文档

附录A 表-12安全管理文档

序号	文档名称	主要内容
1	制度类文档-安全事件报告和处置	关于单位网络安全事件管理、处置、流程等报告制度文档
2	制度类文档-组织安全结构和人员职责制度	关于单位组织结构、人员安排、人员职责制度文档
3	制度类文档-介质管理制度	关于单位介质安全管理工制度文档
4	制度类文档-安全管理组织规范	关于单位组织结构管理规范制度文档

序号	文档名称	主要内容
5	制度类文档-主机安全管理规范	关于规定单位主机系统安全管理要求规范，指导业务平台主机的安全配置和维护的制度文档
6	制度类文档-应用安全管理规范	关于规定单位应用安全管理要求及规范的制度文档
7	制度类文档-外部服务人员管理规范	关于单位针对外部人员工作管理规范制度文档
8	制度类文档-备份与恢复管理制度	关于单位数据备份、恢复管理制度文档
9	制度类文档-组织安全结构和人员职责制度	关于单位安全结构、人员职责
10	制度类文档-离岗人员工作交接规范	关于单位离岗交接工作规范制度文档
11	制度类文档-机房安全管理制度	关于单位机房安全管理工作制度文档
12	制度类文档-信息系统外包运维管理制度	关于单位外包运维工作管理制度文档
13	制度类文档-信息系统恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
14	制度类文档-信息安全漏洞扫描规范	关于单位安全漏洞工作规范制度文档
15	制度类文档-员工考核管理制度	关于单位人员考核工作管理制度文档
16	制度类文档-物理安全管理规范	关于加强单位办公区域及电子计算机机房的管理和设备运行安全，规范办公区域及机房建设，使人员办公高效及机房设备安全、稳定运行的制度文档
17	制度类文档-系统交付管理	关于单位交付工作管理制度文档
18	制度类文档-信息安全奖惩办法	关于单位人员奖惩制度文档
19	制度类文档-办公环境管理制度	关于单位办公环境管理制度文档
20	制度类文档-网络安全管理制度	关于单位网络安全工作管理制度文档
21	制度类文档-安全漏洞管理制度	关于单位安全漏洞管理工作制度文档
22	制度类文档-变更控制管理制度	关于单位变更流程、控制管理制度文档
23	制度类文档-测试及验收方案	关于单位测试验收方案文档
24	制度类文档-工程测试验收管理	关于单位工程测试工作管理制度文档
25	制度类文档-安全审查	关于单位安全检查、审查工作规范制度文档

序号	文档名称	主要内容
	和检查管理规范	
26	制度类文档-外部人员访问管理制度	关于单位针对外来人员访问管控制度文档
27	制度类文档-安全教育和培训制度	关于单位安全培训、安全交流工作制度文档
28	制度类文档-网络安全事件应急预案	关于单位网络安全事件应急处理、流程、培训等管理制度文档
29	制度类文档-应用系统业务用户密码设置规定	关于单位用户密码管理制度文档
30	制度类文档-系统安全管理制度	关于单位系统安全管理、安全服务管理制度文档
31	制度类文档-工程实施管理制度	关于单位工程实施工作管理制度文档
32	制度类文档-人员管理制度	关于单位人员录用、调岗、离岗管理制度文档
33	制度类文档-设备安全管理制度	关于单位设备安全管理制度文档
34	制度类文档-恶意代码防范管理制度	关于单位恶意代码防范工作制度文档
35	制度类文档-信息安全总体策略	关于单位网络安全方针、策略制度文档
36	制度类文档-网络安全管理规范	关于保障单位网络系统的安全稳定运行，抵御内部和外部各种形式的网络攻击或威胁制定的管理文档
37	制度类文档-恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
38	制度类文档-网络安全事件报告制度	关于单位网络安全事件管理报告文档
39	制度类文档-办公环境保密管理	关于单位办公环境管理制度文档
40	制度类文档-服务供应商选择安全管理制度	关于单位安全服务供应商管理规定制度文档
41	制度类文档-岗位安排及岗位职责	关于单位岗位职责、岗位安排制度文档
42	制度类文档-外部接入受控网络访问系统管理规范	关于单位针对外部人员工作接入规范制度文档
43	制度类文档-外包开发软件管理规定	关于单位外包项目管理工作制度文档
44	制度类文档-数据安全管理规范	关于保障关键数据安全，从数据库本身、数据加密、数据备份恢复三个方面对数据安全进行规范的制度文档
45	制度类文档-授权和审批管理规定	关于单位授权审批、审批流程规范制度文档

序号	文档名称	主要内容
46	制度类文档-制度制定、发布、评审和修订管理制度	关于单位制度制定、发布、评审和修订等管理文档
47	制度类文档-网络与信息系统安全设计规范	关于单位网络与信息化安全设计制度文档
48	制度类文档-系统及应用数据备份管理规范	关于单位数据备份、恢复管理制度文档
49	操作类文档-设备操作规程	关于单位相关设备操作指导文档
50	操作类文档-设备及系统软件配置和操作手册	关于单位安全设备操作、Linux服务器配置手册、主机运维操作手册、软件操作手册、防火墙配置和操作手册、数据库日常运维操作手册等指导文档
51	操作类文档-数据备份策略	关于单位数据备份策略文件
52	操作类文档-软硬件日常维护管理规程	关于单位计算机网络系统使用、管理、信息安全、资源共享有所遵循,规范上网操作流程,提高网络系统安全性的指导文档
53	记录类文档-收发文登记记录	关于单位文档签发记录
54	记录类文档-人员入职考核记录	关于人员录用、考核工作记录
55	记录类文档-机房维护日志	关于机房维护工作记录
56	记录类文档-设备维修申请表	关于单位设备维护工作申请记录
57	记录类文档-技能培训记录	关于单位系统培训工作、考核工作记录
58	记录类文档-信息系统存储介质销毁申请表	关于备份介质销毁申请工作记录
59	记录类文档-设备操作维护记录	关于单位设备维护工作记录
60	记录类文档-评审和修订记录	关于单位变更评审、修订工作记录
61	记录类文档-重要操作审批表	关于单位审批工作记录
62	记录类文档-监理审批表	关于单位监理审核工作记录
63	记录类文档-离场信息资料交接表	关于人员离岗交接工作记录
64	记录类文档-通用变更记录表	关于单位变更工作记录
65	记录类文档-设备出入登记记录表	关于设备进出机房登记工作记录
66	记录类文档-软件交付	关于单位交付工作记录

序号	文档名称	主要内容
	清单	
67	记录类文档-网络配置信息	关于单位配置信息登记工作记录
68	记录类文档-人员培训及考核记录表	关于人员培训、考核等工作记录
69	记录类文档-安全建设方案评审纪录	关于单位网络与信息化安全设计方案评审工作记录
70	记录类文档-信息管理系统漏洞检查表	关于单位安全漏洞工作检测记录表
71	记录类文档-信息安全检查记录表	关于单位安全检查工作记录
72	记录类文档-机房出入登记表	关于人员进出机房登记工作记录
73	记录类文档-备份介质使用记录	关于备份介质使用登记工作记录
74	记录类文档-访问记录表	关于人员访问工作记录
75	记录类文档-信息系统存储介质使用清单	关于备份介质存储使用清单
76	记录类文档-接入受控网络申请表	关于外来人员接入工作记录
77	记录类文档-离职员工物品交回登记表	关于人员离岗工物交接工作记录
78	记录类文档-数据恢复申请表	关于单位数据恢复工作申请表
79	记录类文档-网络信息安全事件记录表	关于单位网络安全事件工作记录
80	记录类文档-数据备份记录表	关于单位数据备份工作记录
81	记录类文档-机房设备维修记录表	关于单位机房设备维修工作记录
82	记录类文档-外部会议文件和记录	关于单位外部联系、交流及会议工作记录
83	记录类文档-人员离岗申请表	关于人员离岗申请记录
84	记录类文档-安全管理制度评审记录	关于单位制度审计记录
85	记录类文档-关键岗位人员考核记录	关于关键岗位考核工作记录
86	记录类文档-机房巡检记录表	关于单位机房环境巡检记录
87	记录类文档-存储介质目录清单	关于备份介质存储工作清单

序号	文档名称	主要内容
88	记录类文档-外部人员访问记录表	关于外来人员访问登记工作记录
89	记录类文档-外部人员访问申请表	关于外来人员访问申请流程工作记录
90	记录类文档-系统交付清单	关于单位交付工作记录
91	记录类文档-应急预案培训记录表	关于单位应急预案培训工作记录
92	记录类文档-漏洞检测报告	关于单位安全漏洞检测报告文档
93	记录类文档-机房设备维护记录表	关于设备维护登记工作记录
94	记录类文档-专家论证记录表	关于单位网络方案论证记录
95	记录类文档-信息安全会议记录	关于单位安全培训、安全交流会议记录
96	记录类文档-备份工作汇总表	关于单位数据备份工作总结表
97	证据类文档-信息安全事件分析报告表	关于单位安全事件分析报告
98	证据类文档-网络安全系统设计方案	关于单位网络与信息化安全设计方案文档
99	证据类文档-资产清单	关于单位信息系统资产清单统计表
100	证据类文档-网络安全等级保护工作小组名单	关于单位网络安全等级保护工作小组人员名单文件
101	证据类文档-安全职位人员	关于单位人员岗位安排名单
102	证据类文档-外部联系表	关于单位内部联系及外部联系名单
103	证据类文档-网络安全等级保护测评服务合同	关于单位与安全服务商签定的安全服务合同文件
104	证据类文档-定级备案	关于单位系统定级报告、备案证文件
105	证据类文档-深信服安全采购合同	关于单位与安全厂家服务采购、产品选择合同文件
106	证据类文档-工程项目实施方案	关于单位工程实施方案文档

附录B 上次测评问题整改情况说明

此次为科研创新信息化管理系统初次等级测评，之前未实施过等级保护测评工作。

附录B 表- 1上次测评问题整改情况

序号	主要安全问题	整改情况	情况说明
/	/	□已整改 □未整改	/

附录C 单项测评结果汇总

C.1 安全物理环境

附录 C 表-1 安全物理环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			物理位置选择	物理访问控制	防盗窃和防破坏	防雷击	防火	防水和防潮	防静电	温湿度控制	电力供应	电磁防护
1	信息化机房	符合	2	0	2	1	1	2	0	1	2	1
		部分符合	0	1	0	0	0	0	0	0	0	0
		不符合	0	0	0	0	1	0	1	0	0	0
		不适用	0	0	0	0	0	0	0	0	0	0

附录 C 表-2 安全物理环境单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.2 安全通信网络

附录 C 表-3 安全通信网络单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求		
			网络架构	通信传输	可信验证
1	安全通信网络	符合	1	1	0
		部分符合	1	0	0
		不符合	0	0	1
		不适用	0	0	0

附录 C 表-4 安全通信网络单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.3 安全区域边界

附录 C 表-5 安全区域边界单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求					
			边界防护	访问控制	入侵防范	恶意代码和垃圾邮件防范	安全审计	可信验证
1	外网边界区域	符合	1	4	1	1	3	0
		部分符合	0	0	0	0	0	0
		不符合	0	0	0	0	0	1
		不适用	0	0	0	0	0	0
2	安全管理区域	符合	1	4	0	0	3	0
		部分符合	0	0	0	1	0	0
		不符合	0	0	1	0	0	1
		不适用	0	0	0	0	0	0
3	服务器存储区域	符合	1	4	1	1	3	0
		部分符合	0	0	0	0	0	0
		不符合	0	0	0	0	0	1
		不适用	0	0	0	0	0	0
4	办公网区域	符合	1	4	0	0	3	0
		部分符合	0	0	0	1	0	0
		不符合	0	0	1	0	0	1
		不适用	0	0	0	0	0	0

附录 C 表-6 安全区域边界单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.4 安全计算环境

C.4.1 网络设备

附录 C 表-7 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	汇聚交换机	符合	3	4	3	4	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	1	0	0	1	1	--
2	核心交换机	符合	3	4	3	4	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
		不适用	0	0	0	1	1	0	0	1	1	--

C.4.2 安全设备

附录 C 表-8 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	基线核查系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
2	上网行为管理系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
3	WEB应用防火墙	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
4	防火墙-1	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
5	防火墙-2	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
6	日志审计系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
7	运维安全	符合	3	4	3	5	0	0	1	1	0	--
		部分符	0	0	0	0	0	0	0	0	0	--

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
	管理系统	合										
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--

C.4.3 服务器和终端

附录 C 表-9 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	应用/数据库服务器	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
2	业务终端-2	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
3	业务终端-1	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
4	运维及管理终端-2	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
5	运维及管理终端-1	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--

C.4.4 系统管理软件/平台

附录 C 表-10 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	应用/数据库服务器-Tomcat	符合	0	4	3	2	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	3	0	0	3	1	1	0	0	0	--
2	应用/数据库服务器-MSSQL	符合	3	4	3	2	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	0	0	0	3	1	1	0	0	0	--

C.4.5 业务应用系统/平台

附录 C 表-11 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	科研创新信息化管理系统	符合	3	4	3	3	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	0	0	0	2	1	1	0	0	0	--

C.4.6 数据资源

附录 C 表-12 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	重要个人信息	符合	--	--	--	--	--	--	1	1	0	2
		部分符合	--	--	--	--	--	--	0	0	0	0
		不符合	--	--	--	--	--	--	0	1	0	0
		不适用	--	--	--	--	--	--	0	0	1	0
2	重要业务	符合	--	--	--	--	--	--	1	1	0	0
		部分符	--	--	--	--	--	--	0	0	0	0

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
	数据	合										
		不符合	--	--	--	--	--	--	0	1	0	0
		不适用	--	--	--	--	--	--	0	0	1	2

C.4.7 其他系统或设备

附录 C 表-13 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	--	符合	--	--	--	--	--	--	--	--	--	--
		部分符合	--	--	--	--	--	--	--	--	--	--
		不符合	--	--	--	--	--	--	--	--	--	--
		不适用	--	--	--	--	--	--	--	--	--	--

C.5 安全管理中心

附录 C 表-14 安全管理中心单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求	
			系统管理	审计管理
1	管理中心	符合	1	2
		部分符合	0	0
		不符合	1	0
		不适用	0	0

附录 C 表-15 安全管理中心单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.6 安全管理制度

附录 C 表-16 安全管理制度单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求			
			安全策略	管理制度	制定和发布	评审和修订
1	制度文件、执行/记录文件	符合	1	2	2	1
		部分符合	0	0	0	0
		不符合	0	0	0	0
		不适用	0	0	0	0

C.7 安全管理机构

附录 C 表-17 安全管理机构单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求				
			岗位设置	人员配备	授权和审批	沟通和合作	审核和检查
1	制度文件、执行/记录文件	符合	2	1	2	3	0
		部分符合	0	0	0	0	1
		不符合	0	0	0	0	0
		不适用	0	0	0	0	0

C.8 安全管理人员

附录 C 表-18 安全管理人员单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求			
			人员录用	人员离岗	安全意识教育和培训	外部人员访问管理
1	制度文件、执行/记录文件	符合	2	1	1	2
		部分符合	0	0	0	0
		不符合	0	0	0	1
		不适用	0	0	0	0

C.9 安全建设管理

附录 C 表-19 安全建设管理单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			定级和备案	安全方案设计	产品采购和使用	自行软件开发	外包软件开发	工程实施	测试验收	系统交付	等级测评	服务供应商选择
1	制度文件、执行/记录文件	符合	4	0	2	0	1	2	0	3	3	2
		部分符合	0	0	0	0	0	0	1	0	0	0
		不符合	0	3	0	0	1	0	1	0	0	0
		不适用	0	0	0	2	0	0	0	0	0	0

附录 C 表-20 安全建设管理单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.10 安全运维管理

附录 C 表-21 安全运维管理单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求												
			环境管理	资产管理	介质管理	设备维护管理	漏洞和风险管理	网络和系统安全管理	恶意代码防范管理	配置管理	密码管理	变更管理	备份与恢复管理	安全事件处置	应急预案管理	外包运维管理
1	制度文件、执行/记录文件	符合	3	1	2	2	0	5	2	1	0	1	3	3	2	0
		部分符合	0	0	0	0	0	0	1	0	0	0	0	0	0	0
		不符合	0	0	0	0	1	0	0	0	1	0	0	0	0	0
		不适用	0	0	0	0	0	0	0	0	1	0	0	0	0	2

附录 C 表-22 安全运维管理单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.11 其他安全要求指标

附录 C 表-23 其他指标单项测评结果汇总表

序号	测评对象	符合情况
本报告不涉及		

附录D 单项测评结果记录

D.1 安全物理环境

D.1.1 安全通用要求

D.1.1.1 信息化机房

安全控制点	测评指标	结果结论	符合程度
物理位置选择	a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；	（1）机房和办公场地场所在建筑物具有建筑验收文档，包含对防震、防风和防雨能力的说明；	符合

安全控制点	测评指标	结果结论	符合程度
		■机房建设地址为：茂名市茂南区文明北路232号大院大楼 （2）机房和办公场地未出严重的问题。 ■无雨水渗透痕迹 ■无因风导致的较严重尘土 ■无屋顶、墙体、地面等破损开裂	
	b）机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	（1）机房未部署在易发生问题的位置； （2）机房对于空调设备的排水管等部位采取密封防漏处理； （3）机房对于楼板进行了防护措施。	符合
物理访问控制	机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。	（1）制定了《机房安全管理制度》，内容包含机房出入方面的管理规定； （2）对未配置电子门禁系统的出入口指定专人7*24小时负责机房出入，对出入的人员进行身份鉴别和登记，可查出入记录，且出入有专人陪同； （3）机房存在未配置门禁系统的开放出入口。	部分符合
防盗窃和防破坏	a）应将设备或主要部件进行固定，并设置明显的不易除去的标识；	（1）机房设备或主要部件都固定在机架上； （2）机房内对主要部件已绑定相应不易除去的标签； ■包括网络设备 ■包括安全设备 ■包括服务器 ■包括网络线缆 （3）重要机柜已进行上锁处理。	符合
	b）应将通信线缆铺设在隐蔽安全处。	（1）通信线缆铺设在下走线槽隐蔽处中； （2）通信线缆设有明显的源目的标识； （3）通信线缆均铺设整齐、规范。	符合
防雷击	应将各类机柜、设施和设备等通过接地系统安全接地。	（1）机房设置专用地线； （2）机房内机柜、设施和设备等进行接地处理； （3）交流电源接地验收检测结果符合要求。	符合
防火	a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；	（1）机房采用经消防检测部门检测合格并在有效期内的（如 七氟丙烷）气体自动灭火设备，火灾自动报警类型为烟感+红外； （2）自动消防系统工作状态正常，有定期巡检和维护记录《机房巡检记录表》； （3）建立机房消防的管理制度相关文档《机房安全管理制度》，按管理要求机房无人情况下气体灭火配置为自动模式，进入机房调整为手动模式，机房报警有7*24小时值班人员进行监控。	符合
	b）机房及相关的工作房间	（1）机房及相关的工作房间和辅助房没有采	不符合

安全控制点	测评指标	结果结论	符合程度
	和辅助房应采用具有耐火等级的建筑材料。	用具有耐火等级的建筑材料； （2）缺乏机房防火设计文档； （3）缺乏机房防火验收文档。	
防水和防潮	a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	（1）机房不存在雨水渗透、破损等不合规情况； （2）机房不位于建筑的顶层、边缘区域。	符合
	b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。	（1）机房区域范围已部署1台科华品牌（精密）空调，机房内分别配置1组温湿度传感器监控； （2）机房内空调下方已铺设安装好挡水和排水设施； （3）机房墙壁或楼板的管道采取必要的防渗防漏等防水保护措施； （4）机房安装检测设备（如：漏水检测绳）检测地下积水，及时处理机房水蒸气结露和地下积水的转移与渗透； （5）目前防水\防潮检测未发现异常情况，并且有防水防潮的运维记录《机房维护日志》。	符合
防静电	应采用防静电地板或地面并采用必要的接地防静电措施。	（1）对机房内设备（可导电金属线槽）采用了接地静电泄放措施； （2）机房未采用防静电地板或铺设防静电地毯。	不符合
温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。	（1）机房范围已部署1组科华品牌精密空调进行温湿度调节； （2）机房范围已部署空调及加湿机进行温湿度调节； （3）温湿度自动调节设施运作正常，有运行和维护记录《机房维护日志》； （4）机房温度能保持在24摄氏度到28摄氏度之间； （5）机房湿度能保持在40%到65%之间。	符合
电力供应	a）应在机房供电线路上配置稳压器和过电压防护设备；	（1）机房配备了稳压器和过电压防护设备； （2）稳压器和过电压防护设备正常工作； （3）机房具备电力供应安全设计，并在其中标明配备稳压器、过电压防护设备等要求。	符合
	b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。	（1）机房配备了1组科华品牌UPS； （2）UPS正常工作，可满足主要设备断电情况下的至少1小时正常运行要求； （3）UPS有定期（至少每年）检查和维护，有运行和维护记录《机房巡检记录表》。	符合
电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。	（1）通信线缆铺设采用独立的具有电磁屏蔽作用线槽； （2）电源线缆铺设采用独立的具有电磁屏蔽作用线槽；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）弱电线缆隔离铺设，没有干扰。	

D.2 安全通信网络

D.2.1 安全通用要求

D.2.1.1 安全通信网络

安全控制点	测评指标	结果结论	符合程度
网络架构	a）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；	（1）已对网络地址划分，且便于管理和控制； （2）网络地址划分采用核心交换机实现外网边界区域、服务器存储区域等的划分； （3）重要核心网络区域与非重要网络在同一网段； （4）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	部分符合
	b）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	（1）网络内重要网段未部署在网络边界处，且未直接连接外部信息系统； （2）系统通过防火墙对重要网段采取访问控制策略； （3）各安全域（子网）的出口唯一。	符合
通信传输	应采用校验技术保证通信过程中数据的完整性。	（1）网络系统中未涉及完整性保障设备，但在安全计算环境方面网络设备采用SSH协议、安全设备采用HTTPS协议、操作系统采用SSH协议、应用系统采用HTTPS协议来保证通信过程中数据的完整性。	符合
可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对通信设备可信验证方面的安全设计要求； （2）现有的通信设备存在未能实现操作系统到上层应用的信任链的情况，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■通信应用连接过程	不符合

D.3 安全区域边界

D.3.1 安全通用要求

D.3.1.1 办公网区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■办公网区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机	符合

安全控制点	测评指标	结果结论	符合程度
		（3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	不符合
恶意代码和垃		（1）在关键网络节点处部署合规的防恶意代	部分符合

安全控制点	测评指标	结果结论	符合程度
圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试； （4）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	
安全审计	a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数	不符合

安全控制点	测评指标	结果结论	符合程度
	录送至安全管理中心。	■边界防护应用程序	

D.3.1.2 外网边界区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■外网边界区域 （2）网络边界处部署了可提供访问控制功能的设备； ■防火墙 ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	符合
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■防火墙 ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和	符合

安全控制点	测评指标	结果结论	符合程度
		会话机制检测的访问控制设备； ■防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制,能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署支持对内部发起的攻击行为进行防范的设备； ■防火墙(带入侵防御模块) ■WEB应用防火墙 （2）现有的防范措施满足相应防护要求； ■所有关键网络边界均有检测措施 ■设备的规则库及时更新 ■检测(模块)符合国家相关产品检测要求 ■其安全策略有效 （3）内部安全防范措施能检测相应攻击行为。 ■端口扫描 ■强力攻击 ■木马后门攻击 ■拒绝服务攻击 ■缓冲区溢出攻击 ■碎片攻击 ■网络蠕虫攻击 ■应用漏洞攻击	符合
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试。	符合
安全审计	a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合

安全控制点	测评指标	结果结论	符合程度
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.3.1.3 安全管理区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■安全管理区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	符合
访问控制	a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能；	符合

安全控制点	测评指标	结果结论	符合程度
		（4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	不符合
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试； （4）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	部分符合
安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计；	符合

安全控制点	测评指标	结果结论	符合程度
	要的用户行为和重要安全事件进行审计；	■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.3.1.4 服务器存储区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■服务器存储区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略；	符合

安全控制点	测评指标	结果结论	符合程度
		（4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■WEB应用防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署支持对内部发起的攻击行为进行防范的设备； ■WEB应用防火墙 （2）现有的防范措施满足相应防护要求； ■所有关键网络边界均有检测措施 ■设备的规则库及时更新 ■检测(模块)符合国家相关产品检测要求	符合

安全控制点	测评指标	结果结论	符合程度
		■其安全策略有效 （3）内部安全防范措施能检测相应攻击行为。 ■端口扫描 ■强力攻击 ■木马后门攻击 ■拒绝服务攻击 ■缓冲区溢出攻击 ■碎片攻击 ■网络蠕虫攻击 ■应用漏洞攻击	
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■WEB应用防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试。	符合
安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■WEB应用防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个	符合

安全控制点	测评指标	结果结论	符合程度
		月； （5）定期收集日志记录并定期备份。	
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.4 安全计算环境

D.4.1 安全通用要求

D.4.1.1 网络设备

D.4.1.1.1 核心交换机

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括VTY认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的全局密码策略； ■Password control:Enabled ■Password aging:Enabled (180 days) ■Password length:Enabled (8 characters) ■Password composition:Enabled (4 types, 1 characters per type) （6）设备配置加密的super认证。	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备配置合规的全局登录失败处理策略； ■Password control: Enabled ■Maximum login attempts: 5 ■Action for exceeding login attempts: Lock user for 5 minutes （2）设备配置合规的操作超时退出措施。 ■VTY配置idle-timeout 15 0	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式。 ■未启用TELNET ■启用SSH	符合

安全控制点	测评指标	结果结论	符合程度
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； ■Information Center: Enabled ■Console: Enabled ■Monitor: Enabled ■Log host: Enabled 10.2.1.2 ■Security log file: Enabled （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保	（1）设备限制审计文件的访问控制权限，普	符合

安全控制点	测评指标	结果结论	符合程度
	护，定期备份，避免受到未预期的删除、修改或覆盖等。	通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效； （5）日志及审计记录保存大于6个月。	
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制； ■对ssh 登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）网络层相关设备不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的交换功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。	不符合

安全控制点	测评指标	结果结论	符合程度
	结果形成审计记录送至安全管理中心。	■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施; ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施; ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能;	（1）设备定义了相关重要数据; ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范; （3）设备定期完全依照备份策略，采用正确的配置进行本地备份; （4）设备的备份周期为：每月一次; （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息;	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.1.2 汇聚交换机

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括VTY认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的全局密码策略； ■Password control:Enabled ■Password aging:Enabled (180 days) ■Password length:Enabled (8 characters) ■Password composition:Enabled (4 types, 1 characters per type) （6）设备配置加密的super认证。	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备配置合规的全局登录失败处理策略； ■Password control: Enabled ■Maximum login attempts: 5 ■Action for exceeding login attempts: Lock user for 5 minutes （2）设备配置合规的操作超时退出措施。 ■VTY配置idle-timeout 15 0	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式。 ■未启用TELNET ■启用SSH	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户	（1）设备根据安全策略要求对特权用户进行分离；	符合

安全控制点	测评指标	结果结论	符合程度
	的权限分离。	■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； ■Information Center: Enabled ■Console: Enabled ■Monitor: Enabled ■Log host: Enabled 10.2.1.2 ■Security log file: Enabled （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）漏洞扫描未发现设备启用高危端口。	
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制； ■对ssh 登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）网络层相关设备不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的交换功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。	符合

安全控制点	测评指标	结果结论	符合程度
		■使用SSH加密协议进行传输	
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2 安全设备

D.4.1.2.1 WEB应用防火墙

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会	（1）设备启用合规登录失败处理策略； ■启用登录失败策略	符合

安全控制点	测评指标	结果结论	符合程度
	话、限制非法登录次数和当登录连接超时自动退出等相关措施；	■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型	符合

安全控制点	测评指标	结果结论	符合程度
		■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合

安全控制点	测评指标	结果结论	符合程度
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配	（1）网络层设备不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	前得到完全清除。		
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.2 上网行为管理系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令	符合

安全控制点	测评指标	结果结论	符合程度
		■未设置空口令	
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合

安全控制点	测评指标	结果结论	符合程度
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。	符合

安全控制点	测评指标	结果结论	符合程度
		■使用SSH加密协议进行传输	
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.3 基线核查系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次	符合

安全控制点	测评指标	结果结论	符合程度
	当登录连接超时自动退出等相关措施；	■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识	符合

安全控制点	测评指标	结果结论	符合程度
		■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的基线核查功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施	不符合

安全控制点	测评指标	结果结论	符合程度
	程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.4 日志审计系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合

安全控制点	测评指标	结果结论	符合程度
	享账户的存在；		
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合

安全控制点	测评指标	结果结论	符合程度
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据	符合

安全控制点	测评指标	结果结论	符合程度
		（2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.5 运维安全管理系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信	（1）设备配置合规的远程管理模式； ■未启用HTTP	符合

安全控制点	测评指标	结果结论	符合程度
	息在网络传输过程中被窃听。	■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改；	符合

安全控制点	测评指标	结果结论	符合程度
	未预期的删除、修改或覆盖等。	（2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制。 ■对Web登录配置管理地址，限制登录范围	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数	不符合

安全控制点	测评指标	结果结论	符合程度
		■缺乏关键应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.6 防火墙-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身	（1）设备对各登录模式均启用身份鉴别；	符合

安全控制点	测评指标	结果结论	符合程度
	份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员	符合

安全控制点	测评指标	结果结论	符合程度
		(2)设备不存在多个管理级别高的特权用户; (3) 设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计;	(1) 设备开启审计功能，审计进程正常; (2) 设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息;	(1) 设备日期、时间正常; (2) 设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	(1) 设备限制审计文件的访问控制权限，普通用户不可删除及修改; (2) 设备针对日志、审计记录具备充足的存储容量; (3) 对审计记录进行定期存档备份，其备份策略有效; (4) 部署日志审计系统实时对日志进行统一收集存储; (5) 日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序;	(1) 设备在全局模式下禁用部分不必要的服务; (2) 设备在部分接口模式下禁用部分不必要的服务; (3) 漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口;	(1) 设备采用安全策略限制部分高危端口; (2)设备采用安全策略限制部分不必要服务; (3) 漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制;	(1) 设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制; ■对Web登录配置管理地址，限制登录范围 (2) 通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要	(1) 设备管理具备数据有效性检验功能; ■可校验录入数据 ■可校验文档内容 (2) 设备管理的校验接口范围较全面。	符合

安全控制点	测评指标	结果结论	符合程度
	求；	■包括人机接口校验 ■包括通信接口校验	
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.7 防火墙-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS	符合

安全控制点	测评指标	结果结论	符合程度
		（2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序	不符合

安全控制点	测评指标	结果结论	符合程度
		■缺乏重要设备配置参数 ■缺乏关键应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施; ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施; ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能;	（1）设备定义了相关重要数据; ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范; （3）设备定期完全依照备份策略，采用正确的配置进行本地备份; （4）设备的备份周期为：每月一次; （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息;	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.3 服务器和终端

D.4.1.3.1 应用/数据库服务器

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 (5)用户属性策略未勾选“密码永不过期”。	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用‘RDP安全层’参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令	符合

安全控制点	测评指标	结果结论	符合程度
		■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下：运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份	符合

安全控制点	测评指标	结果结论	符合程度
		策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信	不符合

安全控制点	测评指标	结果结论	符合程度
	程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用	（1）设备为服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要	不适用

安全控制点	测评指标	结果结论	符合程度
	场地。	求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施： 安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.2 业务终端-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”	符合

安全控制点	测评指标	结果结论	符合程度
	听。	参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间	符合

安全控制点	测评指标	结果结论	符合程度
		■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下：运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端	符合

安全控制点	测评指标	结果结论	符合程度
		口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据	符合

安全控制点	测评指标	结果结论	符合程度
		■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.3 业务终端-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	符合
	b）应具有登录失败处理功	（1）操作系统启用登录失败处理策略，且配	符合

安全控制点	测评指标	结果结论	符合程度
	能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败	符合

安全控制点	测评指标	结果结论	符合程度
	全事件进行审计；	■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下：运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合

安全控制点	测评指标	结果结论	符合程度
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据:	符合

安全控制点	测评指标	结果结论	符合程度
		（1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.4 运维及管理终端-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码	符合

安全控制点	测评指标	结果结论	符合程度
	更换；	（2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c）应及时删除或停用多余的、过期的账户，避免共	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对	符合

安全控制点	测评指标	结果结论	符合程度
	享账户的存在；	应。	
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下：运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合

安全控制点	测评指标	结果结论	符合程度
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数	不符合

安全控制点	测评指标	结果结论	符合程度
	全管理中心。	■业务应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配	（1）身份鉴别信息释放或清除机制正常且满足要求；	符合

安全控制点	测评指标	结果结论	符合程度
	前得到完全清除。	（2）操作系统用户的鉴别信息释放措施： 安全选项“不显示上次的用户名”->启用	
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.5 运维及管理终端-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账	（1）可提供操作系统权限表；	符合

安全控制点	测评指标	结果结论	符合程度
	户和权限；	（2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功）	符合

安全控制点	测评指标	结果结论	符合程度
		■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下：运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或	（1）操作系统安装深信服EDR防恶意代码软	符合

安全控制点	测评指标	结果结论	符合程度
	配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确	符合

安全控制点	测评指标	结果结论	符合程度
		的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.4 系统管理软件/平台

D.4.1.4.1 应用/数据库服务器-MSSQL

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）数据库系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）数据库系统不存在弱口令用户； ■MS_SQL数据库已修改默认sa口令 ■MS_SQL数据库不存在空口令用户 （3）数据库系统不存在默认信任的登录模式； ■MS_SQL数据库登录未勾选“记住密码” ■MS_SQL数据库系统配置服务器身份验证方式为：SQL Server和Windows身份验证模式” （4）数据库系统为登录用户设置的身份标识具有唯一性； （5）数据库系统配置合规的密码长度及复杂度策略； ■MS_SQL数据库系统勾选“强制实施密码策略” ■MS_SQL数据库宿主系统配置合规密码复杂度策略	符合

安全控制点	测评指标	结果结论	符合程度
		（6）数据库系统配置合规的密码有效周期策略。 ■MS_SQL数据库系统勾选“强制密码过期策略” ■MS_SQL数据库宿主系统配置合规密码有效期策略	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）数据库系统启用合规登录失败处理策略； ■MS_SQL数据库系统勾选“强制实施密码策略” ■宿主操作系统启用“账户锁定策略” （2）数据库系统执行合规的锁定策略； ■复位帐号锁定计数器=30（分钟） ■账户锁定时间=30（分钟） ■账户锁定阀值=15 （3）数据库系统配置合规的操作超时锁定。 ■“连接”--“远程查询超时值”<900秒	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）宿主操作系统配置合规的远程管理模式； ■主机启用了安全的远程管理模式（如 RDP 高密级 ），且只能通过本地对数据库进行管理 （2）使用运维安全管理系统统一管理操作系统远程登录，运维安全管理系统采用了 HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供数据库系统权限表； （2）登录数据库系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在所有用户均属于sysadmin的情况； （4）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）数据库系统对多余帐户进行删除、锁定或禁止其登录； （2）数据库系统账户口令设置合规。 ■MS_SQL数据库系统勾选“强制实施密码策略”	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）数据库系统不存在多余或过期账户； （2）数据库系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）数据库系统根据安全策略要求对特权用户进行分离； ■配置系统管理员	符合

安全控制点	测评指标	结果结论	符合程度
		■配置安全审计员 ■配置系统操作员 （2）数据库系统不存除sa外的特权用户； （3）数据库系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）数据库系统开启审计功能，审计进程正常； ■MS_SQL 数据库系统审计级别为“失败和成功的登陆” ■MS_SQL 数据库系统启用C2审核跟踪 （2）审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）数据库宿主系统日期、时间正常； （2）数据库系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括重要用户行为 ■包括系统资源的异常使用情况 ■包括重要系统命令的使用 ■包括重要的安全相关事件	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）数据库系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）数据库系统针对日志、审计记录具备充足的存储容量； （3）MS_SQL数据库系统日志文件安装路径下的log文件（\SQL Server\MSSQLMSSQLSERVER\MSSQL\Log\ERRORLOG）everyone用户没有写权限； （4）日志及审计记录保存大于6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要	（1）数据库系统不存在此部分的控制需求，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	求；		
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）数据库系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）补丁安装前进行安全性和兼容性测试； （3）在系统上线或发生重大变更时测试并安装数据库安全补丁； （4）MS_SQL分离默认安装的示例数据库； （5）数据库系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■使用数据库级的加密（TDE） 重要配置数据: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■使用数据库级的加密（TDE）	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）数据库系统定义了相关重要数据； ■包括鉴别数据 ■包括重要配置数据 ■包括重要审计数据 （2）单位具备合理的重要数据的备份策略规范； （3）数据库系统定期完全依照备份策略，采用正确的配置进行本地备份；	符合

安全控制点	测评指标	结果结论	符合程度
		（4）系统的备份周期为：每天一次增量、每月一次全备； （5）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）数据库系统未能提供异地数据备份功能。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）数据库系统不保存终端历史记录； （3）MS_SQL引用产品测试结果，信息删除后可法保证完全清除。	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）数据库存储的用户个人信息均为业务应用必需的环节。	符合
	b）应禁止未授权访问和非法使用用户个人信息。	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； ■包括信息采集 ■包括信息保存 ■包括信息访问 ■包括信息使用 （2）数据库具备控制措施禁止未授权访问用户个人信息表单； （3）数据库具备控制措施禁止非法使用用户个人信息表单。	符合

D.4.1.4.2 应用/数据库服务器-Tomcat

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）Tomcat中间件关闭web管理控制台，其身份鉴别功能由宿主操作系统实现，不适用。	不适用
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）Tomcat中间件关闭web管理控制台，其身份鉴别功能由宿主操作系统实现，不适用。	不适用
	c）当进行远程管理时，应	（1）Tomcat中间件关闭web管理控制台，其	不适用

安全控制点	测评指标	结果结论	符合程度
	采取必要措施防止鉴别信息在网络传输过程中被窃听。	身份鉴别功能由宿主操作系统实现，不适用。	
访问控制	a) 应对登录的用户分配账户和权限；	（1）对应不同的账户均按需分配不同的用户权限，不存在中间件用户均属于管理级别、高权限的情况； （2）中间件配置可降权启动Tomcat的用户； （3）宿主系统针对中间件用户分别赋予相应的管理操作权限。 ■包括审计权限 ■包括操作权限	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）中间件不存在除如:Tomcat、admin、manager、role1等默认账户名； （2）中间件账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）中间件不存在多余或过期账户； （2）中间件管理员用户与账户之间一一对应； （3）中间件启用合规的管理用户名配置。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）中间件根据安全策略要求对特权用户及宿主管理用户进行分离； （2）中间件管理不存在多个管理级别高的特权用户； （3）中间件管理按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）中间件开启审计功能，审计进程正常； ■开启Cataline引擎的日志文件 catalina.org.apache.juli.FileHandler.level = FINE ■开启内部代码丢出的日志 localhost.org.apache.juli.FileHandler.level = FINE ■开启manager应用日志 manager.org.apache.juli.FileHandler.level = FINE ■开启控制台输出的日志 java.util.logging.ConsoleHandler.level = FINE ■开启Access访问日志。 server.xml文件配置正常，未被注释标记<!-- -->。 （2）系统的日志审计级别满足要求。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件	（1）中间件日期、时间正常； （2）中间件审计记录开启审核策略且日志级	符合

安全控制点	测评指标	结果结论	符合程度
	类型、事件是否成功及其他与审计相关的信息；	别正常。 ■日志级别不低于“FINE” ■日志配置pattern值设为common ■日志配置pattern值为自定义格式，至少包含：%h %l %u %t %s	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）中间件限制审计文件的访问控制权限，普通用户不可删除及修改； ■localhost.log 644 ■catalina.log 644 ■host-manager.log 644 ■manager.log 644 （2）宿主系统针对中间件日志、审计记录具备充足的存储容量； ■日志存储在/log/tomcat/目录下 ■日志创建计划为每天/每周/每月 ■不限制最大日志文件大小 （3）对中间件审计记录进行定期存档备份，其备份策略有效； （4）审计记录及日志保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）中间件系统不存在此部分的安装控制需求，不适用。	不适用
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）Tomcat中间件的管理地址限制功能由宿主操作系统实现，故该项不适用。	不适用
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）中间件管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）中间件管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）中间件已根据需要不定期地对已发布的版本进行更新； （2）中间件更新安装前进行安全性和兼容性测试； （3）在系统上线或发生重大变更时测试并安装最新的中间件版本或更新补丁； （4）在不影响业务系统正常运行情况下，对发现的中间件漏洞在确保安全的情况下进行修补；	符合

安全控制点	测评指标	结果结论	符合程度
		（5）中间件进行扫描未发现存在可造成高风险的漏洞。	
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输 ■宿主机使用RDP高密级加密协议进行传输 重要配置数据: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输 ■宿主机使用RDP高密级加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）中间件系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）中间件系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）中间件系统的备份周期为：每天一次增量、每月一次全备； （5）中间件系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合

安全控制点	测评指标	结果结论	符合程度
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	(1)宿主系统具有清除用户鉴别信息的功能; （2）经测试，宿主系统退出后无法访问先前中间件登录过的页面; （3）经测试，宿主系统关闭后无残留的中间件用户鉴别信息。	符合
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息;	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用

D.4.1.5 业务应用系统/平台

D.4.1.5.1 科研创新信息化管理系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换;	（1）系统对各登录模式均启用身份鉴别; ■包括管理后台认证 （2）系统对登录管理的用户进行身份鉴别; ■采用用户名 ■采用密码 （3）系统登录用户设置的身份标识具有唯一性; （4）系统不存在空口令用户; （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施;	（1）系统启用合规登录失败处理策略; ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）系统配置合规的操作超时退出措施。 ■管理后台配置超时15分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）应用系统的用户鉴别数据采用SHA-512算法在可控网络环境中传输; （2）系统配置合规的远程管理模式。 ■启用HTTPS	符合
访问控制	a) 应对登录的用户分配账户和权限;	（1）可提供系统权限分配表; (2)登录系统的用户均相应分配不同的账户，不存在使用共用账户的情况; （3）对应不同的账户均按需分配不同的用户	符合

安全控制点	测评指标	结果结论	符合程度
		权限，不存在所有用户均属于管理级别、高权限的情况。	
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）系统禁用默认账户名； （2）系统账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）系统不存在多余或过期账户； （2）系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）系统不存在多个管理级别高的特权用户； （2）系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）系统开启审计功能，审计进程正常； （2）系统的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）系统日期、时间正常； （2）系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）系统针对日志、审计记录具备充足的存储容量； （3）审计记录及日志保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）应用软件系统不存在此部分的安装控制需求，不适用。	不适用
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）应用软件系统不存在此部分的控制需求，不适用。	不适用
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）系统自身设定有效的终端访问策略，通过访问措施进行管理地址的限制。 ■系统管理页面仅能内网登录	符合
	d) 应提供数据有效性检验	（1）系统具备数据有效性检验功能；	符合

安全控制点	测评指标	结果结论	符合程度
	功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	■可校验录入数据 ■可校验文档内容 （2）系统的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）系统已根据需要不定期地对已发布的版本进行更新； （2）在系统上线或发生重大变更时测试并安装最新的版本或更新补丁； （3）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）应用软件系统不存在此部分的控制需求，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）应用软件系统不存在此部分的控制需求，不适用。	不适用
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规	符合

安全控制点	测评指标	结果结论	符合程度
		范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）系统具有清除用户鉴别信息的功能； （2）经测试，系统退出后无法访问先前登录过的页面； （3）经测试，系统关闭后无残留的用户鉴别信息。	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息； （3）系统采集的用户个人信息均为业务应用必需的环节。	符合
	b）应禁止未授权访问和非法使用用户个人信息。	（1）系统不采集和保存任何形式的用户个人信息； （2）系统对所有涉及个人信息的环节均有明确的授权同意过程； ■包括信息采集 ■包括信息保存 ■包括信息访问 ■包括信息使用 （3）系统具备控制措施禁止未授权访问用户个人信息； （4）系统具备控制措施禁止非法使用用户个人信息。	符合

D.4.1.6 数据资源

D.4.1.6.1 重要业务数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	（1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要业务数据	符合

安全控制点	测评指标	结果结论	符合程度
		（2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份重要数据； ■包括重要业务数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）该测评项测评对象鉴别数据，已在安全计算环境层面其他对象判定，此项不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）该测评项测评对象为重要个人信息的内容，已在安全计算环境层面其他对象判定，该项不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）该测评项测评对象为重要个人信息的内容，已在安全计算环境层面其他对象判定，该项不适用。	不适用

D.4.1.6.2 重要个人信息

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	（1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要个人信息 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份重要数据； ■包括重要个人信息 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、	符合

安全控制点	测评指标	结果结论	符合程度
		每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）该测评项测评对象鉴别数据，已在安全计算环境层面其他对象判定，此项不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息； （3）系统采集的用户个人信息均为业务应用必需的环节。	符合
	b）应禁止未授权访问和非法使用用户个人信息。	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； ■包括信息采集 ■包括信息保存 ■包括信息访问 ■包括信息使用 （2）系统具备控制措施禁止未授权访问用户个人信息； （3）系统具备控制措施禁止非法使用用户个人信息。	符合

D.4.1.6.3 鉴别数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	业务终端-1、业务终端-2、应用/数据库服务器、运维及管理终端-1、运维及管理终端-2: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	符合

安全控制点	测评指标	结果结论	符合程度
		WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 应用/数据库服务器-MSSQL: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■使用数据库级的加密（TDE） 科研创新信息化管理系统: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输 应用/数据库服务器-Tomcat: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输 ■宿主机使用RDP高密级加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	该测评项在各系统及设备已做判定,数据资源针对鉴别数据不做判定	不适用
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	该测评项在各系统及设备已做判定,数据资源针对鉴别数据不做判定，不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	应用/数据库服务器-Tomcat: （1）宿主系统具有清除用户鉴别信息的功能； （2）经测试，宿主系统退出后无法访问先前中间件登录过的页面； （3）经测试，宿主系统关闭后无残留的中间	符合

安全控制点	测评指标	结果结论	符合程度
		件用户鉴别信息。 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）网络层设备不适用。 业务终端-1、业务终端-2、应用/数据库服务器、运维及管理终端-1、运维及管理终端-2: （1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用 科研创新信息化管理系统: （1）系统具有清除用户鉴别信息的功能； （2）经测试，系统退出后无法访问先前登录过的页面； （3）经测试，系统关闭后无残留的用户鉴别信息。 应用/数据库服务器-MSSQL: （1）身份鉴别信息释放或清除机制正常且满足要求； （2）数据库系统不保存终端历史记录； （3）MS_SQL引用产品测试结果，信息删除后可法保证完全清除。	
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	鉴别数据不存在此部分的控制需求,故此项不适用	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	鉴别数据不存在此部分的控制需求,故此项不适用	不适用

D.4.1.6.4 重要配置数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	科研创新信息化管理系统: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输 应用/数据库服务器-Tomcat: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）中间件对重要数据在传输过程中采取必	符合

安全控制点	测评指标	结果结论	符合程度
		要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输 ■宿主机使用RDP高密级加密协议进行传输 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 应用/数据库服务器-MSSQL: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■使用数据库级的加密（TDE） 业务终端-1、业务终端-2、应用/数据库服务器、运维及管理终端-1、运维及管理终端-2: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	应用/数据库服务器-Tomcat: （1）中间件系统定义了相关重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）中间件系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）中间件系统的备份周期为：每天一次增量、每月一次全备； （5）中间件系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢	符合

安全控制点	测评指标	结果结论	符合程度
		复申请表》。 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）设备定义了相关重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 业务终端-1、业务终端-2、应用/数据库服务器、运维及管理终端-1、运维及管理终端-2: （1）操作系统定义了相关重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 科研创新信息化管理系统: （1）系统定义了相关需要备份重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 应用/数据库服务器-MSSQL: （1）数据库系统定义了相关重要数据； ■包括重要配置数据	

安全控制点	测评指标	结果结论	符合程度
		（2）单位具备合理的重要数据的备份策略规范； （3）数据库系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	应用/数据库服务器: （1）设备为服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、运维安全管理系统、防火墙-1、防火墙-2: （1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 应用/数据库服务器-MSSQL: （1）数据库系统未能提供异地数据备份功能。 应用/数据库服务器-Tomcat、科研创新信息化管理系统: （1）单位未能提供异地数据备份措施。 业务终端-1、业务终端-2、运维及管理终端-1、运维及管理终端-2: （1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 核心交换机、汇聚交换机: （1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配	重要配置数据不存在此部分的控制需求,故此项不适用	不适用

安全控制点	测评指标	结果结论	符合程度
	前得到完全清除。		
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	重要配置数据不存在此部分的控制需求,故此项不适用	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	重要配置数据不存在此部分的控制需求,故此项不适用	不适用

D.4.1.7 其他系统或设备

无

D.5 安全管理中心

D.5.1 安全通用要求

D.5.1.1 管理中心

安全控制点	测评指标	结果结论	符合程度
系统管理	a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；	（1）网络中部署运维安全管理系统实现集中的系统管理； （2）系统对登录用户进行身份鉴别； ■包括合规的用户名 ■包括合规的口令策略 （3）系统用户标识具有唯一性； ■不存在多人共享 ■增加、删除用户或权限变更需经过审批 （4）系统可实现对账户的身份鉴别数据进行保密性和完整性保护； （5）系统管理操作模式具备控制措施； ■只允许系统管理员登录 ■具备特定的登录命令 ■具备特定的登录操作界面 （6）系统具备相应的管理操作审计措施。 ■可实现对系统管理操作进行审计 ■审计范围覆盖所有用户 ■操作审计不可被删除	符合
	b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。	（1）系统管理员对系统的资源和运行进行配置、控制和管理； ■包括用户身份管理 ■包括资源配置管理 ■包括系统加载和启动管理 ■包括系统运行的异常处理管理 ■包括数据和设备的备份与恢复管理 （2）系统的资源、运行及配置管理不够全面。 ■缺乏可信证书管理 ■缺乏可信基准库管理	不符合
审计管理	a) 应对审计管理员进行身份鉴别，只允许其通过特	（1）网络中部署运维安全管理系统实现集中安全审计功能；	符合

安全控制点	测评指标	结果结论	符合程度
	定的命令或操作界面进行安全审计操作，并对这些操作进行审计；	（2）审计系统对审计管理员进行身份鉴别； ■包括合规的用户名 ■包括合规的口令策略 （3）审计系统用户标识具有唯一性； ■不存在多人共享 ■增加、删除用户或权限变更需经过审批 （4）审计系统管理操作模式具备控制措施； ■只允许审计管理员登录 ■具备特定的登录命令 ■具备特定的登录操作界面 (5)审计系统具备相应的管理操作审计措施。 ■可实现对安全审计操作进行审计 ■审计范围覆盖所有审计管理用户 ■操作审计不可被删除	
	b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	科研创新信息化管理系统: （1）审计管理员定期对审计记录进行分析，对发现的安全可疑事件及时处理； （2）单位具有安全审计策略文件，规范审计记录的存储、管理和查询要求； （3）审计管理员按规范要求对审计记录进行管理。 ■审计记录不可随意删除/修改 ■定期备份、存储审计记录 ■审计记录存储周期满足6个月要求 重要审计数据: 日志审计系统、运维安全管理系统: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要审计数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■网络设备、安全设备使用rsyslog协议进行传输 ■Windows操作系统使用插件+SSL协议进行传输	符合

D.6 安全管理制度

D.6.1 安全通用要求

D.6.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度

安全控制点	测评指标	结果结论	符合程度
安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。	（1）单位具有网络安全工作的总体方针和安全策略文件； ■具备独立的网络安全总体方针文件 ■具备涵盖网络安全总体方针策略要求的相关管理文件 ■具备安全策略文件 （2）制度内容包括明确的单位安全工作要求； ■安全目标 ■安全范围 ■安全原则 ■安全框架 ■各类安全策略 （3）管理文件详见《信息安全总体策略》。	符合
管理制度	a）应对安全管理活动中的主要管理内容建立安全管理制度；	（1）单位有针对安全管理活动中的各类管理内容建立安全管理制度； （2）现有制度已覆盖管理活动的主要的方面； ■具备文件控制管理 ■具备安全检查管理 ■具备人力资源及培训 ■具备设备管理 ■具备软件开发/外包开发项目管理 ■具备机房安全管理 ■具备信息分类及管理 ■具备网络安全管理 ■具备系统安全管理 ■具备恶意代码管理 ■具备变更控制 ■具备备份及介质管理 ■具备事件管理 ■具备应急预案 （3）制度详见：《信息安全总体策略》、《网络安全管理规范》、《组织安全结构和人员职责制度》、《人员管理制度》、《员工考核管理制度》。	符合
	b）应对管理人员或操作人员执行的日常管理操作建立操作规程。	（1）单位针对相关业务日常管理的操作建立规程类管理制度； （2）现有制度已覆盖重要管理方面的系统维护手册和用户操作规程等； ■具备网络/安全管理 ■具备服务器管理 ■具备数据库管理 ■具备机房硬件设施管理 ■具备业务应用管理	符合

安全控制点	测评指标	结果结论	符合程度
		（3）管理文件详见《设备及系统软件配置和操作手册》。	
制定和发布	a）应指定或授权专门的部门或人员负责安全管理制度的制定；	（1）单位针对安全管理制度的制定，指定教育信息与网络中心部主要负责； （2）在已制定的相关制度中可查阅到被授权制定管理制度的部门/人员信息； （3）管理文件详见《安全管理组织规范》。	符合
	b）安全管理制度应通过正式、有效的方式发布，并进行版本控制。	（1）单位针对制度的制定和发布要求，制定管理规范文件； （2）管理规范文件对文件制定及发布定义了规范要求； ■包括安全管理制度的制定和发布程序 ■包括格式要求 ■包括版本编号要求 （3）安全管理制度的收发登记记录有效； ■具备通过正式、有效的方式收发 ■具备正式发文 ■具备领导签署、单位盖章等 （4）管理文件详见《制度制定、发布、评审和修订管理制度》、《收发文登记记录》。	符合
评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	（1）单位针对制度的合理性和适用性需进行论证和审定及修订的要求，制定管理规范文件； （2）管理规范文件对制度的评审及修订定义了规范要求； （3）单位具有安全管理制度的审定或论证的过程记录； （4）单位对做过修订的制度，具备有修订版本的安全管理过程记录； （5）管理文件详见《制度制定、发布、评审和修订管理制度》及 《安全管理制度评审记录》。	符合

D.7 安全管理机构

D.7.1 安全通用要求

D.7.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
岗位设置	a）应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；	（1）单位已明确网络安全管理工作的职能部门，并明确了各岗位职责； ■已设置机房管理员 ■已设置网络管理员 ■已设置安全管理员	符合

安全控制点	测评指标	结果结论	符合程度
		（2）单位各部门职责文档已明确网络安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备网络安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	
	b）应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。	（1）单位已明确系统安全管理工作的职能部门，并明确了各岗位职责； ■已设置系统管理员 ■已设置数据管理员 ■已设置审计管理员 ■已设置应用管理员 （2）单位各部门职责文档已明确系统安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备系统安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	符合
人员配备	应配备一定数量的系统管理员、审计管理员和安全管理员等。	（1）单位针对人员配备要求，制定了管理制度； （2）单位按要求配备一定数量的重要岗位管理人员； （3）单位针对各岗位人员，制定并维护人员档案； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	符合
授权和审批	a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；	（1）单位在制度中用文字描述或在流程图中明确，对关键活动进行审批； ■具备部门职责文档明确各部门审批事项 ■具备岗位职责文档明确各岗位审批事项 （2）单位对审批过程明确审批权限，对各项信息系统的重要操作与变更明确审批部门和批准人； （3）管理文件详见《授权和审批管理规定》。	符合
	b）应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。	（1）单位针对各项业务操作及变更等建立了审批程序规定； ■包括系统变更 ■包括重要操作 ■包括物理访问 ■包括系统接入 （2）单位针对系统变更、系统接入、物理范围等事项已明确按审批程序执行,记录有批准人签字；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）管理文件详见《授权和审批管理规定》。	
沟通和合作	a）应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；	（1）单位针对机构内部管理人员之间、部门之间的沟通与合作，制定了管理制度； （2）单位的管理制度规范了合作和沟通的方式和周期； （3）单位有组织机构内部人员联系表； （4）单位有定期召开信息安全会议，保存有会议纪要； （5）管理文件详见《安全教育和培训制度》、《技能培训记录》《外部联系表》。	符合
	b）应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；	（1）单位针对加强与外部单位的合作与沟通，制定了管理制度规定； ■包括公安机关 ■包括网络安全职能部门 ■包括职能监管机构 ■包括各类供应商 ■包括业界专家 ■包括安全组织 （2）单位能按要求与相关单位保持沟通合作，并提供相关单位联系方式和交流会议纪要； （3）管理文件详见《安全教育和培训制度》、《技能培训记录》、《外部联系表》。	符合
	c）应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	（1）单位建立了完善的对外联单位的联系列表； ■记录单位名称 ■记录合作内容 ■记录联系人 ■记录联系方式 （2）管理文件详见《外部联系表》。	符合
审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。	（1）单位针对定期开展常规安全检查，制定了管理制度； （2）单位对检查工作的范围、过程、要求等管理的比较完善； ■系统日常运行 ■系统漏洞 ■数据备份 ■包括敏感系统检查人员 （3）单位已按要求由安全管理员定期检查，检查内容需覆盖系统运行相关的管理活动，并能提供安全检查报告； （4）管理文件详见《安全审查和检查管理规范》； （5）单位开展的检查工作不够完善。	部分符合

安全控制点	测评指标	结果结论	符合程度
		■未定期检查	

D.8 安全管理人员

D.8.1 安全通用要求

D.8.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
人员录用	a) 应指定或授权专门的部门或人员负责人员录用；	（1）单位授权专门的部门负责人员录用工作，制定了管理制度规范； （2）由人力资源保障科负责人员录用工作； （3）管理文件详见《人员管理制度》。	符合
	b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查。	（1）单位针对人员录用过程，制定了明确要求，并形成人员安全管理制度； （2）单位现有管理制度明确说明录用人员应具备的条件； ■包括学历/学位要求 ■包括技术人员的专业技术要求 ■包括管理人员的安全管理要求 （3）单位按规定执行人员录用的相关审查过程； ■包括录用人身份 ■包括安全背景 ■包括专业资格 ■包括资质 （4）管理文件详见《人员管理制度》、《人员入职考核记录》。	符合
人员离岗	应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。	（1）单位针对离岗人员权限终止及取回机构提供的各种设施的要求，制定了管理制度； （2）单位按规范开展对离岗人员的相关管理工作； ■明确负责部门 ■及时终止其访问权限 ■交还身份证件 ■交还软硬件设备 （3）管理文件详见《人员管理度》、《人员离岗申请表》、《离场信息资料交接表》。	符合
安全意识教育和培训	应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。	（1）单位针对人员安全培训及责任和惩戒措施，制定了管理制度； （2）单位已开展安全意识教育及岗位技能培训 ■具备明确培训周期 ■具备有效的培训方式 ■具备清晰的培训内容	符合

安全控制点	测评指标	结果结论	符合程度
		■具备考核要求 （3）管理文件详见《安全教育和培训制度》。	
外部人员访问管理	a）应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；	（1）单位针对外部人员物理访问，制定了外部人员访问管理文档； ■明确允许外部人员访问的范围 ■明确外部人员进入的条件 ■明确外部人员进入的访问控制措施 （2）单位具备有效的外部人员访问重要区域的书面申请文档； ■具有申请人 ■具有申请原因 ■具有范围 ■具有日期 ■具有批准人签字 （3）单位具备外部人员访问重要区域的登记记录； ■记录进入时间、 ■记录离开时间 ■记录访问区域 ■记录陪同人信息 （4）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。	符合
	b）应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；	（1）单位针对外部接入受控网络访问系统，制定了管理制度； （2）单位具备外部人员接入受控网络前的申请审批流程； （3）单位具备外部人员接入及访问系统的书面申请文档； ■具有申请人 ■具有申请原因 ■具有访问权限 ■具有日期 ■具有批准人签字 （4）单位具备外部人员接入及访问系统的登记记录； ■记录访问权限 ■记录访问时限 ■记录账户 （5）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申	符合

安全控制点	测评指标	结果结论	符合程度
		请表》、《外部人员访问记录表》。	
	c) 外部人员离场后应及时清除其所有的访问权限。	（1）单位针对人员离场后的清理工作，制定了管理制度； （2）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》； （3）单位未完全按管理规范开展人员离场后的清理工作。 ■缺乏清理记录 ■未及时清除离场后的所有访问权限 ■未记录访问权限清除时间	不符合

D.9 安全建设管理

D.9.1 安全通用要求

D.9.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
定级和备案	a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；	（1）单位的被测系统于2022年4月已完成备案； （2）系统备案相关文档（定级报告）中明确等级划分方法和理由，SAG三个方面的级别描述清晰； （3）管理文件详见《定级备案》。	符合
	b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；	（1）单位针对系统定级结果的审批及评审工作等要求，制定了管理制度； （2）现有系统的定级已具备合理性和正确性审定； ■具备单位部门审定 （3）管理文件详见《定级备案》。	符合
	c) 应保证定级结果经过相关部门的批准；	（1）单位针对系统定级结果的上级批准要求，制定了管理制度； （2）现有系统的定级获得了相关部门的批准； （3）管理文件详见《定级备案》。	符合
	d) 应将备案材料报主管部门和相应公安机关备案。	（1）单位对被测系统的等级备案表、定级报告等备案材料已经报相应公安机关备案； （2）单位具备公安机关出具的备案号； （3）管理文件详见《定级备案》。	符合
安全方案设计	a) 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；	（1）单位未具备适用于被测系统的安全规划设计方案； （2）现有方案文档未能完全按照规范要求选择安全措施。 ■缺乏安全保护等级的要求	不符合

安全控制点	测评指标	结果结论	符合程度
		■缺乏风险分析结果的要求 ■缺乏实际安全需求	
	b) 应根据保护对象的安全保护等级进行安全方案设计；	（1）单位未具备完整的安全设计方案相关的文档。 ■缺乏总体规划 ■缺乏安全设计方案 ■缺乏相关配套文件 ■缺乏保护对象的安全保护等级要求	不符合
	c) 应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； ■缺乏安全整体规划 ■缺乏安全设计方案 ■缺乏安全配套文件 （2）单位未对相关论证过程及内容进行完整的记录。	不符合
产品采购和使用	a) 应确保网络安全产品采购和使用符合国家的有关规定；	（1）单位已建立安全产品管理的相关管理规定； ■包括采购要求 ■包括使用要求 （2）单位具备安全产品采购流程及相关实施文档； （3）被测系统使用的安全产品具备销售许可资质； （4）安全产品具均为国内产品； （5）管理文件详见《设备安全管理制度》。	符合
	b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。	（1）单位已建立密码产品与服务管理的相关管理制度； ■包括采购要求 ■包括使用要求 （2）系统未使用密码产品； （3）管理文件详见《设备安全管理制度》。	符合
自行软件开发	a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。	不适用
	b) 应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。	不适用
外包软件开发	a) 应在软件交付前检测其中可能存在的恶意代码；	（1）单位针对软件交付前测试恶意代码的要求，制定了管理制度； （2）管理文件详见《外包开发软件管理规定》； （3）单位未在软件交付之前按要求对所有软件开展恶意代码检测。	不符合

安全控制点	测评指标	结果结论	符合程度
		■缺乏恶意代码检测报告	
	b) 应保证开发单位提供软件设计文档和使用指南。	（1）单位制定软件开发项目验收要求，明确开发单位的提交材料； （2）开发单位提供软件日常维护和使用所需的文档； ■包括需求分析说明书 ■包括软件设计说明书 ■包括软件操作手册 （3）管理文件详见《外包开发软件管理规定》、《设备及系统软件配置和操作手册》。	符合
工程实施	a) 应指定或授权专门的部门或人员负责工程实施过程的管理；	（1）单位针对专门的部门负责工程实施过程的管理要求，制定管理度； （2）单位由专岗负责系统建设的工程实施，且按照实施方案的要求对进度和质量进行控制； （3）管理文件详见《工程实施管理制度》。	符合
	b) 应制定安全工程实施方案控制工程实施过程。	（1）单位制定了详细的工程实施方案； ■包括工程时间限制 ■包括进度控制 ■包括质量控制 （2）工程实施单位严格按照方案执行，并有过程记录； （3）管理文件详见《测试及验收方案》、《工程项目实施方案》。	符合
测试验收	a) 应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；	（1）单位可提供被测系统的合规测试验收方案； ■包括测试人员 ■包括测试验收内容 ■包括现场操作过程 （2）管理文件详见《测试及验收方案》、《工程项目实施方案》； （3）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。 ■缺乏验收报告 ■缺乏报告审定意见	部分符合
	b) 应进行上线前的安全性测试，并出具安全测试报告。	（1）单位对系统上线前需开展安全性测试的要求，制定管理制度； （2）管理文件详见《外包开发软件管理规定》、《系统交付管理》； （3）针对系统上线前的安全性测试工作存在问题。 ■缺乏测试报告	不符合
系统交付	a) 应制定交付清单，并根	（1）单位具备系统交付清单；	符合

安全控制点	测评指标	结果结论	符合程度
	据交付清单对所交接的设备、软件和文档等进行清点；	（2）系统交付清单内容较详细； ■包括设备 ■包括软件 ■包括文档 （3）单位的清点工作较合规； ■已依据交付清单开展清点工作 （4）管理文件详见《系统交付管理》、《资产清单》。	
	b）应对负责运行维护的技术人员进行相应的技能培训；	（1）单位已对负责系统运行维护的技术人员进行了技能培训； （2）具备运维人员的培训记录； ■包括培训时间 ■包括培训地点 ■包括培训对象 ■包括培训内容 ■包括培训参与人员签字 （3）管理文件详见《系统交付管理》、《资产清单》、《系统交付清单》、《技能培训记录》。	符合
	c）应提供建设过程文档和运行维护文档。	（1）单位提供了系统建设过程中的文档； （2）单位提供了指导用户进行系统运维的文档和系统培训手册； （3）管理文件详见《系统交付管理》、《系统交付清单》、《设备及系统软件配置和操作手册》。	符合
等级测评	a）应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；	（1）单位针对系统等级测评要求，制定管理制度； （2）系统按要求开展首次测评工作； （3）管理文件详见《系统安全管理制度》。	符合
	b）应在发生重大变更或级别发生变化时进行等级测评；	（1）管理制度中已规定在系统发生变更时及时对系统进行等级测评； （2）系统未发生过重大变更，系统等级未发生变化； （3）管理文件详见《系统安全管理制度》。	符合
	c）应确保测评机构的选择符合国家有关规定。	（1）已选择在“全国等级保护测评机构推荐目录”中的测评单位进行等级测评； （2）管理文件详见《系统安全管理制度》、《网络安全等级保护测评服务合同》。	符合
服务供应商选择	a）应确保服务供应商的选择符合国家的有关规定；	（1）单位在管理制度内明确提出安全服务供应商选择的要求； （2）单位选择的安全服务商符合国家的有关规定，具备相应的安全服务资质； （3）管理文件详见《服务供应商选择安全管	符合

安全控制点	测评指标	结果结论	符合程度
		理制度》、《深信服安全采购合同》。	
	b) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。	（1）单位的管理制度中已规定，需与安全服务商签订安全相关的协议并明确整个服务供应链各方需履行的网络安全相关义务； （2）单位已按规定与选定的安全服务商签订合规的协议； ■明确整个服务供应链各方需履行的网络安全相关义务 ■包括保密范围 ■包括安全责任 ■包括违约责任 ■包括协议的有效期限 ■包括责任人签字 （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。	符合

D.10 安全运维管理

D.10.1 安全通用要求

D.10.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
环境管理	a) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；	（1）单位建立机房安全方面的管理制度，对有关运维方面的管理作出规定； ■指定教育信息与网络中心部门负责管理 ■包括出入管理要求 ■包括定期维护要求 ■包括空调要求 ■包括供配电设备要求 ■包括消防设施要求 ■包括温湿度控制要求 （2）单位具备完整的机房出入登记记录； ■记录来访人员 ■记录来访时间 ■记录离开时间 ■记录携带物品 （3）单位具备完整的机房基础设施的维护记录； ■记录维护日期 ■记录维护人 ■记录维护设备 ■记录故障原因 ■记录维护结果 （4）管理文件详见《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、	符合

安全控制点	测评指标	结果结论	符合程度
		《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。	
	b) 应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；	（1）单位建立机房安全方面的管理制度； ■包括物理访问管理 ■包括物品进出管理 ■包括环境安全管理 （2）单位现有机房管理记录与制度相符； ■具备物理访问记录 ■具备物品进出记录 ■具备环境安全相关记录 （3）制度详见：《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。	符合
	c) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	（1）单位机房安全管理制度已明确来访人员的接待区域的要求； （2）单位按规范要求开展人员来访接待； ■划分来访人员的接待区域 ■记录来访人员的情况 （3）单位办公环境未发现有随意放置含有敏感信息介质的情况； ■无纸档文件 ■无移动介质 （4）制度详见：《机房安全管理制度》、《物理安全管理规范》、《办公环境保密管理》。	符合
资产管理	应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。	（1）单位已建立有效的资产清单； （2）单位现有资产清单内容较全面； ■包括设备设施类别 ■包括软件类别 ■包括文档类别 ■包括资产责任人 ■包括所属级别 ■包括所处位置 ■包括所处部门 （3）制度详见：《设备安全管理制度》、《资产清单》。	符合
介质管理	a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；	（1）介质按管理要求放置于受控的环境中（如：机房）； （2）介质管理具备较全面的记录； ■包括介质归档 ■包括使用情况 ■包括定期盘点记录 （3）制度详见：《设备安全管理制度》、《介	符合

安全控制点	测评指标	结果结论	符合程度
		质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。	
	b) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。	（1）介质管理制度中对介质安全传输有明确规定； ■包括人员选择 ■包括打包要求 ■包括交付要求 （2）存储重要信息的介质在物理传输过程，具备严格的环节控制，无重大环节疏漏； （3）对介质的归档和查询均具备记录； （4）制度详见：《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。	符合
设备维护管理	a) 应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	（1）单位人员岗位职责相关文档已明确设备维护管理的责任部门； （2）单位对各类设施、设备进行定期维护； （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。	符合
	b) 应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。	（1）单位建立了配套设施、软硬件维护管理方面的管理制度； ■包括维护人员的责任 ■包括维修和服务的审批 ■包括维修过程的监督控制 （2）单位开展相关工作与制度相符，且保留记录； ■包括维修和服务审批 ■包括维修过程记录 （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。	符合
漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。	（1）单位制定管理制度，规范对安全漏洞和隐患的检测、识别及评估修补要求； （2）制度详见：《恶意代码防范管理制度》； （3）单位未严格按规范开展漏洞及安全隐患检测工作。 ■未定期开展漏洞扫描	不符合
网络和系统安全管理	a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；	（1）单位建立系统安全管理文档，对系统管理员的管理制定了要求； ■包括角色划分 ■包括角色的责任	符合

安全控制点	测评指标	结果结论	符合程度
		■包括角色权限 （2）单位对各类关键角色建立了相应的工作职责文档； ■包括安全管理员 ■包括网络管理员 ■包括系统管理员 ■包括数据管理员 ■包括审计管理员 （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	
	b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	（1）单位制定管理制度，对系统账号进行管理； ■指定专人 ■包括申请账户管理 ■包括建立账户管理 ■包括删除账户管理 （2）单位按管理规范开展账号管理工作； ■具备相关审批流程 ■具备相关审批记录 ■具备管理登记记录 （3）账户管理记录内容较完整； ■包括变更日期 ■包括变更时间 ■包括变更人 ■包括变更设备/系统 ■包括变更结果 （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	符合
	c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	（1）单位建立了网络和系统安全管理制度； （2）网络和系统安全管理制度内容较全面； ■包括安全策略要求 ■包括账户管理 ■包括配置文件的生成及备份 ■包括变更审批管理 ■包括授权访问 ■包括最小服务控制 ■包括升级与打补丁管理 ■包括审计日志管理 ■包括口令管理 （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	符合
	d）应制定重要设备的配置和操作手册，依据手册对	（1）单位对重要设备、系统的配置和操作建立配置手册；	符合

安全控制点	测评指标	结果结论	符合程度
	设备进行安全配置和优化配置等；	■包括操作系统 ■包括数据库 ■包括网络设备 ■包括安全设备 ■包括应用和组件 （2）现有操作配置手册已明确操作步骤、参数配置； （3）制度详见：《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。	
	e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。	（1）单位制定日常运维管理的相关制度规范； （2）单位按制度规范开展日常运维管理工作； （3）单位具备合规的运维记录； ■包括日常巡检记录 ■包括运行维护记录 ■包括参数的设置记录 ■包括参数的修改记录 （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》、《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。	符合
恶意代码防范管理	a）应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	（1）单位制定恶意代码防范管理制度，明确对外来计算机或存储设备接入系统前进行恶意代码检查； （2）单位按外来计算机接入恶意代码检查规范开展工作； ■对外来计算机接入进行恶意代码检查 ■具备合规的检测记录 （3）单位制定培训管理制度，明确需通过培训提升员工的防恶意代码意识； （4）单位按培训管理要求开展工作； ■定期对员工开展防恶意代码意识培训 ■具备合规的培训记录 （5）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申请表》、《信息管理系统漏洞检查表》。	符合
	b）应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；	（1）建立恶意代码防范管理文档； （2）管理制度中覆盖防恶意代码软件的授权使用、恶意代码库升级、定期查杀等内容； （3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》。	符合
	c）应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处	（1）单位指定专门的部门负责定期验证防范恶意代码攻击的技术措施的有效性； （2）单位近期未发生过严重的恶意代码攻击	部分符合

安全控制点	测评指标	结果结论	符合程度
	理。	事件； （3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申请表》、《信息管理系统漏洞检查表》； （4）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。 ■未定期对相关产品的恶意代码库进行升级 ■未对所有防病毒产品上截获的恶意代码进行分析并汇总上报	
配置管理	应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。	（1）单位制定了基本配置信息管理的制度要求； ■包括网络拓扑结构 ■包括设备安装的软件组件 ■包括软件组件的版本 （2）管理文件详见：《主机安全管理规范》、《网络安全管理规范》、《应用安全管理规范》、《网络配置信息》。	符合
密码管理	a）应遵循密码相关国家标准和行业标准；	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	不符合
	b）应使用国家密码管理主管部门认证核准的密码技术和产品。	（1）单位未采购涉及密码技术的产品，不适用。	不适用
变更管理	应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。	（1）单位建立了关于系统变更管理的制度文件； （2）现有变更管理制度覆盖了变更管理的各方面要求； ■包括变更管理要求 ■包括整体变更管理流程 ■包括变更内容分析与论证 ■包括变更方案审批流程 ■包括变更后通报 （3）制度详见：《变更控制管理制度》、《通用变更记录表》。	符合
备份与恢复管理	a）应识别需要定期备份的重要业务信息、系统数据及软件系统等；	（1）单位根据业务重要程度，制定了需要定期备份的重要业务信息列表或清单。清单内需要定期备份的重要数据已经过用户方确认； （2）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。	符合
	b）应规定备份信息的备份	（1）单位建立了备份与恢复管理相关的安全	符合

安全控制点	测评指标	结果结论	符合程度
	方式、备份频度、存储介质、保存期等；	管理制度； （2）备份与恢复管理的相关要求比较明确； ■规定备份方式 ■规定备份频度 ■规定存储介质 ■规定保存期 （3）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。	
	c）应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	（1）单位现有管理制度，明确了数据备份策略和数据恢复策略，以及备份程序和恢复程序； （2）单位可按策略要求实现重要数据的定期备份与恢复性测试； （3）单位现有的备份的数据均经过恢复性测试，可确保备份的数据可用； （4）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。	符合
安全事件处置	a）应及时向安全管理部门报告所发现的安全弱点和可疑事件；	（1）单位已在安全培训及宣传过程中告知用户在发现安全弱点和可疑事件时及时向安全管理部门报告； （2）单位在系统运维过程中对发现的安全弱点和可疑事件均编制了对应的报告或相关文档； （3）单位现有安全弱点和可疑事件报告文档内容较详实； （4）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	符合
	b）应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；	（1）单位制定了安全事件报告和处置管理制度； （2）现有安全事件管理制度内容较完整； ■包括安全事件类型分类 ■包括安全事件有关的工作职责 ■包括安全事件的报告 ■包括安全事件的处置 ■包括安全事件的响应流程 （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	符合
	c）应在安全事件报告和响应处理过程中，分析和鉴	（1）单位具备对安全事件的分析、处理、总结、防范等的报告／过程文档；	符合

安全控制点	测评指标	结果结论	符合程度
	定事件产生的原因，收集证据，记录处理过程，总结经验教训。	（2）单位提供的安全事件报告和响应处置记录内容较完整； ■记录引发安全事件的原因 ■记录事件的证据 ■记录处置过程 ■包括经验教训 ■提出补救措施 （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	
应急预案管理	a）应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；	（1）单位制定重要事件的应急预案； （2）单位现有应急预案涉及的类型范围较全面； ■包括针对机房的预案 ■包括针对网络传输的预案 ■包括针对网络设备的预案 ■包括针对操作系统的预案 ■包括针对数据库的预案 ■包括针对安全漏洞攻击的预案 ■包括针对恶意代码的预案 ■包括针对数据泄露的预案 （3）单位现有应急预案的内容较完整； ■明确重要事件的应急处理流程 ■明确系统恢复流程等内容 （4）制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。	符合
	b）应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。	（1）单位定期对相关人员进行应急预案培训； （2）单位根据不同的应急预案，按要求进行应急演练； （3）单位具备近期应急预案工作开展的相关记录； ■具备培训记录 ■具备演练记录 （4）单位提供的应急预案培训记录比较完整； ■明确培训对象 ■明确培训内容 ■明确培训结果 （5）单位提供的应急预案演练记录比较完整； ■记录演练时间 ■记录主要操作内容 ■记录演练结果 （6）经检查单位目前一旦出现应急事件，可参照预案合理有序的进行应急事件处置过程； （7）制度详见：《网络安全事件应急预案》、	符合

安全控制点	测评指标	结果结论	符合程度
		《应急预案培训记录表》。	
外包运维管理	a) 应确保外包运维服务商的选择符合国家的有关规定；	(1)单位目前未涉及任何外包运维服务情况，不适用。	不适用
	b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。	(1)单位目前未涉及任何外包运维服务情况，不适用。	不适用

D.11 其他安全要求

本次测评不涉及其他安全要求指标。

附录E 漏洞扫描结果记录

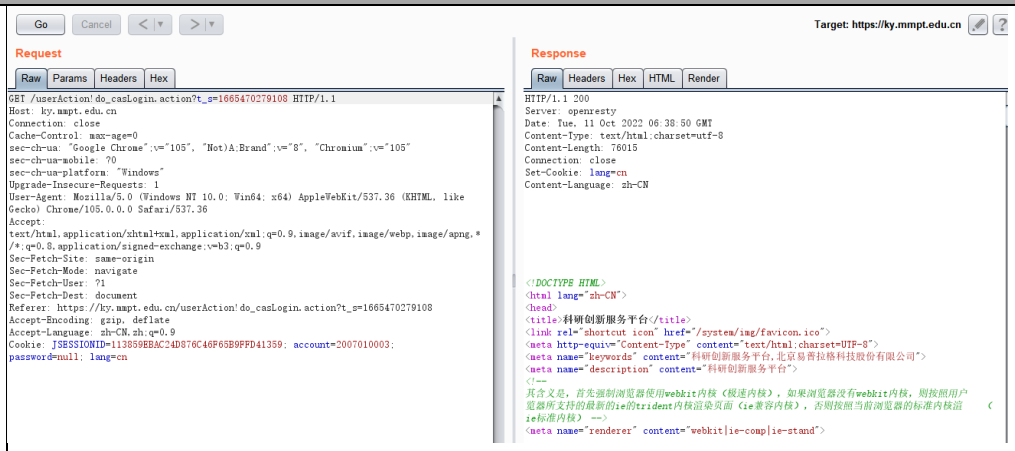
附录E表-1漏洞扫描主要安全漏洞

序号	危险程度	漏洞名称	影响IP
1	低	允许Traceroute探测 此类漏洞涉及网络设备、安全设备、服务器存储设备。	10.2.4.10/应用/数据库服务器 10.2.1.4/运维安全管理系统 10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/上网行为管理系统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/汇聚交换机 172.16.1.2/核心交换机
2	低	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161) 此类漏洞涉及网络设备。	172.16.1.2/核心交换机

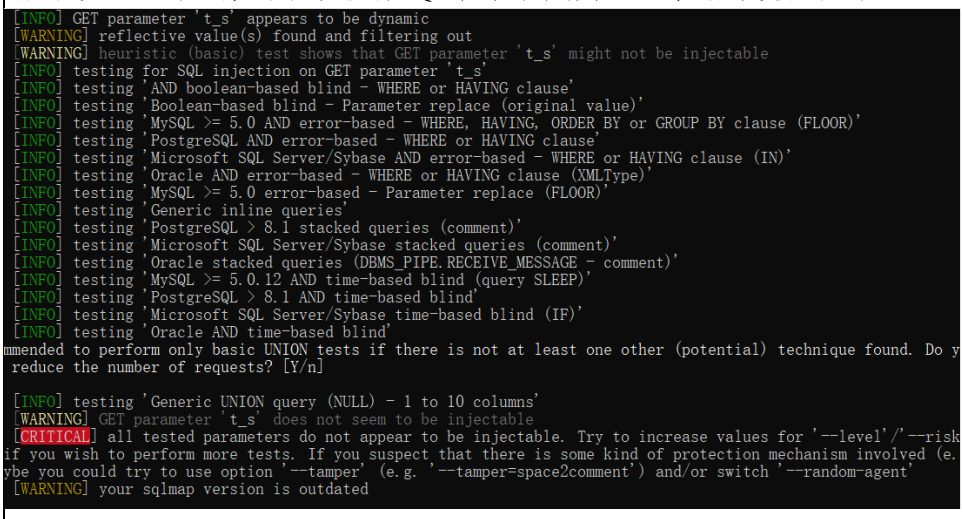
附录F 渗透测试结果记录

F.1 业务应用软件平台 缺少“X-Content-Type-Options”响应头

缺少“X-Content-Type-Options”响应头	
危险程度	低
渗透位置	JB,JC
影响URL实体	https://ky.mmpt.edu.cn/userAction!do_casLogin.action?t_s=1665470279108
渗透详情	渗透方法：BurpSuite抓包检测 采用的工具：BurpSuite 测试过程：响应包中没有X-Content-Type-Options响应头，如下图：

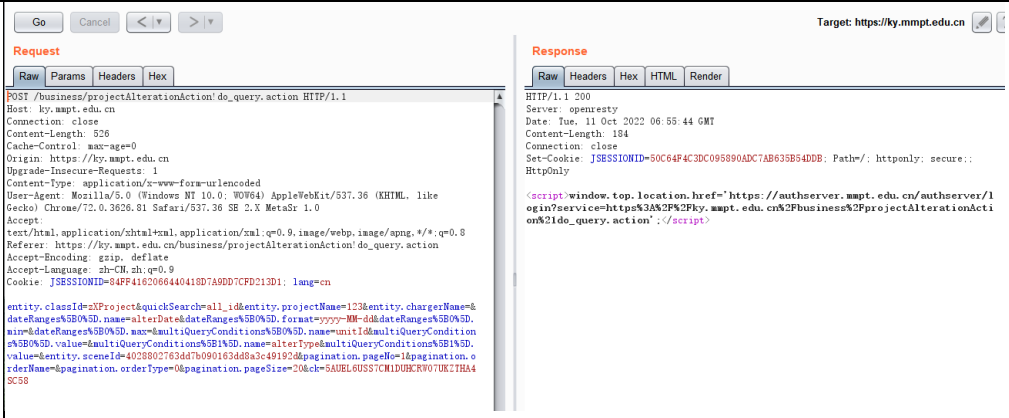
缺少“X-Content-Type-Options”响应头


F.2 业务应用软件平台 SQL注入漏洞

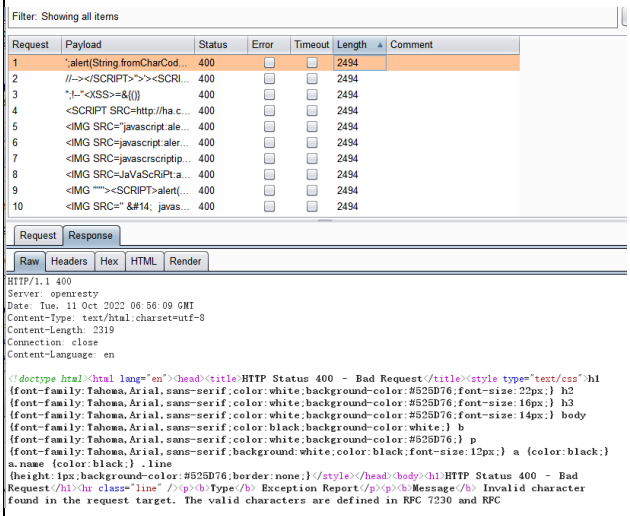
SQL注入漏洞	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：通过手工或工具检测系统在执行SQL语句时是否存在注入。 采用的工具：Sqlmap 测试过程：已检测，系统在执行SQL语句时不存在注入，暂未发现该漏洞。 

F.3 业务应用软件平台 未授权访问

未授权访问	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：测试能否在系统未登录的状态下进行登录后功能访问或操作。 采用的工具：Burpsuite 测试过程：已检测，不能在系统未登录的状态下进行功能访问或操作。

未授权访问	
	

F.4 业务应用软件平台　　XSS跨站脚本攻击

XSS跨站脚本攻击	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：测试是否对客户端输入的HTML代码、客户端脚本进行过滤或限制。 采用的工具：Burpsuite 测试过程：经检测，已对客户端输入的HTML代码、客户端脚本进行过滤或限制，暂未发现该漏洞。 

附录G 威胁列表

附录G 表- 1威胁列表

序号	威胁列表	描述
1	恶意攻击	利用工具和技术对信息系统进行攻击和入侵。威胁行为包括：恶意代码、邮件勒索、网络攻击等。
2	软硬件故障	对业务实施或系统运行产生影响的设备硬件故障、通讯链路中断、系统本身或软件缺陷造等问题。威胁行为包括：设备故障、软件故障等。
3	管理不到位	由于制度缺失、不完善等原因导致安全管理无法落实或者不到位。威胁行为包括：管理不到位、媒体负面报道等。

序号	威胁列表	描述
4	无作为或操作失误	应该执行而没有执行相应的操作，或者无意执行了错误的操作。威胁行为包括：操作失误、维护错误等。
5	敏感信息泄漏	敏感信息泄露给不应了解的他人。威胁行为包括：内部信息泄露、外部信息泄露等。
6	物理环境影响	对信息系统正常运行造成影响的物理环境问题和自然灾害。威胁行为包括：物理损害等。
7	越权或滥用	越权访问本来无权访问的资源，或者滥用自己的权限破坏信息系统。威胁行为包括：未授权的设备使用、权限滥用、权限伪造等。
8	物理攻击	通过物理的接触造成对软件、硬件和数据的破坏。威胁行为包括：设备失效等。
9	篡改	非法修改信息，破坏信息的完整性使系统的安全性降低或信息不可用。威胁行为包括：硬件篡改、数据篡改等。
10	抵赖	否认所做的操作。威胁行为包括：行为否认（抵赖）、媒体负面报道等。

报告编号：44090243008-00001-22-0163-01

网络安全等级保护
门户网站系统等级测评报告

委托单位：茂名职业技术学院

测评单位：广东南方信息安全研究院

报告时间：2022年10月30日

网络安全等级测评基本信息表

被测对象				
被测对象名称	门户网站系统		安全保护等级	第二级（S2A2）
备案证明编号	44090243008-00001			
被测单位				
单位名称	茂名职业技术学院			
单位地址	广东省茂名市茂南区文明北路232号大院		邮政编码	525000
联系人	姓名	龙恒	职务/职称	教师
	所属部门	教育信息与网络中心	办公电话	0668-2920122
	移动电话	13377766618	电子邮件	372383968@qq.com
测评单位				
单位名称	广东南方信息安全研究院		机构代码	SC202127130010163
单位地址	广州市科学城彩频路9号B座12楼1202		邮政编码	510663
联系人	姓名	谢若雨	职务/职称	助理
	所属部门	办公室	办公电话	020-32290702
	移动电话	18819149895	电子邮件	office@cybersec-gd.cn
审核批准	编制人	林炳良	编制日期	2022.10.30
	审核人	王[illegible]	审核日期	2022.10.30
	批准人	陈[illegible]	批准日期	2022.10.30

声明

本报告是门户网站系统的等级测评报告。

本报告测评结论的有效性建立在被测评单位提供相关证据的真实性基础之上。

本报告中给出的测评结论仅对被测对象当时的安全状态有效。当测评工作完成后，由于被测对象发生变更而涉及到的系统构成组件（或子系统）本报告不再适用。

本报告中给出的测评结论不能作为对被测对象内部部署的相关系统构成组件（或产品）的测评结论。

在任何情况下，若需引用本报告中的测评结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。

单位名称：广东南方信息安全研究院

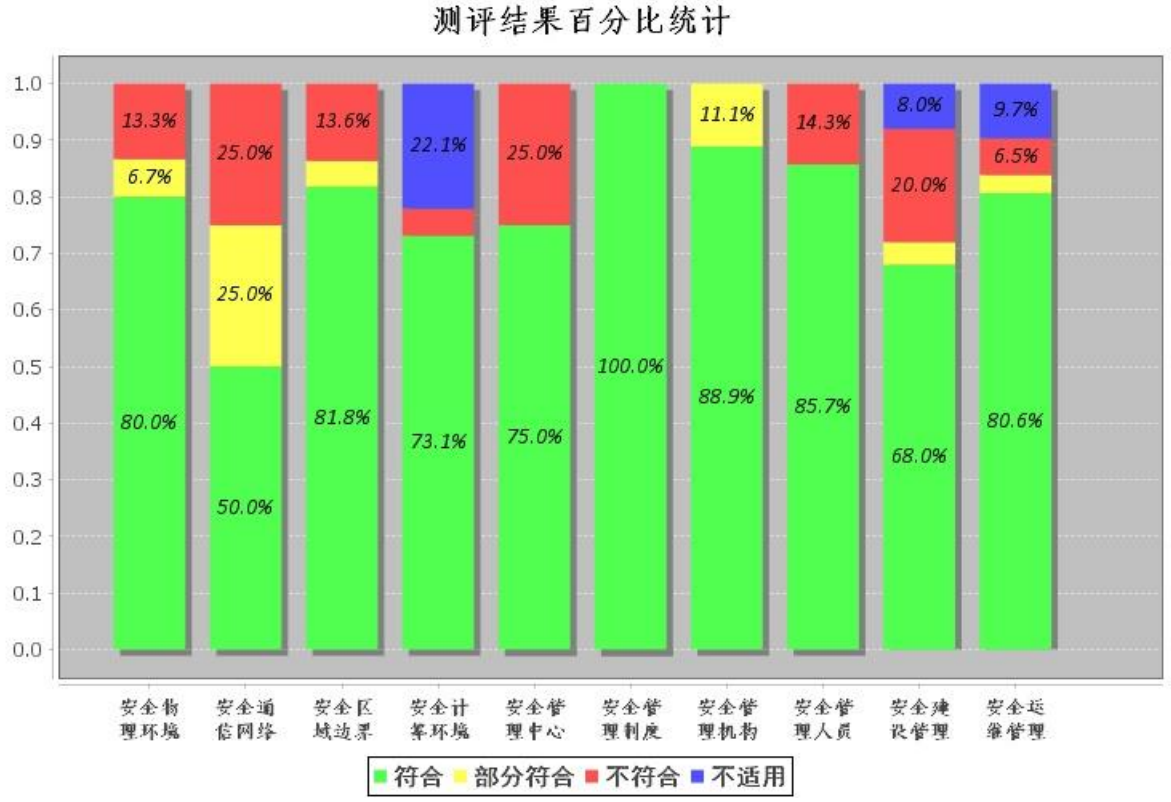
2022年10月30日

等级测评结论

测评结论和综合得分			
被测对象名称	门户网站系统	安全保护等级	第二级（S2A2）
扩展要求应用情况	□云计算 □移动互联 □物联网 □工业控制系统 □大数据		
被测对象描述	门户网站系统是由茂名职业技术学院统一组织规划建设，由西安博达软件股份有限公司负责开发，于2018年10月正式投入运行，由教育信息与网络中心负责运行维护。茂名职业技术学院是该信息系统的业务主管部门，茂名职业技术学院为该信息系统定级的责任单位。 门户网站系统网络主要分为4个区域，分别为外网边界区域、安全管理区域、服务器存储区域、办公网区域，主要由网络设备、安全设备组成，对互联网提供业务访问。门户网站系统为B/S结构，主要由Linux平台的操作系统，PostgreSQL平台的数据库系统，及Tomcat中间件系统组成。单位采用自主运维模式，通过部署运维及管理终端提供专用运维环境管理，采用运维安全管理系统实现设备的统一管理，并进行操作运维审计，日志审计系统进行设备日志统一收集存储与分析。 门户网站系统是学校对外的信息门户，前台包含学院概况、机构设置、教学在线、学术科研、招生就业、队伍建设、学工在线、团员青年、校友会等栏目。后台包括新增/删除站点，用户管理，数据备份和恢复，安全检测、敏感词检测、运维监控等功能，通过门户网站对外发布学校动态、消息，是学院对外宣传的官方门户。		
安全状况描述	门户网站系统通信传输具备一定的保护措施，安全区域边界较清晰，网络层具备访问控制、安全审计的相应技术措施。各设备在访问控制、安全审计、入侵防范方面具备控制措施。重要数据在数据完整性方面具备保护措施。在安全管理制度层面较为完善。在网络架构不够完整，网络层在入侵防范、恶意代码和垃圾邮件防范的技术措施存在不足。各设备在身份鉴别方面控制措施存在不足。重要数据在数据备份恢复方面存在不足。 门户网站系统在本次测评中总共出现28类问题，其中0类高风险问题，12类中风险问题，16类低风险问题。在本次测评通过扫描及渗透发现4类漏洞问题，其中0类危险程度为高的漏洞，0类危险程度为中的漏洞，4类危险程度为低的漏洞。 门户网站系统本次等级测评的综合得分为73.35，且不存在高等级安全风险，等级测评结论为中。		
等级测评结论	中	综合得分	73.35

总体评价

通过对信息系统基本安全保护状态的分析，茂名职业技术学院针对门户网站系统面临的主要安全威胁采取了相应的安全机制，基本达到保护信息系统重要资产的作用。门户网站系统在本次测评中采用了GB/T 22239-2019，其中安全通用要求135项，不适用7项。



在安全物理环境方面，针对安全通用要求，基础设施在防雷击、电磁防护、防水和防潮、物理位置选择、电力供应、防盗窃和防破坏、温湿度控制等方面较为完善（如：信息化机房）。在物理访问控制、防静电等方面还不够完善（如：信息化机房），机房出入口未配置电子门禁系统，机房内缺乏防静电措施（如防静电地板或铺设防静电地毯）。

在安全通信网络方面,针对安全通用要求,网络环境在通信传输等方面较为完善(如:安全通信网络)。在网络架构等方面还不够完善（如：安全通信网络），关键的应用服务和数据库服务网段未独立进行子网划分的情况。

在安全区域边界方面，针对安全通用要求，网络环境在边界防护、安全审计、访问控制等方面较为完善（如：外网边界区域，安全管理区域，服务器存储区域等）。在入侵防范、恶意代码和垃圾邮件防范等方面还不够完善(如:安全管理区域,办公网区域),网络层部署防火墙,防火墙未配置对内部发起的攻击行为实现防范功能策略,无法检测、防止或限制从内部发起的网络攻击行为,现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。

在安全计算环境方面，针对安全通用要求，计算环境在安全审计、数据完整性、访问控制、入侵防范、恶意代码防范、剩余信息保护等方面较为完善（如：业务终端-2，业务终端-1，应用服务器-1等）。在主机方面，在可信验证等方面还不够完善（如：业务终端-2，业务终端-1，运维及管理终端-2等），缺乏对计算设备可信验证方面的安全设计要求，现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。在应用方面，在身份鉴别等方面还不够完善（如：数据库服务器-PostgreSQL），数据库系统未配置鉴别失败处理功能，数据库系统存在不合规的登录连接超时及自动退出策略；在数据备份恢复等方面还不够完善（如：应用服务器-1-Tomcat），未能提供中间件重要数据的异地定时数据备份功能。在网络及安全设备方面,在可信验证等方面还不够完善(如:基线核查系统，上网行为管理系统，WEB应用防火墙等），设备不具备相关可信验证的技术措施。在数据保护方面,在数据备份恢复等方面还不够完善(如:重要业务数据),未能提供应用软件系统重要数据的异地定时数据备份功能。

在安全管理中心方面，针对安全通用要求，安全控制措施在审计管理等方面较为完善（如：管理中心）。在系统管理等方面还不够完善（如：管理中心），系统管理的资源、运行及配置管理不够全面。

在安全管理制度方面，针对安全通用要求，管理制度体系在制定和发布、安全策略、管理制度、评审和修订等方面较为完善（如：制度文件、执行/记录文件）。

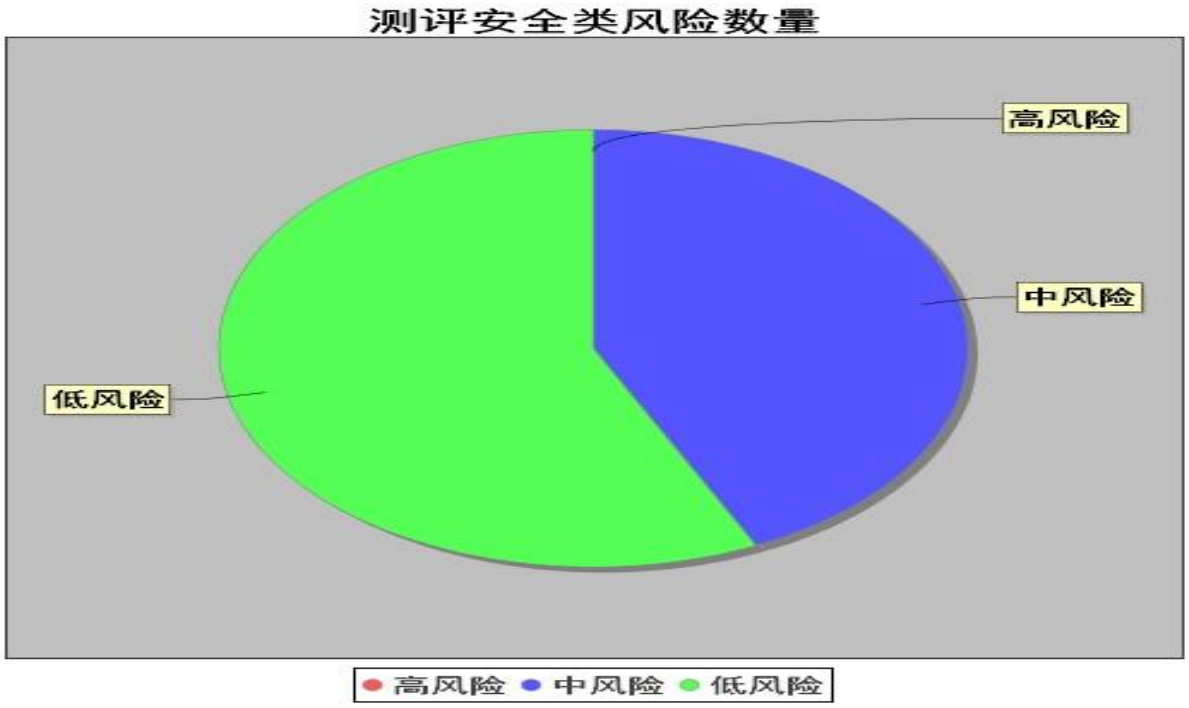
在安全管理机构方面，针对安全通用要求，机构建设在人员配备、沟通和合作、授权和审批、岗位设置等方面较为完善（如：制度文件、执行/记录文件）。在审核和检查等方面还不够完善（如：制度文件、执行/记录文件），单位开展的检查工作不够完善。

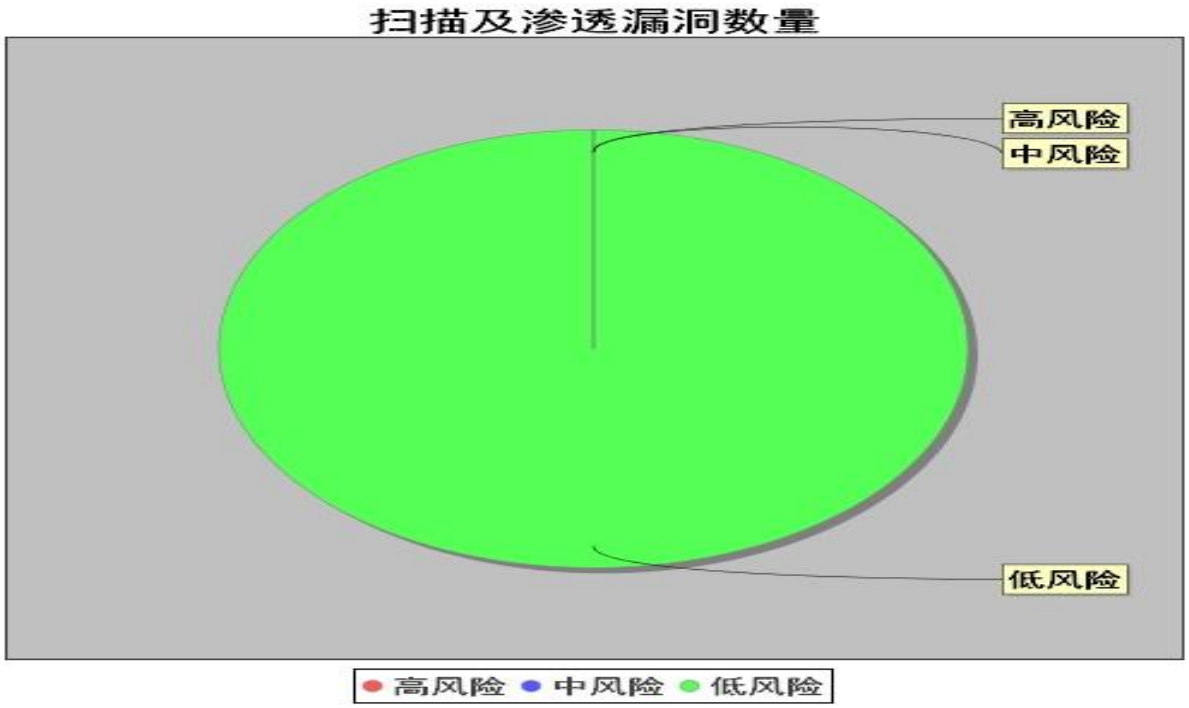
在安全管理人员方面，针对安全通用要求，人员在人员录用、安全意识教育和培训、人员离岗等方面较为完善（如：制度文件、执行/记录文件）。在外部人员访问管理等方面还不够完善（如：制度文件、执行/记录文件），单位未完全按管理规范开展人员离场后的清理工作。

在安全建设管理方面，针对安全通用要求，系统建设在定级和备案、工程实施、等级测评、产品采购和使用、服务供应商选择、系统交付等方面较为完善（如：制度文件、执行/记录文件）。在安全方案设计等方面还不够完善（如：制度文件、执行/记录文件），单位未具备完整的安全设计方案相关的文档，单位相关方案的设计的内容不够完善。

在安全运维管理方面，针对安全通用要求，系统运维在介质管理、设备维护管理、网络和系统安全管理、备份与恢复管理、资产管理、应急预案管理、环境管理、配置管理、安全事件处置、变更管理等方面较为完善（如：制度文件、执行/记录文件）。在密码管理等方面还不够完善（如：制度文件、执行/记录文件），单位不了解现有密码相关的国家标准和行业标准，单位缺乏密码管理要求的制度文档。

门户网站系统在本次测评中总共出现28类问题，其中0类高风险问题,12类中风险问题，16类低风险问题。在本次测评通过扫描及渗透发现4类漏洞问题，其中0类危险程度为高的漏洞，0类危险程度为中的漏洞，4类危险程度为低的漏洞。





门户网站系统本次等级测评的综合得分为73.35，且不存在高等级安全风险，等级测评结论为中。

主要安全问题及整改建议

一、安全物理环境

安全通用要求

(1)中风险 机房出入口未配置电子门禁系统（如：信息化机房）。 上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域,可能对系统的平稳运行造成影响。

建议安排专人7*24小时负责机房出入，对出入的人员进行身份鉴别和登记，且出入有专人陪同或在机房出入口配置电子门禁系统，控制、鉴别和记录进入的人员。

(2)中风险 机房内缺乏防静电措施（如防静电地板或铺设防静电地毯 ）（如：信息化机房）。 存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。

建议采用防静电地板或地面并采用必要的接地防静电措施。

二、安全通信网络

安全通用要求

(1)中风险 关键的应用服务和数据库服务网段未独立进行子网划分的情况（如：安全通信网络）。 上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变得更为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。

建议独立划分出应用服务器网段、数据库服务器网段。

三、安全区域边界

安全通用要求

(1)中风险 网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为（如：办公网区域）。 存在不

能及时发现内部主机作为攻击跳板，或网络攻击行为而造成系统损坏/网络资源浪费的风险。

建议网络层部署的防火墙配置对内部发起的攻击行为实现防范功能策略，实现检测、防止或限制从内部发起的网络攻击行为。

(2)中风险 现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面（如：办公网区域）。 无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。

建议现有部署的恶意代码防范措施网络边界覆盖全面，及时对恶意代码及逆行检测和清除。

四、安全计算环境

1、网络设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

2、安全设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

3、服务器和终端

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

4、系统管理软件/平台

安全通用要求

(1)中风险 数据库系统未配置鉴别失败处理功能。数据库系统存在不合规的登录连接

超时及自动退出策略（如：数据库服务器-PostgreSQL）。 登录验证可能被恶意用户猜测获得，合法用户身份被仿冒，导致系统被非授权访问。

建议数据库系统开启失败登录处理功能，如限制非法登录次数、自动退出功能、锁定时间等。

(2)中风险 未能提供中间件重要数据的异地定时数据备份功能（如：应用服务器-1-Tomcat）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。

建议利用通信网络将中间件关键数据定时批量传送至备用场地，实现异地数据异地备份。

5、业务应用系统/平台

安全通用要求

(1)中风险 未能提供应用软件系统重要数据的异地定时数据备份功能（如：门户网站系统）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。

建议利用通信网络将应用软件系统关键数据定时批量传送至备用场地，实现异地数据异地备份。

6、数据资源

安全通用要求

重要业务数据

(1)中风险 未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要业务数据）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。

建议利用通信网络将应用软件系统关键数据定时批量传送至备用场地，实现异地数据异地备份。

7、其他系统或设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

五、安全管理中心

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

六、安全管理制度

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

七、安全管理机构

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

八、安全管理人员

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

九、安全建设管理

安全通用要求

(1)中风险 单位未具备完整的安全设计方案相关的文档。单位相关方案的设计的内容不够完善（如：制度文件、执行/记录文件）。 相关合规的规划配套文件缺失，可能导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。

建议根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件。

十、安全运维管理

安全通用要求

(1)中风险 **单位不了解现有密码相关的国家标准和行业标准。单位缺乏密码管理要求的制度文档（如：制度文件、执行/记录文件）。 密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不到位，存在违反国家政策的风险。**

建议单位学习现有密码相关的国家标准和行业标准。建立密码管理要求的制度文档。

目录

网络安全等级测评基本信息表 I
声明 II
等级测评结论 III
总体评价 IV
主要安全问题及整改建议 VIII
一、安全物理环境 VIII
安全通用要求 VIII
二、安全通信网络 VIII
安全通用要求 VIII
三、安全区域边界 VIII
安全通用要求 VIII
四、安全计算环境 IX
1、网络设备 IX
安全通用要求 IX
2、安全设备 IX
安全通用要求 IX
3、服务器和终端 IX
安全通用要求 IX
4、系统管理软件/平台 IX
安全通用要求 IX
5、业务应用系统/平台 X
安全通用要求 X
6、数据资源 X
安全通用要求 X
7、其他系统或设备 XI
安全通用要求 XI
五、安全管理中心 XI
安全通用要求 XI
六、安全管理制度 XI
安全通用要求 XI
七、安全管理机构 XI
安全通用要求 XI
八、安全管理人员 XI
安全通用要求 XI
九、安全建设管理 XI
安全通用要求 XI
十、安全运维管理 XII
安全通用要求 XII

目录.....XIII
1 测评项目概述.....1
1.1 测评目的.....1
1.2 测评依据.....1
1.3 测评过程.....2
1.4 报告分发范围.....5
2 被测对象描述.....5
2.1 被测对象概述.....5
2.1.1 定级结果.....5
2.1.2 业务和采用的技术.....5
2.1.3 网络结构.....5
2.2 测评指标.....7
2.2.1 安全通用要求指标.....7
2.2.2 安全扩展要求指标.....9
2.2.3 其他安全要求指标.....10
2.2.4 不适用安全要求指标.....10
2.3 测评对象.....11
2.3.1 测评对象选择方法.....12
2.3.2 测评对象选择结果.....13
2.3.2.1 物理机房.....13
2.3.2.2 网络设备.....13
2.3.2.3 安全设备.....13
2.3.2.4 服务器.....14
2.3.2.5 终端设备.....14
2.3.2.6 其他系统或设备.....15
2.3.2.7 系统管理软件/平台.....15
2.3.2.8 业务应用软件/平台.....15
2.3.2.9 数据资源.....16
2.3.2.10 安全相关人员.....16
2.3.2.11 安全管理文档.....17
3 单项测评结果分析.....22
3.1 安全物理环境.....22
3.1.1 已有安全控制措施汇总分析.....22
3.1.2 主要安全问题汇总分析.....24
3.2 安全通信网络.....24
3.2.1 已有安全控制措施汇总分析.....24
3.2.2 主要安全问题汇总分析.....25
3.3 安全区域边界.....25
3.3.1 已有安全控制措施汇总分析.....25
3.3.2 主要安全问题汇总分析.....27
3.4 安全计算环境.....27
3.4.1 网络设备.....27

3.4.1.1 已有安全控制措施汇总分析 27
3.4.1.2 主要安全问题汇总分析 29
3.4.2 安全设备 29
3.4.2.1 已有安全控制措施汇总分析 30
3.4.2.2 主要安全问题汇总分析 33
3.4.3 服务器和终端 33
3.4.3.1 已有安全控制措施汇总分析 33
3.4.3.2 主要安全问题汇总分析 38
3.4.4 系统管理软件/平台 38
3.4.4.1 已有安全控制措施汇总分析 38
3.4.4.2 主要安全问题汇总分析 41
3.4.5 业务应用系统/平台 41
3.4.5.1 已有安全控制措施汇总分析 41
3.4.5.2 主要安全问题汇总分析 43
3.4.6 数据资源 43
3.4.6.1 已有安全控制措施汇总分析 43
3.4.6.2 主要安全问题汇总分析 44
3.4.7 其他系统或设备 44
3.4.7.1 已有安全控制措施汇总分析 44
3.4.7.2 主要安全问题汇总分析 44
3.5 安全管理中心 44
3.5.1 已有安全控制措施汇总分析 44
3.5.2 主要安全问题汇总分析 45
3.6 安全管理制度 46
3.6.1 已有安全控制措施汇总分析 46
3.6.2 主要安全问题汇总分析 47
3.7 安全管理机构 47
3.7.1 已有安全控制措施汇总分析 47
3.7.2 主要安全问题汇总分析 48
3.8 安全管理人员 49
3.8.1 已有安全控制措施汇总分析 49
3.8.2 主要安全问题汇总分析 50
3.9 安全建设管理 50
3.9.1 已有安全控制措施汇总分析 50
3.9.2 主要安全问题汇总分析 52
3.10 安全运维管理 53
3.10.1 已有安全控制措施汇总分析 53
3.10.2 主要安全问题汇总分析 57
3.11 其他安全要求指标 58
3.11.1 已有安全控制措施汇总分析 58
3.11.2 主要安全问题汇总分析 58
3.12 验证测试 58
3.12.1 漏洞扫描 58
3.12.1.1 漏洞扫描结果统计 58

3.12.1.2 漏洞扫描问题描述 63
3.12.2 渗透测试 63
3.12.2.1 渗透测试过程说明 64
3.12.2.2 渗透测试问题描述 65
3.13 单项测评小结 65
3.13.1 控制点符合情况汇总 65
3.13.2 安全问题汇总 69
4 整体测评 73
4.1 安全控制点间安全测评 73
4.1.1 安全建设管理 74
4.1.1.1 安全通用要求 74
4.1.2 安全运维管理 74
4.1.2.1 安全通用要求 74
4.2 区域间安全测评 75
4.2.1 安全物理环境 75
4.2.1.1 安全通用要求 75
4.2.2 安全通信网络 75
4.2.2.1 安全通用要求 75
4.2.3 安全区域边界 75
4.2.3.1 安全通用要求 75
4.3 整体测评结果汇总 76
5 安全问题风险分析 78
6 等级测评结论 82
7 安全问题整改建议 84
附录A 被测对象资产 91
A.1 物理机房 91
A.2 网络设备 91
A.3 安全设备 91
A.4 服务器 92
A.5 终端设备 92
A.6 其他系统或设备 92
A.7 系统管理软件/平台 92
A.8 业务应用软件/平台 93
A.9 数据资源 93
A.10 密码产品 94
A.11 安全相关人员 94
A.12 安全管理文档 94
附录B 上次测评问题整改情况说明 100
附录C 单项测评结果汇总 100
C.1 安全物理环境 100

C.2 安全通信网络 100
C.3 安全区域边界 101
C.4 安全计算环境 101
C.4.1 网络设备 101
C.4.2 安全设备 102
C.4.3 服务器和终端 103
C.4.4 系统管理软件/平台 104
C.4.5 业务应用系统/平台 104
C.4.6 数据资源 105
C.4.7 其他系统或设备 105
C.5 安全管理中心 105
C.6 安全管理制度 105
C.7 安全管理机构 106
C.8 安全管理人员 106
C.9 安全建设管理 106
C.10 安全运维管理 107
C.11 其他安全要求指标 107

附录D 单项测评结果记录 108

D.1 安全物理环境 108
D.1.1 安全通用要求 108
D.1.1.1 信息化机房 108
D.2 安全通信网络 110
D.2.1 安全通用要求 110
D.2.1.1 安全通信网络 110
D.3 安全区域边界 110
D.3.1 安全通用要求 110
D.3.1.1 办公网区域 111
D.3.1.2 外网边界区域 113
D.3.1.3 安全管理区域 115
D.3.1.4 服务器存储区域 117
D.4 安全计算环境 120
D.4.1 安全通用要求 120
D.4.1.1 网络设备 120
D.4.1.2 安全设备 127
D.4.1.3 服务器和终端 152
D.4.1.4 系统管理软件/平台 182
D.4.1.5 业务应用系统/平台 189
D.4.1.6 数据资源 192
D.4.1.7 其他系统或设备 199
D.5 安全管理中心 199
D.5.1 安全通用要求 199
D.5.1.1 管理中心 199
D.6 安全管理制度 200
D.6.1 安全通用要求 201

D.6.1.1 制度文件、执行/记录文件 201
D.7 安全管理机构 202
D.7.1 安全通用要求 202
D.7.1.1 制度文件、执行/记录文件 202
D.8 安全管理人员 205
D.8.1 安全通用要求 205
D.8.1.1 制度文件、执行/记录文件 205
D.9 安全建设管理 207
D.9.1 安全通用要求 207
D.9.1.1 制度文件、执行/记录文件 207
D.10 安全运维管理 211
D.10.1 安全通用要求 211
D.10.1.1 制度文件、执行/记录文件 211
D.11 其他安全要求 219
附录E 漏洞扫描结果记录 219
附录F 渗透测试结果记录 219
附录G 威胁列表 223

1 测评项目概述

1.1 测评目的

安全等级测评的目标是通过对目标系统在安全技术及管理方面的测评,对目标系统的安全技术状态及安全管理状况做出初步判断,给出目标系统在安全技术及安全管理方面与其相应安全等级保护要求之间的差距。测评结论作为委托方进一步完善系统安全策略及安全技术防护措施依据。

项目背景是为进一步提高信息系统的保障能力,根据《信息安全等级保护管理办法》（公通字2007【43】号）的精神，茂名职业技术学院委托广东南方信息安全研究院（SC202127130010163）对门户网站系统实施等级测评，以期发现信息系统和等级保护标准的差距以及存在的安全隐患，为后续的安全整改工作提供参考依据。

1.2 测评依据

测评过程中主要依据的标准:

测评标准

（1）GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》

（2）GB/T 28448-2019 《信息安全技术 网络安全等级保护测评要求》

测评参考标准

（1）GB 17859-1999 《计算机信息系统 安全保护等级划分准则》

（2）GB/T 28449-2018 《信息安全技术 网络安全等级保护测评过程指南》

（3）GB/T 20984-2007 《信息安全技术 信息安全风险评估规范》

（4）GB/T 25058-2019 《信息安全技术 网络安全等级保护实施指南》

测评参考法律法规

（1）《中华人民共和国网络安全法》

（2）《中华人民共和国密码法》

（3）《中华人民共和国数据安全法》

1.3 测评过程

本次等级测评分为四个过程：测评准备活动、方案编制活动、测评实施活动、报告编制活动。具体如图 1-1 所示。其中，各阶段的时间安排如下：

⑴ 测评准备活动

测评准备活动的目标是顺利启动测评项目,收集定级对象相关资料,准备测评所需资料,为编制测评方案打下良好的基础。测评准备活动包括工作启动、信息收集和分析、工具和表单准备三项主要任务。

（2）方案编制活动

方案编制活动的目标是整理测评准备活动中获取的定级对象相关资料,为现场测评活动提供最基本的文档和指导方案。方案编制活动包括测评对象确定、测评指标确定、测评内容确定、工具测试方法确定、测评指导书开发及测评方案编制六项主要任务。

（3）现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调,为现场测评的顺利开展打下良好基础,依据测评方案实施现场测评工作,将测评方案和测评方法等内容具体落实到现场测评活动中。现场测评工作应取得报告编制活动所需的、足够的证据和资料。现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

（4）报告编制活动

在现场测评工作结束后,测评机构应对现场测评获得的测评结果(或称测评证据)进行汇总分析,形成等级测评结论,并编制测评报告。测评人员在初步判定单项测评结果后,还需进行单元测评结果判定、整体测评、系统安全保障评估,经过整体测评后,有的单项

测评结果可能会有所变化,需进一步修订单项测评结果,而后针对安全问题进行风险评估,形成等级测评结论。分析与报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、系统安全保障评估、安全问题风险评估、等级测评结论形成及测评报告编制七项主要任务。

各阶段完成的关键任务：

序号	阶段	任务	对象	开始日期	结束日期
1	测评准备活动	工作启动	项目甲乙双方	2022年8月15日	2022年8月19日
2		信息收集与分析	调研表	2022年8月22日	2022年8月25日
3		工具和表单准备	测评工具、测评授权书、文档交接单	2022年8月25日	2022年8月30日
4	方案编制活动	测评对象确认	测评方案-对象列表	2022年8月31日	2022年8月31日
5		测评指标确认	测评方案-指标列表	2022年8月31日	2022年8月31日
6		测评内容确认	测评方案-内容列表	2022年9月1日	2022年9月1日
7		工具测试方法确认	测评方案-工具测试方法列表	2022年9月1日	2022年9月1日
8		测评指导书开发	测评作业指导书	2022年9月2日	2022年9月2日
9		测评方案编制	测评方案	2022年9月5日	2022年9月5日
10	现场测评活动	现场测评准备	工具、人员、表单准备	2022年9月28日	2022年9月28日
11		现场测评和结果记录	安全管理访谈	2022年9月28日	2022年9月28日
12			安全管理文档检查	2022年9月28日	2022年9月28日
13			安全物理环境测评	2022年9月28日	2022年9月28日
14			安全通信网络	2022年9月28日	2022年9月29日
15			安全区域边界	2022年9月28日	2022年9月29日
16			安全计算环境	2022年9月28日	2022年9月29日
17			工具测试	2022年9月29日	2022年10月9日
18		结果确认和资料归还	检测人员出入场确认单、测评现场服务评价单	2022年10月8日	2022年10月9日
19	报告编制活动	单项测评结果	测评报告	2022年10月9日	2022年10月12日

序号	阶段	任务	对象	开始日期	结束日期
		判定			
20		单元测评结果判定		2022年10月9日	2022年10月17日
21		整体测评		2022年10月9日	2022年10月17日
22		系统安全保障评估		2022年10月9日	2022年10月17日
23		安全问题风险分析		2022年10月9日	2022年10月17日
24		等级测评结论形成		2022年10月17日	2022年10月30日
25		测评报告编制		2022年10月17日	2022年10月30日

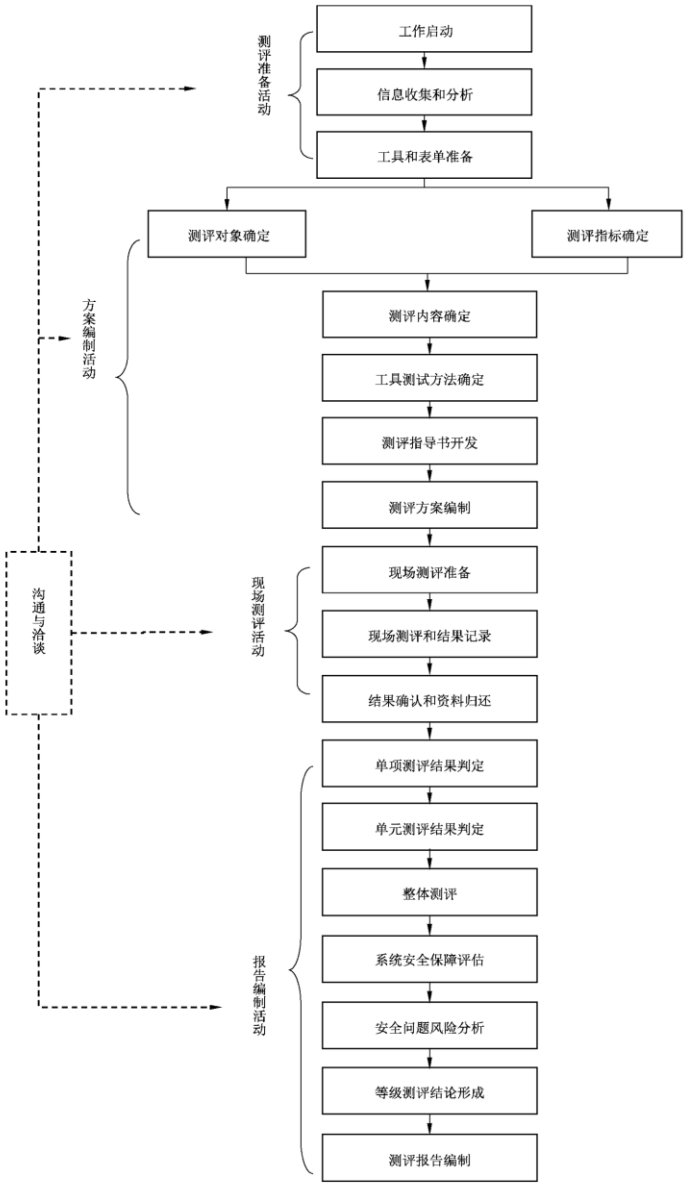


图 1-1 等级保护测评工作流程图

其中，于项目前期召开了项目启动会议，确定了工作方案及项目人员名单；于现场测评完成后召开了项目末次会议，确认了测评发现的问题；于2022年10月30日在对系统的整改情况进行了复核确认后，完成报告编制。

1.4 报告分发范围

等级测评报告正本一式3份，其中茂名职业技术学院1份，广东南方信息安全研究院1份，受理备案的公安机关1份。

2 被测对象描述

2.1 被测对象概述

2.1.1 定级结果

表 2-1定级结果

被测对象名称	安全保护等级	业务信息安全等级	系统服务安全等级
门户网站系统	2	2	2

2.1.2 业务和采用的技术

门户网站系统是学校对外的信息门户，前台包含学院概况、机构设置、教学在线、学术科研、招生就业、队伍建设、学工在线、团员青年、校友会等栏目。后台包括新增/删除站点，用户管理，数据备份和恢复，安全检测、敏感词检测、运维监控等功能，通过门户网站对外发布学校动态、消息，是学院对外宣传的官方门户。

被测对象未采用云计算/移动互联/物联网/工业控制/大数据等技术情况。

2.1.3 网络结构

门户网站系统主要是对互联网提供服务，相关设备部署在信息化机房当中,其简要拓扑如下:

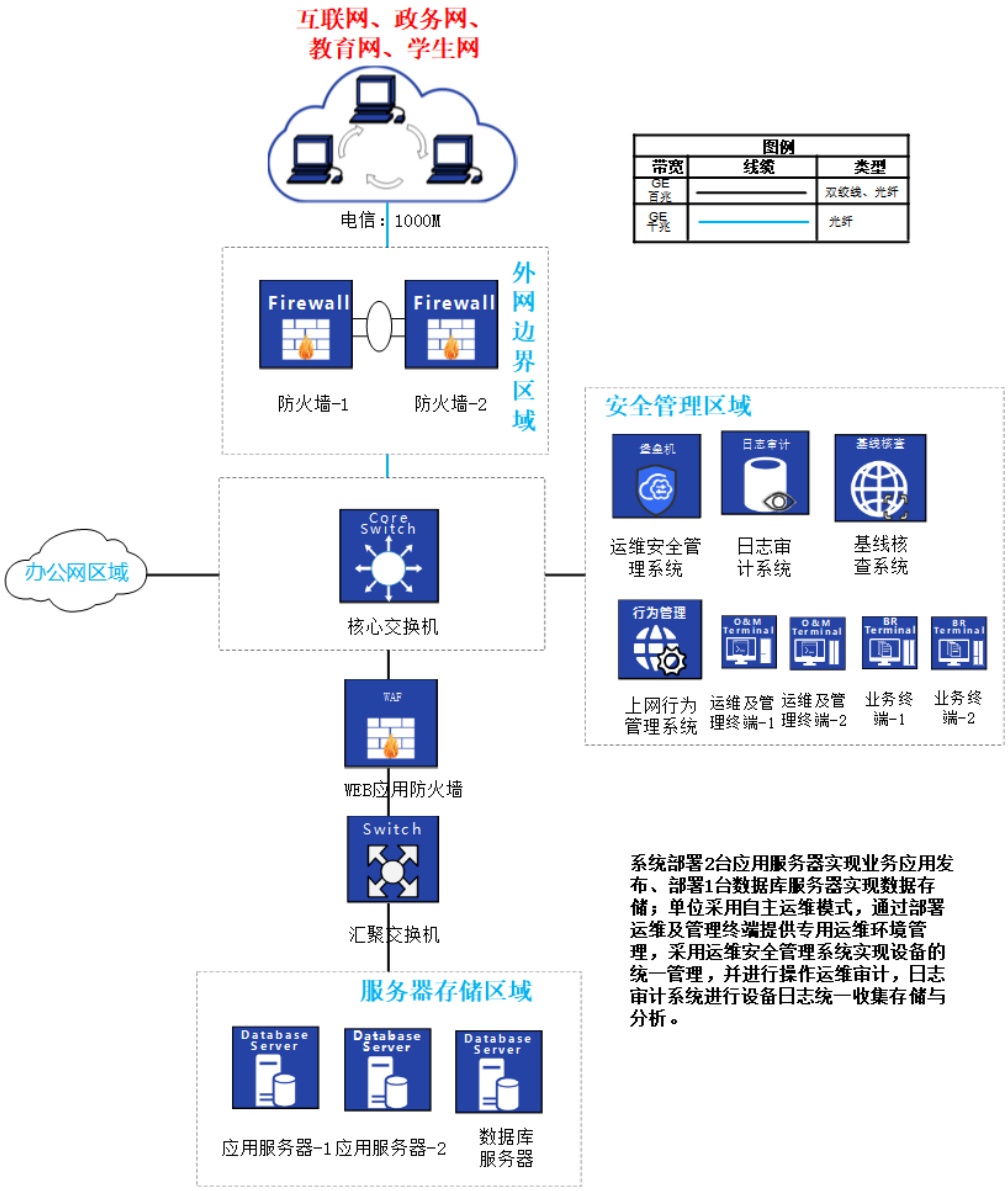


图 2-1 门户网站系统网络拓扑图

如图2-1门户网站系统网络拓扑图所示，门户网站系统网络安全域划分为4个，分别为外网边界区域、安全管理区域、服务器存储区域、办公网区域。

1、外网边界区域：

外网边界区域网络主要包括门户网站系统的业务服务和信息交换应用，是安全管理区域、服务器存储区域、办公网区域的出口边界；其链路接入为光纤线，带宽为1000mb。通过部署核心交换机、防火墙等设备实施网络访问控制，防火墙（入侵防御模块）实现网络入侵攻击行为防御。

2、办公网区域：

办公网区域网络主要包括门户网站系统与办公区域的信息交换应用，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、防火墙、上网行为管理系统等设备实施网络访问控制、防火墙（入侵防御模块）实现网络入侵攻击行为防御。

3、安全管理区域：

安全管理区域网络主要包括日志审计系统、运维安全管理系统、上网行为管理系统，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、上网行为管理系统等设备实施网络访问控制。

4、服务器存储区域：

服务器存储区域网络主要包括门户网站系统的应用服务器、数据库服务器，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、上网行为管理系统等设备实现一定的网络访问控制。

5、服务器部署情况：

门户网站系统由2台应用服务器实现应用发布；1台数据库服务器实现数据处理、存储、维护。

6、灾备及冗余

门户网站系统无异地备份机房，未实现异地备份数据定时传输功能。系统重要数据根据需求采用每天增量、每月全备到本地信息化机房。

门户网站系统未实现冗余措施。

2.2 测评指标

2.2.1 安全通用要求指标

表 2-2 安全通用要求指标

安全类	安全控制点	测评项数
安全物理环境	物理位置选择	2
	物理访问控制	1
	防盗窃和防破坏	2
	防雷击	1
	防火	2
	防水和防潮	2
	防静电	1
	温湿度控制	1
	电力供应	2
	电磁防护	1
安全通信网络	网络架构	2
	通信传输	1
	可信验证	1
安全区域边界	边界防护	1
	访问控制	4
	入侵防范	1
	恶意代码和垃圾邮件防范	1
	安全审计	3
	可信验证	1
安全计算环境	身份鉴别	3
	访问控制	4
	安全审计	3
	入侵防范	5
	恶意代码防范	1
	可信验证	1
	数据完整性	1
	数据备份恢复	2
	剩余信息保护	1
	个人信息保护	2
安全管理中心	系统管理	2
	审计管理	2
安全管理制度	安全策略	1
	管理制度	2
	制定和发布	2
	评审和修订	1
安全管理机构	岗位设置	2
	人员配备	1
	授权和审批	2
	沟通和合作	3

安全类	安全控制点	测评项数
	审核和检查	1
安全管理人员	人员录用	2
	人员离岗	1
	安全意识教育和培训	1
	外部人员访问管理	3
安全建设管理	定级和备案	4
	安全方案设计	3
	产品采购和使用	2
	自行软件开发	2
	外包软件开发	2
	工程实施	2
	测试验收	2
	系统交付	3
	等级测评	3
	服务供应商选择	2
安全运维管理	环境管理	3
	资产管理	1
	介质管理	2
	设备维护管理	2
	漏洞和风险管理	1
	网络和系统安全管理	5
	恶意代码防范管理	3
	配置管理	1
	密码管理	2
	变更管理	1
	备份与恢复管理	3
	安全事件处置	3
	应急预案管理	2
	外包运维管理	2
安全通用要求指标数量统计		135

2.2.2 安全扩展要求指标

表 2-3 安全扩展要求指标

扩展类型	安全类	安全控制点	测评项数
本次测评不涉及安全扩展要求指标			

2.2.3 其他安全要求指标

表 2-4 其他安全要求指标

安全类	安全控制点	测评项数
本次测评不涉及其他安全要求指标		

2.2.4 不适用安全要求指标

表 2-5-1 不适用安全要求指标

安全类	安全控制点	不适用项	不适用原因
安全计算环境	个人信息保护	a) 应仅采集和保存业务必需的用户个人信息;	应用服务器-1、数据库服务器、应用服务器-2: （1）本设备不存在此部分的控制需求，故此项不适用 数据库服务器-PostgreSQL、门户网站系统、重要业务数据: （1）系统完全不采集和保存任何形式的用户个人信息。 业务终端-2、业务终端-1、运维及管理终端-2、运维及管理终端-1: （1）操作系统不存在此部分的控制需求，不适用。 应用服务器-1-Tomcat: （1）中间件系统不存在此部分的控制需求，不适用。 基线核查系统、上网行为管理系统、WEB应用防火墙、汇聚交换机、防火墙-1、防火墙-2、日志审计系统、运维安全管理系统、核心交换机: （1）网络层设备不适用。
安全计算环境	个人信息保护	b) 应禁止未授权访问和非法使用用户个人信息。	应用服务器-1、数据库服务器、应用服务器-2: （1）本设备不存在此部分的控制需求，故此项不适用 业务终端-2、业务终端-1、运维及管理终端-2、运维及管理终端-1: （1）操作系统不存在此部分

安全类	安全控制点	不适用项	不适用原因
			的控制需求，不适用。 门户网站系统、重要业务数据： （1）系统完全不采集、保存及使用任何形式的用户个人信息。 应用服务器-1-Tomcat： （1）中间件系统不存在此部分的控制需求，不适用。 基线核查系统、上网行为管理系统、WEB应用防火墙、汇聚交换机、防火墙-1、防火墙-2、日志审计系统、运维安全管理系统、核心交换机： （1）网络层设备不适用。 数据库服务器-PostgreSQL： （1）数据库完全不采集、保存及使用任何形式的用户个人信息。
安全建设管理	自行软件开发	a）应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。
安全建设管理	自行软件开发	b）应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。
安全运维管理	密码管理	b）应使用国家密码管理主管部门认证核准的密码技术和产品。	（1）单位未采购涉及密码技术的产品，不适用。
安全运维管理	外包运维管理	a）应确保外包运维服务商的选择符合国家的有关规定；	（1）单位目前未涉及任何外包运维服务情况，不适用。
安全运维管理	外包运维管理	b）应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。	（1）单位目前未涉及任何外包运维服务情况，不适用。

表 2-5-2 其他不适用安全要求指标

安全类	安全控制点	不适用项	不适用原因
本次测评不涉及其他安全要求指标			

2.3 测评对象

2.3.1 测评对象选择方法

门户网站系统等级测评的测评对象种类上基本覆盖、数量进行抽样，重点抽查主要的设备、设施、人员和文档等。结合门户网站系统的网络拓扑结构和业务情况，本次等级测评的测评对象在抽样时主要考虑以下几个方面：

（1） 主机房（包括其环境、设备和设施等）和灾备机房；

（2） 存储被测系统重要数据的介质的存放环境；

（3） 办公场地；

（4） 整个系统的网络拓扑结构；

（5） 安全设备，包括防火墙等；

（6） 边界网络设备，包括路由器、楼层交换机等；

（7） 对整个信息系统或其局部的安全性起作用的网络互联设备，如核心交换机、路由器等；

（8） 承载业务处理系统主要业务或数据的服务器（包括其操作系统和数据库）；

（9） 管理终端和主要应用系统终端；

（10） 能够完成系统不同业务使命的业务应用系统；

（11） 业务备份系统；

（12） 信息安全主管人员、各方面的负责人员、具体负责安全管理的当事人、业务负责人；

（13） 涉及到信息系统安全的所有管理制度和记录。

抽样原则：在等级测评时，业务处理系统中配置相同的安全设备、边界网络设备、网络互联设备、服务器、终端以及备份设备，每类至少抽查两台作为测评对象。

2.3.2 测评对象选择结果

2.3.2.1 物理机房

表 2-6 物理机房

序号	机房名称	物理位置	重要程度
1	信息化机房	茂名市茂南区文明北路232号大院大楼	关键

2.3.2.2 网络设备

表 2-7 网络设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度
1	汇聚交换机	否	H3C version 7.1.070, Release 6126P20	H3C S5560X-30C-EI	数据交换	重要
2	核心交换机	否	H3C version 7.1.070, Release 7585P07	H3C S7500E-X	核心数据交换、访问控制	关键

2.3.2.3 安全设备

表 2-8 安全设备

序号	设备名称	是否虚拟设备	系统及版本	品牌型号	用途	重要程度
1	日志审计系统	否	深信服LAS 3.0.5	深信服AC-1000-D601-PT	日志审计	重要
2	基线核查系统	否	深信服V3.0.3	深信服AC-1000-D602-PT	漏洞扫描	重要
3	上网行为管理系统	否	深信服AC12.0.26	深信服AC-1000-D600-PT	上网行为管理及终端准入控制	重要
4	防火墙-2	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键
5	运维安全管理系统	否	深信服V3.0.6	深信服AC-1000-D603-	运维审计	重要

序号	设备名称	是否虚拟设备	系统及版本	品牌型号	用途	重要程度
				PT		
6	WEB应用防火墙	否	深信服AF 8.0.9	深信服WAF-2000-H642	应用防护、入侵防范、病毒防护	重要
7	防火墙-1	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键

2.3.2.4 服务器

表 2-9 服务器

序号	设备名称	所属业务应用系统/平台	是否虚拟设备	操作系统及版本	数据库管理系统及版本	中间件及版本	重要程度
1	应用服务器-2	门户网站系统	否	CentOS 7.7	/	Tomcat 8.5	关键
2	数据库服务器	门户网站系统	否	CentOS 6.8	PostgreSQL 9.6.12	Tomcat 8.0.37	关键
3	应用服务器-1	门户网站系统	否	CentOS 7.7	/	Tomcat 8.5	关键

2.3.2.5 终端设备

表 2-10 终端设备

序号	设备名称	是否虚拟设备	操作系统及版本	用途	重要程度
1	运维及管理终端-2	否	Windows 10 （版本 21H2（内部版本 19044.1889））	运维管理、系统管理	一般
2	运维及管理终端-1	否	Windows 10 （版本 20H2（内部版本 19044.1889）	运维管理、系统管理	一般
3	业务终端-2	否	Windows 10 （版本 20H2（内部版本 19044.1889）	业务管理	一般
4	业务终端-1	否	Windows 10 （版本 20H2（内部版本 19044.1889）	业务管理	一般

2.3.2.6 其他系统或设备

表 2-11 其他系统或设备

序号	设备名称	是否虚拟设备	系统及版本	用途	重要程度
/	/	/	/	/	/

注释：本次测评对象中不涉及专用移动互联终端等，不开展抽测。

2.3.2.7 系统管理软件/平台

表 2-12 系统管理软件/平台

序号	系统管理软件/平台名称	主要功能	版本	所在设备名称	重要程度
1	数据库服务器-PostgreSQL	数据生产、存储	9.6.12	应用/数据库服务器	关键
2	应用服务器-1-Tomcat	页面发布	8.5	应用/数据库服务器	关键

2.3.2.8 业务应用软件/平台

表 2-13 业务应用系统/平台

序号	业务应用软件/平台名称	主要功能	业务应用软件及版本	开发厂商	重要程度
1	门户网站系统	门户网站系统是学校对外的信息门户，前台包含学院概况、机构设置、教学在线、学术科研、招生就业、队伍建设、学工在线、团员青年、校友会等栏目。后台包括新增/删除站点，用户管理，数据备份和恢复，安全检测、敏感词检测、运维监控等功能，通过门	V6.0	西安博达软件股份有限公司	关键

序号	业务应用软件/平台名称	主要功能	业务应用软件及版本	开发厂商	重要程度
		户网站对外发布学校动态、消息，是学院对外宣传的官方门户。			

2.3.2.9 数据资源

表 2-14 数据资源

序号	数据类别	所属业务应用	安全防护需求	重要程度
1	重要业务数据	门户网站系统	完整性、保密性	关键
2	鉴别数据	门户网站系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性、保密性	关键
3	重要审计数据	门户网站系统（安全管理中心）	完整性	重要
4	重要配置数据	门户网站系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性	关键

注释：网络设备、安全设备、服务器、终端、系统管理软件/平台和业务应用系统等所涉及的鉴别数据和重要配置数据分别在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。重要审计数据在安全管理中心进行汇总测评证据，包括数据完整性。重要业务数据在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。系统不涉及重要个人信息。

2.3.2.10 安全相关人员

表 2-15 安全相关人员

序号	姓名	岗位/角色	联系方式	所属单位
1	吴国华	系统管理员	0668-2920122	茂名职业技术学院
2	杨云	审计管理员	0668-2920122	茂名职业技术

序号	姓名	岗位/角色	联系方式	所属单位
				学院
3	龙恒	数据管理员	13377766618	茂名职业技术学院
4	吴国华	机房管理员	0668-2920122	茂名职业技术学院
5	龙恒	应用管理员	13377766618	茂名职业技术学院
6	龙恒	网络管理员	13377766618	茂名职业技术学院
7	叶永利	安全管理员	0668-2920122	茂名职业技术学院
8	杨云	资产管理员	0668-2920122	茂名职业技术学院

2.3.2.11 安全管理文档

表 2-16 安全管理文档

序号	文档名称	主要内容
1	制度类文档-机房安全管理制度	关于单位机房安全管理工作制度文档
2	制度类文档-人员管理制度	关于单位人员录用、调岗、离岗管理制度文档
3	制度类文档-安全教育和培训制度	关于单位安全培训、安全交流工作制度文档
4	制度类文档-办公环境管理制度	关于单位办公环境管理制度文档
5	制度类文档-恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
6	制度类文档-组织安全结构和人员职责制度	关于单位组织结构、人员安排、人员职责制度文档
7	制度类文档-网络安全管理制度	关于单位网络安全工作管理制度文档
8	制度类文档-服务供应商选择安全管理制度	关于单位安全服务供应商管理规定制度文档
9	制度类文档-应用安全管理规范	关于规定单位应用安全管理要求及规范的制度文档
10	制度类文档-授权和审批管理规定	关于单位授权审批、审批流程规范制度文档
11	制度类文档-应用系统业务用户密码设置规定	关于单位用户密码管理制度文档
12	制度类文档-信息系统恶意	关于单位恶意代码工作管理制度文档

序号	文档名称	主要内容
	代码防范管理制度	
13	制度类文档-介质管理制度	关于单位介质安全管理工制度文档
14	制度类文档-信息安全漏洞扫描规范	关于单位安全漏洞工作规范制度文档
15	制度类文档-外部服务人员管理规范	关于单位针对外部人员工作管理规范制度文档
16	制度类文档-主机安全管理规范	关于规定单位主机系统安全管理要求规范，指导业务平台主机的安全配置和维护的制度文档
17	制度类文档-信息安全总体策略	关于单位网络安全方针、策略制度文档
18	制度类文档-数据安全管理规范	关于保障关键数据安全，从数据库本身、数据加密、数据备份恢复三个方面对数据安全进行规范的制度文档
19	制度类文档-变更控制管理制度	关于单位变更流程、控制管理制度文档
20	制度类文档-网络安全管理规范	关于保障单位网络系统的安全稳定运行，抵御内部和外部各种形式的网络攻击或威胁制定的管理文档
21	制度类文档-外部人员访问管理制度	关于单位针对外来人员访问管控制度文档
22	制度类文档-测试及验收方案	关于单位测试验收方案文档
23	制度类文档-组织安全结构和人员职责制度	关于单位安全结构、人员职责
24	制度类文档-系统交付管理	关于单位交付工作管理制度文档
25	制度类文档-制度制定、发布、评审和修订管理制度	关于单位制度制定、发布、评审和修订等管理文档
26	制度类文档-安全事件报告和处置	关于单位网络安全事件管理、处置、流程等报告制度文档
27	制度类文档-网络安全事件应急预案	关于单位网络安全事件应急处理、流程、培训等管理制度文档
28	制度类文档-外包开发软件管理规定	关于单位外包项目管理工作制度文档
29	制度类文档-工程实施管理制度	关于单位工程实施工作管理制度文档
30	制度类文档-信息系统外包运维管理制度	关于单位外包运维工作管理制度文档
31	制度类文档-设备安全管理制度	关于单位设备安全管理制度文档
32	制度类文档-员工考核管理制度	关于单位人员考核工作管理制度文档
33	制度类文档-备份与恢复管理制度	关于单位数据备份、恢复管理制度文档
34	制度类文档-系统及应用数	关于单位数据备份、恢复管理制度文档

序号	文档名称	主要内容
	据备份管理规范	
35	制度类文档-网络安全事件报告制度	关于单位网络安全事件管理报告文档
36	制度类文档-信息安全奖惩办法	关于单位人员奖惩制度文档
37	制度类文档-岗位安排及岗位职责	关于单位岗位职责、岗位安排制度文档
38	制度类文档-安全漏洞管理制度	关于单位安全漏洞管理工作制度文档
39	制度类文档-系统安全管理制度	关于单位系统安全管理、安全服务管理制度文档
40	制度类文档-安全管理组织规范	关于单位组织结构管理规范制度文档
41	制度类文档-办公环境保密管理	关于单位办公环境管理制度文档
42	制度类文档-网络与信息系统安全设计规范	关于单位网络与信息化安全设计制度文档
43	制度类文档-恶意代码防范管理制度	关于单位恶意代码防范工作制度文档
44	制度类文档-工程测试验收管理	关于单位工程测试工作管理制度文档
45	制度类文档-物理安全管理规范	关于加强单位办公区域及电子计算机机房的管理和设备运行安全，规范办公区域及机房建设，使人员办公高效及机房设备安全、稳定运行的制度文档
46	制度类文档-离岗人员工作交接规范	关于单位离岗交接工作规范制度文档
47	制度类文档-外部接入受控网络访问系统管理规范	关于单位针对外部人员工作接入规范制度文档
48	制度类文档-安全审查和检查管理规范	关于单位安全检查、审查工作规范制度文档
49	操作类文档-设备及系统软件配置和操作手册	关于单位安全设备操作、Linux服务器配置手册、主机运维操作手册、软件操作手册、防火墙配置和操作手册、数据库日常运维操作手册等指导文档
50	操作类文档-软硬件日常维护管理规程	关于单位计算机网络系统使用、管理、信息安全、资源共享有所遵循,规范上网操作流程,提高网络系统安全性的指导文档
51	操作类文档-设备操作规程	关于单位相关设备操作指导文档
52	操作类文档-数据备份策略	关于单位数据备份策略文件
53	记录类文档-评审和修订记录	关于单位变更评审、修订工作记录
54	记录类文档-人员离岗申请表	关于人员离岗申请记录
55	记录类文档-备份工作汇总	关于单位数据备份工作总结表

序号	文档名称	主要内容
	表	
56	记录类文档-离场信息资料交接表	关于人员离岗交接工作记录
57	记录类文档-设备出入登记记录表	关于设备进出机房登记工作记录
58	记录类文档-存储介质目录清单	关于备份介质存储工作清单
59	记录类文档-网络信息安全事件记录表	关于单位网络安全事件工作记录
60	记录类文档-备份介质使用记录	关于备份介质使用登记工作记录
61	记录类文档-信息安全检查记录表	关于单位安全检查工作记录
62	记录类文档-访问记录表	关于人员访问工作记录
63	记录类文档-数据恢复申请表	关于单位数据恢复工作申请表
64	记录类文档-信息管理系统漏洞检查表	关于单位安全漏洞工作检测记录表
65	记录类文档-机房维护日志	关于机房维护工作记录
66	记录类文档-机房巡检记录表	关于单位机房环境巡检记录
67	记录类文档-外部人员访问申请表	关于外来人员访问申请流程工作记录
68	记录类文档-信息安全会议记录	关于单位安全培训、安全交流会议记录
69	记录类文档-机房设备维护记录表	关于设备维护登记工作记录
70	记录类文档-专家论证记录表	关于单位网络方案论证记录
71	记录类文档-通用变更记录表	关于单位变更工作记录
72	记录类文档-机房设备维修记录表	关于单位机房设备维修工作记录
73	记录类文档-信息系统存储介质使用清单	关于备份介质存储使用清单
74	记录类文档-系统交付清单	关于单位交付工作记录
75	记录类文档-收发文登记记录	关于单位文档签发记录
76	记录类文档-关键岗位人员考核记录	关于关键岗位考核工作记录
77	记录类文档-漏洞检测报告	关于单位安全漏洞检测报告文档
78	记录类文档-人员入职考核	关于人员录用、考核工作记录

序号	文档名称	主要内容
	记录	
79	记录类文档-人员培训及考核记录表	关于人员培训、考核等工作记录
80	记录类文档-网络配置信息	关于单位配置信息登记工作记录
81	记录类文档-监理审批表	关于单位监理审核工作记录
82	记录类文档-技能培训记录	关于单位系统培训工作、考核工作记录
83	记录类文档-离职员工物品交回登记表	关于人员离岗工物交接工作记录
84	记录类文档-机房出入登记表	关于人员进出机房登记工作记录
85	记录类文档-设备操作维护记录	关于单位设备维护工作记录
86	记录类文档-应急预案培训记录表	关于单位应急预案培训工作记录
87	记录类文档-安全管理制度评审记录	关于单位制度审计记录
88	记录类文档-外部人员访问记录表	关于外来人员访问登记工作记录
89	记录类文档-安全建设方案评审纪录	关于单位网络与信息化安全设计方案评审工作记录
90	记录类文档-接入受控网络申请表	关于外来人员接入工作记录
91	记录类文档-数据备份记录表	关于单位数据备份工作记录
92	记录类文档-软件交付清单	关于单位交付工作记录
93	记录类文档-重要操作审批表	关于单位审批工作记录
94	记录类文档-设备维修申请表	关于单位设备维护工作申请记录
95	记录类文档-信息系统存储介质销毁申请表	关于备份介质销毁申请工作记录
96	记录类文档-外部会议文件和记录	关于单位外部联系、交流及会议工作记录
97	证据类文档-深信服安全采购合同	关于单位与安全厂家服务采购、产品选择合同文件
98	证据类文档-信息安全事件分析报告表	关于单位安全事件分析报告
99	证据类文档-网络安全等级保护工作小组名单	关于单位网络安全等级保护工作小组人员名单文件
100	证据类文档-资产清单	关于单位信息系统资产清单统计表
101	证据类文档-网络安全系统设计方案	关于单位网络与信息化安全设计方案文档

序号	文档名称	主要内容
102	证据类文档-外部联系表	关于单位内部联系及外部联系名单
103	证据类文档-工程项目实施方案	关于单位工程实施方案文档
104	证据类文档-网络安全等级保护测评服务合同	关于单位与安全服务商签定的安全服务合同文件
105	证据类文档-定级备案	关于单位系统定级报告、备案证文件
106	证据类文档-安全职位人员	关于单位人员岗位安排名单

3 单项测评结果分析

3.1 安全物理环境

3.1.1 已有安全控制措施汇总分析

安全通用要求

物理位置选择	
a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；	
信息化机房	（1）机房和办公场地场所在建筑物具有建筑验收文档，包含对防震、防风和防雨能力的说明； （2）机房和办公场地未出严重的问题。
b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	
信息化机房	（1）机房未部署在易发生问题的位置； （2）机房对于空调设备的排水管等部位采取密封防漏处理； （3）机房对于楼板进行了防护措施。
防盗窃和防破坏	
a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识；	
信息化机房	（1）机房设备或主要部件都固定在机架上； （2）机房内对主要部件已绑定相应不易除去的标签； （3）重要机柜已进行上锁处理。
b) 应将通信线缆铺设在隐蔽安全处。	
信息化机房	（1）通信线缆铺设在下走线槽隐蔽处中； （2）通信线缆设有明显的源目的标识； （3）通信线缆均铺设整齐、规范。
防雷击	
应将各类机柜、设施和设备等通过接地系统安全接地。	
信息化机房	（1）机房设置专用地线； （2）机房内机柜、设施和设备等进行接地处理； （3）交流电源接地验收检测结果符合要求。
防火	

a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；	
信息化机房	（1）机房采用经消防检测部门检测合格并在有效期内的（如 七氟丙烷）气体自动灭火设备，火灾自动报警类型为烟感+红外； （2）自动消防系统工作状态正常，有定期巡检和维护记录《机房巡检记录表》； （3）建立机房消防的管理制度相关文档《机房安全管理制度》，按管理要求机房无人情况下气体灭火配置为自动模式，进入机房调整为手动模式，机房报警有7*24小时值班人员进行监控。
防水和防潮	
a) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	
信息化机房	（1）机房不存在雨水渗透、破损等不合规情况； （2）机房不位于建筑的顶层、边缘区域。
b) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。	
信息化机房	（1）机房区域范围已部署1台科华品牌（精密）空调，机房内分别配置1组温湿度传感器监控； （2）机房内空调下方已铺设安装好挡水和排水设施； （3）机房墙壁或楼板的管道采取必要的防渗防漏等防水保护措施； （4）机房安装检测设备（如：漏水检测绳）检测地下积水，及时处理机房水蒸气结露和地下积水的转移与渗透； （5）目前防水\防潮检测未发现异常情况，并且有防水防潮的运维记录《机房维护日志》。
温湿度控制	
应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。	
信息化机房	（1）机房范围已部署1组科华品牌精密空调进行温湿度调节； （2）机房范围已部署空调及加湿机进行温湿度调节； (3)温湿度自动调节设施运作正常,有运行和维护记录《机房维护日志》; （4）机房温度能保持在24摄氏度到28摄氏度之间； （5）机房湿度能保持在40%到65%之间。
电力供应	
a) 应在机房供电线路上配置稳压器和过电压防护设备；	
信息化机房	（1）机房配备了稳压器和过电压防护设备； （2）稳压器和过电压防护设备正常工作； （3）机房具备电力供应安全设计，并在其中标明配备稳压器、过电压防护设备等要求。
b) 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。	
信息化机房	（1）机房配备了1组科华品牌UPS； （2）UPS正常工作，可满足主要设备断电情况下的至少1小时正常运行要求； （3）UPS有定期（至少每年）检查和维护，有运行和维护记录《机房巡检记录表》。
电磁防护	
电源线和通信线缆应隔离铺设，避免互相干扰。	
信息化机房	（1）通信线缆铺设采用独立的具有电磁屏蔽作用线槽； （2）电源线缆铺设采用独立的具有电磁屏蔽作用线槽；

	（3）弱电线缆隔离铺设，没有干扰。

3.1.2 主要安全问题汇总分析

安全通用要求

（1）机房出入口未配置电子门禁系统（如：信息化机房）。上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域,可能对系统的平稳运行造成影响。中风险。

（2）机房建设未完全采用符合耐火等级的建筑材料。机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级（如：信息化机房）。存在发生火情时助燃火灾的风险。 低风险。

（3）机房内缺乏防静电措施（如防静电地板或铺设防静电地毯 ）（如：信息化机房）。存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。 中风险。

3.2 安全通信网络

3.2.1 已有安全控制措施汇总分析

安全通用要求

网络架构	
b) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	
安全通信网络	(1)网络内重要网段未部署在网络边界处,且未直接连接外部信息系统; （2）系统通过防火墙对重要网段采取访问控制策略; （3）各安全域（子网）的出口唯一。
通信传输	
应采用校验技术保证通信过程中数据的完整性。	
安全通信网络	（1）网络系统中未涉及完整性保障设备，但在安全计算环境方面网络设备采用SSH协议、安全设备采用HTTPS协议、操作系统采用SSH协议、应用系统采用HTTPS协议来保证通信过程中数据的完整性。

3.2.2 主要安全问题汇总分析

安全通用要求

（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况（如：安全通信网络）。上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变得更为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。 中风险。

（2）缺乏对通信设备可信验证方面的安全设计要求。现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况（如：安全通信网络）。缺乏对系统可执行程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致计算资源被干扰和破坏造成损失。 低风险。

3.3 安全区域边界

3.3.1 已有安全控制措施汇总分析

安全通用要求

边界防护	
应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络存在受保护的边界； （2）网络边界处部署了可提供访问控制功能的设备； （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。
访问控制	
a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。
b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	

办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。
c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。
d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。
入侵防范	
应在关键网络节点处监视网络攻击行为。	
外网边界区域 服务器存储区域	（1）网络层部署支持对内部发起的攻击行为进行防范的设备； （2）现有的防范措施满足相应防护要求； （3）内部安全防范措施能检测相应攻击行为。
恶意代码和垃圾邮件防范	
应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	
外网边界区域 服务器存储区域	（1）在关键网络节点处部署合规的防恶意代码措施； （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试。
安全审计	
a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； （3）现有的审计措施满足相应的审计要求。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； （3）设备本地时间正常。
c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。

3.3.2 主要安全问题汇总分析

安全通用要求

(1)网络层部署防火墙,防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为（如：办公网区域）。存在不能及时发现内部主机作为攻击跳板，或网络攻击行为而造成系统损坏/网络资源浪费的风险。中风险。

(2)现有部署的恶意代码防范措施存在不合规的问题,网络边界覆盖不全面(如：办公网区域）。无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。 中风险。

(3) 缺乏对边界设备可信验证方面的安全设计要求。现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况（如：办公网区域）。缺乏对边界设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4 安全计算环境

3.4.1 网络设备

3.4.1.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
核心交换机 汇聚交换机	(1) 设备对各登录模式均启用身份鉴别； (2) 设备对登录管理的用户进行身份鉴别； (3) 设备名及登录用户设置的身份标识具有唯一性； (4) 设备不存在明文或空口令用户；

	（5）设备配置合规的全局密码策略； （6）设备配置加密的super认证。
b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
核心交换机 汇聚交换机	（1）设备配置合规的全局登录失败处理策略； （2）设备配置合规的操作超时退出措施。
c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
核心交换机 汇聚交换机	（1）设备配置合规的远程管理模式。
访问控制	
a）应对登录的用户分配账户和权限；	
核心交换机 汇聚交换机	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。
b）应重命名或删除默认账户，修改默认账户的默认口令；	
核心交换机 汇聚交换机	（1）设备不存在默认账户名； （2）设备账户口令设置合规。
c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
核心交换机 汇聚交换机	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。
d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	
核心交换机 汇聚交换机	（1）设备根据安全策略要求对特权用户进行分离； （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
核心交换机 汇聚交换机	（1）设备开启审计功能，审计进程正常； （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
核心交换机 汇聚交换机	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。
c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
核心交换机 汇聚交换机	（1）设备限制审计文件的访问控制权限，普通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效； （5）日志及审计记录保存大于6个月。
入侵防范	

a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	
核心交换机 汇聚交换机	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。
b) 应关闭不需要的系统服务、默认共享和高危端口；	
核心交换机 汇聚交换机	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。
c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
核心交换机 汇聚交换机	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
核心交换机 汇聚交换机	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
核心交换机 汇聚交换机	鉴别数据、重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； （2）设备对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
核心交换机 汇聚交换机	（1）设备定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。

3.4.1.2 主要安全问题汇总分析

安全通用要求

（1）设备不具备相关可信验证的技术措施（如：核心交换机）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.2 安全设备

3.4.2.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备对各登录模式均启用身份鉴别； （2）设备对登录管理的用户进行身份鉴别； （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备启用合规登录失败处理策略； （2）设备配置合规的操作超时退出措施。
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备配置合规的远程管理模式； （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。
访问控制	
a) 应对登录的用户分配账户和权限；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。
b) 应重命名或删除默认账户，修改默认账户的默认口令；	
WEB应用防火墙 上网行为管理系统	（1）设备不存在默认账户名； （2）设备账户口令设置合规。

基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备不存在多余或过期账户； (2) 设备管理员用户与账户之间一一对应。
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备根据安全策略要求对特权用户进行分离； (2) 设备不存在多个管理级别高的特权用户； (3) 设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备开启审计功能，审计进程正常； (2)设备的日志审计级别满足要求,审计覆盖所有用户操作审计和记录。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备日期、时间正常； (2) 设备审计记录内容基本完整。
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
WEB应用防火墙 上网行为管理系统 基线核查系统 运维安全管理系统 防火墙-1	(1) 设备限制审计文件的访问控制权限，普通用户不可删除及修改； (2) 设备针对日志、审计记录具备充足的存储容量； (3) 对审计记录进行定期存档备份，其备份策略有效； (4) 部署日志审计系统实时对日志进行统一收集存储； (5) 日志及审计记录保存大于6个月。

防火墙-2	
日志审计系统	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）日志及审计记录保存大于6个月。
入侵防范	
a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。
b）应关闭不需要的系统服务、默认共享和高危端口；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。
c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 防火墙-1 防火墙-2	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
运维安全管理系统	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制。
d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备管理具备数据有效性检验功能； （2）设备管理的校验接口范围较全面。
e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
WEB应用防火墙 上网行为管理系统 基线核查系统	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。

日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	
恶意代码防范	
应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	
WEB应用防火墙 防火墙-1 防火墙-2	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	鉴别数据、重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； （2）设备对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。

3.4.2.2 主要安全问题汇总分析

安全通用要求

（1）设备不具备相关可信验证的技术措施（如：WEB应用防火墙）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.3 服务器和终端

3.4.3.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统对登录系统的用户进行身份鉴别； （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； （5）用户属性策略未勾选“密码永不过期”。
应用服务器-1 应用服务器-2 数据库服务器	（1）操作系统对登录系统的用户进行身份鉴别； （2）操作系统不存在空口令用户； （3）操作系统不存在默认信任的登录模式； （4）操作系统为登录用户设置的身份标识具有唯一性； （5）操作系统配置的一定的密码长度且定期更换； （6）操作系统配置一定的密码复杂度策略。
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统启用登录失败处理策略。 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略。
应用服务器-1 应用服务器-2 数据库服务器	（1）操作系统启用pam_tally2模块的合规登录失败处理策略； （2）操作系统配置合规的操作超时锁定； （3）操作系统启用SSH的合规登录超时策略。
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS的管理。
应用服务器-1 应用服务器-2 数据库服务器	（1）操作系统配置合规的远程管理模式； （2）操作系统远程端口使用情况合规； （3）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
访问控制	
a) 应对登录的用户分配账户和权限；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。
应用服务器-1	（1）可提供操作系统权限表；

应用服务器-2 数据库服务器	（2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在所有用户均属于root组的情况。
b）应重命名或删除默认账户，修改默认账户的默认口令；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统针对默认账户采用相应的安全策略配置； （2）操作系统账户不存在弱口令或空口令。
应用服务器-1 应用服务器-2 数据库服务器	（1）操作系统对多余帐户进行删除、锁定或禁止其登录； （2）操作系统账户口令设置合规。
c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
业务终端-1 业务终端-2 应用服务器-1 应用服务器-2 数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。
d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统根据安全策略要求对特权用户进行分离； （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
应用服务器-1 应用服务器-2 数据库服务器	（1）操作系统根据安全策略要求对特权用户进行分离； （2）操作系统不存在除root外的特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统开启审计策略，操作系统审计策略基本完整； （2）审计覆盖所有用户操作审计和记录。
应用服务器-1 应用服务器-2 数据库服务器	（1）操作系统开启审计功能，审计进程正常； （2）操作系统开启审计范围及策略满足要求，审计覆盖所有用户操作审计和记录。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
业务终端-1 业务终端-2 应用服务器-1 应用服务器-2 数据库服务器	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。

运维及管理终端-1 运维及管理终端-2	
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统采取对审计记录存储容量如下： 运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。
应用服务器-1 应用服务器-2 数据库服务器	(1)操作系统限制审计文件的访问控制权限,普通用户不可删除及修改; （2）操作系统针对日志、审计记录具备充足的存储容量； （3）操作系统采取合规的日志文件权限策略； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。
入侵防范	
a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。
应用服务器-1 应用服务器-2 数据库服务器	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。
b) 应关闭不需要的系统服务、默认共享和高危端口；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统不存在多余的默认共享及其它文件共享； （2）操作系统关闭不必要端口； （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。
应用服务器-1 应用服务器-2 数据库服务器	（1）操作系统关闭不必要端口； （2）操作系统禁用不必要服务； （3）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口； （4）漏洞扫描未发现高风险主机端口。
c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
应用服务器-1 应用服务器-2	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制；

数据库服务器	（2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。
应用服务器-1 应用服务器-2 数据库服务器	（1）操作系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。
恶意代码防范	
应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。
应用服务器-1 应用服务器-2 数据库服务器	（1）操作系统安装深信服edr防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	鉴别数据、重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。
应用服务器-1 应用服务器-2 数据库服务器	鉴别数据: （1）系统在通信传输过程中对鉴别数据采取完整性保护措施。 重要配置数据: （1）系统在通信传输过程中对重要配置数据采取完整性保护措施。
数据备份恢复	
a）应提供重要数据的本地数据备份与恢复功能；	
业务终端-1 业务终端-2 应用服务器-1 应用服务器-2 数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	

业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施： 安全选项“不显示上次的用户名”->启用
应用服务器-1 应用服务器-2 数据库服务器	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统不保存过多终端历史记录。

3.4.3.2 主要安全问题汇总分析

安全通用要求

（1）缺乏对计算设备可信验证方面的安全设计要求。现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。现有的计算设备存在对系统运行过程中的可信检验不全面的情况。现有的可信验证存在部分告警、审计及联动措施不全面的情况(如：应用服务器-1）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.4 系统管理软件/平台

3.4.4.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
数据库服务器-PostgreSQL	（1）数据库系统对登录系统的用户进行身份鉴别； （2）数据库系统不存在弱口令用户； （3）数据库系统不存在默认信任的登录模式； （4）数据库系统为登录用户设置的身份标识具有唯一性； （5）数据库系统配置合规的密码长度及复杂度策略； （6）数据库系统配置合规的密码有效周期策略。
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
数据库服务器-PostgreSQL	（1）宿主操作系统配置合规的远程管理模式； （2）数据库系统禁用远程登录管理。
访问控制	
a) 应对登录的用户分配账户和权限；	

应用服务器-1-Tomcat	（1）对应不同的账户均按需分配不同的用户权限，不存在中间件用户均属于管理级别、高权限的情况； （2）中间件配置可降权启动Tomcat的用户； （3）宿主系统针对中间件用户分别赋予相应的管理操作权限。
数据库服务器-PostgreSQL	（1）登录数据库系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （2）对应不同的账户均按需分配不同的用户组及对应的权限，不存在多用户均与dba类用户权限一致的情况。
b）应重命名或删除默认账户，修改默认账户的默认口令；	
应用服务器-1-Tomcat	（1）中间件不存在除如:Tomcat、admin、manager、role1等默认账户名； （2）中间件账户口令设置合规。
数据库服务器-PostgreSQL	（1）数据库系统账户口令设置合规； （2）已修改默认帐户的默认口令。
c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
应用服务器-1-Tomcat	（1）中间件不存在多余或过期账户； （2）中间件管理员用户与账户之间一一对应； （3）中间件启用合规的管理用户名配置。
数据库服务器-PostgreSQL	（1）数据库系统不存在多余或过期账户； （2）数据库系统管理员用户与账户之间一一对应。
d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	
应用服务器-1-Tomcat	（1）中间件根据安全策略要求对特权用户及宿主管理用户进行分离； （2）中间件管理不存在多个管理级别高的特权用户； （3）中间件管理按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
数据库服务器-PostgreSQL	（1）数据库系统根据安全策略要求对特权用户进行分离； （2）数据库系统用户权限合理，非管理员未设置过大权限； （3）数据库系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
应用服务器-1-Tomcat	（1）中间件开启审计功能，审计进程正常； （2）系统的日志审计级别满足要求。
数据库服务器-PostgreSQL	（1）数据库系统开启审计功能，审计进程正常。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
应用服务器-1-Tomcat	（1）中间件日期、时间正常； （2）中间件审计记录开启审核策略且日志级别正常。
数据库服务器-PostgreSQL	（1）数据库宿主系统日期、时间正常； （2）数据库系统审计记录内容基本完整。
c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
应用服务器-1-Tomcat	（1）中间件限制审计文件的访问控制权限，普通用户不可删除及修改； （2）宿主系统针对中间件日志、审计记录具备充足的存储容量； （3）对中间件审计记录进行定期存档备份，其备份策略有效； （4）审计记录及日志保存大于6个月。
数据库服务器-PostgreSQL	（1）数据库系统限制审计文件的访问控制权限，普通用户不可删除及修

	改； （2）数据库系统针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份； （4）审计记录和日志记录保存大于6个月。
入侵防范	
c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
数据库服务器-PostgreSQL	（1）数据库系统设定有效的终端接入策略，对通过网络进行管理的终端进行限制。
d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	
应用服务器-1-Tomcat	（1）中间件管理具备数据有效性检验功能； （2）中间件管理的校验接口范围较全面。
e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
应用服务器-1-Tomcat	（1）中间件已根据需要不定期地对已发布的版本进行更新； （2）中间件更新安装前进行安全性和兼容性测试； （3）在系统上线或发生重大变更时测试并安装最新的中间件版本或更新补丁； （4）在不影响业务系统正常运行情况下，对发现的中间件漏洞在确保安全的情况下进行修补； （5）中间件进行扫描未发现存在可造成高风险的漏洞。
数据库服务器-PostgreSQL	（1）数据库系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）补丁安装前进行安全性和兼容性测试； （3）在系统上线或发生重大变更时测试并安装数据库安全补丁； （4）在不影响业务系统正常运行情况下，对发现的数据库系统漏洞在确保安全的情况下进行修补； （5）数据库宿主系统不存在启用未加控制的高危端口； （6）数据库系统进行渗透及扫描未发现存在可造成高风险的漏洞。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
应用服务器-1-Tomcat	鉴别数据、重要配置数据: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。
数据库服务器-PostgreSQL	鉴别数据、重要配置数据: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a）应提供重要数据的本地数据备份与恢复功能；	
应用服务器-1-Tomcat	（1）系统定义了相关需要备份的中间件重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）宿主系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）中间件相关数据的备份周期合理：每天增量一次、每月全备一次； （5）中间件开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
数据库服务器-PostgreSQL	（1）数据库系统定义了相关重要数据；

	（2）单位具备合理的重要数据的备份策略规范； （3）数据库系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	
应用服务器-1-Tomcat	（1）宿主系统具有清除用户鉴别信息的功能； （2）经测试，宿主系统退出后无法访问先前中间件登录过的页面； （3）经测试，宿主系统关闭后无残留的中间件用户鉴别信息。
数据库服务器-PostgreSQL	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）数据库系统不保存终端历史记录； （3）引用产品测试结果，信息删除后可法保证完全清除。

3.4.4.2 主要安全问题汇总分析

安全通用要求

（1）数据库系统未配置鉴别失败处理功能。数据库系统存在不合规的登录连接超时及自动退出策略（如：数据库服务器-PostgreSQL）。登录验证可能被恶意用户猜测获得，合法用户身份被仿冒，导致系统被非授权访问。 中风险。

(2)未能提供中间件重要数据的异地定时数据备份功能(如:应用服务器-1-Tomcat)。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

3.4.5 业务应用系统/平台

3.4.5.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
门户网站系统	（1）系统对各登录模式均启用身份鉴别； （2）系统对登录管理的用户进行身份鉴别； （3）系统登录用户设置的身份标识具有唯一性；

	（4）系统不存在空口令用户； （5）设备配置合规的密码策略。
b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
门户网站系统	（1）系统启用合规登录失败处理策略； （2）系统配置合规的操作超时退出措施。
c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
门户网站系统	（1）应用系统的用户鉴别数据采用SHA-512算法在可控网络环境中传输； （2）系统配置合规的远程管理模式。
访问控制	
a）应对登录的用户分配账户和权限；	
门户网站系统	（1）可提供系统权限分配表； （2）登录系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需分配不同的用户权限，不存在所有用户均属于管理级别、高权限的情况。
b）应重命名或删除默认账户，修改默认账户的默认口令；	
门户网站系统	（1）系统禁用默认账户名； （2）系统账户口令设置合规。
c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
门户网站系统	（1）系统不存在多余或过期账户； （2）系统管理员用户与账户之间一一对应。
d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	
门户网站系统	（1）系统不存在多个管理级别高的特权用户； （2）系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
门户网站系统	（1）系统开启审计功能，审计进程正常； （2）系统的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
门户网站系统	（1）系统日期、时间正常； （2）系统审计记录内容基本完整。
c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
门户网站系统	（1）系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）系统针对日志、审计记录具备充足的存储容量； （3）审计记录及日志保存大于6个月。
入侵防范	
c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
门户网站系统	（1）系统自身设定有效的终端访问策略，通过访问措施进行管理地址的限制。
d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	

门户网站系统	（1）系统具备数据有效性检验功能； （2）系统的校验接口范围较全面。
e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
门户网站系统	（1）系统已根据需要不定期地对已发布的版本进行更新； （2）在系统上线或发生重大变更时测试并安装最新的版本或更新补丁； （3）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
门户网站系统	鉴别数据、重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； （2）系统对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a）应提供重要数据的本地数据备份与恢复功能；	
门户网站系统	（1）系统定义了相关需要备份重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	
门户网站系统	（1）系统具有清除用户鉴别信息的功能； （2）经测试，系统退出后无法访问先前登录过的页面； （3）经测试，系统关闭后无残留的用户鉴别信息。

3.4.5.2 主要安全问题汇总分析

安全通用要求

（1）未能提供应用软件系统重要数据的异地定时数据备份功能（如：门户网站系统）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

3.4.6 数据资源

3.4.6.1 已有安全控制措施汇总分析

安全通用要求

数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
重要业务数据	（1）系统在通信传输过程中对相关数据采取完整性保护措施； （2）系统对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
重要业务数据	（1）系统定义了相关需要备份重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。

3.4.6.2 主要安全问题汇总分析

安全通用要求

重要业务数据

（1）未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要业务数据）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

3.4.7 其他系统或设备

3.4.7.1 已有安全控制措施汇总分析

安全通用要求

无其他系统或设备，不涉及相关测评

3.4.7.2 主要安全问题汇总分析

安全通用要求

无其他系统或设备，不涉及相关测评

3.5 安全管理中心

3.5.1 已有安全控制措施汇总分析

安全通用要求

系统管理	
a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；	
管理中心	（1）网络中部署运维安全管理系统实现集中的系统管理； （2）系统对登录用户进行身份鉴别； （3）系统用户标识具有唯一性； （4）系统可实现对账户的身份鉴别数据进行保密性和完整性保护； （5）系统管理操作模式具备控制措施； （6）系统具备相应的管理操作审计措施。
审计管理	
a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；	
管理中心	（1）网络中部署运维安全管理系统实现集中安全审计功能； （2）审计系统对审计管理员进行身份鉴别； （3）审计系统用户标识具有唯一性； （4）审计系统管理操作模式具备控制措施； （5）审计系统具备相应的管理操作审计措施。
b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	
管理中心	门户网站系统: （1）审计管理员定期对审计记录进行分析，对发现的安全可疑事件及时处理； （2）单位具有安全审计策略文件，规范审计记录的存储、管理和查询要求； （3）审计管理员按规范要求对审计记录进行管理。 重要审计数据: 日志审计系统、运维安全管理系统: （1）设备在通信传输过程中对相关数据采取完整性保护措施； （2）设备对重要数据在传输过程中采取必要的完整性保护措施。

3.5.2 主要安全问题汇总分析

安全通用要求

（1）系统管理的资源、运行及配置管理不够全面（如：管理中心）。系统的资源和运行缺少统一的管理，将导致系统可能无法按规划实现基于资源配置、 系统加载、异常处理、及备份/恢复等的安全控制措施。 低风险。

3.6 安全管理制度

3.6.1 已有安全控制措施汇总分析

安全通用要求

安全策略	
应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。	
制度文件、执行/记录文件	（1）单位具有网络安全工作的总体方针和安全策略文件； （2）制度内容包括明确的单位安全工作要求； （3）管理文件详见《信息安全总体策略》。
管理制度	
a) 应对安全管理活动中的主要管理内容建立安全管理制度；	
制度文件、执行/记录文件	（1）单位有针对安全管理活动中的各类管理内容建立安全管理制度； （2）现有制度已覆盖管理活动的主要的方面； （3）制度详见：《信息安全总体策略》、《网络安全管理规范》、《组织安全结构和人员职责制度》、《人员管理制度》、《员工考核管理制度》。
b) 应对管理人员或操作人员执行的日常管理操作建立操作规程。	
制度文件、执行/记录文件	（1）单位针对相关业务日常管理的操作建立规程类管理制度； （2）现有制度已覆盖重要管理方面的系统维护手册和用户操作规程等； （3）管理文件详见《设备及系统软件配置和操作手册》。
制定和发布	
a) 应指定或授权专门的部门或人员负责安全管理制度的制定；	
制度文件、执行/记录文件	（1）单位针对安全管理制度的制定，指定教育信息与网络中心部主要负责； （2）在已制定的相关制度中可查阅到被授权制定管理制度的部门/人员信息； （3）管理文件详见《安全管理组织规范》。
b) 安全管理制度应通过正式、有效的方式发布，并进行版本控制。	
制度文件、执行/记录文件	（1）单位针对制度的制定和发布要求，制定管理规范文件； （2）管理规范文件对文件制定及发布定义了规范要求； （3）安全管理制度的收发登记记录有效； （4）管理文件详见《制度制定、发布、评审和修订管理制度》、《收发文登记记录》。
评审和修订	

应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	
制度文件、执行/记录文件	（1）单位针对制度的合理性和适用性需进行论证和审定及修订的要求，制定管理规范文件； （2）管理规范文件对制度的评审及修订定义了规范要求； （3）单位具有安全管理制度的审定或论证的过程记录； （4）单位对做过修订的制度，具备有修订版本的安全管理过程记录； （5）管理文件详见《制度制定、发布、评审和修订管理制度》及 《安全管理制度评审记录》。

3.6.2 主要安全问题汇总分析

安全通用要求

门户网站系统针对安全管理制度层面的安全通用要求采取的安全措施比较完善，未发现不符合项。

3.7 安全管理机构

3.7.1 已有安全控制措施汇总分析

安全通用要求

岗位设置	
a) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；	
制度文件、执行/记录文件	（1）单位已明确网络安全管理工作的职能部门，并明确了各岗位职责； （2）单位各部门职责文档已明确网络安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备网络安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。
b) 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。	
制度文件、执行/记录文件	（1）单位已明确系统安全管理工作的职能部门，并明确了各岗位职责； （2）单位各部门职责文档已明确系统安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备系统安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。

人员配备	
应配备一定数量的系统管理员、审计管理员和安全管理员等。	
制度文件、执行/记录文件	（1）单位针对人员配备要求，制定了管理制度； （2）单位按要求配备一定数量的重要岗位管理人员； （3）单位针对各岗位人员，制定并维护人员档案； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。
授权和审批	
a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；	
制度文件、执行/记录文件	（1）单位在制度中用文字描述或在流程图中明确，对关键活动进行审批； （2）单位对审批过程明确审批权限，对各项信息系统的重要操作与变更明确审批部门和批准人； （3）管理文件详见《授权和审批管理规定》。
b) 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。	
制度文件、执行/记录文件	（1）单位针对各项业务操作及变更等建立了审批程序规定； （2）单位针对系统变更、系统接入、物理范围等事项已明确按审批程序执行，记录有批准人签字； （3）管理文件详见《授权和审批管理规定》。
沟通和合作	
a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；	
制度文件、执行/记录文件	（1）单位针对机构内部管理人员之间、部门之间的沟通与合作，制定了管理制度； （2）单位的管理制度规范了合作和沟通的方式和周期； （3）单位有组织机构内部人员联系表； （4）单位有定期召开信息安全会议，保存有会议纪要； （5）管理文件详见《安全教育和培训制度》、《技能培训记录》《外部联系表》。
b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；	
制度文件、执行/记录文件	（1）单位针对加强与外部单位的合作与沟通，制定了管理制度规定； （2）单位能按要求与相关单位保持沟通合作，并提供相关单位联系方式和交流会议纪要； （3）管理文件详见《安全教育和培训制度》、《技能培训记录》、《外部联系表》。
c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	
制度文件、执行/记录文件	（1）单位建立了完善的对外联单位的联系列表； （2）管理文件详见《外部联系表》。

3.7.2 主要安全问题汇总分析

安全通用要求

（1）单位开展的检查工作不够完善（如：制度文件、执行/记录文件）。检查工作开展不仔细，可能对存在或潜在的安全风险不能被及时发现并进行处理。 低风险。

3.8 安全管理人员

3.8.1 已有安全控制措施汇总分析

安全通用要求

人员录用	
a) 应指定或授权专门的部门或人员负责人员录用；	
制度文件、执行/记录文件	（1）单位授权专门的部门负责人员录用工作，制定了管理制度规范； （2）由人力资源保障科负责人员录用工作； （3）管理文件详见《人员管理制度》。
b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查。	
制度文件、执行/记录文件	（1）单位针对人员录用过程，制定了明确要求，并形成人员安全管理制度； （2）单位现有管理制度明确说明录用人员应具备的条件； （3）单位按规定执行人员录用的相关审查过程； （4）管理文件详见《人员管理制度》、《人员入职考核记录》。
人员离岗	
应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。	
制度文件、执行/记录文件	（1）单位针对离岗人员权限终止及取回机构提供的各种设施的要求，制定了管理制度； （2）单位按规范开展对离岗人员的相关管理工作； （3）管理文件详见《人员管理度》、《人员离岗申请表》、《离场信息资料交接表》。
安全意识教育和培训	
应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。	
制度文件、执行/记录文件	（1）单位针对人员安全培训及责任和惩戒措施，制定了管理制度； （2）单位已开展安全意识教育及岗位技能培训。 （3）管理文件详见《安全教育和培训制度》。
外部人员访问管理	
a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；	
制度文件、执行/记录文件	（1）单位针对外部人员物理访问，制定了外部人员访问管理文档； （2）单位具备有效的外部人员访问重要区域的书面申请文档； （3）单位具备外部人员访问重要区域的登记记录； （4）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。
b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并	

登记备案；	
制度文件、执行/记录文件	（1）单位针对外部接入受控网络访问系统，制定了管理制度； （2）单位具备外部人员接入受控网络前的申请审批流程； （3）单位具备外部人员接入及访问系统的书面申请文档； （4）单位具备外部人员接入及访问系统的登记记录； （5）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。

3.8.2 主要安全问题汇总分析

安全通用要求

（1）单位未完全按管理规范开展人员离场后的清理工作（如：制度文件、执行/记录文件）。人员离场后的清理工作开展不规范，可能导致遗留外部人员访问受控区域的记录，存在被二次非法利用，造成泄密。 低风险。

3.9 安全建设管理

3.9.1 已有安全控制措施汇总分析

安全通用要求

定级和备案	
a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；	
制度文件、执行/记录文件	（1）单位的被测系统于2022年4月已完成备案； （2）系统备案相关文档（定级报告）中明确等级划分方法和理由，SAG三个方面的级别描述清晰； （3）管理文件详见《定级备案》。
b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；	
制度文件、执行/记录文件	(1)单位针对系统定级结果的审批及评审工作等要求,制定了管理制度; （2）现有系统的定级已具备合理性和正确性审定； （3）管理文件详见《定级备案》。
c) 应保证定级结果经过相关部门的批准；	
制度文件、执行/记录文件	（1）单位针对系统定级结果的上级批准要求，制定了管理制度； （2）现有系统的定级获得了相关部门的批准； （3）管理文件详见《定级备案》。
d) 应将备案材料报主管部门和相应公安机关备案。	
制度文件、执行/记录文件	（1）单位对被测系统的等级备案表、定级报告等备案材料已经报相应公安机关备案；

	（2）单位具备公安机关出具的备案号； （3）管理文件详见《定级备案》。
产品采购和使用	
a）应确保网络安全产品采购和使用符合国家的有关规定；	
制度文件、执行/记录文件	（1）单位已建立安全产品管理的相关管理规定； （2）单位具备安全产品采购流程及相关实施文档； （3）被测系统使用的安全产品具备销售许可资质； （4）安全产品具均为国内产品； （5）管理文件详见《设备安全管理制度》。
b）应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。	
制度文件、执行/记录文件	（1）单位已建立密码产品与服务管理的相关管理制度； （2）系统未使用密码产品； （3）管理文件详见《设备安全管理制度》。
外包软件开发	
b）应保证开发单位提供软件设计文档和使用指南。	
制度文件、执行/记录文件	（1）单位制定软件开发项目验收要求，明确开发单位的提交材料； （2）开发单位提供软件日常维护和使用所需的文档； （3）管理文件详见《外包开发软件管理规定》、《设备及系统软件配置和操作手册》。
工程实施	
a）应指定或授权专门的部门或人员负责工程实施过程的管理；	
制度文件、执行/记录文件	（1）单位针对专门的部门负责工程实施过程的管理要求，制定管理度； （2）单位由专岗负责系统建设的工程实施，且按照实施方案的要求对进度和质量进行控制； （3）管理文件详见《工程实施管理制度》。
b）应制定安全工程实施方案控制工程实施过程。	
制度文件、执行/记录文件	（1）单位制定了详细的工程实施方案； （2）工程实施单位严格按照方案执行，并有过程记录； （3）管理文件详见《测试及验收方案》、《工程项目实施方案》。
系统交付	
a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；	
制度文件、执行/记录文件	（1）单位具备系统交付清单； （2）系统交付清单内容较详细； （3）单位的清点工作较合规； （4）管理文件详见《系统交付管理》、《资产清单》。
b）应对负责运行维护的技术人员进行相应的技能培训；	
制度文件、执行/记录文件	（1）单位已对负责系统运行维护的技术人员进行了技能培训； （2）具备运维人员的培训记录； （3）管理文件详见《系统交付管理》、《资产清单》、《系统交付清单》、《技能培训记录》。
c）应提供建设过程文档和运行维护文档。	
制度文件、执行/记录文件	（1）单位提供了系统建设过程中的文档； （2）单位提供了指导用户进行系统运维的文档和系统培训手册； （3）管理文件详见《系统交付管理》、《系统交付清单》、《设备及系

	统软件配置和操作手册》。
等级测评	
a) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；	
制度文件、执行/记录文件	（1）单位针对系统等级测评要求，制定管理制度； （2）系统按要求开展首次测评工作； （3）管理文件详见《系统安全管理制度》。
b) 应在发生重大变更或级别发生变化时进行等级测评；	
制度文件、执行/记录文件	（1）管理制度中已规定在系统发生变更时及时对系统进行等级测评； （2）系统未发生过重大变更，系统等级未发生变化； （3）管理文件详见《系统安全管理制度》。
c) 应确保测评机构的选择符合国家有关规定。	
制度文件、执行/记录文件	（1）已选择在“全国等级保护测评机构推荐目录”中的测评单位进行等级测评； （2）管理文件详见《系统安全管理制度》、《网络安全等级保护测评服务合同》。
服务供应商选择	
a) 应确保服务供应商的选择符合国家的有关规定；	
制度文件、执行/记录文件	（1）单位在管理制度内明确提出安全服务供应商选择的要求； （2）单位选择的安全服务商符合国家的有关规定，具备相应的安全服务资质； （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。
b) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。	
制度文件、执行/记录文件	（1）单位的管理制度中已规定，需与安全服务商签订安全相关的协议并明确整个服务供应链各方需履行的网络安全相关义务； （2）单位已按规定与选定的安全服务商签订合规的协议； （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。

3.9.2 主要安全问题汇总分析

安全通用要求

（1）单位未具备适用于被测系统的安全规划设计方案（如：制度文件、执行/记录文件）。规划设计需求不全面，可能导致安全方案设计不完善，信息系统存在安全缺陷。低风险。

（2）单位未具备完整的安全设计方案相关的文档。单位相关方案的设计的内容不够完善（如：制度文件、执行/记录文件）。相关合规的规划配套文件缺失，可能导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。 中风险。

（3）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定。单位未对相关论证过程及内容进行完整的记录（如：制度文件、执行/记录文件）。未开展规范的审批过程，可能存在安全整体规划缺乏合理性和可行性，导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。 低风险。

（4）单位未在软件开发过程中对所有软件安全性进行测试。单位未在软件安装之前按要求对所有软件开展恶意代码检测（如：制度文件、执行/记录文件）。软件交付前恶意代码检测不规范，可能在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。 低风险。

（5）单位未完全根据测试验收方案组织相关部门和人员开展验收工作（如：制度文件、执行/记录文件）。可能由于验收测试不严谨，造成测试过程缺乏计划性及操作性，无法保证经过测试验收的系统达到既定的安全性等目标。 低风险。

(6)针对系统上线前的安全性测试工作存在问题(如:制度文件、执行/记录文件)。未按规定开展上线前测试，安全隐患可能在系统上线运行前未被发现并作出相应处理。低风险。

3.10 安全运维管理

3.10.1 已有安全控制措施汇总分析

安全通用要求

环境管理
a) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；

制度文件、执行/记录文件	（1）单位建立机房安全方面的管理制度，对有关运维方面的管理作出规定； （2）单位具备完整的机房出入登记记录； （3）单位具备完整的机房基础设施的维护记录； （4）管理文件详见《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。
b）应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；	
制度文件、执行/记录文件	（1）单位建立机房安全方面的管理制度； （2）单位现有机房管理记录与制度相符； （3）制度详见：《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。
c）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	
制度文件、执行/记录文件	（1）单位机房安全管理制度已明确来访人员的接待区域的要求； （2）单位按规范要求开展人员来访接待； （3）单位办公环境未发现有随意放置含有敏感信息介质的情况； （4）制度详见：《机房安全管理制度》、《物理安全管理规范》、《办公环境保密管理》。
资产管理	
应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。	
制度文件、执行/记录文件	（1）单位已建立有效的资产清单； （2）单位现有资产清单内容较全面； （3）制度详见：《设备安全管理制度》、《资产清单》。
介质管理	
a）应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；	
制度文件、执行/记录文件	（1）介质按管理要求放置于受控的环境中（如：机房）； （2）介质管理具备较全面的记录； （3）制度详见：《设备安全管理制度》、《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。
b）应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。	
制度文件、执行/记录文件	（1）介质管理制度中对介质安全传输有明确规定； （2）存储重要信息的介质在物理传输过程，具备严格的环节控制，无重大环节疏漏； （3）对介质的归档和查询均具备记录； （4）制度详见：《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。
设备维护管理	
a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	
制度文件、执行/记录文件	（1）单位人员岗位职责相关文档已明确设备维护管理的责任部门；

	（2）单位对各类设施、设备进行定期维护； （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。
b）应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。	
制度文件、执行/记录文件	（1）单位建立了配套设施、软硬件维护管理方面的管理制度； （2）单位开展相关工作与制度相符，且保留记录； （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。
网络和系统安全管理	
a）应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；	
制度文件、执行/记录文件	（1）单位建立系统安全管理文档，对系统管理员的管理制定了要求； （2）单位对各类关键角色建立了相应的工作职责文档； （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。
b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	
制度文件、执行/记录文件	（1）单位制定管理制度，对系统账号进行管理； （2）单位按管理规范开展账号管理工作； （3）账户管理记录内容较完整； （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。
c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	
制度文件、执行/记录文件	（1）单位建立了网络和系统安全管理制度； （2）网络和系统安全管理制度内容较全面； （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。
d）应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；	
制度文件、执行/记录文件	（1）单位对重要设备、系统的配置和操作建立配置手册； （2）现有操作配置手册已明确操作步骤、参数配置； （3）制度详见：《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。
e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。	
制度文件、执行/记录文件	（1）单位制定日常运维管理的相关制度规范； （2）单位按制度规范开展日常运维管理工作； （3）单位具备合规的运维记录； （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》、《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。
恶意代码防范管理	
a）应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	
制度文件、执行/记录文件	（1）单位制定恶意代码防范管理制度，明确对外来计算机或存储设备接入系统前进行恶意代码检查； （2）单位按外来计算机接入恶意代码检查规范开展工作；

	（3）单位制定培训管理制度，明确需通过培训提升员工的防恶意代码意识； （4）单位按培训管理要求开展工作； （5）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申请表》、《信息管理系统漏洞检查表》。
b）应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；	
制度文件、执行/记录文件	（1）建立恶意代码防范管理文档； （2）管理制度中覆盖防恶意代码软件的授权使用、恶意代码库升级、定期查杀等内容； （3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》。
配置管理	
应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。	
制度文件、执行/记录文件	（1）单位制定了基本配置信息管理的制度要求； （2）管理文件详见：《主机安全管理规范》、《网络安全管理规范》、《应用安全管理规范》、《网络配置信息》。
变更管理	
应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。	
制度文件、执行/记录文件	（1）单位建立了关于系统变更管理的制度文件； （2）现有变更管理制度覆盖了变更管理的各方面要求； （3）制度详见：《变更控制管理制度》、《通用变更记录表》。
备份与恢复管理	
a）应识别需要定期备份的重要业务信息、系统数据及软件系统等；	
制度文件、执行/记录文件	（1）单位根据业务重要程度，制定了需要定期备份的重要业务信息列表或清单。清单内需要定期备份的重要数据已经过用户方确认； （2）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。
b）应规定备份信息的备份方式、备份频度、存储介质、保存期等；	
制度文件、执行/记录文件	（1）单位建立了备份与恢复管理相关的安全管理制度； （2）备份与恢复管理的相关要求比较明确； （3）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。
c）应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	
制度文件、执行/记录文件	（1）单位现有管理制度，明确了数据备份策略和数据恢复策略，以及备份程序和恢复程序； （2）单位可按策略要求实现重要数据的定期备份与恢复性测试； （3）单位现有的备份的数据均经过恢复性测试，可确保备份的数据可用； （4）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。
安全事件处置	
a）应及时向安全管理部门报告所发现的安全弱点和可疑事件；	
制度文件、执行/记录文件	（1）单位已在安全培训及宣传过程中告知用户在发现安全弱点和可疑事

	件时及时向安全管理部门报告； （2）单位在系统运维过程中对发现的安全弱点和可疑事件均编制了对应的报告或相关文档； （3）单位现有安全弱点和可疑事件报告文档内容较详实； （4）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。
b）应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；	
制度文件、执行/记录文件	（1）单位制定了安全事件报告和处置管理制度； （2）现有安全事件管理制度内容较完整； （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。
c）应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。	
制度文件、执行/记录文件	（1）单位具备对安全事件的分析、处理、总结、防范等的报告／过程文档； （2）单位提供的安全事件报告和响应处置记录内容较完整； （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。
应急预案管理	
a）应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；	
制度文件、执行/记录文件	（1）单位制定重要事件的应急预案； （2）单位现有应急预案涉及的类型范围较全面； （3）单位现有应急预案的内容较完整； （4）制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。
b）应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。	
制度文件、执行/记录文件	（1）单位定期对相关人员进行应急预案培训； （2）单位根据不同的应急预案，按要求进行应急演练； （3）单位具备近期应急预案工作开展的相关记录； （4）单位提供的应急预案培训记录比较完整； （5）单位提供的应急预案演练记录比较完整； （6）经检查单位目前一旦出现应急事件，可参照预案合理有序的进行应急事件处置过程； （7）制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。

3.10.2 主要安全问题汇总分析

安全通用要求

（1）单位未严格按规范开展漏洞及安全隐患检测工作（如：制度文件、执行/记录文件）。漏洞检测、修补工作不到位，可能存在未授权人员利用漏洞攻击信息系统的风险。 低风险。

（2）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作（如：制度文件、执行/记录文件）。可能导致系统恶意代码检测管理不到位，存在信息系统感染恶意代码，从而导致严重的信息安全风险。 低风险。

（3）单位不了解现有密码相关的国家标准和行业标准。单位缺乏密码管理要求的制度文档（如：制度文件、执行/记录文件）。密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不到位，存在违反国家政策的风险。 中风险。

3.11 其他安全要求指标

3.11.1 已有安全控制措施汇总分析

本次测评未涉及其他安全要求指标。

3.11.2 主要安全问题汇总分析

本次测评未涉及其他安全要求指标。

3.12 验证测试

验证测试包括漏洞扫描，渗透测试等，验证测试发现的安全问题对应到相应的测评项的结果记录中。详细验证测试报告见报告附录。

3.12.1 漏洞扫描

3.12.1.1 漏洞扫描结果统计

本次测评主要使用了[绿盟远程安全评估系统]对系统的设备进行了安全扫描，其所涉及的系统版本为：[V6.0R04F01SP06]，规则库版本为：[V6.0R02F01.2900]。扫描结果如下：

经分析统计，共发现各接入点存在3类漏洞，其中0类危险程度为高的漏洞，0类危害程度为中的漏洞，3类危害程度为低的漏洞。

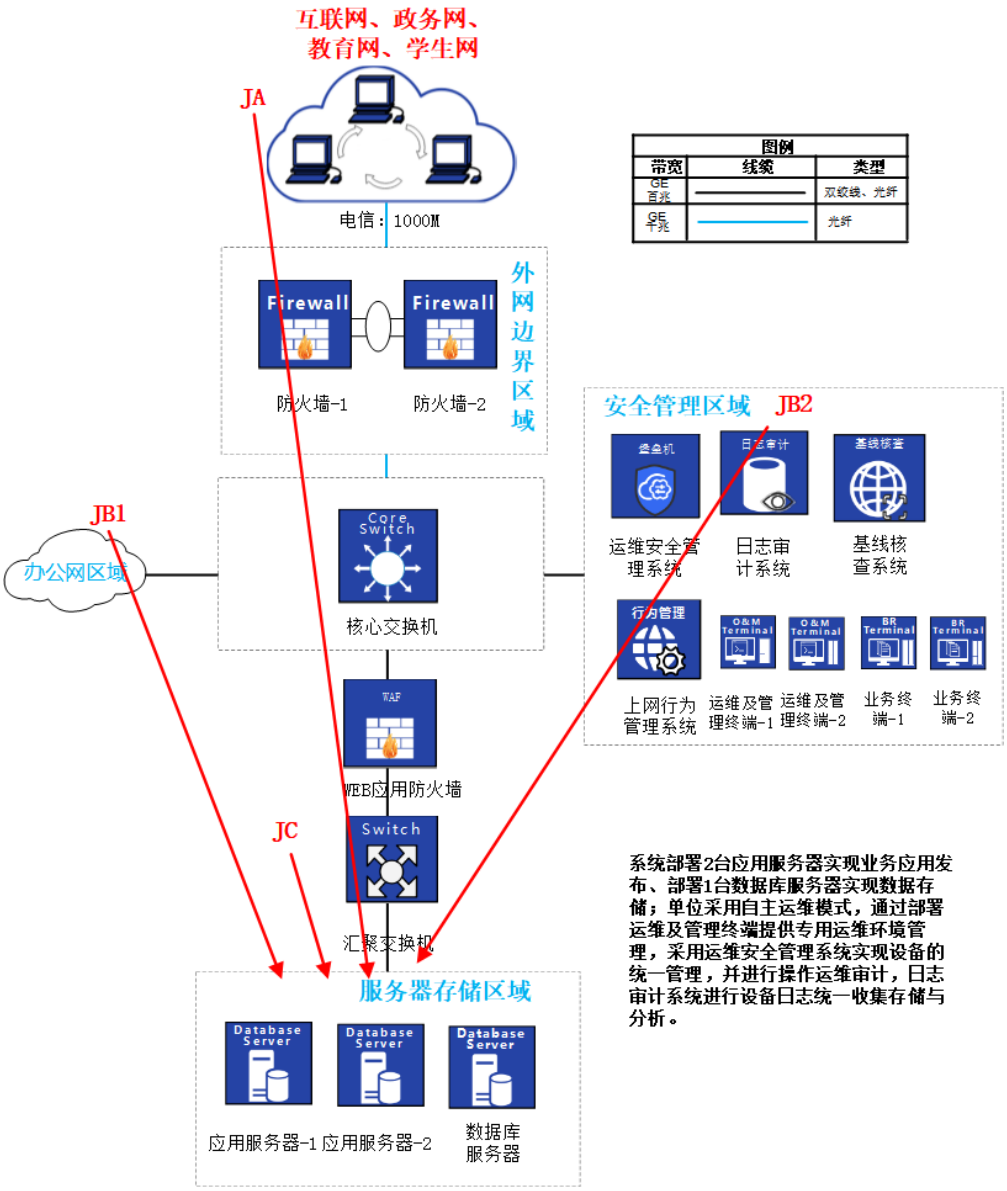


图 3-1 漏洞扫描工具接入测试示意图

接入点JA：在防火墙外侧接入，开展扫描/渗透主要目的是，探测对外服务功能区上各服务器、应用系统对外部网络边界暴露的安全漏洞情况，并根据漏洞扫描的结果接入渗透测试工具集，试图利用服务器、应用的安全漏洞入侵网络的行为。

接入点JB：在办公网区域VLAN段、安全管理区域VLAN段接入，开展扫描/渗透主要目的是，模拟外联单位/内部恶意用户发现操作系统、数据库、Web应用、第三方产品等安全漏洞的过程，并尝试利用以上漏洞实施诸如获取系统控制权（GetShell）、获得大量敏感信息（DragLibrary）等模拟攻击行为。

接入点JC：在系统所在VLAN的交换机接入，开展扫描/渗透主要目的是，直接测试对服务功能区上各服务器在最小化防御的基础上，对网络暴露的安全漏洞情况。

（1）接入点A漏洞扫描结果统计

根据在接入点A对16台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-1 接入点 A 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	0	0	0	0
2	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	0	0	0	0
3	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	0	0	0	0
4	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	0	0	0	0
5	172.16.1.14/上网行为管理系统	(安全设备)深信服 AC12.0.26	0	0	0	0
6	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	0	0	0	0
7	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	0	0	0	0
8	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	0	0	0	0
9	192.168.33.11/业务终端-1	(终端设备) Windows 10 （版本 20H2（内部版本 19044.1889）	0	0	0	0
10	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10 （版本 20H2（内部版本 19044.1889）	0	0	0	0
11	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10 （版本 20H2（内部版本 19044.1889）	0	0	0	0
12	192.168.33.10/业务终端-2	(终端设备) Windows 10 （版本 20H2（内部版本 19044.1889）	0	0	0	0
13	10.1.8.30/应用服务器-1	(服务器存储设备)CentOS 7.7	0	0	0	0
14	10.1.8.31/数据库服务器	(服务器存储设备)CentOS 6.8	0	0	0	0
15	10.1.8.29/应用服务器-2	(服务器存储设备)CentOS 7.7	0	0	0	0
16	https://www.mmpt.edu.cn/门户网站系统	(业务应用软件平台) V6.0	0	0	0	0

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
安全漏洞数量小计			0	0	0	0

（2）接入点B漏洞扫描结果统计

根据在接入点B对16台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-2 接入点 B 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	1	0	0	1
2	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	1	0	0	1
3	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	1	0	0	1
4	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	2	0	0	2
5	172.16.1.14/上网行为管理系统	(安全设备)深信服AC12.0.26	1	0	0	1
6	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	1	0	0	1
7	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	1	0	0	1
8	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	1	0	0	1
9	192.168.33.11/业务终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
10	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
11	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
12	192.168.33.10/业务终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
13	10.1.8.30/应用服务器-1	(服务器存储设备)CentOS 7.7	2	0	0	2
14	10.1.8.31/数据库服务器	(服务器存储设备)CentOS 6.8	2	0	0	2
15	10.1.8.29/应用服务器-2	(服务器存储设备)CentOS 7.7	2	0	0	2

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
16	https://www.mmpt.edu.cn/门户网站系统	(业务应用软件平台) V6.0	0	0	0	0
安全漏洞数量小计			15	0	0	15

(3) 接入点C漏洞扫描结果统计

根据在接入点C对16台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-3 接入点 C 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	1	0	0	1
2	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	1	0	0	1
3	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	1	0	0	1
4	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	2	0	0	2
5	172.16.1.14/上网行为管理系统	(安全设备)深信服AC12.0.26	1	0	0	1
6	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	1	0	0	1
7	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	1	0	0	1
8	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	1	0	0	1
9	192.168.33.11/业务终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
10	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
11	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
12	192.168.33.10/业务终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
13	10.1.8.30/应用服务器-1	(服务器存储设备)CentOS 7.7	2	0	0	2
14	10.1.8.31/数据库服务器	(服务器存储设备)CentOS 6.8	2	0	0	2

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
15	10.1.8.29/应用服务器-2	(服务器存储设备)CentOS 7.7	2	0	0	2
16	https://www.mmpt.edu.cn/门户网站系统	(业务应用软件平台) V6.0	0	0	0	0
安全漏洞数量小计			15	0	0	15

3.12.1.2 漏洞扫描问题描述

通过对漏洞扫描结果进行分析,门户网站系统存在的主要安全漏洞汇总如下表所示

表 3-4 主要安全漏洞汇总表

序号	安全漏洞名称	关联资产/域名	严重程度
1	SSH版本信息可被获取 此类漏洞涉及服务器存储设备。	10.1.8.30/应用服务器-1 10.1.8.31/数据库服务器 10.1.8.29/应用服务器-2	低
2	允许Traceroute探测 此类漏洞涉及网络设备、安全设备、服务器存储设备。	10.1.8.29/应用服务器-2 10.1.8.30/应用服务器-1 10.1.8.31/数据库服务器 10.2.1.4/运维安全管理系统 10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/上网行为管理系统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/汇聚交换机 172.16.1.2/核心交换机	低
3	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161) 此类漏洞涉及网络设备。	172.16.1.2/核心交换机	低

3.12.2 渗透测试

经分析统计，共发现各接入点存在1类漏洞，其中0类危险程度为高的漏洞，0类危害程度为中的漏洞，1类危害程度为低的漏洞。

3.12.2.1 渗透测试过程说明

方案制定：

在得到委托单位的书面授权许可后，才进行渗透测试的实施。并且将实施范围、方法、时间、人员等具体的方案委托单位进行交流，并得到委托单位的认同。在测试实施之前，会做到让委托单位对渗透测试过程和风险的知晓，使随后的正式测试流程都在委托单位的管控下。

信息收集：

此阶段中，渗透测试人员对目标信息系统进行必要的信息收集，如操作系统类型、开放的端口和服务、中间件信息、后台数据库类型、web开发语言等，即收集有利于漏洞挖掘的相关信息，为渗透测试做准备。

漏洞挖掘方法：

此阶段中，渗透测试人员对目标信息系统开始进行渗透测试，利用已知信息和现有条件及技术进行漏洞挖掘，尽可能发现目标信息系统中存在的所有安全风险，并进行记录。

漏洞利用：

此阶段中，渗透测试人员对目标信息系统对上一阶段漏洞挖掘中发现的漏洞进行必要的利用以证明其危害性，再对渗透测试过程所产生的测试数据进行清除。

输出报告：

此阶段中，渗透测试人员把渗透测试记录、截图等相关信息进行整理，然后撰写渗透测试报告，最终提交给委托单位。

漏洞修复：

此阶段中，委托单位依据收到的渗透测试报告对其中所提出的漏洞进行整改，可参考报告中所提出的修复建议，整改完成后联系本单位相关人员准备回归测试。

回归测试：

此阶段中，渗透测试人员对整改后的目标信息系统进行复测，以确定报告中提出的漏洞是否已被修复，若已被修复，则进入下一阶段；否则，返回上一阶段。

测试工具：

序号	工具	工具用途
1	Burpsuite Pro	用于攻击Web应用程序的集成软件
2	Sqlmap	开源的自动化SQL注入工具
3	Nmap	开源的网络发现和安全审计工具
4	OWASP ZAP	自动化Web应用漏洞扫描工具
5	其他测试工具	根据信息系统的类别选择不同的工具（如自写脚本、目录扫描器、木马扫描器、其它开源工具等）

3.12.2.2 渗透测试问题描述

通过渗透测试发现，门户网站系统存在的安全问题汇总如下表所示。

表 3-5 渗透测试结果汇总表

序号	安全问题	关联资产/域名	严重程度
1	缺少“Content-Security-Policy”响应头 此类漏洞涉及业务应用软件平台。	https://www.mmpt.edu.cn/ 门户网站系统	低

3.13 单项测评小结

3.13.1 控制点符合情况汇总

根据单项测评结果汇总控制点符合情况如下表所示。（表格以不同颜色对测评结果进行区分，不符合的安全控制点采用红色标识，部分符合的采用黄色标识，不适用的采用蓝色标识且不做勾选。）

表 3-6 控制点符合情况汇总表

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
1	安全通用要求	安全物理环境	物理位置选择	√		
2			物理访问控制		√	
3			防盗窃和防破坏	√		
4			防雷击	√		
5			防火		√	
6			防水和防潮	√		
7			防静电			√
8			温湿度控制	√		
9			电力供应	√		
10			电磁防护	√		
11	安全通用要求	安全通信网络	网络架构		√	
12			通信传输	√		
13			可信验证			√
14	安全通用要求	安全区域边界	边界防护	√		
15			访问控制	√		
16			入侵防范		√	
17			恶意代码和垃圾邮件防范		√	
18			安全审计	√		
19			可信验证			√

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
20	安全通用要求	安全计算环境	身份鉴别		√	
21			访问控制	√		
22			安全审计	√		
23			入侵防范	√		
24			恶意代码防范	√		
25			可信验证			√
26			数据完整性	√		
27			数据备份恢复		√	
28			剩余信息保护	√		
29			个人信息保护			
30	安全通用要求	安全管理中心	系统管理		√	
31			审计管理	√		
32	安全通用要求	安全管理制度	安全策略	√		
33			管理制度	√		
34			制定和发布	√		
35			评审和修订	√		
36	安全通用要求	安全管理机构	岗位设置	√		
37			人员配备	√		
38			授权和审批	√		
39			沟通和合作	√		

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
40			审核和检查		√	
41	安全通用要求	安全管理人员	人员录用	√		
42			人员离岗	√		
43			安全意识教育和培训	√		
44			外部人员访问管理		√	
45	安全通用要求	安全建设管理	定级和备案	√		
46			安全方案设计			√
47			产品采购和使用	√		
48			自行软件开发			
49			外包软件开发		√	
50			工程实施	√		
51			测试验收		√	
52			系统交付	√		
53			等级测评	√		
54			服务供应商选择	√		
55	安全通用要求	安全运维管理	环境管理	√		
56			资产管理	√		
57			介质管理	√		
58			设备维护管理	√		
59			漏洞和风险管理			√

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
60			网络和系统安全管理	√		
61			恶意代码防范管理		√	
62			配置管理	√		
63			密码管理			√
64			变更管理	√		
65			备份与恢复管理	√		
66			安全事件处置	√		
67			应急预案管理	√		
68			外包运维管理			
安全通用要求控制点符合情况数量统计				45	13	7
控制点符合情况数量统计				45	13	7

3.13.2 安全问题汇总

针对单项测评结果中存在的部分符合和不符合项进行汇总，形成了安全问题如下表所示。

表 3-7 安全问题汇总表

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T1	（1）机房出入口未配置电子门禁系统。	信息化机房	安全通用要求	安全物理环境	物理访问控制	机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。
T2	（1）机房建设未完全采用符合耐火等级的建筑材料； （2）机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级。	信息化机房	安全通用要求	安全物理环境	防火	b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T3	（1）机房内缺乏防静电措施（如防静电地板或铺设防静电地毯 ）。	信息化机房	安全通用要求	安全物理环境	防静电	应采用防静电地板或地面并采用必要的接地防静电措施。
T4	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	安全通用要求	安全通信网络	网络架构	a）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
T5	（1）缺乏对通信设备可信验证方面的安全设计要求； （2）现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况。	安全通信网络	安全通用要求	安全通信网络	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T6	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	安全通用要求	安全区域边界	入侵防范	应在关键网络节点处监视网络攻击行为。
T7	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	安全通用要求	安全区域边界	恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。
T8	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	办公网区域 外网边界区域 安全管理区域 服务器存储区域	安全通用要求	安全区域边界	可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T9	（1）数据库系统未配置鉴别失败处理功能； （2）数据库系统存在不合规的登录连接超时及自动退出策略。	数据库服务器-PostgreSQL	安全通用要求	安全计算环境	身份鉴别	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T10	（1）设备不具备相关可信验证的技术措施。	WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2	安全通用要求	安全计算环境	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T11	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。	业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	安全通用要求	安全计算环境	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T12	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况； （3）现有的计算设备存在对系统运行过程中的可信检验不全面的情况； （4）现有的可信验证存在部分告警、审计及联动措施不全面的情况。	应用服务器-1 应用服务器-2 数据库服务器	安全通用要求	安全计算环境	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T13	（1）未能提供中间件重要数据的异地定时数据备份功能。	应用服务器-1-Tomcat	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T14	（1）未能提供数据库系统重要数据的异地定时数据备份功能。	数据库服务器-PostgreSQL	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T15	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	重要业务数据	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T16	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	门户网站系统	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T17	（1）系统管理的资源、运行及配置管理不够全面。	管理中心	安全通用要求	安全管理中心	系统管理	b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
T18	（1）单位开展的检查工作不够完善。	制度文件、执行/记录文件	安全通用要求	安全管理机构	审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。
T19	（1）单位未完全按管理规范开展人员离场后的清理工作。	制度文件、执行/记录文件	安全通用要求	安全管理人员	外部人员访问管理	c）外部人员离场后应及时清除其所有的访问权限。
T20	（1）单位未具备适用于被测系统的安全规划设计方案。	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
T21	（1）单位未具备完整的安全设计方案相关的文档； （2）单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	b）应根据保护对象的安全保护等级进行安全方案设计；
T22	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； （2）单位未对相关论证过程及内容进行完整的记录。	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	c）应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。
T23	（1）单位未在软件开发过程中对所有软件安全性进行测试； （2）单位未在软件安装之	制度文件、执行/记录文件	安全通用要求	安全建设管理	外包软件开发	a）应在软件交付前检测其中可能存在的恶意代码；

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
	前按要求对所有软件开展恶意代码检测。					
T24	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	安全通用要求	安全建设管理	测试验收	a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；
T25	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	安全通用要求	安全建设管理	测试验收	b）应进行上线前的安全性测试，并出具安全测试报告。
T26	（1）单位未严格按规范开展漏洞及安全隐患检测工作。	制度文件、执行/记录文件	安全通用要求	安全运维管理	漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。
T27	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	安全通用要求	安全运维管理	恶意代码防范管理	c）应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。
T28	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	制度文件、执行/记录文件	安全通用要求	安全运维管理	密码管理	a）应遵循密码相关国家标准和行业标准；

4 整体测评

从安全控制间、区域间和验证测试等方面对单元测评的结果进行验证、分析和整体评价。

具体内容参见《GB/T 28448-2019信息安全技术 网络安全等级保护测评要求》。

4.1 安全控制点间安全测评

安全控制间的安全测评主要考虑同一区域内、同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用。安全功能上的增强和补充可以使两个不同强度、不

同等级的安全控制发挥更强的综合效能,可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。

4.1.1 安全建设管理

4.1.1.1 安全通用要求

（T24）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。

单位未具备适用于被测系统的安全规划设计方案。安全方案设计不完善，导致规划设计需求不全面，信息系统存在安全缺陷。可升高单位未完全根据测试验收方案组织相关部门和人员开展验收工作的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

（T25）针对系统上线前的安全性测试工作存在问题。

单位未在软件交付之前按要求对所有软件开展恶意代码检测,导致在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。可升高针对系统上线前的安全性测试工作存在问题的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

4.1.2 安全运维管理

4.1.2.1 安全通用要求

（T27）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。

单位未严格按规范开展漏洞及安全隐患检测工作，漏洞检测工作不到位，导致存在未授权人员利用漏洞攻击信息系统的风险。可升高单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

4.2 区域间安全测评

区域间的安全测评主要考虑互连互通（包括物理上和逻辑上的互连互通等）的不同区域之间存在的安全功能增强、补充和削弱等关联作用，特别是有数据交换的两个不同区域。

4.2.1 安全物理环境

4.2.1.1 安全通用要求

（T1）机房出入口未配置电子门禁系统。

机房所在位置处于内部受控区域，非授权人员无法随意通过现有控制措施（如机械锁）进出机房，且具备相对完善的机房出入管理要求（具备《机房安全管理制度》），并实际执行措施效果良好（具备《机房出入登记表》），可降低机房出入口访问控制措施缺失的问题严重程度（如信息化机房）。根据整体测评分析，问题严重程度变化为降低。

4.2.2 安全通信网络

4.2.2.1 安全通用要求

（T4）关键的应用服务和数据库服务网段未独立进行子网划分的情况。

单位有完整的IP地址规范，对IP地址的使用、回收均有记录《资产清单》，且系统具备相对完善的设备自身访问控制策略管理要求（具备《网络安全管理规范》、《设备及系统软件配置和操作手册》），措施效果良好，有助于部分补充未划分子网的安全功能不足（如安全通信网络）。根据整体测评分析，问题严重程度变化为降低。

4.2.3 安全区域边界

4.2.3.1 安全通用要求

（T6）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。

网络环境划分了相应的安全区域，区域间具备有效的访问控制措施，区域内各主机设备部署深信服EDR单机版，策略库、规则库更新及时，能够对攻击行为进行检测、阻断或限制，实际措施效果良好，且系统具备相对完善的策略库、规则库更新/校准管理要求，管理措施效果良好且及时检查更新有效性（具备《漏洞检测报告》、《主机安全管理规范》），可降低外部网络攻击防御措施缺失的问题严重程度（如办公网区域、安全管理区域）。根据整体测评分析，问题严重程度变化为降低。

（T7）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。

系统部署于可控的网络环境内（具备有效的访问控制、入侵防护措施）限制相关主机对象访问非受控网络，操作系统层面配置防御策略（具备本地防火墙策略、核心交换机地址限制策略、部署深信服EDR单机版），恶意代码入侵的可能性相对较低，可降低恶意代码防范措施缺失的问题严重程度（如办公网区域、安全管理区域）。根据整体测评分析，问题严重程度变化为降低。

4.3 整体测评结果汇总

经整体测评后安全问题严重程度变化情况如下表所示

表 4-1 整体测评结果汇总表

问题编号	安全问题描述	测评对象	整体测评描述	严重程度变化
T1	（1）机房出入口未配置电子门禁系统。	信息化机房	（1）机房所在位置处于内部受控区域，非授权人员无法随意通过现有控制措施（如机械锁）进出机房，且具备相对完善的机房出入管理要求（具备《机房安全管理制度》），并实际执行措施效果良好（具备《机房出入登记表》），可降低机房出	□升高 ☑降低

问题编号	安全问题描述	测评对象	整体测评描述	严重程度变化
			入口访问控制措施缺失的问题严重程度。	
T4	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	（1）单位有完整的IP地址规范，对IP地址的使用、回收均有记录《资产清单》，且系统具备相对完善的设备自身访问控制策略管理要求（具备《网络安全管理规范》、《设备及系统软件配置和操作手册》），措施效果良好，有助于部分补充未划分子网的安全功能不足。	□升高 ☑降低
T6	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	（1）网络环境划分了相应的安全区域，区域间具备有效的访问控制措施，区域内各主机设备部署深信服EDR单机版，策略库、规则库更新及时，能够对攻击行为进行检测、阻断或限制，实际措施效果良好，且系统具备相对完善的策略库、规则库更新/校准管理要求，管理措施效果良好且及时检查更新有效性（具备《漏洞检测报告》、《主机安全管理规范》），可降低外部网络攻击防御措施缺失的问题严重程度。	□升高 ☑降低
T7	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	（1）系统部署于可控的网络环境内（具备有效的访问控制、入侵防护措施）限制相关主机对象访问非受控网络，操作系统层面配置防御策略（具备本地防火墙策略、核心交换机地址限制策略、部署深信服EDR单机版），恶意代码入侵的可能性相对较低，可降低恶意代码防范措施缺失的问题严重程度。	□升高 ☑降低
T24	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	（1）单位未具备适用于被测系统的安全规划设计方案。安全方案设计不完善，导致规划设计需求不全面，信息系统存在安全缺陷。可升高单位未完全根据测试验收方案组织相关部门和人员开展验收工作的问题严重程度。	☑升高 □降低
T25	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	（1）单位未在软件交付之前按要求对所有软件开展恶意代码检测，导	☑升高

问题编号	安全问题描述	测评对象	整体测评描述	严重程度变化
			致在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。可升高针对系统上线前的安全性测试工作存在问题的问题严重程度。	□降低
T27	(1)单位未严格按规范要求,针对防范恶意代码攻击的技术措施的有效性验证,开展工作。	制度文件、执行/记录文件	（1）单位未严格按规范开展漏洞及安全隐患检测工作，漏洞检测工作不到位，导致存在未授权人员利用漏洞攻击信息系统的风险。可升高单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作的问题严重程度。	☑升高 □降低

5 安全问题风险分析

针对等级测评结果中存在的所有安全问题,结合关联资产和威胁分别分析安全问题可能产生的危害结果,找出可能对系统、单位、社会及国家造成的最大安全危害(损失),并根据最大安全危害(损失)的严重程度进一步确定安全问题的风险等级,结果为“高”、“中”或“低”。最大安全危害（损失）结果应结合安全问题所影响业务的重要程度、相关系统组件的重要程度、安全问题严重程度以及安全事件影响范围等进行综合分析。

表 5-1 安全问题风险分析

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
1	安全物理环境	（1）机房出入口未配置电子门禁系统。	信息化机房	物理攻击	（1）上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域，可能对系统的平稳运行造成影响。	中风险
2	安全物理环境	（1）机房建设未完全采用符合耐火等级的建筑材料; （2）机房建设不具备防火设计/验收文档，或机房验收文档未明确相关	信息化机房	物理环境影响	（1）存在发生火情时助燃火灾的风险。	低风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
		建筑材料的耐火等级。				
3	安全物理环境	（1）机房内缺乏防静电措施（如防静电地板或铺设防静电地毯）。	信息化机房	软硬件故障	（1）存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。	中风险
4	安全通信网络	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	恶意攻击	（1）上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变得更为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。	中风险
5	安全通信网络	（1）缺乏对通信设备可信验证方面的安全设计要求； （2）现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况。	安全通信网络	恶意攻击	（1）缺乏对系统可执行程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致计算资源被干扰和破坏造成损失。	低风险
6	安全区域边界	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	恶意攻击	（1）存在不能及时发现内部主机作为攻击跳板，或网络攻击行为而造成系统损坏/网络资源浪费的风险。	中风险
7	安全区域边界	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	恶意攻击	（1）无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。	中风险
8	安全区域边界	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	办公网区域 外网边界区域 安全管理区域 服务器存储区域	恶意攻击	（1）缺乏对边界设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险
9	安全计算环境	（1）数据库系统未配置鉴别失败处理功能；	数据库服务器-PostgreSQL	恶意攻击	（1）登录验证可能被恶意用户猜测获得，合法用户	中风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
		（2）数据库系统存在不合规的登录连接超时及自动退出策略。			身份被仿冒，导致系统被非授权访问。	
10	安全计算环境	（1）设备不具备相关可信验证的技术措施。	WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2	恶意攻击	（1）缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险
11	安全计算环境	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。	业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	恶意攻击	（1）缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险
12	安全计算环境	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况； （3）现有的计算设备存在对系统运行过程中的可信检验不全面的情况； （4）现有的可信验证存在部分告警、审计及联动措施不全面的情况。	应用服务器-1 应用服务器-2 数据库服务器	恶意攻击	（1）缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险
13	安全计算环境	（1）未能提供中间件重要数据的异地定时数据备份功能。	应用服务器-1-Tomcat	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。	中风险
14	安全计算环境	（1）未能提供数据库系统重要数据的异地定时数据备份功能。	数据库服务器-PostgreSQL	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的	中风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
					持续提供，使企业的经济利益或声誉受到损害。	
15	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	重要业务数据	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。	中风险
16	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	门户网站系统	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。	中风险
17	安全管理中心	（1）系统管理的资源、运行及配置管理不够全面。	管理中心	恶意攻击	（1）系统的资源和运行缺少统一的管理，将导致系统可能无法按规划实现基于资源配置、 系统加载、异常处理、及备份/恢复等的安全控制措施。	低风险
18	安全管理机构	（1）单位开展的检查工作不够完善。	制度文件、执行/记录文件	管理不到位	（1）检查工作开展不仔细，可能对存在或潜在的安全风险不能被及时发现并进行处理。	低风险
19	安全管理人员	（1）单位未完全按管理规范开展人员离场后的清理工作。	制度文件、执行/记录文件	管理不到位	（1）人员离场后的清理工作开展不规范，可能导致遗留外部人员访问受控区域的记录，存在被二次非法利用，造成泄密。	低风险
20	安全建设管理	（1）单位未具备适用于被测系统的安全规划设计方案。	制度文件、执行/记录文件	管理不到位	（1）规划设计需求不全面，可能导致安全方案设计不完善，信息系统存在安全缺陷。	低风险
21	安全建设管理	（1）单位未具备完整的安全设计方案相关的文档； （2）单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	管理不到位	（1）相关合规的规划配套文件缺失，可能导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。	中风险
22	安全建设管理	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； （2）单位未对相关论证过程及内容进行完整的	制度文件、执行/记录文件	管理不到位	（1）未开展规范的审批过程，可能存在安全整体规划缺乏合理性和可行性，导致信息系统安全防御能力缺乏完整性、系统性，	低风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
		记录。			不足以满足业务发展需要。	
23	安全建设管理	（1）单位未在软件开发过程中对所有软件安全性进行测试； （2）单位未在软件安装之前按要求对所有软件开展恶意代码检测。	制度文件、执行/记录文件	管理不到位	（1）软件交付前恶意代码检测不规范，可能在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。	低风险
24	安全建设管理	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	管理不到位	（1）可能由于验收测试不严谨，造成测试过程缺乏计划性及操作性，无法保证经过测试验收的系统达到既定的安全性等目标。	低风险
25	安全建设管理	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	管理不到位	（1）未按规定开展上线前测试，安全隐患可能在系统上线运行前未被发现并作出相应处理。	低风险
26	安全运维管理	（1）单位未严格按规范开展漏洞及安全隐患检测工作。	制度文件、执行/记录文件	管理不到位	（1）漏洞检测、修补工作不到位，可能存在未授权人员利用漏洞攻击信息系统的风险。	低风险
27	安全运维管理	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	管理不到位	（1）可能导致系统恶意代码检测管理不到位，存在信息系统感染恶意代码，从而导致严重的信息安全风险。	低风险
28	安全运维管理	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	制度文件、执行/记录文件	管理不到位	（1）密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不到位，存在违反国家政策的风险。	中风险

6 等级测评结论

等级测评结论由安全问题风险分析结果和综合得分共同确定，判定依据如下表所示。

表 6-1 等级测评结论判别依据

测评结论	判别依据
优	被测对象中存在安全问题，但不会导致被测对象面临中、高等级安全风险，且系统综合得分 90 分以上（含90 分）。
良	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分 80分以上（含 80分）。
中	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分 70分以上（含 70分）
差	被测对象中存在安全问题，而且会导致被测对象面临高等级安全风险，或被测对象综合得分低于 70 分。

综合得分计算方法如下：

设M为被测对象的综合得分，$M = V_t + V_m$，V_t和V_m根据下列公式计算。

$$V_t = \begin{cases} 100 \cdot y - \sum_{k=1}^{t} f(\omega_k) \cdot (1 - x_k) \cdot S, & V_t > 0 \\ 0, & V_t \le 0 \end{cases}$$

$$V_m = \begin{cases} 100 \cdot (1 - y) - \sum_{k=1}^{m} f(\omega_k) \cdot (1 - x_k) \cdot S, & V_m > 0 \\ 0, & V_m \le 0 \end{cases}$$

$$0 \le x_k \le 1,\ S = 100 \cdot \frac{1}{n},\ f(\omega_k) = \begin{cases} 1, & \omega_k = \text{一般} \\ 2, & \omega_k = \text{重要} \\ 3, & \omega_k = \text{关键} \end{cases}$$

其中，y为关注系数，取值在0至1之间，由等级保护工作管理部门给出，默认值为0.5。n为被测对象涉及的总测评项数（不含不适用项，下同），t为技术方面对应的总测评项数，V_t为技术方面的得分，m为管理方面对应的总测评项数，V_m为管理方面的得分，ω_k为测评项k的重要程度（分为一般、重要和关键），x_k为测评项k的得分，如果测评项k涉及多测评项对象，则x_k取值为多测评对象得分的算术平均值。

x_k的得分计算如下：

测评项k涉及对象 / 测评项k定性判定	只涉及单个对象	涉及多个对象
符合	1	1
部分符合	0.5	计算测评对象平均分，取值在0至1之间
不符合	0	0

注：当测评项k涉及多个对象时，针对每个对象的得分取值为1、0.5和0。

根据第5章安全问题风险分析结果统计高、中、低风险安全问题的数量，利用综合得分计算公式计算出被测对象的综合得分，并将相关结果填入下表。

表 6-2 安全问题统计和综合得分

被测对象名称	安全问题数量			综合得分
	高风险	中风险	低风险	
门户网站系统	0	12	16	73.35

依据 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》和GB/T 28448—2019《信息安全技术 网络安全等级保护测评要求》的第二级要求，经对门户网站系统的安全保护状况进行综合分析评价，等级测评结论如下：

门户网站系统本次等级测评的综合得分为73.35，且不存在高等级安全风险，等级测评结论为中。

7 安全问题整改建议

表 7-1 安全问题整改建议

序号	安全类	安全问题	关联资产	整改建议
1	安全物理环境	（1）机房出入口未配置电子门禁系统。	信息化机房	（1）采用电子门禁系统严格控制机房其他出入口的进出，或安排专人值守；

序号	安全类	安全问题	关联资产	整改建议
				（2）采用电子门禁系统，对机房所有人员出入进行登记记录，并保存。
2	安全物理环境	（1）机房建设未完全采用符合耐火等级的建筑材料； （2）机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级。	信息化机房	（1）机房及相关的工作房间和辅助房采用具有耐火等级的建筑材料； （2）机房建设采用符合相关耐火等级（二级）的建筑材料。（内外墙壁均应采用具有防火涂料、隔热板、铝板、钢板等阻燃或不燃的材料）； （3）机房耐火等级建筑材料有相关合格证，并留存机房验收文档。
3	安全物理环境	（1）机房内缺乏防静电措施（如防静电地板或铺设防静电地毯）。	信息化机房	（1）机房铺设防静电地板或铺设防静电地毯； （2）机房房静电设计可依据GB50174-2008和GB50314-2006相关规定进行机房设计和验收。
4	安全通信网络	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	（1）建议独立划分出应用服务器网段、数据库服务器网段。
5	安全通信网络	（1）缺乏对通信设备可信验证方面的安全设计要求； （2）现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况。	安全通信网络	（1）建议在管理规范文档内对通信设备可信验证方面的安全设计提出要求； （2）建议系统实现对所有可执行环节进行可信验证，包括： 运行过程中的可信检验： ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■通信应用连接过程。
6	安全区域边界	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	（1）建议网络层部署的防火墙配置对内部发起的攻击行为实现防范功能策略，实现检测、防止或限制从内部发起的网络攻击行为； （2）内部安全防范措施能检测以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、碎片攻击、网络蠕虫攻击、应用漏洞攻击。
7	安全区域边界	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	（1）建议现有部署的恶意代码防范措施网络边界覆盖全面，及时对恶意代码及逆行检测和清除。
8	安全区域边界	（1）缺乏对边界设备可信验证方面的安全设计要求；	办公网区域 外网边界区域	（1）建议对边界设备系统程序的可信验证设计并保存设计文件；

序号	安全类	安全问题	关联资产	整改建议
		(2)现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	安全管理区域 服务器存储区域	（2）建议系统实现对所有可执行环节进行可信验证。
9	安全计算环境	(1)数据库系统未配置鉴别失败处理功能； (2)数据库系统存在不合规的登录连接超时及自动退出策略。	数据库服务器-PostgreSQL	（1）建议数据库系统配置合规的锁定策略，可参考：失败15次锁定15分钟； （2）建议数据库系统配置合规的操作超时锁定，可参考：超时15分钟退出。
10	安全计算环境	(1)设备不具备相关可信验证的技术措施。	WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2	（1）建议通过设备的启动过程和运行过程中对预装软件（包括系统引导程序、系统程序、相关应用程序和重要配置参数）的完整性验证或检测，确保对系统引导程序、系统程序、重要配置参数和关键应用程序可信根验证； （2）建议设备启用在检测到其可信性受到破坏后进行报警的相关功能。
11	安全计算环境	(1)缺乏对计算设备可信验证方面的安全设计要求； (2)现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。	业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）建议对计算设备系统程序的可信验证设计并保存设计文件； （2）建议系统实现对所有可执行环节进行可信验证。
12	安全计算环境	(1)缺乏对计算设备可信验证方面的安全设计要求； (2)现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况； (3)现有的计算设备存在对系统运行过程中的可信检验不全面的情况； (4)现有的可信验证存在部分告警、审计及联动措施不全面的情况。	应用服务器-1 应用服务器-2 数据库服务器	（1）建议对计算设备系统程序的可信验证设计并保存设计文件； （2）建议系统实现对所有可执行环节进行可信验证。
13	安全计算环境	(1)未能提供中间件重要数据的异地定时数据备份功能。	应用服务器-1-Tomcat	（1）建议设置异地灾备机房，并利用通信网络将中间件重要数据定时备份至备份场地； （2）异地备份的中间件数据范围（不

序号	安全类	安全问题	关联资产	整改建议
				限于）包括系统的： ■配置数据 ■重要日志数据。
14	安全计算环境	（1）未能提供数据库系统重要数据的异地定时数据备份功能。	数据库服务器-PostgreSQL	（1）建议设置异地灾备机房，并利用通信网络将重要数据定时备份至备份场地； （2）异地备份的数据范围（不限于）包括系统的： ■配置数据 ■重要业务数据。
15	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	重要业务数据	（1）建议设置异地灾备机房，并利用通信网络将应用软件系统重要数据定时备份至备份场地。
16	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	门户网站系统	（1）建议设置异地灾备机房，并利用通信网络将应用软件系统重要数据定时备份至备份场地； （2）异地备份的应用软件系统数据范围（不限于）包括系统的：配置数据、重要日志数据，业务数据。
17	安全管理中心	（1）系统管理的资源、运行及配置管理不够全面。	管理中心	（1）需实现系统包括对可信证书管理、可信基准库的管理。
18	安全管理机构	（1）单位开展的检查工作不够完善。	制度文件、执行/记录文件	（1）建议单位按要求提供安全检查报告。
19	安全管理人员	（1）单位未完全按管理规范开展人员离场后的清理工作。	制度文件、执行/记录文件	（1）建议单位按管理规范开展人员离场后的清理工作。至少包括：保留清理记录、及时清除离场后的所有访问权限、记录访问权限清除时间。
20	安全建设管理	（1）单位未具备适用于被测系统的安全规划设计方案。	制度文件、执行/记录文件	（1）建议单位根据等保要求进行过全面的自查或对比，根据系统的安全级别选择基本安全措施； （2）建议规划方案需根据风险分析结果对系统安全措施进行补充和整，并在系统建设\\整改方案中有详细描述。
21	安全建设管理	（1）单位未具备完整的安全设计方案相关的文档； （2）单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	（1）建议单位根据信息系统的等级划分情况，准备安全设计方案、安全管理策略、安全建设规划文档等； （2）建议相关文档内容应完善，包括统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、密码技术要求、总体建设规划和详细设计方案，并形成一致性的配套文件。

序号	安全类	安全问题	关联资产	整改建议
22	安全建设管理	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； （2）单位未对相关论证过程及内容进行完整的记录。	制度文件、执行/记录文件	（1）建议单位组织相关部门和安全技术专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定； （2）保存论证和审定记录，记录包括批准时间、批准人员签字； （3）文件经过批准后，才能正式实施。
23	安全建设管理	（1）单位未在软件开发过程中对所有软件安全性进行测试； （2）单位未在软件安装之前按要求对所有软件开展恶意代码检测。	制度文件、执行/记录文件	（1）建议开发商提供软件源代码，软件安装前检测软件中的恶意代码； （2）输出检测报告（或提供第三方检测报告），内容包括测试时间、测试地点、测试对象、测试结论、测试人员。
24	安全建设管理	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	（1）建议根据测试验收过程记录与结果，形成测试验收报告。
25	安全建设管理	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	（1）建议系统建设完成后，委托第三方测试单位对系统进行安全性测试，并出具安全性测试报告； （2）测试报告内容至少包括测试时间、测试地点、测试人、测试对象、测试方法、测试过程、测试发现的安全问题、整改建议、测试结论，并有第三方测试机构的签字盖章。
26	安全运维管理	（1）单位未严格按规范开展漏洞及安全隐患检测工作。	制度文件、执行/记录文件	（1）建议单位定期开展漏洞扫描，对发现的安全漏洞和隐患进行及时修补评估； （2）对必需修补的安全漏洞和隐患进行加固测试，测试无误后，备份系统数据，再从生产环境进行修补； （3）对于剩余安全漏洞和隐患进行残余风险分析，明确安全风险整改原则。
27	安全运维管理	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	（1）建议单位按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。包括;定期对相关产品的恶意代码库进行升级；对相关设备升级情况进行记录；对各类防病毒产品上截获的恶意代码进行分析并汇总上报； （2）单位需保留完整的恶意代码检测/升级的记录。至少具备：执行人、升级结果/检测结果、处理方式、负责人签字 。

序号	安全类	安全问题	关联资产	整改建议
28	安全运维管理	(1)单位不了解现有密码相关的国家标准和行业标准；(2)单位缺乏密码管理要求的制度文档。	制度文件、执行/记录文件	（1）建议单位学习现有密码相关的国家标准和行业标准。建立密码管理要求的制度文档。

漏洞安全问题整改建议

序号	安全类	安全问题	关联资产	整改建议
1	安全计算环境	SSH版本信息可被获取 此类漏洞涉及服务器存储设备。	10.1.8.30/应用服务器-1 10.1.8.31/数据库服务器 10.1.8.29/应用服务器-2	NSFOCUS建议您采取以下措施以降低威胁：*修改源代码或者配置文件改变SSH服务的缺省banner。
2	安全计算环境	允许Traceroute探测 此类漏洞涉及网络设备、安全设备、服务器存储设备。	10.1.8.29/应用服务器-2 10.1.8.30/应用服务器-1 10.1.8.31/数据库服务器 10.2.1.4/运维安全管理系统 10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/上网行为管理系统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/汇聚交换机 172.16.1.2/核心交换机	在防火墙出站规则中禁用echo-reply（type 0）、time-exceeded（type 11）、destination-unreachable（type 3）类型的ICMP包。
3	安全计算环境	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)	172.16.1.2/核心交换机	临时解决方法：*在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 厂

序号	安全类	安全问题	关联资产	整改建议
		此类漏洞涉及网络设备。		商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://downloads.ssh.com/ 对于具体Linux发行版中使用的版本，可以参考如下链接,确认系统是否受该漏洞影响: Redhat ------- https://rhn.redhat.com/errata/RHSA-2009-1287.html Suse ------- http://support.novell.com/security/cve/CVE-2008-5161.html Ubuntu ------- http://people.canonical.com/~ubuntu-security/cve/2008/CVE-2008-5161.html
4	安全计算环境	缺少“Content-Security-Policy”响应头 此类漏洞涉及业务应用软件平台。	https://www.mmpt.edu.cn/ 门户网站系统	在服务器中配置Content-Security-Policy响应头为“default-src 'self’”。

【正文结束】

附录A 被测对象资产

A.1 物理机房

附录A 表- 1物理机房

序号	机房名称	物理位置	重要程度
1	信息化机房	茂名市茂南区文明北路232号大院大楼	关键

A.2 网络设备

附录A 表- 2网络设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度	备注
1	汇聚交换机	否	H3C version 7.1.070, Release 6126P20	H3C S5560X-30C-EI	数据交换	重要	
2	核心交换机	否	H3C version 7.1.070, Release 7585P07	H3C S7500E-X	核心数据交换、访问控制	关键	

A.3 安全设备

附录A 表- 3安全设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度	备注
1	日志审计系统	否	深信服LAS 3.0.5	深信服AC-1000-D601-PT	日志审计	重要	
2	基线核查系统	否	深信服V3.0.3	深信服AC-1000-D602-PT	漏洞扫描	重要	
3	上网行为管理系统	否	深信服AC12.0.26	深信服AC-1000-D600-PT	上网行为管理及终端准入控制	重要	
4	防火墙-2	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键	
5	运维安全管理系统	否	深信服V3.0.6	深信服AC-1000-D603-PT	运维审计	重要	
6	WEB应用防火墙	否	深信服AF 8.0.9	深信服WAF-2000-H642	应用防护、入侵防范、病毒防护	重要	
7	防火墙-1	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键	

A.4 服务器

附录A 表-4服务器

序号	设备名称	所属业务应用系统/平台名称	是否虚拟设备	操作系统及版本	数据库管理系统及版本	中间件及版本	重要程度	备注
1	应用服务器-2	门户网站系统	否	CentOS 7.7	/	Tomcat 8.5	关键	
2	数据库服务器	门户网站系统	否	CentOS 6.8	PostgreSQL 9.6.12	Tomcat 8.0.37	关键	
3	应用服务器-1	门户网站系统	否	CentOS 7.7	/	Tomcat 8.5	关键	

A.5 终端设备

附录A 表-5终端设备

序号	设备名称	是否虚拟设备	操作系统/控制软件及版本	用途	重要程度	备注
1	运维及管理终端-2	否	Windows 10（版本21H2（内部版本19044.1889））	运维管理、系统管理	一般	
2	运维及管理终端-1	否	Windows 10（版本20H2（内部版本19044.1889）	运维管理、系统管理	一般	
3	业务终端-2	否	Windows 10（版本20H2（内部版本19044.1889）	业务管理	一般	
4	业务终端-1	否	Windows 10（版本20H2（内部版本19044.1889）	业务管理	一般	

A.6 其他系统或设备

附录A 表-6其他系统或设备

序号	设备名称	是否虚拟设备	操作系统/控制软件及版本	用途	重要程度	备注
/	/	/	/	/	/	/

注释：本次测评对象中不涉及专用移动互联终端等，不开展抽测。

A.7 系统管理软件/平台

附录A 表- 7系统管理软件/平台

序号	系统管理软件/平台名称	所在设备名称	版本	主要功能	重要程度	备注
1	数据库服务器-PostgreSQL	应用/数据库服务器	9.6.12	数据生产、存储	关键	
2	应用服务器-1-Tomcat	应用/数据库服务器	8.5	页面发布	关键	

A.8 业务应用软件/平台

附录A 表- 8业务应用系统/平台

序号	业务应用系统/平台名称	主要功能	业务应用软件及版本	开发厂商	重要程度
1	门户网站系统	门户网站系统是学校对外的信息门户，前台包含学院概况、机构设置、教学在线、学术科研、招生就业、队伍建设、学工在线、团员青年、校友会等栏目。后台包括新增/删除站点，用户管理，数据备份和恢复，安全检测、敏感词检测、运维监控等功能，通过门户网站对外发布学校动态、消息，是学院对外宣传的官方门户。	V6.0	西安博达软件股份有限公司	关键

A.9 数据资源

附录A 表- 9数据资源

序号	数据类别	所属业务应用	安全防护需求	重要程度
1	重要业务数据	门户网站系统	完整性、保密性	关键
2	鉴别数据	门户网站系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性、保密性	关键
3	重要审计数据	门户网站系统（安全管理中心)	完整性	重要
4	重要配置数据	门户网站系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/	完整性	关键

序号	数据类别	所属业务应用	安全防护需求	重要程度
		平台)		

注释：网络设备、安全设备、服务器、终端、系统管理软件/平台和业务应用系统等所涉及的鉴别数据和重要配置数据分别在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。重要审计数据在安全管理中心进行汇总测评证据，包括数据完整性。重要业务数据在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。系统不涉及重要个人信息。

A.10 密码产品

附录A 表- 10密码产品

序号	产品/模块名称	生成厂商	商密型号	密码算法	用途	重要程度
/	/	/	/	/	/	/

注释：本次测评不存在加密机等密码产品。

A.11 安全相关人员

附录A 表- 11安全相关人员

序号	姓名	岗位/角色	联系方式	所属单位
1	吴国华	系统管理员	0668-2920122	茂名职业技术学院
2	杨云	审计管理员	0668-2920122	茂名职业技术学院
3	龙恒	数据管理员	13377766618	茂名职业技术学院
4	吴国华	机房管理员	0668-2920122	茂名职业技术学院
5	龙恒	应用管理员	13377766618	茂名职业技术学院
6	龙恒	网络管理员	13377766618	茂名职业技术学院
7	叶永利	安全管理员	0668-2920122	茂名职业技术学院
8	杨云	资产管理员	0668-2920122	茂名职业技术学院

A.12 安全管理文档

附录A 表- 12安全管理文档

序号	文档名称	主要内容
1	制度类文档-机房安全	关于单位机房安全管理工作制度文档

序号	文档名称	主要内容
	管理制度	
2	制度类文档-人员管理制度	关于单位人员录用、调岗、离岗管理制度文档
3	制度类文档-安全教育和培训制度	关于单位安全培训、安全交流工作制度文档
4	制度类文档-办公环境管理制度	关于单位办公环境管理制度文档
5	制度类文档-恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
6	制度类文档-组织安全结构和人员职责制度	关于单位组织结构、人员安排、人员职责制度文档
7	制度类文档-网络安全管理制度	关于单位网络安全工作管理制度文档
8	制度类文档-服务供应商选择安全管理制度	关于单位安全服务供应商管理规定制度文档
9	制度类文档-应用安全管理规范	关于规定单位应用安全管理要求及规范的制度文档
10	制度类文档-授权和审批管理规定	关于单位授权审批、审批流程规范制度文档
11	制度类文档-应用系统业务用户密码设置规定	关于单位用户密码管理制度文档
12	制度类文档-信息系统恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
13	制度类文档-介质管理制度	关于单位介质安全管理工制度文档
14	制度类文档-信息安全漏洞扫描规范	关于单位安全漏洞工作规范制度文档
15	制度类文档-外部服务人员管理规范	关于单位针对外部人员工作管理规范制度文档
16	制度类文档-主机安全管理规范	关于规定单位主机系统安全管理要求规范，指导业务平台主机的安全配置和维护的制度文档
17	制度类文档-信息安全总体策略	关于单位网络安全方针、策略制度文档
18	制度类文档-数据安全管理规范	关于保障关键数据安全，从数据库本身、数据加密、数据备份恢复三个方面对数据安全进行规范的制度文档
19	制度类文档-变更控制管理制度	关于单位变更流程、控制管理制度文档
20	制度类文档-网络安全管理规范	关于保障单位网络系统的安全稳定运行，抵御内部和外部各种形式的网络攻击或威胁制定的管理文档
21	制度类文档-外部人员访问管理制度	关于单位针对外来人员访问管控制度文档

序号	文档名称	主要内容
22	制度类文档-测试及验收方案	关于单位测试验收方案文档
23	制度类文档-组织安全结构和人员职责制度	关于单位安全结构、人员职责
24	制度类文档-系统交付管理	关于单位交付工作管理制度文档
25	制度类文档-制度制定、发布、评审和修订管理制度	关于单位制度制定、发布、评审和修订等管理文档
26	制度类文档-安全事件报告和处置	关于单位网络安全事件管理、处置、流程等报告制度文档
27	制度类文档-网络安全事件应急预案	关于单位网络安全事件应急处理、流程、培训等管理制度文档
28	制度类文档-外包开发软件管理规定	关于单位外包项目管理工作制度文档
29	制度类文档-工程实施管理制度	关于单位工程实施工作管理制度文档
30	制度类文档-信息系统外包运维管理制度	关于单位外包运维工作管理制度文档
31	制度类文档-设备安全管理制度	关于单位设备安全管理制度文档
32	制度类文档-员工考核管理制度	关于单位人员考核工作管理制度文档
33	制度类文档-备份与恢复管理制度	关于单位数据备份、恢复管理制度文档
34	制度类文档-系统及应用数据备份管理规范	关于单位数据备份、恢复管理制度文档
35	制度类文档-网络安全事件报告制度	关于单位网络安全事件管理报告文档
36	制度类文档-信息安全奖惩办法	关于单位人员奖惩制度文档
37	制度类文档-岗位安排及岗位职责	关于单位岗位职责、岗位安排制度文档
38	制度类文档-安全漏洞管理制度	关于单位安全漏洞管理工作制度文档
39	制度类文档-系统安全管理制度	关于单位系统安全管理、安全服务管理制度文档
40	制度类文档-安全管理组织规范	关于单位组织结构管理规范制度文档
41	制度类文档-办公环境保密管理	关于单位办公环境管理制度文档
42	制度类文档-网络与信息系统安全设计规范	关于单位网络与信息化安全设计制度文档

序号	文档名称	主要内容
43	制度类文档-恶意代码防范管理制度	关于单位恶意代码防范工作制度文档
44	制度类文档-工程测试验收管理	关于单位工程测试工作管理制度文档
45	制度类文档-物理安全管理规范	关于加强单位办公区域及电子计算机机房的管理和设备运行安全，规范办公区域及机房建设，使人员办公高效及机房设备安全、稳定运行的制度文档
46	制度类文档-离岗人员工作交接规范	关于单位离岗交接工作规范制度文档
47	制度类文档-外部接入受控网络访问系统管理规范	关于单位针对外部人员工作接入规范制度文档
48	制度类文档-安全审查和检查管理规范	关于单位安全检查、审查工作规范制度文档
49	操作类文档-设备及系统软件配置和操作手册	关于单位安全设备操作、Linux服务器配置手册、主机运维操作手册、软件操作手册、防火墙配置和操作手册、数据库日常运维操作手册等指导文档
50	操作类文档-软硬件日常维护管理规程	关于单位计算机网络系统使用、管理、信息安全、资源共享有所遵循,规范上网操作流程,提高网络系统安全性的指导文档
51	操作类文档-设备操作规程	关于单位相关设备操作指导文档
52	操作类文档-数据备份策略	关于单位数据备份策略文件
53	记录类文档-评审和修订记录	关于单位变更评审、修订工作记录
54	记录类文档-人员离岗申请表	关于人员离岗申请记录
55	记录类文档-备份工作汇总表	关于单位数据备份工作总结表
56	记录类文档-离场信息资料交接表	关于人员离岗交接工作记录
57	记录类文档-设备出入登记记录表	关于设备进出机房登记工作记录
58	记录类文档-存储介质目录清单	关于备份介质存储工作清单
59	记录类文档-网络信息安全事件记录表	关于单位网络安全事件工作记录
60	记录类文档-备份介质使用记录	关于备份介质使用登记工作记录
61	记录类文档-信息安全检查记录表	关于单位安全检查工作记录
62	记录类文档-访问记录表	关于人员访问工作记录

序号	文档名称	主要内容
63	记录类文档-数据恢复申请表	关于单位数据恢复工作申请表
64	记录类文档-信息管理系统漏洞检查表	关于单位安全漏洞工作检测记录表
65	记录类文档-机房维护日志	关于机房维护工作记录
66	记录类文档-机房巡检记录表	关于单位机房环境巡检记录
67	记录类文档-外部人员访问申请表	关于外来人员访问申请流程工作记录
68	记录类文档-信息安全会议记录	关于单位安全培训、安全交流会议记录
69	记录类文档-机房设备维护记录表	关于设备维护登记工作记录
70	记录类文档-专家论证记录表	关于单位网络方案论证记录
71	记录类文档-通用变更记录表	关于单位变更工作记录
72	记录类文档-机房设备维修记录表	关于单位机房设备维修工作记录
73	记录类文档-信息系统存储介质使用清单	关于备份介质存储使用清单
74	记录类文档-系统交付清单	关于单位交付工作记录
75	记录类文档-收发文登记记录	关于单位文档签发记录
76	记录类文档-关键岗位人员考核记录	关于关键岗位考核工作记录
77	记录类文档-漏洞检测报告	关于单位安全漏洞检测报告文档
78	记录类文档-人员入职考核记录	关于人员录用、考核工作记录
79	记录类文档-人员培训及考核记录表	关于人员培训、考核等工作记录
80	记录类文档-网络配置信息	关于单位配置信息登记工作记录
81	记录类文档-监理审批表	关于单位监理审核工作记录
82	记录类文档-技能培训记录	关于单位系统培训工作、考核工作记录
83	记录类文档-离职员工物品交回登记表	关于人员离岗工物交接工作记录
84	记录类文档-机房出入	关于人员进出机房登记工作记录

序号	文档名称	主要内容
	登记表	
85	记录类文档-设备操作维护记录	关于单位设备维护工作记录
86	记录类文档-应急预案培训记录表	关于单位应急预案培训工作记录
87	记录类文档-安全管理制度评审记录	关于单位制度审计记录
88	记录类文档-外部人员访问记录表	关于外来人员访问登记工作记录
89	记录类文档-安全建设方案评审纪录	关于单位网络与信息化安全设计方案评审工作记录
90	记录类文档-接入受控网络申请表	关于外来人员接入工作记录
91	记录类文档-数据备份记录表	关于单位数据备份工作记录
92	记录类文档-软件交付清单	关于单位交付工作记录
93	记录类文档-重要操作审批表	关于单位审批工作记录
94	记录类文档-设备维修申请表	关于单位设备维护工作申请记录
95	记录类文档-信息系统存储介质销毁申请表	关于备份介质销毁申请工作记录
96	记录类文档-外部会议文件和记录	关于单位外部联系、交流及会议工作记录
97	证据类文档-深信服安全采购合同	关于单位与安全厂家服务采购、产品选择合同文件
98	证据类文档-信息安全事件分析报告表	关于单位安全事件分析报告
99	证据类文档-网络安全等级保护工作小组名单	关于单位网络安全等级保护工作小组人员名单文件
100	证据类文档-资产清单	关于单位信息系统资产清单统计表
101	证据类文档-网络安全系统设计方案	关于单位网络与信息化安全设计方案文档
102	证据类文档-外部联系表	关于单位内部联系及外部联系名单
103	证据类文档-工程项目实施方案	关于单位工程实施方案文档
104	证据类文档-网络安全等级保护测评服务合同	关于单位与安全服务商签定的安全服务合同文件
105	证据类文档-定级备案	关于单位系统定级报告、备案证文件

序号	文档名称	主要内容
106	证据类文档-安全职位人员	关于单位人员岗位安排名单

附录B 上次测评问题整改情况说明

此次为门户网站系统初次等级测评，之前未实施过等级保护测评工作。

附录B 表- 1上次测评问题整改情况

序号	主要安全问题	整改情况	情况说明
/	/	□已整改 □未整改	/

附录C 单项测评结果汇总

C.1 安全物理环境

附录 C 表-1 安全物理环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			物理位置选择	物理访问控制	防盗窃和防破坏	防雷击	防火	防水和防潮	防静电	温湿度控制	电力供应	电磁防护
1	信息化机房	符合	2	0	2	1	1	2	0	1	2	1
		部分符合	0	1	0	0	0	0	0	0	0	0
		不符合	0	0	0	0	1	0	1	0	0	0
		不适用	0	0	0	0	0	0	0	0	0	0

附录 C 表-2 安全物理环境单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.2 安全通信网络

附录 C 表-3 安全通信网络单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求		
			网络架构	通信传输	可信验证
1	安全通信网络	符合	1	1	0
		部分符合	1	0	0
		不符合	0	0	1
		不适用	0	0	0

附录 C 表-4 安全通信网络单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.3 安全区域边界

附录 C 表-5 安全区域边界单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求					
			边界防护	访问控制	入侵防范	恶意代码和垃圾邮件防范	安全审计	可信验证
1	外网边界区域	符合	1	4	1	1	3	0
		部分符合	0	0	0	0	0	0
		不符合	0	0	0	0	0	1
		不适用	0	0	0	0	0	0
2	安全管理区域	符合	1	4	0	0	3	0
		部分符合	0	0	0	1	0	0
		不符合	0	0	1	0	0	1
		不适用	0	0	0	0	0	0
3	服务器存储区域	符合	1	4	1	1	3	0
		部分符合	0	0	0	0	0	0
		不符合	0	0	0	0	0	1
		不适用	0	0	0	0	0	0
4	办公网区域	符合	1	4	0	0	3	0
		部分符合	0	0	0	1	0	0
		不符合	0	0	1	0	0	1
		不适用	0	0	0	0	0	0

附录 C 表-6 安全区域边界单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.4 安全计算环境

C.4.1 网络设备

附录 C 表-7 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	汇聚交换机	符合	3	4	3	4	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	1	0	0	1	1	--
2	核心交换机	符合	3	4	3	4	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	1	0	0	1	1	--

C.4.2 安全设备

附录 C 表-8 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	基线核查系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
2	上网行为管理系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
3	WEB应用防火墙	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
4	防火墙-1	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
5	防火墙-2	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
6	日志	符合	3	4	3	5	0	0	1	1	0	--

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
	审计系统	部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
7	运维安全管理系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--

C.4.3 服务器和终端

附录 C 表-9 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	应用服务器-1	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
2	数据库服务器	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
3	应用服务器-2	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
4	业务终端-2	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
5	业务终端-1	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
		不适用	0	0	0	1	0	0	0	1	0	--
6	运维及管理终端-2	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
7	运维及管理终端-1	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--

C.4.4 系统管理软件/平台

附录 C 表-10 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	应用服务器-1-Tomcat	符合	0	4	3	2	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	3	0	0	3	1	1	0	0	0	--
2	数据库服务器-PostgreSQL	符合	2	4	3	2	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	1	0	0	0	0	0	0	1	0	--
		不适用	0	0	0	3	1	1	0	0	0	--

C.4.5 业务应用系统/平台

附录 C 表-11 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	门户网站系统	符合	3	4	3	3	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	0	0	0	2	1	1	0	0	0	--

C.4.6 数据资源

附录 C 表-12 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	重要业务数据	符合	--	--	--	--	--	--	1	1	0	0
		部分符合	--	--	--	--	--	--	0	0	0	0
		不符合	--	--	--	--	--	--	0	1	0	0
		不适用	--	--	--	--	--	--	0	0	1	2

C.4.7 其他系统或设备

附录 C 表-13 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	--	符合	--	--	--	--	--	--	--	--	--	--
		部分符合	--	--	--	--	--	--	--	--	--	--
		不符合	--	--	--	--	--	--	--	--	--	--
		不适用	--	--	--	--	--	--	--	--	--	--

C.5 安全管理中心

附录 C 表-14 安全管理中心单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求	
			系统管理	审计管理
1	管理中心	符合	1	2
		部分符合	0	0
		不符合	1	0
		不适用	0	0

附录 C 表-15 安全管理中心单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.6 安全管理制度

附录 C 表-16 安全管理制度单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求			
			安全策略	管理制度	制定和发布	评审和修订
1	制度文件、执行/记录文件	符合	1	2	2	1
		部分符合	0	0	0	0
		不符合	0	0	0	0
		不适用	0	0	0	0

C.7 安全管理机构

附录 C 表-17 安全管理机构单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求				
			岗位设置	人员配备	授权和审批	沟通和合作	审核和检查
1	制度文件、执行/记录文件	符合	2	1	2	3	0
		部分符合	0	0	0	0	1
		不符合	0	0	0	0	0
		不适用	0	0	0	0	0

C.8 安全管理人员

附录 C 表-18 安全管理人员单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求			
			人员录用	人员离岗	安全意识教育和培训	外部人员访问管理
1	制度文件、执行/记录文件	符合	2	1	1	2
		部分符合	0	0	0	0
		不符合	0	0	0	1
		不适用	0	0	0	0

C.9 安全建设管理

附录 C 表-19 安全建设管理单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			定级和备案	安全方案设计	产品采购和使用	自行软件开发	外包软件开发	工程实施	测试验收	系统交付	等级测评	服务供应商选择
1	制度文件、执行/记录文件	符合	4	0	2	0	1	2	0	3	3	2
		部分符合	0	0	0	0	0	0	1	0	0	0
		不符合	0	3	0	0	1	0	1	0	0	0
		不适用	0	0	0	2	0	0	0	0	0	0

附录 C 表-20 安全建设管理单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.10 安全运维管理

附录 C 表-21 安全运维管理单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求													
			环境管理	资产管理	介质管理	设备维护管理	漏洞和风险管理	网络和系统安全管理	恶意代码防范管理	配置管理	密码管理	变更管理	备份与恢复管理	安全事件处置	应急预案管理	外包运维管理
1	制度文件、执行/记录文件	符合	3	1	2	2	0	5	2	1	0	1	3	3	2	0
		部分符合	0	0	0	0	0	0	1	0	0	0	0	0	0	0
		不符合	0	0	0	0	1	0	0	0	1	0	0	0	0	0
		不适用	0	0	0	0	0	0	0	0	1	0	0	0	0	2

附录 C 表-22 安全运维管理单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.11 其他安全要求指标

附录 C 表-23 其他指标单项测评结果汇总表

序号	测评对象	符合情况
本报告不涉及		

附录D 单项测评结果记录

D.1 安全物理环境

D.1.1 安全通用要求

D.1.1.1 信息化机房

安全控制点	测评指标	结果结论	符合程度
物理位置选择	a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；	（1）机房和办公场地场所在建筑物具有建筑验收文档，包含对防震、防风和防雨能力的说明； ■机房建设地址为：茂名市茂南区文明北路232号大院大楼 （2）机房和办公场地未出严重的问题。 ■无雨水渗透痕迹 ■无因风导致的较严重尘土 ■无屋顶、墙体、地面等破损开裂	符合
	b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	（1）机房未部署在易发生问题的位置； （2）机房对于空调设备的排水管等部位采取密封防漏处理； （3）机房对于楼板进行了防护措施。	符合
物理访问控制	机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。	（1）制定了《机房安全管理制度》，内容包含机房出入方面的管理规定； （2）对未配置电子门禁系统的出入口指定专人7*24小时负责机房出入，对出入的人员进行身份鉴别和登记，可查出入记录，且出入有专人陪同； （3）机房存在未配置门禁系统的开放出入口。	部分符合
防盗窃和防破坏	a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识；	（1）机房设备或主要部件都固定在机架上； （2）机房内对主要部件已绑定相应不易除去的标签； ■包括网络设备 ■包括安全设备 ■包括服务器 ■包括网络线缆 （3）重要机柜已进行上锁处理。	符合
	b) 应将通信线缆铺设在隐蔽安全处。	（1）通信线缆铺设在下走线槽隐蔽处中； （2）通信线缆设有明显的源目的标识； （3）通信线缆均铺设整齐、规范。	符合
防雷击	应将各类机柜、设施和设备等通过接地系统安全接地。	（1）机房设置专用地线； （2）机房内机柜、设施和设备等进行接地处理； （3）交流电源接地验收检测结果符合要求。	符合
防火	a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭	（1）机房采用经消防检测部门检测合格并在有效期内的（如 七氟丙烷）气体自动灭火设备，火灾自动报警类型为烟感+红外；	符合

安全控制点	测评指标	结果结论	符合程度
	火；	（2）自动消防系统工作状态正常，有定期巡检和维护记录《机房巡检记录表》； （3）建立机房消防的管理制度相关文档《机房安全管理制度》，按管理要求机房无人情况下气体灭火配置为自动模式，进入机房调整为手动模式，机房报警有7*24小时值班人员进行监控。	
	b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。	（1）机房及相关的工作房间和辅助房没有采用具有耐火等级的建筑材料； （2）缺乏机房防火设计文档； （3）缺乏机房防火验收文档。	不符合
防水和防潮	a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	（1）机房不存在雨水渗透、破损等不合规情况； （2）机房不位于建筑的顶层、边缘区域。	符合
	b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。	（1）机房区域范围已部署1台科华品牌（精密）空调，机房内分别配置1组温湿度传感器监控； （2）机房内空调下方已铺设安装好挡水和排水设施； （3）机房墙壁或楼板的管道采取必要的防渗防漏等防水保护措施； （4）机房安装检测设备（如：漏水检测绳）检测地下积水，及时处理机房水蒸气结露和地下积水的转移与渗透； （5）目前防水\防潮检测未发现异常情况，并且有防水防潮的运维记录《机房维护日志》。	符合
防静电	应采用防静电地板或地面并采用必要的接地防静电措施。	（1）对机房内设备（可导电金属线槽）采用了接地静电泄放措施； （2）机房未采用防静电地板或铺设防静电地毯。	不符合
温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。	（1）机房范围已部署1组科华品牌精密空调进行温湿度调节； （2）机房范围已部署空调及加湿机进行温湿度调节； （3）温湿度自动调节设施运作正常，有运行和维护记录《机房维护日志》； （4）机房温度能保持在24摄氏度到28摄氏度之间； （5）机房湿度能保持在40%到65%之间。	符合
电力供应	a）应在机房供电线路上配置稳压器和过电压防护设备；	（1）机房配备了稳压器和过电压防护设备； （2）稳压器和过电压防护设备正常工作； （3）机房具备电力供应安全设计，并在其中标明配备稳压器、过电压防护设备等要求。	符合
	b）应提供短期的备用电力	（1）机房配备了1组科华品牌UPS；	符合

安全控制点	测评指标	结果结论	符合程度
	供应，至少满足设备在断电情况下的正常运行要求。	（2）UPS正常工作，可满足主要设备断电情况下的至少1小时正常运行要求； （3）UPS有定期（至少每年）检查和维护，有运行和维护记录《机房巡检记录表》。	
电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。	（1）通信线缆铺设采用独立的具有电磁屏蔽作用线槽； （2）电源线缆铺设采用独立的具有电磁屏蔽作用线槽； （3）弱电线缆隔离铺设，没有干扰。	符合

D.2 安全通信网络

D.2.1 安全通用要求

D.2.1.1 安全通信网络

安全控制点	测评指标	结果结论	符合程度
网络架构	a）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；	（1）已对网络地址划分，且便于管理和控制； （2）网络地址划分采用核心交换机实现外网边界区域、服务器存储区域等的划分； （3）重要核心网络区域与非重要网络在同一网段； （4）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	部分符合
	b）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	（1）网络内重要网段未部署在网络边界处，且未直接连接外部信息系统； （2）系统通过防火墙对重要网段采取访问控制策略； （3）各安全域（子网）的出口唯一。	符合
通信传输	应采用校验技术保证通信过程中数据的完整性。	（1）网络系统中未涉及完整性保障设备，但在安全计算环境方面网络设备采用SSH协议、安全设备采用HTTPS协议、操作系统采用SSH协议、应用系统采用HTTPS协议来保证通信过程中数据的完整性。	符合
可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对通信设备可信验证方面的安全设计要求； （2）现有的通信设备存在未能实现操作系统到上层应用的信任链的情况，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■通信应用连接过程	不符合

D.3 安全区域边界

D.3.1 安全通用要求

D.3.1.1 办公网区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■办公网区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	符合
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问	符合

安全控制点	测评指标	结果结论	符合程度
		的能力。	
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略,无法检测、防止或限制从内部发起的网络攻击行为。	不符合
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试； （4）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	部分符合
安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备	（1）缺乏对边界设备可信验证方面的安全设	不符合

安全控制点	测评指标	结果结论	符合程度
	的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	

D.3.1.2 外网边界区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■外网边界区域 （2）网络边界处部署了可提供访问控制功能的设备； ■防火墙 ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	符合
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■防火墙 ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址	符合

安全控制点	测评指标	结果结论	符合程度
		■源端口 ■目的端口 ■协议	
	d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制,能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署支持对内部发起的攻击行为进行防范的设备； ■防火墙(带入侵防御模块) ■WEB应用防火墙 （2）现有的防范措施满足相应防护要求； ■所有关键网络边界均有检测措施 ■设备的规则库及时更新 ■检测(模块)符合国家相关产品检测要求 ■其安全策略有效 (3)内部安全防范措施能检测相应攻击行为。 ■端口扫描 ■强力攻击 ■木马后门攻击 ■拒绝服务攻击 ■缓冲区溢出攻击 ■碎片攻击 ■网络蠕虫攻击 ■应用漏洞攻击	符合
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试。	符合
安全审计	a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块)	符合

安全控制点	测评指标	结果结论	符合程度
		■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.3.1.3 安全管理区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■安全管理区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设	符合

安全控制点	测评指标	结果结论	符合程度
		备通过非法无线热点接入内部网络。	
访问控制	a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	不符合
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容	部分符合

安全控制点	测评指标	结果结论	符合程度
		性进行测试； （4）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	
安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.3.1.4 服务器存储区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和	（1）网络存在受保护的边界；	符合

安全控制点	测评指标	结果结论	符合程度
	数据流通过边界设备提供的受控接口进行通信。	■服务器存储区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■WEB应用防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视	（1）网络层部署支持对内部发起的攻击行为	符合

安全控制点	测评指标	结果结论	符合程度
	网络攻击行为。	进行防范的设备； ■WEB应用防火墙 （2）现有的防范措施满足相应防护要求； ■所有关键网络边界均有检测措施 ■设备的规则库及时更新 ■检测(模块)符合国家相关产品检测要求 ■其安全策略有效 （3）内部安全防范措施能检测相应攻击行为。 ■端口扫描 ■强力攻击 ■木马后门攻击 ■拒绝服务攻击 ■缓冲区溢出攻击 ■碎片攻击 ■网络蠕虫攻击 ■应用漏洞攻击	
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■WEB应用防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试。	符合
安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■WEB应用防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c）应对审计记录进行保	（1）网络层部署日志审计系统，统一接收及	符合

安全控制点	测评指标	结果结论	符合程度
	护，定期备份，避免受到未预期的删除、修改或覆盖等。	保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.4 安全计算环境

D.4.1 安全通用要求

D.4.1.1 网络设备

D.4.1.1.1 核心交换机

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括VTY认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的全局密码策略； ■Password control:Enabled ■Password aging:Enabled (180 days) ■Password length:Enabled (8 characters) ■Password composition:Enabled (4 types, 1 characters per type) （6）设备配置加密的super认证。	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备配置合规的全局登录失败处理策略； ■Password control: Enabled ■Maximum login attempts: 5 ■Action for exceeding login attempts: Lock user for 5 minutes	符合

安全控制点	测评指标	结果结论	符合程度
		（2）设备配置合规的操作超时退出措施。 ■VTY配置idle-timeout 15 0	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式。 ■未启用TELNET ■启用SSH	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； ■Information Center: Enabled ■Console: Enabled ■Monitor: Enabled ■Log host: Enabled 10.2.1.2 ■Security log file: Enabled （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间	符合

安全控制点	测评指标	结果结论	符合程度
		■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制； ■对ssh 登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）网络层相关设备不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的交换功能，不具备恶意代码防范模块，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配	（1）网络层设备不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	前得到完全清除。		
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.1.2 汇聚交换机

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括VTY认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的全局密码策略； ■Password control:Enabled ■Password aging:Enabled (180 days) ■Password length:Enabled (8 characters) ■Password composition:Enabled (4 types, 1 characters per type) （6）设备配置加密的super认证。	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备配置合规的全局登录失败处理策略； ■Password control: Enabled ■Maximum login attempts: 5 ■Action for exceeding login attempts: Lock user for 5 minutes （2）设备配置合规的操作超时退出措施。 ■VTY配置idle-timeout 15 0	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式。 ■未启用TELNET ■启用SSH	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令	符合

安全控制点	测评指标	结果结论	符合程度
		■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； ■Information Center: Enabled ■Console: Enabled ■Monitor: Enabled ■Log host: Enabled 10.2.1.2 ■Security log file: Enabled （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效；	符合

安全控制点	测评指标	结果结论	符合程度
		（5）日志及审计记录保存大于6个月。	
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制； ■对ssh 登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）网络层相关设备不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的交换功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要	符合

安全控制点	测评指标	结果结论	符合程度
		的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2 安全设备

D.4.1.2.1 WEB应用防火墙

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有	符合

安全控制点	测评指标	结果结论	符合程度
		唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，	（1）设备开启审计功能，审计进程正常；	符合

安全控制点	测评指标	结果结论	符合程度
	审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请	符合

安全控制点	测评指标	结果结论	符合程度
		表》。	
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.2 上网行为管理系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合

安全控制点	测评指标	结果结论	符合程度
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要	符合

安全控制点	测评指标	结果结论	符合程度
		的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.3 基线核查系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性；	符合

安全控制点	测评指标	结果结论	符合程度
		（4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆	符合

安全控制点	测评指标	结果结论	符合程度
	重要的用户行为和重要安全事件进行审计；	盖所有用户操作审计和记录。	
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成	符合

安全控制点	测评指标	结果结论	符合程度
		高风险的漏洞。	
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的基线核查功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要	不适用

安全控制点	测评指标	结果结论	符合程度
	数据定时批量传送至备用场地。	求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.4 日志审计系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合

安全控制点	测评指标	结果结论	符合程度
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 (2)设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合

安全控制点	测评指标	结果结论	符合程度
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施；	符合

安全控制点	测评指标	结果结论	符合程度
		■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.5 运维安全管理系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合

安全控制点	测评指标	结果结论	符合程度
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期	符合

安全控制点	测评指标	结果结论	符合程度
	他与审计相关的信息；	■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制。 ■对Web登录配置管理地址，限制登录范围	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备	（1）设备不具备相关可信验证的技术措施；	不符合

安全控制点	测评指标	结果结论	符合程度
	的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.6 防火墙-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合

安全控制点	测评指标	结果结论	符合程度
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方	（1）设备通过核心交换机的访问控制策略，	符合

安全控制点	测评指标	结果结论	符合程度
	式或网络地址范围对通过网络进行管理的管理终端进行限制；	通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要	符合

安全控制点	测评指标	结果结论	符合程度
		的完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.7 防火墙-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会	（1）设备启用合规登录失败处理策略； ■启用登录失败策略	符合

安全控制点	测评指标	结果结论	符合程度
	话、限制非法登录次数和当登录连接超时自动退出等相关措施；	■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型	符合

安全控制点	测评指标	结果结论	符合程度
		■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合

安全控制点	测评指标	结果结论	符合程度
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配	（1）网络层设备不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	前得到完全清除。		
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.3 服务器和终端

D.4.1.3.1 应用服务器-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）操作系统不存在空口令用户； ■etc/passwd文件中各用户的第二字段处不为空 ■/etc/shadow文件中各用户密码字段处不为空 （3）操作系统不存在默认信任的登录模式； （4）操作系统为登录用户设置的身份标识具有唯一性； ■UID具有唯一性 ■UID=0只能root用户 （5）操作系统配置的一定的密码长度且定期更换； ■PASS_MAX_DAYS 180 ■PASS_MIN_DAYS 1 ■PASS_MIN_LEN 8 ■PASS_WARN_AGE 28 （6）操作系统配置一定的密码复杂度策略。 ■minlen=8 ■ucredit=-2 ■lcredit=-1 ■dcredit=-4 ■ocredit=-1	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用pam_tally2模块的合规登录失败处理策略； auth required /lib/security/pam_tally.so onerr=fail no_magic_root和 account required /lib/security/pam_tally.so deny=10 no_magic_root reset （2）操作系统配置合规的操作超时锁定； ■配置具备以下措施：	符合

安全控制点	测评指标	结果结论	符合程度
		/etc/profile设置TMOUT=300 （3）操作系统启用SSH的合规登录超时策略。 ■配置具备以下措施： /sshd_config设置 ClientAliveInterval 60 ClientAliveCountMax 3	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）操作系统配置合规的远程管理模式； ■启用SSH （2）操作系统远程端口使用情况合规； ■21（FTP）未启用 ■23（Telnet）未启用 （3）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在所有用户均属于root组的情况。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统对多余帐户进行删除、锁定或禁止其登录； （2）操作系统账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； （2）操作系统不存在除root外的特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计功能，审计进程正常； ■rsyslog：loaded ■auditctl：enabled=1 （2）操作系统开启审计范围及策略满足要求，审计覆盖所有用户操作审计和记录。 ■rsyslog：*.info;mail.none;news.none;authpriv.none;cron.none /var/log/messages	符合

安全控制点	测评指标	结果结论	符合程度
		■auditctl： 关键目录、文件的审计行为采用 perm=rwxa	
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）操作系统针对日志、审计记录具备充足的存储容量； （3）操作系统采取合规的日志文件权限策略； ■/var/log/messages：640 ■/var/log/secure：640 ■/var/log/audit/audit.log：640 对审计记录进行定期存档备份，其备份策略有效 （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统关闭不必要端口； （2）操作系统禁用不必要服务； （3）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口； （4）漏洞扫描未发现高风险主机端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服edr防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证； ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序 （3）现有的可信验证缺乏以下措施。 ■对可信性破坏报警 ■将可信性验证结果形成审计记录 ■对可信性审计的动态关联感知	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对鉴别数据采取完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）系统在通信传输过程中对重要配置数据采取完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确	符合

安全控制点	测评指标	结果结论	符合程度
		的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为服务器设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统不保存过多终端历史记录。 ■通过echo $HISTSIZE查看history保留数目为30	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）本设备不存在此部分的控制需求，故此项不适用	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）本设备不存在此部分的控制需求，故此项不适用	不适用

D.4.1.3.2 应用服务器-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）操作系统不存在空口令用户； ■etc/passwd文件中各用户的第二字段处不为空 ■/etc/shadow文件中各用户密码字段处不为空 （3）操作系统不存在默认信任的登录模式； （4）操作系统为登录用户设置的身份标识具有唯一性； ■UID具有唯一性 ■UID=0只能root用户 （5）操作系统配置的一定的密码长度且定期更换； ■PASS_MAX_DAYS 180 ■PASS_MIN_DAYS 1 ■PASS_MIN_LEN 8 ■PASS_WARN_AGE 28	符合

安全控制点	测评指标	结果结论	符合程度
		（6）操作系统配置一定的密码复杂度策略。 ■minlen=8 ■ucredit=-2 ■lcredit=-1 ■dcredit=-4 ■ocredit=-1	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用pam_tally2模块的合规登录失败处理策略； auth required /lib/security/pam_tally.so onerr=fail no_magic_root和 account required /lib/security/pam_tally.so deny=10 no_magic_root reset （2）操作系统配置合规的操作超时锁定； ■配置具备以下措施： /etc/profile设置TMOUT=300 （3）操作系统启用SSH的合规登录超时策略。 ■配置具备以下措施： /sshd_config设置 ClientAliveInterval 60 ClientAliveCountMax 3	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）操作系统配置合规的远程管理模式； ■启用SSH （2）操作系统远程端口使用情况合规； ■21（FTP）未启用 ■23（Telnet）未启用 （3）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在所有用户均属于root组的情况。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统对多余帐户进行删除、锁定或禁止其登录； （2）操作系统账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合

安全控制点	测评指标	结果结论	符合程度
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； （2）操作系统不存在除root外的特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计功能，审计进程正常； ■rsyslog：loaded ■auditctl：enabled=1 （2）操作系统开启审计范围及策略满足要求，审计覆盖所有用户操作审计和记录。 ■rsyslog：*.info;mail.none;news.none;authpriv.none;cron.none /var/log/messages ■auditctl： 关键目录、文件的审计行为采用 perm=rwxa	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）操作系统针对日志、审计记录具备充足的存储容量； （3）操作系统采取合规的日志文件权限策略； ■/var/log/messages：640 ■/var/log/secure：640 ■/var/log/audit/audit.log：640 对审计记录进行定期存档备份,其备份策略有效 （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合

安全控制点	测评指标	结果结论	符合程度
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统关闭不必要端口； （2）操作系统禁用不必要服务； （3）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口； （4）漏洞扫描未发现高风险主机端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服edr防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证； ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序 （3）现有的可信验证缺乏以下措施。 ■对可信性破坏报警 ■将可信性验证结果形成审计记录 ■对可信性审计的动态关联感知	不符合
数据完整性	应采用校验技术保证重要	鉴别数据:	符合

安全控制点	测评指标	结果结论	符合程度
	数据在传输过程中的完整性。	（1）系统在通信传输过程中对鉴别数据采取完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）系统在通信传输过程中对重要配置数据采取完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为服务器设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统不保存过多终端历史记录。 ■通过echo $HISTSIZE查看history保留数目为30	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）本设备不存在此部分的控制需求，故此项不适用	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）本设备不存在此部分的控制需求，故此项不适用	不适用

D.4.1.3.3 数据库服务器

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）操作系统不存在空口令用户； ■etc/passwd文件中各用户的第二字段处不为	符合

安全控制点	测评指标	结果结论	符合程度
		空 ■/etc/shadow文件中各用户密码字段处不为空 （3）操作系统不存在默认信任的登录模式； （4）操作系统为登录用户设置的身份标识具有唯一性； ■UID具有唯一性 ■UID=0只能root用户 （5）操作系统配置的一定的密码长度且定期更换； ■PASS_MAX_DAYS 180 ■PASS_MIN_DAYS 1 ■PASS_MIN_LEN 8 ■PASS_WARN_AGE 28 （6）操作系统配置一定的密码复杂度策略。 ■minlen=8 ■ucredit=-2 ■lcredit=-1 ■dcredit=-4 ■ocredit=-1	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用pam_tally2模块的合规登录失败处理策略； auth required /lib/security/pam_tally.so onerr=fail no_magic_root和 account required /lib/security/pam_tally.so deny=10 no_magic_root reset （2）操作系统配置合规的操作超时锁定； ■配置具备以下措施： /etc/profile设置TMOUT=300 （3）操作系统启用SSH的合规登录超时策略。 ■配置具备以下措施： /sshd_config设置 ClientAliveInterval 60 ClientAliveCountMax 3	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）操作系统配置合规的远程管理模式； ■启用SSH （2）操作系统远程端口使用情况合规； ■21（FTP）未启用 ■23（Telnet）未启用 （3）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的	符合

安全控制点	测评指标	结果结论	符合程度
		账户，不存在使用共用账户的情况； （3）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在所有用户均属于root组的情况。	
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统对多余帐户进行删除、锁定或禁止其登录； （2）操作系统账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； （2）操作系统不存在除root外的特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计功能，审计进程正常； ■rsyslog：loaded ■auditctl：enabled=1 （2）操作系统开启审计范围及策略满足要求，审计覆盖所有用户操作审计和记录。 ■rsyslog：*.info;mail.none;news.none;authpriv.none;cron.none /var/log/messages ■auditctl： 关键目录、文件的审计行为采用 perm=rwxa	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）操作系统针对日志、审计记录具备充足的存储容量；	符合

安全控制点	测评指标	结果结论	符合程度
		(3)操作系统采取合规的日志文件权限策略; ■/var/log/messages：640 ■/var/log/secure：640 ■/var/log/audit/audit.log：640 对审计记录进行定期存档备份,其备份策略有效 （4）部署日志审计系统实时对日志进行统一收集存储; （5）日志及审计记录保存大于6个月。	
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序;	（1）操作系统仅安装必需的组件; （2）操作系统仅安装必需的应用程序; （3）操作系统遵循最小安装的原则，仅启用必需的功能软件; （4）漏洞扫描未发现高风险主机漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口;	（1）操作系统关闭不必要端口; （2）操作系统禁用不必要服务; （3）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口; （4）漏洞扫描未发现高风险主机端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制;	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制; （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求;	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已根据需要不定期地对已发布的安全性补丁进行更新; （2）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补; （3）操作系统不存在启用未加控制的高危端口; （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服edr防恶意代码软件; （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能; （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的	符合

安全控制点	测评指标	结果结论	符合程度
		危害。	
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证； ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序 （3）现有的可信验证缺乏以下措施。 ■对可信性破坏报警 ■将可信性验证结果形成审计记录 ■对可信性审计的动态关联感知	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对鉴别数据采取完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）系统在通信传输过程中对重要配置数据采取完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为服务器设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统不保存过多终端历史记录。 ■通过echo $HISTSIZE查看history保留数目	符合

安全控制点	测评指标	结果结论	符合程度
		为30	
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）本设备不存在此部分的控制需求，故此项不适用	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）本设备不存在此部分的控制需求，故此项不适用	不适用

D.4.1.3.4 业务终端-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 (5)用户属性策略未勾选“密码永不过期”。	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的	符合

安全控制点	测评指标	结果结论	符合程度
		账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合

安全控制点	测评指标	结果结论	符合程度
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	(1)操作系统采取对审计记录存储容量如下:运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G; (2) 限制审计文件的访问控制权限，用户不可删除及修改; (3) “管理审核和安全日志”，除审计员、administrators外其他用户无权限; (4) 对审计记录进行定期存档备份，其备份策略有效; (5) 部署日志审计系统实时对日志进行统一收集存储; (6) 日志及审计记录保存6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序;	(1) 操作系统仅安装必需的组件; (2) 操作系统仅安装必需的应用程序; (3) 操作系统遵循最小安装的原则，仅启用必需的功能软件; (4) 漏洞扫描未发现高风险主机漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口;	(1) 操作系统不存在多余的默认共享及其它文件共享; ■如：C$、D$、E$ (2) 操作系统关闭不必要端口; ■如：137，138、139、445、123、1900 (3) 操作系统禁用不必要服务; (4) 操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制;	(1) 安全设备ACL策略有效限制访问本机的IP地址及管理模式; (2) 通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求;	(1) 操作系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	(1) 操作系统已安装最新的SP及后续的hotfix补丁; (2) 补丁安装前进行安全性和兼容性测试; (3) 操作系统不存在启用未加控制的高危端口; (4) 操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软	(1) 操作系统安装深信服EDR防恶意代码软件;	符合

安全控制点	测评指标	结果结论	符合程度
	件，并定期进行升级和更新防恶意代码库。	（2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份；	符合

安全控制点	测评指标	结果结论	符合程度
		（4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.5 业务终端-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏	符合

安全控制点	测评指标	结果结论	符合程度
		幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败	符合

安全控制点	测评指标	结果结论	符合程度
		■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下：运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验	（1）操作系统不存在此部分的控制需求，不	不适用

安全控制点	测评指标	结果结论	符合程度
	功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	适用。	
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施；	符合

安全控制点	测评指标	结果结论	符合程度
		■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.6 运维及管理终端-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措	符合

安全控制点	测评指标	结果结论	符合程度
		施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员	符合

安全控制点	测评指标	结果结论	符合程度
		■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下:运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合

安全控制点	测评指标	结果结论	符合程度
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据	符合

安全控制点	测评指标	结果结论	符合程度
		（2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非	（1）操作系统不存在此部分的控制需求，不	不适用

安全控制点	测评指标	结果结论	符合程度
	法使用用户个人信息。	适用。	

D.4.1.3.7 运维及管理终端-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 (5)用户属性策略未勾选“密码永不过期”。	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合

安全控制点	测评指标	结果结论	符合程度
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	(1)操作系统采取对审计记录存储容量如下:运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G; （2）限制审计文件的访问控制权限，用户不	符合

安全控制点	测评指标	结果结论	符合程度
		可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的	符合

安全控制点	测评指标	结果结论	符合程度
		危害。	
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请	符合

安全控制点	测评指标	结果结论	符合程度
		表》。	
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施： 安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.4 系统管理软件/平台

D.4.1.4.1 应用服务器-1-Tomcat

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）Tomcat中间件关闭web管理控制台，其身份鉴别功能由宿主操作系统实现，不适用。	不适用
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）Tomcat中间件关闭web管理控制台，其身份鉴别功能由宿主操作系统实现，不适用。	不适用
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）Tomcat中间件关闭web管理控制台，其身份鉴别功能由宿主操作系统实现，不适用。	不适用
访问控制	a) 应对登录的用户分配账户和权限；	（1）对应不同的账户均按需分配不同的用户权限，不存在中间件用户均属于管理级别、高权限的情况； （2）中间件配置可降权启动Tomcat的用户； （3）宿主系统针对中间件用户分别赋予相应的管理操作权限。 ■包括审计权限 ■包括操作权限	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）中间件不存在除如:Tomcat、admin、manager、role1等默认账户名； （2）中间件账户口令设置合规。	符合

安全控制点	测评指标	结果结论	符合程度
		■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）中间件不存在多余或过期账户； (2)中间件管理员用户与账户之间一一对应； （3）中间件启用合规的管理用户名配置。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）中间件根据安全策略要求对特权用户及宿主管理用户进行分离； （2）中间件管理不存在多个管理级别高的特权用户； （3）中间件管理按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）中间件开启审计功能，审计进程正常； ■开启Cataline引擎的日志文件 catalina.org.apache.juli.FileHandler.level = FINE ■开启内部代码丢出的日志 localhost.org.apache.juli.FileHandler.level = FINE ■开启manager应用日志 manager.org.apache.juli.FileHandler.level = FINE ■开启控制台输出的日志 java.util.logging.ConsoleHandler.level = FINE ■开启Access访问日志。 server.xml文件配置正常，未被注释标记<!-- -->； （2）系统的日志审计级别满足要求。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）中间件日期、时间正常； （2）中间件审计记录开启审核策略且日志级别正常。 ■日志级别不低于“FINE” ■日志配置pattern值设为common ■日志配置pattern值为自定义格式，至少包含：%h %l %u %t %s	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）中间件限制审计文件的访问控制权限，普通用户不可删除及修改； ■localhost.log 644 ■catalina.log 644 ■host-manager.log 644 ■manager.log 644 （2）宿主系统针对中间件日志、审计记录具备充足的存储容量； ■日志存储在/log/tomcat/目录下	符合

安全控制点	测评指标	结果结论	符合程度
		■日志创建计划为每天/每周/每月 ■不限制最大日志文件大小 （3）对中间件审计记录进行定期存档备份，其备份策略有效； （4）审计记录及日志保存大于6个月。	
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）中间件系统不存在此部分的安装控制需求，不适用。	不适用
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）Tomcat中间件的管理地址限制功能由宿主操作系统实现，故该项不适用。	不适用
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）中间件管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）中间件管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）中间件已根据需要不定期地对已发布的版本进行更新； （2）中间件更新安装前进行安全性和兼容性测试； （3）在系统上线或发生重大变更时测试并安装最新的中间件版本或更新补丁； （4）在不影响业务系统正常运行情况下，对发现的中间件漏洞在确保安全的情况下进行修补； （5）中间件进行扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输 重要配置数据: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份的中间件重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）宿主系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）中间件相关数据的备份周期合理：每天增量一次、每月全备一次； （5）中间件开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）宿主系统具有清除用户鉴别信息的功能； （2）经测试，宿主系统退出后无法访问先前中间件登录过的页面； （3）经测试，宿主系统关闭后无残留的中间件用户鉴别信息。	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用

D.4.1.4.2 数据库服务器-PostgreSQL

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）数据库系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）数据库系统不存在弱口令用户； ■数据库已修改默认管理员口令 ■数据库不存在空口令用户 （3）数据库系统不存在默认信任的登录模式； （4）数据库系统为登录用户设置的身份标识具有唯一性； （5）数据库系统配置合规的密码长度及复杂度策略； （6）数据库系统配置合规的密码有效周期策略。	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）数据库系统存在不合规的系统登录失败处理策略； ■数据库系统未启用失败登录策略 （2）数据库系统存在不合规的登录连接超时及自动退出策略。 ■未配置超时策略	不符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）宿主操作系统配置合规的远程管理模式； ■宿主主机启用了安全的远程管理模式(高密级别的RDP)，且只能通过本地对数据库进行管理 （2）数据库系统禁用远程登录管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）登录数据库系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （2）对应不同的账户均按需分配不同的用户组及对应的权限，不存在多用户均与dba类用户权限一致的情况。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）数据库系统账户口令设置合规； ■数据库系统各用户未使用空口令 ■数据库系统未使用弱口令或与用户名相同的口令 （2）已修改默认帐户的默认口令。	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）数据库系统不存在多余或过期账户； （2）数据库系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）数据库系统根据安全策略要求对特权用户进行分离； （2）数据库系统用户权限合理，非管理员未设置过大权限； （3）数据库系统按最小授权原则分配，不赋	符合

安全控制点	测评指标	结果结论	符合程度
		予一般用户管理员权限,不赋予用户不必要的操作权限。	
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计;	（1）数据库系统开启审计功能，审计进程正常。 ■数据库系统启用日志 ■数据库系统配置文件正确配置日志策略	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息;	（1）数据库宿主系统日期、时间正常; （2）数据库系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括重要用户行为 ■包括系统资源的异常使用情况 ■包括重要系统命令的使用 ■包括重要的安全相关事件	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）数据库系统限制审计文件的访问控制权限，普通用户不可删除及修改; ■数据库系统日志文件安装路径下的log文件everyone用户没有写权限 （2）数据库系统针对日志、审计记录具备充足的存储容量; （3）对审计记录进行定期存档备份; （4）审计记录和日志记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序;	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
	b) 应关闭不需要的系统服务、默认共享和高危端口;	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制;	（1）数据库系统设定有效的终端接入策略，对通过网络进行管理的终端进行限制。 ■数据库系统不允许远程连接到数据库系统 ■配置有效的宿主系统策略控制访问地址	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求;	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）数据库系统已根据需要不定期地对已发布的安全性补丁进行更新; （2）补丁安装前进行安全性和兼容性测试; （3）在系统上线或发生重大变更时测试并安装数据库安全补丁; （4）在不影响业务系统正常运行情况下，对	符合

安全控制点	测评指标	结果结论	符合程度
		发现的数据库系统漏洞在确保安全的情况下进行修补； （5）数据库宿主系统不存在启用未加控制的高危端口； （6）数据库系统进行渗透及扫描未发现存在可造成高风险的漏洞。	
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■宿主主机启用了安全的远程管理模式(高密级别的RDP)，且只能通过本地对数据库进行管理 重要配置数据: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■宿主主机启用了安全的远程管理模式(高密级别的RDP)，且只能通过本地对数据库进行管理	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）数据库系统定义了相关重要数据； ■包括鉴别数据 ■包括重要配置数据 ■包括重要审计数据 （2）单位具备合理的重要数据的备份策略规范； （3）数据库系统定期完全依照备份策略，采	符合

安全控制点	测评指标	结果结论	符合程度
		用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）数据库系统未能提供异地数据备份功能。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）数据库系统不保存终端历史记录； （3）引用产品测试结果，信息删除后可法保证完全清除。	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）系统完全不采集和保存任何形式的用户个人信息。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）数据库完全不采集、保存及使用任何形式的用户个人信息。	不适用

D.4.1.5 业务应用系统/平台

D.4.1.5.1 门户网站系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）系统对各登录模式均启用身份鉴别； ■包括管理后台认证 （2）系统对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）系统登录用户设置的身份标识具有唯一性； （4）系统不存在空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）系统启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）系统配置合规的操作超时退出措施。 ■管理后台配置超时15分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信	（1）应用系统的用户鉴别数据采用SHA-512算法在可控网络环境中传输；	符合

安全控制点	测评指标	结果结论	符合程度
	息在网络传输过程中被窃听。	（2）系统配置合规的远程管理模式。 ■启用HTTPS	
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供系统权限分配表； （2）登录系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需分配不同的用户权限，不存在所有用户均属于管理级别、高权限的情况。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）系统禁用默认账户名； （2）系统账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）系统不存在多余或过期账户； （2）系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）系统不存在多个管理级别高的特权用户； （2）系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）系统开启审计功能，审计进程正常； （2）系统的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）系统日期、时间正常； （2）系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）系统针对日志、审计记录具备充足的存储容量； （3）审计记录及日志保存大于6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）应用软件系统不存在此部分的安装控制需求，不适用。	不适用
	b）应关闭不需要的系统服	（1）应用软件系统不存在此部分的控制需求，	不适用

安全控制点	测评指标	结果结论	符合程度
	务、默认共享和高危端口;	不适用。	
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制;	（1）系统自身设定有效的终端访问策略，通过访问措施进行管理地址的限制。 ■系统管理页面仅能内网登录	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求;	（1）系统具备数据有效性检验功能; ■可校验录入数据 ■可校验文档内容 （2）系统的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）系统已根据需要不定期地对已发布的版本进行更新; （2）在系统上线或发生重大变更时测试并安装最新的版本或更新补丁; （3）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）应用软件系统不存在此部分的控制需求，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）应用软件系统不存在此部分的控制需求，不适用。	不适用
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施; ■包括鉴别数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施; ■包括重要配置数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。	符合

安全控制点	测评指标	结果结论	符合程度
		■使用HTTPS加密协议进行传输	
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）系统具有清除用户鉴别信息的功能； （2）经测试，系统退出后无法访问先前登录过的页面； （3）经测试，系统关闭后无残留的用户鉴别信息。	符合
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）系统完全不采集和保存任何形式的用户个人信息。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）系统完全不采集、保存及使用任何形式的用户个人信息。	不适用

D.4.1.6 数据资源

D.4.1.6.1 重要业务数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	（1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要业务数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份重要数据； ■包括重要业务数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份；	符合

安全控制点	测评指标	结果结论	符合程度
		（4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）该测评项测评对象鉴别数据，已在安全计算环境层面其他对象判定，此项不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）系统完全不采集和保存任何形式的用户个人信息。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）系统完全不采集、保存及使用任何形式的用户个人信息。	不适用

D.4.1.6.2 鉴别数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	应用服务器-1-Tomcat: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输 业务终端-1、业务终端-2、运维及管理终端-1、运维及管理终端-2: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）设备在通信传输过程中对相关数据采取	符合

安全控制点	测评指标	结果结论	符合程度
		完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 门户网站系统: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输 应用服务器-1、应用服务器-2、数据库服务器: （1）系统在通信传输过程中对鉴别数据采取完整性保护措施。 ■使用SSH加密协议进行传输 数据库服务器-PostgreSQL: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■宿主主机启用了安全的远程管理模式(高密级别的RDP)，且只能通过本地对数据库进行管理	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	该测评项在各系统及设备已做判定,数据资源针对鉴别数据不做判定	不适用
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	该测评项在各系统及设备已做判定,数据资源针对鉴别数据不做判定，不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	应用服务器-1-Tomcat: (1)宿主系统具有清除用户鉴别信息的功能； （2）经测试，宿主系统退出后无法访问先前中间件登录过的页面； （3）经测试，宿主系统关闭后无残留的中间件用户鉴别信息。 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）网络层设备不适用。 数据库服务器-PostgreSQL:	符合

安全控制点	测评指标	结果结论	符合程度
		（1）身份鉴别信息释放或清除机制正常且满足要求； （2）数据库系统不保存终端历史记录； （3）引用产品测试结果，信息删除后可法保证完全清除。 业务终端-1、业务终端-2、运维及管理终端-1、运维及管理终端-2: （1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用 应用服务器-1、应用服务器-2、数据库服务器: （1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统不保存过多终端历史记录。 ■通过echo $HISTSIZE查看history保留数目为30 门户网站系统: （1）系统具有清除用户鉴别信息的功能； （2）经测试，系统退出后无法访问先前登录过的页面； （3）经测试，系统关闭后无残留的用户鉴别信息。	
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	鉴别数据不存在此部分的控制需求,故此项不适用	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	鉴别数据不存在此部分的控制需求,故此项不适用	不适用

D.4.1.6.3 重要配置数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	门户网站系统: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输 应用服务器-1-Tomcat: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。	符合

安全控制点	测评指标	结果结论	符合程度
		■站点使用HTTPS加密协议进行传输 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 数据库服务器-PostgreSQL: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■宿主主机启用了安全的远程管理模式(高密级别的RDP)，且只能通过本地对数据库进行管理 业务终端-1、业务终端-2、运维及管理终端-1、运维及管理终端-2: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 应用服务器-1、应用服务器-2、数据库服务器: （1）系统在通信传输过程中对重要配置数据采取完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）设备定义了相关重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规	符合

安全控制点	测评指标	结果结论	符合程度
		范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 应用服务器-1-Tomcat: （1）系统定义了相关需要备份的中间件重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）宿主系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）中间件相关数据的备份周期合理：每天增量一次、每月全备一次； （5）中间件开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 业务终端-1、业务终端-2、应用服务器-1、应用服务器-2、数据库服务器、运维及管理终端-1、运维及管理终端-2: （1）操作系统定义了相关重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 门户网站系统: （1）系统定义了相关需要备份重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次；	

安全控制点	测评指标	结果结论	符合程度
		（5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 数据库服务器-PostgreSQL: （1）数据库系统定义了相关重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）数据库系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、运维安全管理系统、防火墙-1、防火墙-2: （1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 数据库服务器-PostgreSQL: （1）数据库系统未能提供异地数据备份功能。 应用服务器-1-Tomcat、门户网站系统: （1）单位未能提供异地数据备份措施。 业务终端-1、业务终端-2、运维及管理终端-1、运维及管理终端-2: （1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 应用服务器-1、应用服务器-2、数据库服务器: （1）设备为服务器设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 核心交换机、汇聚交换机: （1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要	不符合

安全控制点	测评指标	结果结论	符合程度
		求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	重要配置数据不存在此部分的控制需求,故此项不适用	不适用
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	重要配置数据不存在此部分的控制需求,故此项不适用	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	重要配置数据不存在此部分的控制需求,故此项不适用	不适用

D.4.1.7 其他系统或设备

无

D.5 安全管理中心

D.5.1 安全通用要求

D.5.1.1 管理中心

安全控制点	测评指标	结果结论	符合程度
系统管理	a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；	（1）网络中部署运维安全管理系统实现集中的系统管理； （2）系统对登录用户进行身份鉴别； ■包括合规的用户名 ■包括合规的口令策略 （3）系统用户标识具有唯一性； ■不存在多人共享 ■增加、删除用户或权限变更需经过审批 （4）系统可实现对账户的身份鉴别数据进行保密性和完整性保护； （5）系统管理操作模式具备控制措施； ■只允许系统管理员登录 ■具备特定的登录命令 ■具备特定的登录操作界面 （6）系统具备相应的管理操作审计措施。 ■可实现对系统管理操作进行审计 ■审计范围覆盖所有用户 ■操作审计不可被删除	符合
	b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。	（1）系统管理员对系统的资源和运行进行配置、控制和管理； ■包括用户身份管理 ■包括资源配置管理 ■包括系统加载和启动管理 ■包括系统运行的异常处理管理 ■包括数据和设备的备份与恢复管理	不符合

安全控制点	测评指标	结果结论	符合程度
		（2）系统的资源、运行及配置管理不够全面。 ■缺乏可信证书管理 ■缺乏可信基准库管理	
审计管理	a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；	（1）网络中部署运维安全管理系统实现集中安全审计功能； （2）审计系统对审计管理员进行身份鉴别； ■包括合规的用户名 ■包括合规的口令策略 （3）审计系统用户标识具有唯一性； ■不存在多人共享 ■增加、删除用户或权限变更需经过审批 （4）审计系统管理操作模式具备控制措施； ■只允许审计管理员登录 ■具备特定的登录命令 ■具备特定的登录操作界面 （5）审计系统具备相应的管理操作审计措施。 ■可实现对安全审计操作进行审计 ■审计范围覆盖所有审计管理用户 ■操作审计不可被删除	符合
	b）应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	门户网站系统: （1）审计管理员定期对审计记录进行分析，对发现的安全可疑事件及时处理； （2）单位具有安全审计策略文件，规范审计记录的存储、管理和查询要求； （3）审计管理员按规范要求对审计记录进行管理。 ■审计记录不可随意删除/修改 ■定期备份、存储审计记录 ■审计记录存储周期满足6个月要求 重要审计数据: 日志审计系统、运维安全管理系统: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要审计数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■网络设备、安全设备使用rsyslog协议进行传输 ■Linux操作系统使用rsyslog协议进行传输 ■Windows操作系统使用插件+SSL协议进行传输	符合

D.6 安全管理制度

D.6.1 安全通用要求

D.6.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。	（1）单位具有网络安全工作的总体方针和安全策略文件； ■具备独立的网络安全总体方针文件 ■具备涵盖网络安全总体方针策略要求的相关管理文件 ■具备安全策略文件 （2）制度内容包括明确的单位安全工作要求； ■安全目标 ■安全范围 ■安全原则 ■安全框架 ■各类安全策略 （3）管理文件详见《信息安全总体策略》。	符合
管理制度	a）应对安全管理活动中的主要管理内容建立安全管理制度；	（1）单位有针对安全管理活动中的各类管理内容建立安全管理制度； （2）现有制度已覆盖管理活动的主要的方面； ■具备文件控制管理 ■具备安全检查管理 ■具备人力资源及培训 ■具备设备管理 ■具备软件开发/外包开发项目管理 ■具备机房安全管理 ■具备信息分类及管理 ■具备网络安全管理 ■具备系统安全管理 ■具备恶意代码管理 ■具备变更控制 ■具备备份及介质管理 ■具备事件管理 ■具备应急预案 （3）制度详见：《信息安全总体策略》、《网络安全管理规范》、《组织安全结构和人员职责制度》、《人员管理制度》、《员工考核管理制度》。	符合
	b）应对管理人员或操作人员执行的日常管理操作建立操作规程。	（1）单位针对相关业务日常管理的操作建立规程类管理制度； （2）现有制度已覆盖重要管理方面的系统维护手册和用户操作规程等； ■具备网络/安全管理 ■具备服务器管理 ■具备数据库管理	符合

安全控制点	测评指标	结果结论	符合程度
		■具备机房硬件设施管理 ■具备业务应用管理 （3）管理文件详见《设备及系统软件配置和操作手册》。	
制定和发布	a）应指定或授权专门的部门或人员负责安全管理制度的制定；	（1）单位针对安全管理制度的制定，指定教育信息与网络中心部主要负责； （2）在已制定的相关制度中可查阅到被授权制定管理制度的部门/人员信息； （3）管理文件详见《安全管理组织规范》。	符合
	b）安全管理制度应通过正式、有效的方式发布，并进行版本控制。	（1）单位针对制度的制定和发布要求，制定管理规范文件； （2）管理规范文件对文件制定及发布定义了规范要求； ■包括安全管理制度的制定和发布程序 ■包括格式要求 ■包括版本编号要求 （3）安全管理制度的收发登记记录有效； ■具备通过正式、有效的方式收发 ■具备正式发文 ■具备领导签署、单位盖章等 （4）管理文件详见《制度制定、发布、评审和修订管理制度》、《收发文登记记录》。	符合
评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	（1）单位针对制度的合理性和适用性需进行论证和审定及修订的要求，制定管理规范文件； （2）管理规范文件对制度的评审及修订定义了规范要求； （3）单位具有安全管理制度的审定或论证的过程记录； （4）单位对做过修订的制度，具备有修订版本的安全管理过程记录； （5）管理文件详见《制度制定、发布、评审和修订管理制度》及 《安全管理制度评审记录》。	符合

D.7 安全管理机构

D.7.1 安全通用要求

D.7.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
岗位设置	a）应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面	（1）单位已明确网络安全管理工作的职能部门，并明确了各岗位职责； ■已设置机房管理员	符合

安全控制点	测评指标	结果结论	符合程度
	的负责人岗位，并定义各负责人的职责；	■已设置网络管理员 ■已设置安全管理员 （2）单位各部门职责文档已明确网络安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备网络安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	
	b）应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。	（1）单位已明确系统安全管理工作的职能部门，并明确了各岗位职责； ■已设置系统管理员 ■已设置数据管理员 ■已设置审计管理员 ■已设置应用管理员 （2）单位各部门职责文档已明确系统安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备系统安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	符合
人员配备	应配备一定数量的系统管理员、审计管理员和安全管理员等。	（1）单位针对人员配备要求，制定了管理制度； （2）单位按要求配备一定数量的重要岗位管理人员； （3）单位针对各岗位人员，制定并维护人员档案； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	符合
授权和审批	a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；	（1）单位在制度中用文字描述或在流程图中明确，对关键活动进行审批； ■具备部门职责文档明确各部门审批事项 ■具备岗位职责文档明确各岗位审批事项 （2）单位对审批过程明确审批权限，对各项信息系统的重要操作与变更明确审批部门和批准人； （3）管理文件详见《授权和审批管理规定》。	符合
	b）应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。	（1）单位针对各项业务操作及变更等建立了审批程序规定； ■包括系统变更 ■包括重要操作 ■包括物理访问 ■包括系统接入 （2）单位针对系统变更、系统接入、物理范	符合

安全控制点	测评指标	结果结论	符合程度
		围等事项已明确按审批程序执行,记录有批准人签字; （3）管理文件详见《授权和审批管理规定》。	
沟通和合作	a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题;	（1）单位针对机构内部管理人员之间、部门之间的沟通与合作，制定了管理制度; （2）单位的管理制度规范了合作和沟通的方式和周期; （3）单位有组织机构内部人员联系表; （4）单位有定期召开信息安全会议，保存有会议纪要; （5）管理文件详见《安全教育和培训制度》、《技能培训记录》《外部联系表》。	符合
	b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通;	（1）单位针对加强与外部单位的合作与沟通,制定了管理制度规定; ■包括公安机关 ■包括网络安全职能部门 ■包括职能监管机构 ■包括各类供应商 ■包括业界专家 ■包括安全组织 （2）单位能按要求与相关单位保持沟通合作,并提供相关单位联系方式和交流会议纪要; （3）管理文件详见《安全教育和培训制度》、《技能培训记录》、《外部联系表》。	符合
	c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	（1）单位建立了完善的对外联单位的联系列表; ■记录单位名称 ■记录合作内容 ■记录联系人 ■记录联系方式 （2）管理文件详见《外部联系表》。	符合
审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。	（1）单位针对定期开展常规安全检查，制定了管理制度; （2）单位对检查工作的范围、过程、要求等管理的比较完善; ■系统日常运行 ■系统漏洞 ■数据备份 ■包括敏感系统检查人员 （3）单位已按要求由安全管理员定期检查,检查内容需覆盖系统运行相关的管理活动,并能提供安全检查报告; （4）管理文件详见《安全审查和检查管理规	部分符合

安全控制点	测评指标	结果结论	符合程度
		范》； （5）单位开展的检查工作不够完善。 ■未定期检查	

D.8 安全管理人员

D.8.1 安全通用要求

D.8.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
人员录用	a）应指定或授权专门的部门或人员负责人员录用；	（1）单位授权专门的部门负责人员录用工作，制定了管理制度规范； （2）由人力资源保障科负责人员录用工作； （3）管理文件详见《人员管理制度》。	符合
	b）应对被录用人员的身份、安全背景、专业资格或资质等进行审查。	（1）单位针对人员录用过程，制定了明确要求，并形成人员安全管理制度； （2）单位现有管理制度明确说明录用人员应具备的条件； ■包括学历/学位要求 ■包括技术人员的专业技术要求 ■包括管理人员的安全管理要求 （3）单位按规定执行人员录用的相关审查过程； ■包括录用人身份 ■包括安全背景 ■包括专业资格 ■包括资质 （4）管理文件详见《人员管理制度》、《人员入职考核记录》。	符合
人员离岗	应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。	（1）单位针对离岗人员权限终止及取回机构提供的各种设施的要求，制定了管理制度； （2）单位按规范开展对离岗人员的相关管理工作； ■明确负责部门 ■及时终止其访问权限 ■交还身份证件 ■交还软硬件设备 （3）管理文件详见《人员管理度》、《人员离岗申请表》、《离场信息资料交接表》。	符合
安全意识教育和培训	应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。	（1）单位针对人员安全培训及责任和惩戒措施，制定了管理制度； （2）单位已开展安全意识教育及岗位技能培训 ■具备明确培训周期	符合

安全控制点	测评指标	结果结论	符合程度
		■具备有效的培训方式 ■具备清晰的培训内容 ■具备考核要求 （3）管理文件详见《安全教育和培训制度》。	
外部人员访问管理	a）应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；	（1）单位针对外部人员物理访问，制定了外部人员访问管理文档； ■明确允许外部人员访问的范围 ■明确外部人员进入的条件 ■明确外部人员进入的访问控制措施 （2）单位具备有效的外部人员访问重要区域的书面申请文档； ■具有申请人 ■具有申请原因 ■具有范围 ■具有日期 ■具有批准人签字 （3）单位具备外部人员访问重要区域的登记记录； ■记录进入时间、 ■记录离开时间 ■记录访问区域 ■记录陪同人信息 （4）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。	符合
	b）应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；	（1）单位针对外部接入受控网络访问系统，制定了管理制度； （2）单位具备外部人员接入受控网络前的申请审批流程； （3）单位具备外部人员接入及访问系统的书面申请文档； ■具有申请人 ■具有申请原因 ■具有访问权限 ■具有日期 ■具有批准人签字 （4）单位具备外部人员接入及访问系统的登记记录； ■记录访问权限 ■记录访问时限 ■记录账户 （5）管理文件详见《外部人员访问管理制度》、	符合

安全控制点	测评指标	结果结论	符合程度
		《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。	
	c) 外部人员离场后应及时清除其所有的访问权限。	（1）单位针对人员离场后的清理工作，制定了管理制度； （2）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》； （3）单位未完全按管理规范开展人员离场后的清理工作。 ■缺乏清理记录 ■未及时清除离场后的所有访问权限 ■未记录访问权限清除时间	不符合

D.9 安全建设管理

D.9.1 安全通用要求

D.9.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
定级和备案	a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；	（1）单位的被测系统于2022年4月已完成备案； （2）系统备案相关文档（定级报告）中明确等级划分方法和理由，SAG三个方面的级别描述清晰； （3）管理文件详见《定级备案》。	符合
	b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；	（1）单位针对系统定级结果的审批及评审工作等要求，制定了管理制度； （2）现有系统的定级已具备合理性和正确性审定； ■具备单位部门审定 （3）管理文件详见《定级备案》。	符合
	c) 应保证定级结果经过相关部门的批准；	（1）单位针对系统定级结果的上级批准要求，制定了管理制度； （2）现有系统的定级获得了相关部门的批准； （3）管理文件详见《定级备案》。	符合
	d) 应将备案材料报主管部门和相应公安机关备案。	（1）单位对被测系统的等级备案表、定级报告等备案材料已经报相应公安机关备案； （2）单位具备公安机关出具的备案号； （3）管理文件详见《定级备案》。	符合
安全方案设计	a) 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整	（1）单位未具备适用于被测系统的安全规划设计方案； （2）现有方案文档未能完全按照规范要求选	不符合

安全控制点	测评指标	结果结论	符合程度
	安全措施；	择安全措施。 ■缺乏安全保护等级的要求 ■缺乏风险分析结果的要求 ■缺乏实际安全需求	
	b) 应根据保护对象的安全保护等级进行安全方案设计；	（1）单位未具备完整的安全设计方案相关的文档。 ■缺乏总体规划 ■缺乏安全设计方案 ■缺乏相关配套文件 ■缺乏保护对象的安全保护等级要求	不符合
	c) 应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； ■缺乏安全整体规划 ■缺乏安全设计方案 ■缺乏安全配套文件 （2）单位未对相关论证过程及内容进行完整的记录。	不符合
产品采购和使用	a) 应确保网络安全产品采购和使用符合国家的有关规定；	（1）单位已建立安全产品管理的相关管理规定； ■包括采购要求 ■包括使用要求 （2）单位具备安全产品采购流程及相关实施文档； （3）被测系统使用的安全产品具备销售许可资质； （4）安全产品具均为国内产品； （5）管理文件详见《设备安全管理制度》。	符合
	b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。	（1）单位已建立密码产品与服务管理的相关管理制度； ■包括采购要求 ■包括使用要求 （2）系统未使用密码产品； （3）管理文件详见《设备安全管理制度》。	符合
自行软件开发	a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。	不适用
	b) 应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。	不适用
外包软件开发	a) 应在软件交付前检测其中可能存在的恶意代码；	（1）单位针对软件交付前测试恶意代码的要求，制定了管理制度； （2）管理文件详见《外包开发软件管理规定》；	不符合

安全控制点	测评指标	结果结论	符合程度
		（3）单位未在软件交付之前按要求对所有软件开展恶意代码检测。 ■缺乏恶意代码检测报告	
	b）应保证开发单位提供软件设计文档和使用指南。	（1）单位制定软件开发项目验收要求，明确开发单位的提交材料； （2）开发单位提供软件日常维护和使用所需的文档； ■包括需求分析说明书 ■包括软件设计说明书 ■包括软件操作手册 （3）管理文件详见《外包开发软件管理规定》、《设备及系统软件配置和操作手册》。	符合
工程实施	a）应指定或授权专门的部门或人员负责工程实施过程的管理；	（1）单位针对专门的部门负责工程实施过程的管理要求，制定管理度； （2）单位由专岗负责系统建设的工程实施，且按照实施方案的要求对进度和质量进行控制； （3）管理文件详见《工程实施管理制度》。	符合
	b）应制定安全工程实施方案控制工程实施过程。	（1）单位制定了详细的工程实施方案； ■包括工程时间限制 ■包括进度控制 ■包括质量控制 （2）工程实施单位严格按照方案执行，并有过程记录； （3）管理文件详见《测试及验收方案》、《工程项目实施方案》。	符合
测试验收	a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；	（1）单位可提供被测系统的合规测试验收方案； ■包括测试人员 ■包括测试验收内容 ■包括现场操作过程 （2）管理文件详见《测试及验收方案》、《工程项目实施方案》； （3）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。 ■缺乏验收报告 ■缺乏报告审定意见	部分符合
	b）应进行上线前的安全性测试，并出具安全测试报告。	（1）单位对系统上线前需开展安全性测试的要求，制定管理制度； （2）管理文件详见《外包开发软件管理规定》、《系统交付管理》； （3）针对系统上线前的安全性测试工作存在问题。	不符合

安全控制点	测评指标	结果结论	符合程度
		■缺乏测试报告	
系统交付	a) 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；	（1）单位具备系统交付清单； （2）系统交付清单内容较详细； ■包括设备 ■包括软件 ■包括文档 （3）单位的清点工作较合规； ■已依据交付清单开展清点工作 （4）管理文件详见《系统交付管理》、《资产清单》。	符合
	b) 应对负责运行维护的技术人员进行相应的技能培训；	（1）单位已对负责系统运行维护的技术人员进行了技能培训； （2）具备运维人员的培训记录； ■包括培训时间 ■包括培训地点 ■包括培训对象 ■包括培训内容 ■包括培训参与人员签字 （3）管理文件详见《系统交付管理》、《资产清单》、《系统交付清单》、《技能培训记录》。	符合
	c) 应提供建设过程文档和运行维护文档。	（1）单位提供了系统建设过程中的文档； （2）单位提供了指导用户进行系统运维的文档和系统培训手册； （3）管理文件详见《系统交付管理》、《系统交付清单》、《设备及系统软件配置和操作手册》。	符合
等级测评	a) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；	（1）单位针对系统等级测评要求，制定管理制度； （2）系统按要求开展首次测评工作； （3）管理文件详见《系统安全管理制度》。	符合
	b) 应在发生重大变更或级别发生变化时进行等级测评；	（1）管理制度中已规定在系统发生变更时及时对系统进行等级测评； （2）系统未发生过重大变更，系统等级未发生变化； （3）管理文件详见《系统安全管理制度》。	符合
	c) 应确保测评机构的选择符合国家有关规定。	（1）已选择在“全国等级保护测评机构推荐目录”中的测评单位进行等级测评； （2）管理文件详见《系统安全管理制度》、《网络安全等级保护测评服务合同》。	符合
服务供应商选择	a) 应确保服务供应商的选择符合国家的有关规定；	（1）单位在管理制度内明确提出安全服务供应商选择的要求； （2）单位选择的安全服务商符合国家的有关	符合

安全控制点	测评指标	结果结论	符合程度
		规定，具备相应的安全服务资质； （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。	
	b）应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。	（1）单位的管理制度中已规定，需与安全服务商签订安全相关的协议并明确整个服务供应链各方需履行的网络安全相关义务； （2）单位已按规定与选定的安全服务商签订合规的协议； ■明确整个服务供应链各方需履行的网络安全相关义务 ■包括保密范围 ■包括安全责任 ■包括违约责任 ■包括协议的有效期限 ■包括责任人签字 （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。	符合

D.10 安全运维管理

D.10.1 安全通用要求

D.10.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
环境管理	a）应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；	（1）单位建立机房安全方面的管理制度，对有关运维方面的管理作出规定； ■指定教育信息与网络中心部门负责管理 ■包括出入管理要求 ■包括定期维护要求 ■包括空调要求 ■包括供配电设备要求 ■包括消防设施要求 ■包括温湿度控制要求 （2）单位具备完整的机房出入登记记录； ■记录来访人员 ■记录来访时间 ■记录离开时间 ■记录携带物品 （3）单位具备完整的机房基础设施的维护记录； ■记录维护日期 ■记录维护人 ■记录维护设备 ■记录故障原因 ■记录维护结果	符合

安全控制点	测评指标	结果结论	符合程度
		（4）管理文件详见《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。	
	b）应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；	（1）单位建立机房安全方面的管理制度； ■包括物理访问管理 ■包括物品进出管理 ■包括环境安全管理 （2）单位现有机房管理记录与制度相符； ■具备物理访问记录 ■具备物品进出记录 ■具备环境安全相关记录 （3）制度详见：《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。	符合
	c）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	（1）单位机房安全管理制度已明确来访人员的接待区域的要求； （2）单位按规范要求开展人员来访接待； ■划分来访人员的接待区域 ■记录来访人员的情况 （3）单位办公环境未发现有随意放置含有敏感信息介质的情况； ■无纸档文件 ■无移动介质 （4）制度详见：《机房安全管理制度》、《物理安全管理规范》、《办公环境保密管理》。	符合
资产管理	应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。	（1）单位已建立有效的资产清单； （2）单位现有资产清单内容较全面； ■包括设备设施类别 ■包括软件类别 ■包括文档类别 ■包括资产责任人 ■包括所属级别 ■包括所处位置 ■包括所处部门 （3）制度详见：《设备安全管理制度》、《资产清单》。	符合
介质管理	a）应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘	（1）介质按管理要求放置于受控的环境中（如：机房）； （2）介质管理具备较全面的记录； ■包括介质归档 ■包括使用情况	符合

安全控制点	测评指标	结果结论	符合程度
	点；	■包括定期盘点记录 （3）制度详见：《设备安全管理制度》、《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。	
	b）应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。	（1）介质管理制度中对介质安全传输有明确规定； ■包括人员选择 ■包括打包要求 ■包括交付要求 （2）存储重要信息的介质在物理传输过程，具备严格的环节控制，无重大环节疏漏； （3）对介质的归档和查询均具备记录； （4）制度详见：《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。	符合
设备维护管理	a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	（1）单位人员岗位职责相关文档已明确设备维护管理的责任部门； （2）单位对各类设施、设备进行定期维护； （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。	符合
	b）应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。	（1）单位建立了配套设施、软硬件维护管理方面的管理制度； ■包括维护人员的责任 ■包括维修和服务的审批 ■包括维修过程的监督控制 （2）单位开展相关工作与制度相符，且保留记录； ■包括维修和服务审批 ■包括维修过程记录 （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。	符合
漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。	（1）单位制定管理制度，规范对安全漏洞和隐患的检测、识别及评估修补要求； （2）制度详见：《恶意代码防范管理制度》； （3）单位未严格按规范开展漏洞及安全隐患检测工作。 ■未定期开展漏洞扫描	不符合
网络和系统安全管理	a）应划分不同的管理员角色进行网络和系统的运维	（1）单位建立系统安全管理文档，对系统管理员的管理制定了要求；	符合

安全控制点	测评指标	结果结论	符合程度
	管理，明确各个角色的责任和权限；	■包括角色划分 ■包括角色的责任 ■包括角色权限 （2）单位对各类关键角色建立了相应的工作职责文档； ■包括安全管理员 ■包括网络管理员 ■包括系统管理员 ■包括数据管理员 ■包括审计管理员 （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	
	b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	（1）单位制定管理制度，对系统账号进行管理； ■指定专人 ■包括申请账户管理 ■包括建立账户管理 ■包括删除账户管理 （2）单位按管理规范开展账号管理工作； ■具备相关审批流程 ■具备相关审批记录 ■具备管理登记记录 （3）账户管理记录内容较完整； ■包括变更日期 ■包括变更时间 ■包括变更人 ■包括变更设备/系统 ■包括变更结果 （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	符合
	c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	（1）单位建立了网络和系统安全管理制度； （2）网络和系统安全管理制度内容较全面； ■包括安全策略要求 ■包括账户管理 ■包括配置文件的生成及备份 ■包括变更审批管理 ■包括授权访问 ■包括最小服务控制 ■包括升级与打补丁管理 ■包括审计日志管理 ■包括口令管理 （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	符合

安全控制点	测评指标	结果结论	符合程度
	d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；	（1）单位对重要设备、系统的配置和操作建立配置手册； ■包括操作系统 ■包括数据库 ■包括网络设备 ■包括安全设备 ■包括应用和组件 （2）现有操作配置手册已明确操作步骤、参数配置； （3）制度详见：《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。	符合
	e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。	（1）单位制定日常运维管理的相关制度规范； （2）单位按制度规范开展日常运维管理工作； （3）单位具备合规的运维记录； ■包括日常巡检记录 ■包括运行维护记录 ■包括参数的设置记录 ■包括参数的修改记录 （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》、《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。	符合
恶意代码防范管理	a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	（1）单位制定恶意代码防范管理制度，明确对外来计算机或存储设备接入系统前进行恶意代码检查； （2）单位按外来计算机接入恶意代码检查规范开展工作； ■对外来计算机接入进行恶意代码检查 ■具备合规的检测记录 （3）单位制定培训管理制度，明确需通过培训提升员工的防恶意代码意识； （4）单位按培训管理要求开展工作； ■定期对员工开展防恶意代码意识培训 ■具备合规的培训记录 （5）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申请表》、《信息管理系统漏洞检查表》。	符合
	b) 应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；	（1）建立恶意代码防范管理文档； （2）管理制度中覆盖防恶意代码软件的授权使用、恶意代码库升级、定期查杀等内容； （3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》。	符合
	c) 应定期检查恶意代码库	（1）单位指定专门的部门负责定期验证防范	部分符合

安全控制点	测评指标	结果结论	符合程度
	的升级情况，对截获的恶意代码进行及时分析处理。	恶意代码攻击的技术措施的有效性； （2）单位近期未发生过严重的恶意代码攻击事件； （3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申请表》、《信息管理系统漏洞检查表》； （4）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。 ■未定期对相关产品的恶意代码库进行升级 ■未对所有防病毒产品上截获的恶意代码进行分析并汇总上报	
配置管理	应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。	（1）单位制定了基本配置信息管理的制度要求； ■包括网络拓扑结构 ■包括设备安装的软件组件 ■包括软件组件的版本 （2）管理文件详见：《主机安全管理规范》、《网络安全管理规范》、《应用安全管理规范》、《网络配置信息》。	符合
密码管理	a）应遵循密码相关国家标准和行业标准；	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	不符合
	b）应使用国家密码管理主管部门认证核准的密码技术和产品。	（1）单位未采购涉及密码技术的产品，不适用。	不适用
变更管理	应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。	（1）单位建立了关于系统变更管理的制度文件； （2）现有变更管理制度覆盖了变更管理的各方面要求； ■包括变更管理要求 ■包括整体变更管理流程 ■包括变更内容分析与论证 ■包括变更方案审批流程 ■包括变更后通报 （3）制度详见：《变更控制管理制度》、《通用变更记录表》。	符合
备份与恢复管理	a）应识别需要定期备份的重要业务信息、系统数据及软件系统等；	（1）单位根据业务重要程度，制定了需要定期备份的重要业务信息列表或清单。清单内需要定期备份的重要数据已经过用户方确认； （2）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管	符合

安全控制点	测评指标	结果结论	符合程度
		理规范》。	
	b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等；	（1）单位建立了备份与恢复管理相关的安全管理制度； （2）备份与恢复管理的相关要求比较明确； ■规定备份方式 ■规定备份频度 ■规定存储介质 ■规定保存期 （3）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。	符合
	c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	（1）单位现有管理制度，明确了数据备份策略和数据恢复策略，以及备份程序和恢复程序； （2）单位可按策略要求实现重要数据的定期备份与恢复性测试； （3）单位现有的备份的数据均经过恢复性测试，可确保备份的数据可用； （4）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。	符合
安全事件处置	a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件；	（1）单位已在安全培训及宣传过程中告知用户在发现安全弱点和可疑事件时及时向安全管理部门报告； （2）单位在系统运维过程中对发现的安全弱点和可疑事件均编制了对应的报告或相关文档； （3）单位现有安全弱点和可疑事件报告文档内容较详实； （4）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	符合
	b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；	（1）单位制定了安全事件报告和处置管理制度； （2）现有安全事件管理制度内容较完整； ■包括安全事件类型分类 ■包括安全事件有关的工作职责 ■包括安全事件的报告 ■包括安全事件的处置 ■包括安全事件的响应流程 （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	符合

安全控制点	测评指标	结果结论	符合程度
	c) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。	（1）单位具备对安全事件的分析、处理、总结、防范等的报告／过程文档； （2）单位提供的安全事件报告和响应处置记录内容较完整； ■记录引发安全事件的原因 ■记录事件的证据 ■记录处置过程 ■包括经验教训 ■提出补救措施 （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	符合
应急预案管理	a) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；	（1）单位制定重要事件的应急预案； （2）单位现有应急预案涉及的类型范围较全面； ■包括针对机房的预案 ■包括针对网络传输的预案 ■包括针对网络设备的预案 ■包括针对操作系统的预案 ■包括针对数据库的预案 ■包括针对安全漏洞攻击的预案 ■包括针对恶意代码的预案 ■包括针对数据泄露的预案 （3）单位现有应急预案的内容较完整； ■明确重要事件的应急处理流程 ■明确系统恢复流程等内容 （4）制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。	符合
	b) 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。	(1)单位定期对相关人员进行应急预案培训； （2）单位根据不同的应急预案，按要求进行应急演练； （3）单位具备近期应急预案工作开展的相关记录； ■具备培训记录 ■具备演练记录 (4)单位提供的应急预案培训记录比较完整； ■明确培训对象 ■明确培训内容 ■明确培训结果 (5)单位提供的应急预案演练记录比较完整； ■记录演练时间 ■记录主要操作内容 ■记录演练结果 （6）经检查单位目前一旦出现应急事件，可	符合

安全控制点	测评指标	结果结论	符合程度
		参照预案合理有序的进行应急事件处置过程；(7) 制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。	
外包运维管理	a) 应确保外包运维服务商的选择符合国家的有关规定；	(1)单位目前未涉及任何外包运维服务情况，不适用。	不适用
	b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。	(1)单位目前未涉及任何外包运维服务情况，不适用。	不适用

D.11 其他安全要求

本次测评不涉及其他安全要求指标。

附录E 漏洞扫描结果记录

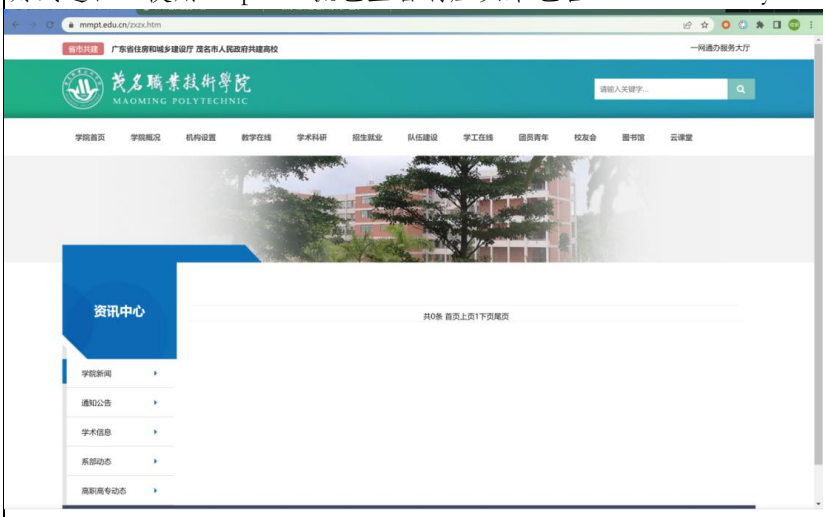
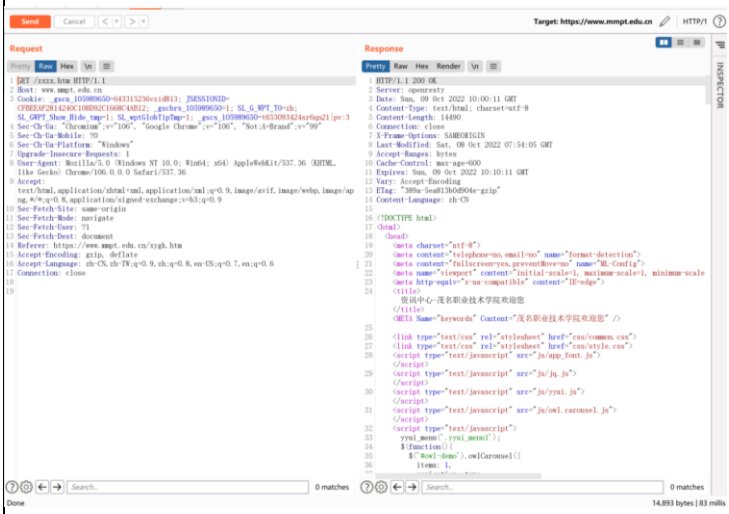
附录E表-1漏洞扫描主要安全漏洞

序号	危险程度	漏洞名称	影响IP
1	低	SSH版本信息可被获取 此类漏洞涉及服务器存储设备。	10.1.8.30/应用服务器-1 10.1.8.31/数据库服务器 10.1.8.29/应用服务器-2
2	低	允许Traceroute探测 此类漏洞涉及网络设备、安全设备、服务器存储设备。	10.1.8.29/应用服务器-2 10.1.8.30/应用服务器-1 10.1.8.31/数据库服务器 10.2.1.4/运维安全管理系统 10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/上网行为管理系统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/汇聚交换机 172.16.1.2/核心交换机
3	低	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161) 此类漏洞涉及网络设备。	172.16.1.2/核心交换机

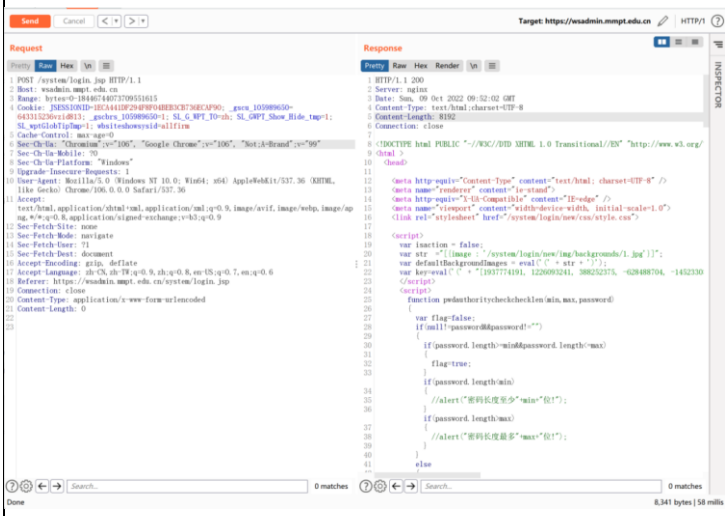
附录F 渗透测试结果记录

F.1 业务应用软件平台 缺少“Content-Security-Policy”响应头

缺少“Content-Security-Policy”响应头	
危险程度	低
渗透位置	JB,JC
影响URL实体	https://www.mmpt.edu.cn/system/resource/js/ajax.js
渗透详情	渗透方法：使用BurpSuite抓包查看响应头未包含Content-Security-Policy字段

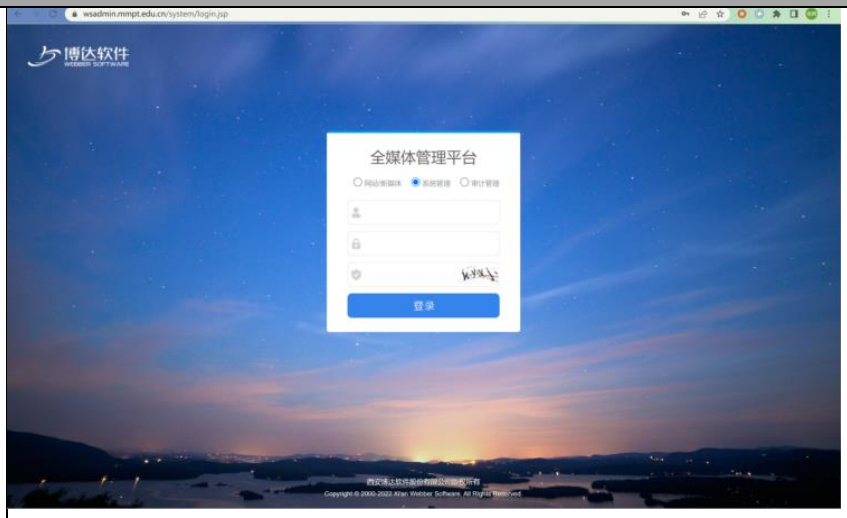
缺少“Content-Security-Policy”响应头	
	采用的工具：BurpSuite 测试过程：使用BurpSuite抓包查看响应头未包含Content-Security-Policy字段  

缺少“Content-Security-Policy”响应头	
危险程度	低
渗透位置	JA,JB,JC
影响URL实体	https://wsadmin.mmpt.edu.cn/system/login.jsp
渗透详情	渗透方法：使用BurpSuite抓包查看响应头未包含Content-Security-Policy字段 采用的工具：BurpSuite 测试过程：使用BurpSuite抓包查看响应头未包含Content-Security-Policy字段

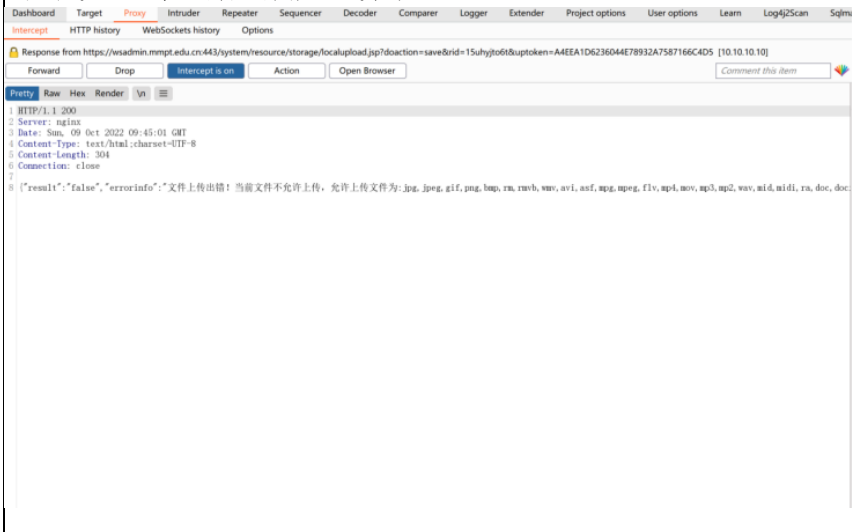
缺少“Content-Security-Policy”响应头
   

F.2 业务应用软件平台　　弱口令漏洞

弱口令漏洞	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：通过手工测试/暴力破解对登录接口测试是否存在弱口令 采用的工具：BurpSuite 测试过程：发现登录模块使用有效的图形验证码。

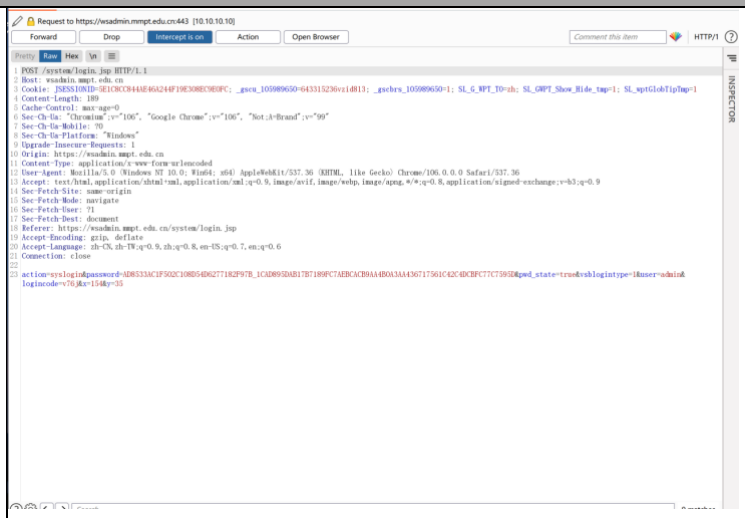
弱口令漏洞	
	

F.3 业务应用软件平台　　任意文件上传

任意文件上传	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：测试能否成功上传含有恶意代码的脚本文件或其他可执行文件 采用的工具：Burp suite 测试过程：对上传文件做了过滤处理 

F.4 业务应用软件平台　　已解密的登录请求

已解密的登录请求	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：测试是否所有登录请求都以加密方式发送到服务器 采用的工具：Burpsuite 测试过程：模拟登录请求，发现口令加密传输。

已解密的登录请求


附录G 威胁列表

附录G 表- 1威胁列表

序号	威胁列表	描述
1	恶意攻击	利用工具和技术对信息系统进行攻击和入侵。威胁行为包括：恶意代码、邮件勒索、网络攻击等。
2	软硬件故障	对业务实施或系统运行产生影响的设备硬件故障、通讯链路中断、系统本身或软件缺陷造等问题。威胁行为包括：设备故障、软件故障等。
3	管理不到位	由于制度缺失、不完善等原因导致安全管理无法落实或者不到位。威胁行为包括：管理不到位、媒体负面报道等。
4	无作为或操作失误	应该执行而没有执行相应的操作，或者无意执行了错误的操作。威胁行为包括：操作失误、维护错误等。
5	敏感信息泄漏	敏感信息泄露给不应了解的他人。威胁行为包括：内部信息泄露、外部信息泄露等。
6	物理环境影响	对信息系统正常运行造成影响的物理环境问题和自然灾害。威胁行为包括：物理损害等。
7	越权或滥用	越权访问本来无权访问的资源，或者滥用自己的权限破坏信息系统。威胁行为包括：未授权的设备使用、权限滥用、权限伪造等。
8	物理攻击	通过物理的接触造成对软件、硬件和数据的破坏。威胁行为包括：设备失效等。
9	篡改	非法修改信息，破坏信息的完整性使系统的安全性降低或信息不可用。威胁行为包括：硬件篡改、数据篡改等。
10	抵赖	否认所做的操作。威胁行为包括：行为否认（抵赖）、媒体负面报道等。

报告编号：44090243008-00004-22-0163-01

网络安全等级保护
招生信息网系统等级测评报告

委托单位：茂名职业技术学院

测评单位：广东南方信息安全研究院

报告时间：2022年10月30日

网络安全等级测评基本信息表

被测对象				
被测对象名称	招生信息网系统		安全保护等级	第二级（S2A2）
备案证明编号	44090243008-00004			
被测单位				
单位名称	茂名职业技术学院			
单位地址	广东省茂名市茂南区文明北路232号大院		邮政编码	525000
联系人	姓名	龙恒	职务/职称	教师
	所属部门	教育信息与网络中心	办公电话	0668-2920122
	移动电话	13377766618	电子邮件	372383968@qq.com
测评单位				
单位名称	广东南方信息安全研究院		机构代码	SC202127130010163
单位地址	广州市科学城彩频路9号B座12楼1202		邮政编码	510663
联系人	姓名	谢若雨	职务/职称	助理
	所属部门	办公室	办公电话	020-32290702
	移动电话	18819149895	电子邮件	office@cybersec-gd.cn
审核批准	编制人	林炳良	编制日期	2022.10.30
	审核人	王东林	审核日期	2022.10.30
	批准人	王东林	批准日期	2022.10.30

声明

本报告是招生信息网系统的等级测评报告。

本报告测评结论的有效性建立在被测评单位提供相关证据的真实性基础之上。

本报告中给出的测评结论仅对被测对象当时的安全状态有效。当测评工作完成后，由于被测对象发生变更而涉及到的系统构成组件（或子系统）本报告不再适用。

本报告中给出的测评结论不能作为对被测对象内部部署的相关系统构成组件（或产品）的测评结论。

在任何情况下，若需引用本报告中的测评结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。

单位名称：广东南方信息安全研究院

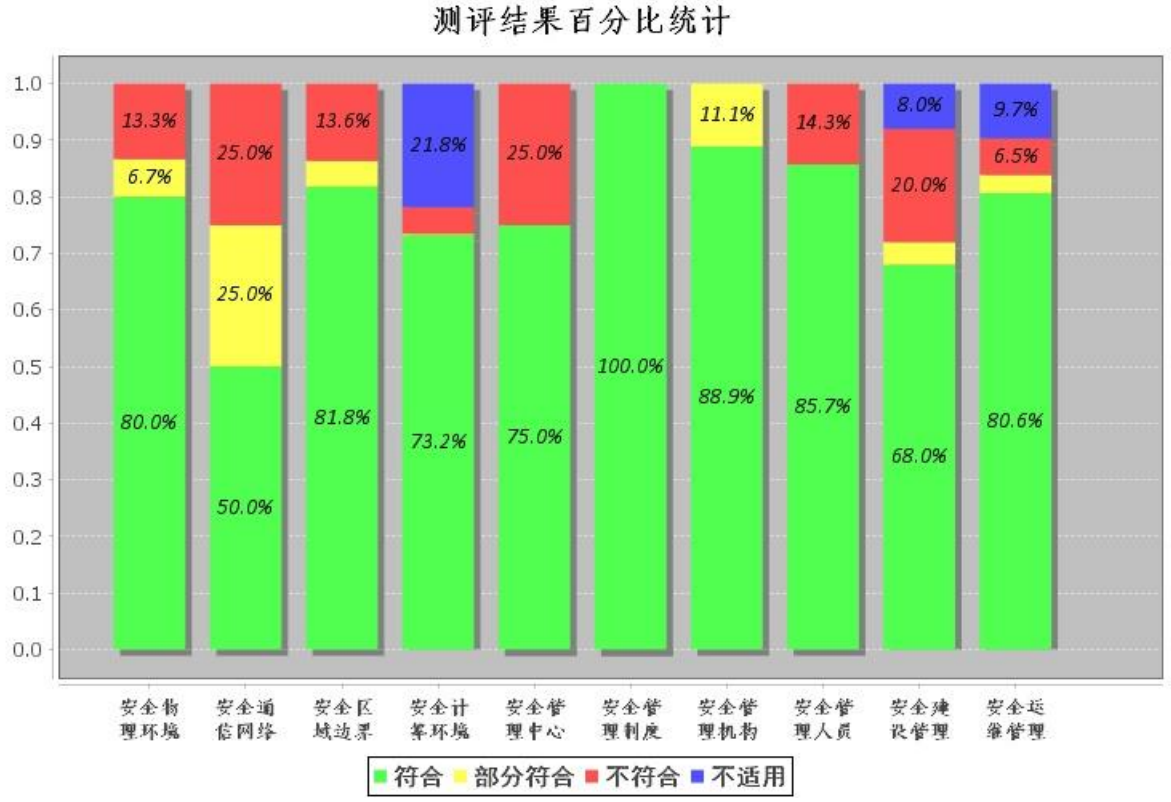
2022年10月30日

等级测评结论

测评结论和综合得分			
被测对象名称	招生信息网系统	安全保护等级	第二级（S2A2）
扩展要求应用情况	□云计算 □移动互联 □物联网 □工业控制系统 □大数据		
被测对象描述	招生信息网系统是由茂名职业技术学院统一组织规划建设，由广东卓锐软件有限公司负责开发，于2019年12月正式投入运行，由教育信息与网络中心负责运行维护。茂名职业技术学院是该信息系统的业务主管部门，茂名职业技术学院为该信息系统定级的责任单位。 招生信息网系统网络主要分为4个区域，分别为外网边界区域、安全管理区域、服务器存储区域、办公网区域，主要由网络设备、安全设备组成，对互联网提供业务访问。招生信息网系统为B/S结构，主要由Linux平台的操作系统，MySQL平台的数据库系统，及nginx中间件系统组成。单位采用自主运维模式，通过部署运维及管理终端提供专用运维环境管理，采用运维安全管理系统实现设备的统一管理，并进行操作运维审计，日志审计系统进行设备日志统一收集存储与分析。 招生信息网系统包括轮播图管理、文档列表管理、专题管理、单页管理、栏目管理、导航管理、内容模型管理、院系专业管理、招生计划、历年录取和自助查询等功能模块，招生信息网为学院提供一个招生信息发布平台，也为有就读意向的学生提供一个了解茂名职业技术学院的平台，通过招生网，为学院和学生建立一个相互了解的通道，同时也为学院的招生工作提供了一个更高效的方式。		
安全状况描述	招生信息网系统通信传输具备一定的保护措施，安全区域边界较清晰，网络层具备访问控制、安全审计的相应技术措施。各设备在访问控制、安全审计、入侵防范方面具备控制措施。重要数据在数据完整性、个人信息保护方面具备保护措施。在安全管理制度层面较为完善。在网络架构不够完整，网络层在入侵防范、恶意代码和垃圾邮件防范的技术措施存在不足。各设备在身份鉴别方面控制措施存在不足。重要数据在数据备份恢复方面存在不足。 招生信息网系统在本次测评中总共出现28类问题，其中0类高风险问题，12类中风险问题，16类低风险问题。在本次测评通过扫描及渗透发现4类漏洞问题，其中0类危险程度为高的漏洞，0类危险程度为中的漏洞，4类危险程度为低的漏洞。 招生信息网系统本次等级测评的综合得分为73.8，且不存在高等级安全风险，等级测评结论为中。		
等级测评结论	中	综合得分	73.8

总体评价

通过对信息系统基本安全保护状态的分析，茂名职业技术学院针对招生信息网系统面临的主要安全威胁采取了相应的安全机制，基本达到保护信息系统重要资产的作用。招生信息网系统在本次测评中采用了GB/T 22239-2019，其中安全通用要求135项，不适用5项。



在安全物理环境方面，针对安全通用要求，基础设施在防雷击、电磁防护、防水和防潮、物理位置选择、电力供应、防盗窃和防破坏、温湿度控制等方面较为完善（如：信息化机房）。在物理访问控制、防静电等方面还不够完善（如：信息化机房），机房出入口未配置电子门禁系统，机房内缺乏防静电措施（如防静电地板或铺设防静电地毯）。

在安全通信网络方面,针对安全通用要求,网络环境在通信传输等方面较为完善(如:安全通信网络)。在网络架构等方面还不够完善（如：安全通信网络），关键的应用服务和数据库服务网段未独立进行子网划分的情况。

在安全区域边界方面，针对安全通用要求，网络环境在边界防护、安全审计、访问控制等方面较为完善（如：外网边界区域，安全管理区域，服务器存储区域等）。在入侵防范、恶意代码和垃圾邮件防范等方面还不够完善(如:安全管理区域,办公网区域)，网络层部署防火墙,防火墙未配置对内部发起的攻击行为实现防范功能策略,无法检测、防止或限制从内部发起的网络攻击行为,现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。

在安全计算环境方面，针对安全通用要求，计算环境在个人信息保护、安全审计、数据完整性、访问控制、入侵防范、恶意代码防范、剩余信息保护等方面较为完善。在主机方面，在可信验证等方面还不够完善（如：业务终端-2，业务终端-1，运维及管理终端-2等），缺乏对计算设备可信验证方面的安全设计要求，现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。在应用方面，在身份鉴别、数据备份恢复等方面还不够完善（如：应用/数据库服务器-MySQL），数据库系统配置不合规的密码有效周期策略,未能提供数据库系统重要数据的异地定时数据备份功能。在网络及安全设备方面，在可信验证等方面还不够完善（如：基线核查系统，上网行为管理系统，WEB应用防火墙等），设备不具备相关可信验证的技术措施。在数据保护方面，在数据备份恢复等方面还不够完善（如：重要个人信息，重要业务数据），未能提供应用软件系统重要数据的异地定时数据备份功能。

在安全管理中心方面，针对安全通用要求，安全控制措施在审计管理等方面较为完善（如：管理中心）。在系统管理等方面还不够完善（如：管理中心），系统管理的资源、运行及配置管理不够全面。

在安全管理制度方面，针对安全通用要求，管理制度体系在制定和发布、安全策略、管理制度、评审和修订等方面较为完善（如：制度文件、执行/记录文件）。

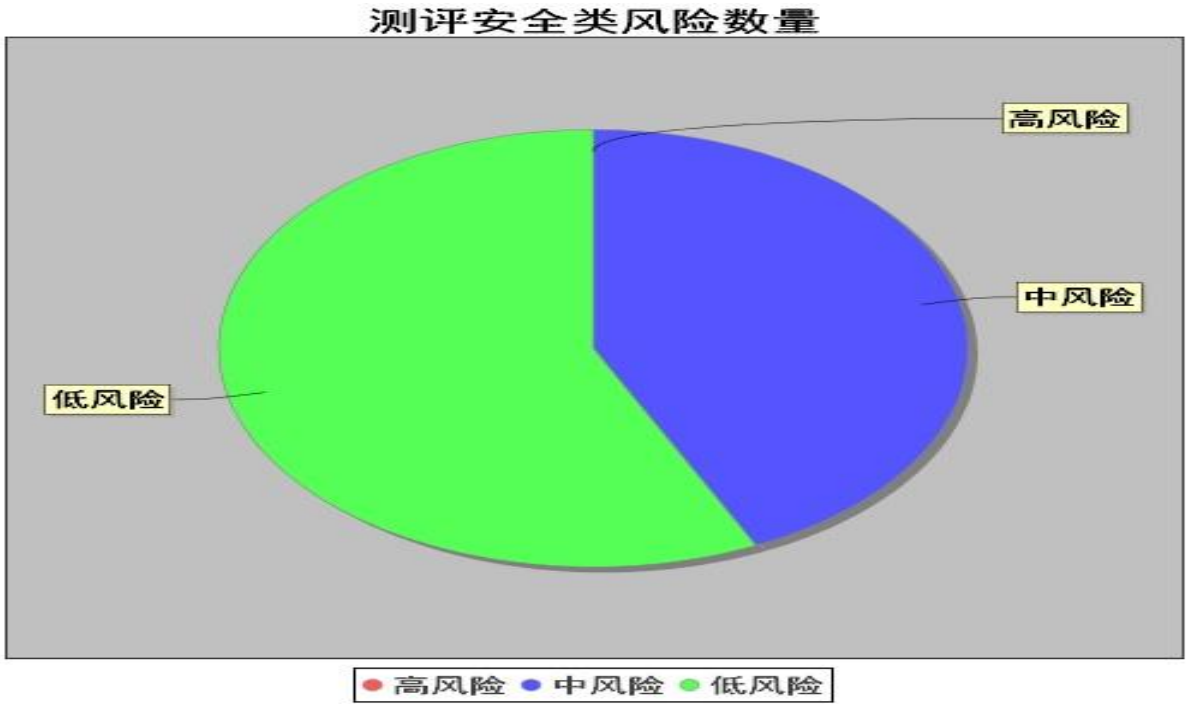
在安全管理机构方面，针对安全通用要求，机构建设在人员配备、沟通和合作、授权和审批、岗位设置等方面较为完善（如：制度文件、执行/记录文件）。在审核和检查等方面还不够完善（如：制度文件、执行/记录文件），单位开展的检查工作不够完善。

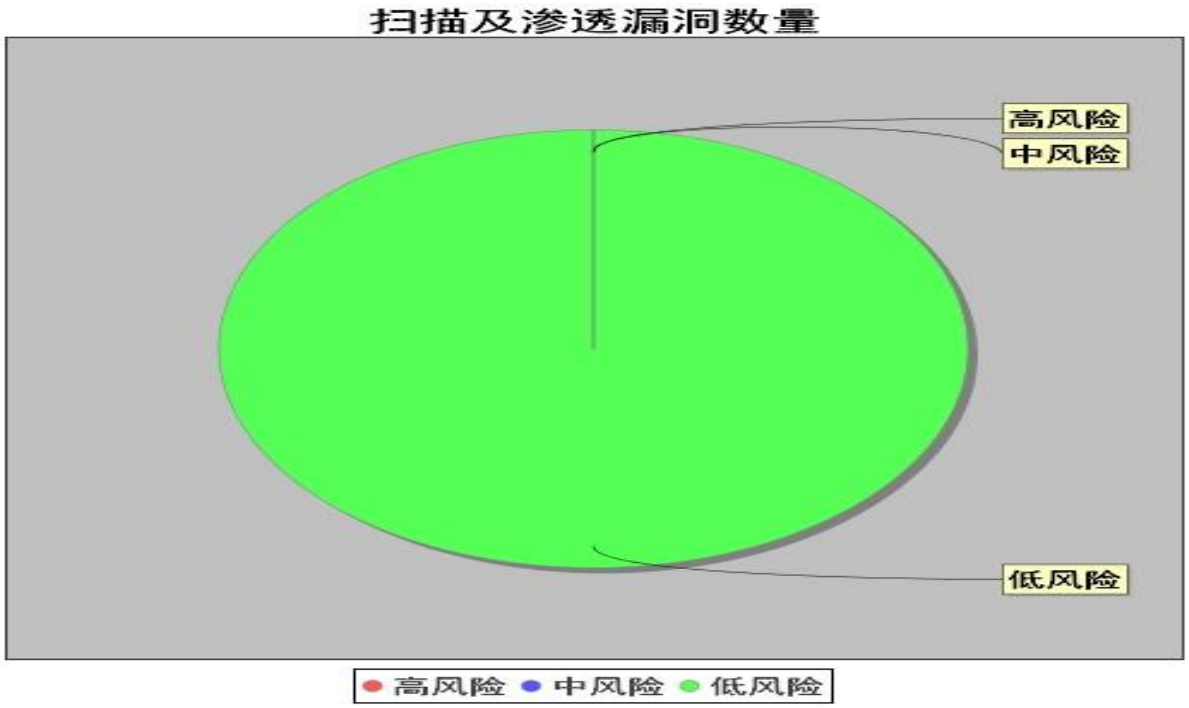
在安全管理人员方面，针对安全通用要求，人员在人员录用、安全意识教育和培训、人员离岗等方面较为完善（如：制度文件、执行/记录文件）。在外部人员访问管理等方面还不够完善（如：制度文件、执行/记录文件），单位未完全按管理规范开展人员离场后的清理工作。

在安全建设管理方面，针对安全通用要求，系统建设在定级和备案、工程实施、等级测评、产品采购和使用、服务供应商选择、系统交付等方面较为完善（如：制度文件、执行/记录文件）。在安全方案设计等方面还不够完善（如：制度文件、执行/记录文件），单位未具备完整的安全设计方案相关的文档，单位相关方案的设计的内容不够完善。

在安全运维管理方面，针对安全通用要求，系统运维在介质管理、设备维护管理、网络和系统安全管理、备份与恢复管理、资产管理、应急预案管理、环境管理、配置管理、安全事件处置、变更管理等方面较为完善（如：制度文件、执行/记录文件）。在密码管理等方面还不够完善（如：制度文件、执行/记录文件），单位不了解现有密码相关的国家标准和行业标准，单位缺乏密码管理要求的制度文档。

招生信息网系统在本次测评中总共出现28类问题，其中0类高风险问题,12类中风险问题，16类低风险问题。在本次测评通过扫描及渗透发现4类漏洞问题，其中0类危险程度为高的漏洞，0类危险程度为中的漏洞，4类危险程度为低的漏洞。





招生信息网系统本次等级测评的综合得分为73.8，且不存在高等级安全风险，等级测评结论为中。

主要安全问题及整改建议

一、安全物理环境

安全通用要求

(1)中风险 机房出入口未配置电子门禁系统（如：信息化机房）。 上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域,可能对系统的平稳运行造成影响。

建议安排专人7*24小时负责机房出入，对出入的人员进行身份鉴别和登记，且出入有专人陪同或在机房出入口配置电子门禁系统，控制、鉴别和记录进入的人员。

(2)中风险 机房内缺乏防静电措施（如防静电地板或铺设防静电地毯 ）（如：信息化机房）。 存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。

建议采用防静电地板或地面并采用必要的接地防静电措施。

二、安全通信网络

安全通用要求

(1)中风险 关键的应用服务和数据库服务网段未独立进行子网划分的情况（如：安全通信网络）。 上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变得更为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。

建议独立划分出应用服务器网段、数据库服务器网段。

三、安全区域边界

安全通用要求

(1)中风险 网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为（如：办公网区域）。 存在不

能及时发现内部主机作为攻击跳板，或网络攻击行为而造成系统损坏/网络资源浪费的风险。

建议网络层部署的防火墙配置对内部发起的攻击行为实现防范功能策略，实现检测、防止或限制从内部发起的网络攻击行为。

(2)中风险 现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面（如：办公网区域）。 无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。

建议现有部署的恶意代码防范措施网络边界覆盖全面，及时对恶意代码及逆行检测和清除。

四、安全计算环境

1、网络设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

2、安全设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

3、服务器和终端

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

4、系统管理软件/平台

安全通用要求

(1)中风险 数据库系统配置不合规的密码有效周期策略（如：应用/数据库服务器

-MySQL）。 上述问题的存在，使恶意用户能够较为容易的访问数据库等资源并实施恶意操作，对相关系统的正常运行造成影响，存在系统被未授权访问、操作的可能性。

建议数据库配置 ‘default_password_lifetime‘；默认密码有效期不为0（具体有效期视业务需求定，一般情况可参考设为90-180天）。

⑵中风险 未能提供数据库系统重要数据的异地定时数据备份功能（如：应用/数据库服务器-MySQL）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供，使企业的经济利益或声誉受到损害。

建议数据库系统利用通信网络将关键数据定时批量传送至备用场地，实现异地数据异地备份。

5、业务应用系统/平台

安全通用要求

⑴中风险 未能提供应用软件系统重要数据的异地定时数据备份功能（如：招生信息网系统）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。

建议利用通信网络将应用软件系统关键数据定时批量传送至备用场地，实现异地数据异地备份。

6、数据资源

安全通用要求

重要业务数据

⑴中风险 未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要业务数据）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。

建议利用通信网络将应用软件系统关键数据定时批量传送至备用场地，实现异地数据异地备份。

重要个人信息

(1)中风险 **未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要个人信息）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。**

建议利用通信网络将应用软件系统关键数据定时批量传送至备用场地，实现异地数据异地备份。

7、其他系统或设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

五、安全管理中心

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

六、安全管理制度

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

七、安全管理机构

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

八、安全管理人员

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

九、安全建设管理

安全通用要求

(1)中风险 **单位未具备完整的安全设计方案相关的文档。单位相关方案的设计的内容不够完善（如：制度文件、执行/记录文件）。 相关合规的规划配套文件缺失，可能导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。**

建议根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件。

十、安全运维管理

安全通用要求

(1)中风险 **单位不了解现有密码相关的国家标准和行业标准。单位缺乏密码管理要求的制度文档（如：制度文件、执行/记录文件）。 密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不到位，存在违反国家政策的风险。**

建议单位学习现有密码相关的国家标准和行业标准。建立密码管理要求的制度文档。

目录

网络安全等级测评基本信息表 I
声明 II
等级测评结论 III
总体评价 IV
主要安全问题及整改建议 VIII
一、安全物理环境 VIII
安全通用要求 VIII
二、安全通信网络 VIII
安全通用要求 VIII
三、安全区域边界 VIII
安全通用要求 VIII
四、安全计算环境 IX
1、网络设备 IX
安全通用要求 IX
2、安全设备 IX
安全通用要求 IX
3、服务器和终端 IX
安全通用要求 IX
4、系统管理软件/平台 IX
安全通用要求 IX
5、业务应用系统/平台 X
安全通用要求 X
6、数据资源 X
安全通用要求 X
7、其他系统或设备 XI
安全通用要求 XI
五、安全管理中心 XI
安全通用要求 XI
六、安全管理制度 XI
安全通用要求 XI
七、安全管理机构 XI
安全通用要求 XI
八、安全管理人员 XI
安全通用要求 XI
九、安全建设管理 XII
安全通用要求 XII
十、安全运维管理 XII
安全通用要求 XII

目录.....XIII
1 测评项目概述.....1
1.1 测评目的.....1
1.2 测评依据.....1
1.3 测评过程.....2
1.4 报告分发范围.....5
2 被测对象描述.....5
2.1 被测对象概述.....5
2.1.1 定级结果.....5
2.1.2 业务和采用的技术.....5
2.1.3 网络结构.....5
2.2 测评指标.....7
2.2.1 安全通用要求指标.....7
2.2.2 安全扩展要求指标.....9
2.2.3 其他安全要求指标.....10
2.2.4 不适用安全要求指标.....10
2.3 测评对象.....10
2.3.1 测评对象选择方法.....10
2.3.2 测评对象选择结果.....11
2.3.2.1 物理机房.....12
2.3.2.2 网络设备.....12
2.3.2.3 安全设备.....12
2.3.2.4 服务器.....13
2.3.2.5 终端设备.....13
2.3.2.6 其他系统或设备.....13
2.3.2.7 系统管理软件/平台.....14
2.3.2.8 业务应用软件/平台.....14
2.3.2.9 数据资源.....15
2.3.2.10 安全相关人员.....15
2.3.2.11 安全管理文档.....16
3 单项测评结果分析.....21
3.1 安全物理环境.....21
3.1.1 已有安全控制措施汇总分析.....21
3.1.2 主要安全问题汇总分析.....23
3.2 安全通信网络.....23
3.2.1 已有安全控制措施汇总分析.....23
3.2.2 主要安全问题汇总分析.....24
3.3 安全区域边界.....24
3.3.1 已有安全控制措施汇总分析.....24
3.3.2 主要安全问题汇总分析.....26
3.4 安全计算环境.....26
3.4.1 网络设备.....26

3.4.1.1 已有安全控制措施汇总分析 26
3.4.1.2 主要安全问题汇总分析 28
3.4.2 安全设备 29
3.4.2.1 已有安全控制措施汇总分析 29
3.4.2.2 主要安全问题汇总分析 32
3.4.3 服务器和终端 32
3.4.3.1 已有安全控制措施汇总分析 33
3.4.3.2 主要安全问题汇总分析 37
3.4.4 系统管理软件/平台 37
3.4.4.1 已有安全控制措施汇总分析 37
3.4.4.2 主要安全问题汇总分析 40
3.4.5 业务应用系统/平台 40
3.4.5.1 已有安全控制措施汇总分析 40
3.4.5.2 主要安全问题汇总分析 42
3.4.6 数据资源 42
3.4.6.1 已有安全控制措施汇总分析 42
3.4.6.2 主要安全问题汇总分析 43
3.4.7 其他系统或设备 44
3.4.7.1 已有安全控制措施汇总分析 44
3.4.7.2 主要安全问题汇总分析 44
3.5 安全管理中心 44
3.5.1 已有安全控制措施汇总分析 44
3.5.2 主要安全问题汇总分析 45
3.6 安全管理制度 45
3.6.1 已有安全控制措施汇总分析 45
3.6.2 主要安全问题汇总分析 46
3.7 安全管理机构 46
3.7.1 已有安全控制措施汇总分析 46
3.7.2 主要安全问题汇总分析 48
3.8 安全管理人员 48
3.8.1 已有安全控制措施汇总分析 48
3.8.2 主要安全问题汇总分析 49
3.9 安全建设管理 49
3.9.1 已有安全控制措施汇总分析 49
3.9.2 主要安全问题汇总分析 52
3.10 安全运维管理 53
3.10.1 已有安全控制措施汇总分析 53
3.10.2 主要安全问题汇总分析 57
3.11 其他安全要求指标 57
3.11.1 已有安全控制措施汇总分析 57
3.11.2 主要安全问题汇总分析 57
3.12 验证测试 57
3.12.1 漏洞扫描 57
3.12.1.1 漏洞扫描结果统计 58

3.12.1.2 漏洞扫描问题描述 62
3.12.2 渗透测试 62
3.12.2.1 渗透测试过程说明 63
3.12.2.2 渗透测试问题描述 64
3.13 单项测评小结 64
3.13.1 控制点符合情况汇总 64
3.13.2 安全问题汇总 68
4 整体测评 72
4.1 安全控制点间安全测评 72
4.1.1 安全建设管理 73
4.1.1.1 安全通用要求 73
4.1.2 安全运维管理 73
4.1.2.1 安全通用要求 73
4.2 区域间安全测评 74
4.2.1 安全物理环境 74
4.2.1.1 安全通用要求 74
4.2.2 安全通信网络 74
4.2.2.1 安全通用要求 74
4.2.3 安全区域边界 74
4.2.3.1 安全通用要求 74
4.2.4 安全计算环境 75
4.2.4.1 安全通用要求 75
4.3 整体测评结果汇总 76
5 安全问题风险分析 77
6 等级测评结论 82
7 安全问题整改建议 84
附录A 被测对象资产 90
A.1 物理机房 90
A.2 网络设备 90
A.3 安全设备 90
A.4 服务器 91
A.5 终端设备 91
A.6 其他系统或设备 91
A.7 系统管理软件/平台 91
A.8 业务应用软件/平台 92
A.9 数据资源 92
A.10 密码产品 93
A.11 安全相关人员 93
A.12 安全管理文档 93
附录B 上次测评问题整改情况说明 99
附录C 单项测评结果汇总 99

C.1 安全物理环境 99
C.2 安全通信网络 99
C.3 安全区域边界 100
C.4 安全计算环境 100
C.4.1 网络设备 100
C.4.2 安全设备 101
C.4.3 服务器和终端 102
C.4.4 系统管理软件/平台 103
C.4.5 业务应用系统/平台 103
C.4.6 数据资源 103
C.4.7 其他系统或设备 104
C.5 安全管理中心 104
C.6 安全管理制度 104
C.7 安全管理机构 105
C.8 安全管理人员 105
C.9 安全建设管理 105
C.10 安全运维管理 106
C.11 其他安全要求指标 106
附录D 单项测评结果记录 107
D.1 安全物理环境 107
D.1.1 安全通用要求 107
D.1.1.1 信息化机房 107
D.2 安全通信网络 109
D.2.1 安全通用要求 109
D.2.1.1 安全通信网络 109
D.3 安全区域边界 109
D.3.1 安全通用要求 109
D.3.1.1 办公网区域 110
D.3.1.2 外网边界区域 112
D.3.1.3 安全管理区域 114
D.3.1.4 服务器存储区域 116
D.4 安全计算环境 119
D.4.1 安全通用要求 119
D.4.1.1 网络设备 119
D.4.1.2 安全设备 126
D.4.1.3 服务器和终端 151
D.4.1.4 系统管理软件/平台 172
D.4.1.5 业务应用系统/平台 179
D.4.1.6 数据资源 183
D.4.1.7 其他系统或设备 190
D.5 安全管理中心 190
D.5.1 安全通用要求 190
D.5.1.1 管理中心 190
D.6 安全管理制度 192

D.6.1 安全通用要求 192
D.6.1.1 制度文件、执行/记录文件 192
D.7 安全管理机构 194
D.7.1 安全通用要求 194
D.7.1.1 制度文件、执行/记录文件 194
D.8 安全管理人员 196
D.8.1 安全通用要求 196
D.8.1.1 制度文件、执行/记录文件 196
D.9 安全建设管理 198
D.9.1 安全通用要求 198
D.9.1.1 制度文件、执行/记录文件 199
D.10 安全运维管理 202
D.10.1 安全通用要求 202
D.10.1.1 制度文件、执行/记录文件 203
D.11 其他安全要求 210
附录E 漏洞扫描结果记录 210
附录F 渗透测试结果记录 211
附录G 威胁列表 214

1 测评项目概述

1.1 测评目的

安全等级测评的目标是通过对目标系统在安全技术及管理方面的测评,对目标系统的安全技术状态及安全管理状况做出初步判断,给出目标系统在安全技术及安全管理方面与其相应安全等级保护要求之间的差距。测评结论作为委托方进一步完善系统安全策略及安全技术防护措施依据。

项目背景是为进一步提高信息系统的保障能力,根据《信息安全等级保护管理办法》（公通字2007【43】号）的精神，茂名职业技术学院委托广东南方信息安全研究院（SC202127130010163）对招生信息网系统实施等级测评，以期发现信息系统和等级保护标准的差距以及存在的安全隐患，为后续的安全整改工作提供参考依据。

1.2 测评依据

测评过程中主要依据的标准:

测评标准

（1）GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》

（2）GB/T 28448-2019 《信息安全技术 网络安全等级保护测评要求》

测评参考标准

（1）GB 17859-1999 《计算机信息系统 安全保护等级划分准则》

（2）GB/T 28449-2018 《信息安全技术 网络安全等级保护测评过程指南》

（3）GB/T 20984-2007 《信息安全技术 信息安全风险评估规范》

（4）GB/T 25058-2019 《信息安全技术 网络安全等级保护实施指南》

测评参考法律法规

（1）《中华人民共和国网络安全法》

（2）《中华人民共和国密码法》

（3）《中华人民共和国数据安全法》

1.3 测评过程

本次等级测评分为四个过程：测评准备活动、方案编制活动、测评实施活动、报告编制活动。具体如图 1-1 所示。其中，各阶段的时间安排如下：

⑴ 测评准备活动

测评准备活动的目标是顺利启动测评项目,收集定级对象相关资料,准备测评所需资料,为编制测评方案打下良好的基础。测评准备活动包括工作启动、信息收集和分析、工具和表单准备三项主要任务。

（2）方案编制活动

方案编制活动的目标是整理测评准备活动中获取的定级对象相关资料,为现场测评活动提供最基本的文档和指导方案。方案编制活动包括测评对象确定、测评指标确定、测评内容确定、工具测试方法确定、测评指导书开发及测评方案编制六项主要任务。

（3）现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调,为现场测评的顺利开展打下良好基础,依据测评方案实施现场测评工作,将测评方案和测评方法等内容具体落实到现场测评活动中。现场测评工作应取得报告编制活动所需的、足够的证据和资料。现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

（4）报告编制活动

在现场测评工作结束后,测评机构应对现场测评获得的测评结果(或称测评证据)进行汇总分析,形成等级测评结论,并编制测评报告。测评人员在初步判定单项测评结果后,还需进行单元测评结果判定、整体测评、系统安全保障评估,经过整体测评后,有的单项

测评结果可能会有所变化,需进一步修订单项测评结果,而后针对安全问题进行风险评估,形成等级测评结论。分析与报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、系统安全保障评估、安全问题风险评估、等级测评结论形成及测评报告编制七项主要任务。

各阶段完成的关键任务：

序号	阶段	任务	对象	开始日期	结束日期
1	测评准备活动	工作启动	项目甲乙双方	2022年8月15日	2022年8月19日
2		信息收集与分析	调研表	2022年8月22日	2022年8月25日
3		工具和表单准备	测评工具、测评授权书、文档交接单	2022年8月25日	2022年8月30日
4	方案编制活动	测评对象确认	测评方案-对象列表	2022年8月31日	2022年8月31日
5		测评指标确认	测评方案-指标列表	2022年8月31日	2022年8月31日
6		测评内容确认	测评方案-内容列表	2022年9月1日	2022年9月1日
7		工具测试方法确认	测评方案-工具测试方法列表	2022年9月1日	2022年9月1日
8		测评指导书开发	测评作业指导书	2022年9月2日	2022年9月2日
9		测评方案编制	测评方案	2022年9月5日	2022年9月5日
10	现场测评活动	现场测评准备	工具、人员、表单准备	2022年9月28日	2022年9月28日
11		现场测评和结果记录	安全管理访谈	2022年9月28日	2022年9月28日
12			安全管理文档检查	2022年9月28日	2022年9月28日
13			安全物理环境测评	2022年9月28日	2022年9月28日
14			安全通信网络	2022年9月28日	2022年9月29日
15			安全区域边界	2022年9月28日	2022年9月29日
16			安全计算环境	2022年9月28日	2022年9月29日
17			工具测试	2022年9月29日	2022年10月9日
18		结果确认和资料归还	检测人员出入场确认单、测评现场服务评价单	2022年10月8日	2022年10月9日
19	报告编制活动	单项测评结果	测评报告	2022年10月9日	2022年10月12日

序号	阶段	任务	对象	开始日期	结束日期
		判定			
20		单元测评结果判定		2022年10月9日	2022年10月17日
21		整体测评		2022年10月9日	2022年10月17日
22		系统安全保障评估		2022年10月9日	2022年10月17日
23		安全问题风险分析		2022年10月9日	2022年10月17日
24		等级测评结论形成		2022年10月17日	2022年10月30日
25		测评报告编制		2022年10月17日	2022年10月30日

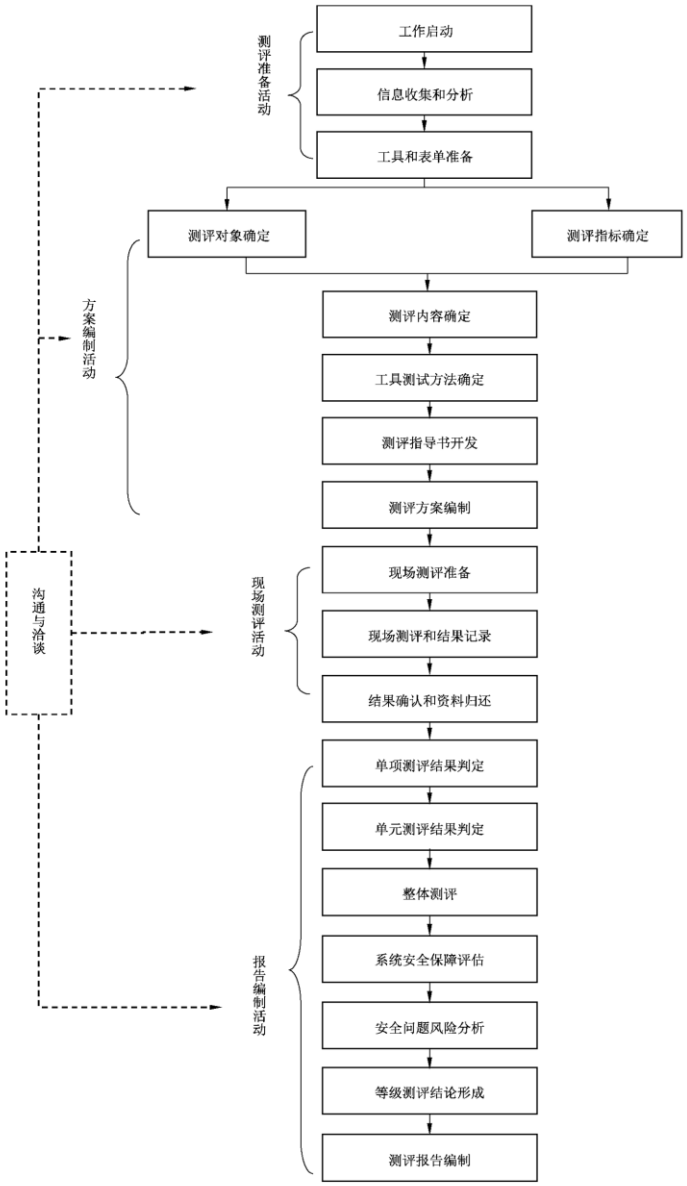


图 1-1 等级保护测评工作流程图

其中，于项目前期召开了项目启动会议，确定了工作方案及项目人员名单；于现场测评完成后召开了项目末次会议，确认了测评发现的问题；于2022年10月30日在对系统的整改情况进行了复核确认后，完成报告编制。

1.4 报告分发范围

等级测评报告正本一式3份，其中茂名职业技术学院1份，广东南方信息安全研究院1份，受理备案的公安机关1份。

2 被测对象描述

2.1 被测对象概述

2.1.1 定级结果

表 2-1定级结果

被测对象名称	安全保护等级	业务信息安全等级	系统服务安全等级
招生信息网系统	2	2	2

2.1.2 业务和采用的技术

招生信息网系统包括轮播图管理、文档列表管理、专题管理、单页管理、栏目管理、导航管理、内容模型管理、院系专业管理、招生计划、历年录取和自助查询等功能模块，招生信息网为学院提供一个招生信息发布平台，也为有就读意向的学生提供一个了解茂名职业技术学院的平台，通过招生网，为学院和学生建立一个相互了解的通道，同时也为学院的招生工作提供了一个更高效的方式。

被测对象未采用云计算/移动互联/物联网/工业控制/大数据等技术情况。

2.1.3 网络结构

招生信息网系统主要是对互联网提供服务，相关设备部署在信息化机房当中,其简要拓扑如下:

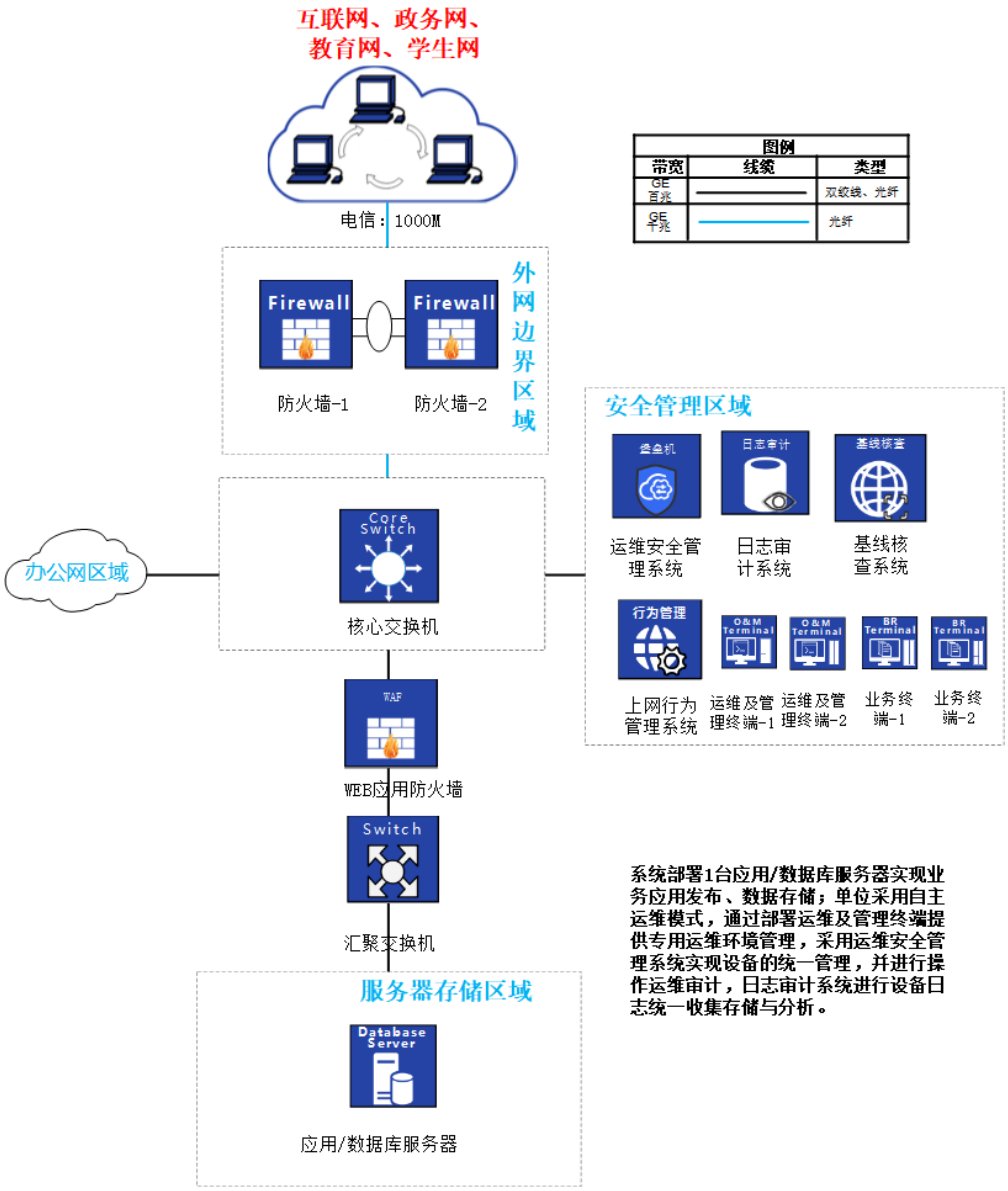


图 2-1 招生信息网系统网络拓扑图

如图2-1招生信息网系统网络拓扑图所示，招生信息网系统网络安全域划分为4个，分别为外网边界区域、安全管理区域、服务器存储区域、办公网区域。

1、外网边界区域：

外网边界区域网络主要包括招生信息网系统的业务服务和信息交换应用，是安全管理区域、服务器存储区域、办公网区域的出口边界；其链路接入为光纤线，带宽为1000mb。通过部署核心交换机、防火墙等设备实施网络访问控制，防火墙（入侵防御模块）实现网络入侵攻击行为防御。

2、办公网区域：

办公网区域网络主要包括招生信息网系统与办公区域的信息交换应用，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、防火墙、上网行为管理系统等设备实施网络访问控制、防火墙（入侵防御模块）实现网络入侵攻击行为防御。

3、安全管理区域：

安全管理区域网络主要包括日志审计系统、运维安全管理系统、上网行为管理系统，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、上网行为管理系统等设备实施网络访问控制。

4、服务器存储区域：

服务器存储区域网络主要包括招生信息网系统的应用服务器、数据库服务器，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、上网行为管理系统等设备实现一定的网络访问控制。

5、服务器部署情况：

招生信息网系统由1台应用/数据库服务器实现应用发布、数据处理、存储、维护。

6、灾备及冗余

招生信息网系统无异地备份机房，未实现异地备份数据定时传输功能。系统重要数据根据需求采用每天增量、每月全备到本地信息化机房。

招生信息网系统未实现冗余措施。

2.2 测评指标

2.2.1 安全通用要求指标

表 2-2 安全通用要求指标

安全类	安全控制点	测评项数
安全物理环境	物理位置选择	2
	物理访问控制	1
	防盗窃和防破坏	2
	防雷击	1
	防火	2
	防水和防潮	2
	防静电	1
	温湿度控制	1
	电力供应	2
	电磁防护	1
安全通信网络	网络架构	2
	通信传输	1
	可信验证	1
安全区域边界	边界防护	1
	访问控制	4
	入侵防范	1
	恶意代码和垃圾邮件防范	1
	安全审计	3
	可信验证	1
安全计算环境	身份鉴别	3
	访问控制	4
	安全审计	3
	入侵防范	5
	恶意代码防范	1
	可信验证	1
	数据完整性	1
	数据备份恢复	2
	剩余信息保护	1
	个人信息保护	2
安全管理中心	系统管理	2
	审计管理	2
安全管理制度	安全策略	1
	管理制度	2
	制定和发布	2
	评审和修订	1
安全管理机构	岗位设置	2
	人员配备	1
	授权和审批	2
	沟通和合作	3

安全类	安全控制点	测评项数
	审核和检查	1
安全管理人员	人员录用	2
	人员离岗	1
	安全意识教育和培训	1
	外部人员访问管理	3
安全建设管理	定级和备案	4
	安全方案设计	3
	产品采购和使用	2
	自行软件开发	2
	外包软件开发	2
	工程实施	2
	测试验收	2
	系统交付	3
	等级测评	3
	服务供应商选择	2
安全运维管理	环境管理	3
	资产管理	1
	介质管理	2
	设备维护管理	2
	漏洞和风险管理	1
	网络和系统安全管理	5
	恶意代码防范管理	3
	配置管理	1
	密码管理	2
	变更管理	1
	备份与恢复管理	3
	安全事件处置	3
	应急预案管理	2
	外包运维管理	2
安全通用要求指标数量统计		135

2.2.2 安全扩展要求指标

表 2-3 安全扩展要求指标

扩展类型	安全类	安全控制点	测评项数
本次测评不涉及安全扩展要求指标			

2.2.3 其他安全要求指标

表 2-4 其他安全要求指标

安全类	安全控制点	测评项数
本次测评不涉及其他安全要求指标		

2.2.4 不适用安全要求指标

表 2-5-1 不适用安全要求指标

安全类	安全控制点	不适用项	不适用原因
安全建设管理	自行软件开发	a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。
安全建设管理	自行软件开发	b) 应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。
安全运维管理	密码管理	b) 应使用国家密码管理主管部门认证核准的密码技术和产品。	（1）单位未采购涉及密码技术的产品，不适用。
安全运维管理	外包运维管理	a) 应确保外包运维服务商的选择符合国家的有关规定；	（1）单位目前未涉及任何外包运维服务情况，不适用。
安全运维管理	外包运维管理	b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。	（1）单位目前未涉及任何外包运维服务情况，不适用。

表 2-5-2 其他不适用安全要求指标

安全类	安全控制点	不适用项	不适用原因
本次测评不涉及其他安全要求指标			

2.3 测评对象

2.3.1 测评对象选择方法

招生信息网系统等级测评的测评对象种类上基本覆盖、数量进行抽样，重点抽查主要的设备、设施、人员和文档等。结合招生信息网系统的网络拓扑结构和业务情况，本次等级测评的测评对象在抽样时主要考虑以下几个方面：

（1） 主机房（包括其环境、设备和设施等）和灾备机房；

（2） 存储被测系统重要数据的介质的存放环境；

（3） 办公场地；

（4） 整个系统的网络拓扑结构；

（5） 安全设备，包括防火墙等；

（6） 边界网络设备，包括路由器、楼层交换机等；

（7） 对整个信息系统或其局部的安全性起作用的网络互联设备，如核心交换机、路由器等；

（8） 承载业务处理系统主要业务或数据的服务器（包括其操作系统和数据库）；

（9） 管理终端和主要应用系统终端；

（10） 能够完成系统不同业务使命的业务应用系统；

（11） 业务备份系统；

（12） 信息安全主管人员、各方面的负责人员、具体负责安全管理的当事人、业务负责人；

（13） 涉及到信息系统安全的所有管理制度和记录。

抽样原则：在等级测评时，业务处理系统中配置相同的安全设备、边界网络设备、网络互联设备、服务器、终端以及备份设备，每类至少抽查两台作为测评对象。

2.3.2 测评对象选择结果

2.3.2.1 物理机房

表 2-6 物理机房

序号	机房名称	物理位置	重要程度
1	信息化机房	茂名市茂南区文明北路232号大院大楼	关键

2.3.2.2 网络设备

表 2-7 网络设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度
1	核心交换机	否	H3C version 7.1.070, Release 7585P07	H3C S7500E-X	核心数据交换、访问控制	关键
2	汇聚交换机	否	H3C version 7.1.070, Release 6126P20	H3C S5560X-30C-EI	数据交换	重要

2.3.2.3 安全设备

表 2-8 安全设备

序号	设备名称	是否虚拟设备	系统及版本	品牌型号	用途	重要程度
1	防火墙-1	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键
2	运维安全管理系统	否	深信服V3.0.6	深信服AC-1000-D603-PT	运维审计	重要
3	WEB应用防火墙	否	深信服AF 8.0.9	深信服WAF-2000-H642	应用防护、入侵防范、病毒防护	重要
4	基线核查系统	否	深信服V3.0.3	深信服AC-1000-D602-PT	漏洞扫描	重要
5	日志审计系统	否	深信服LAS 3.0.5	深信服AC-1000-D601-PT	日志审计	重要
6	上网行为管理系	否	深信服AC12.0.26	深信服	上网行为管理及终	重要

序号	设备名称	是否虚拟设备	系统及版本	品牌型号	用途	重要程度
	统			AC-1000-D600-PT	端准入控制	
7	防火墙-2	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键

2.3.2.4 服务器

表 2-9 服务器

序号	设备名称	所属业务应用系统/平台	是否虚拟设备	操作系统及版本	数据库管理系统及版本	中间件及版本	重要程度
1	应用/数据库服务器	招生信息网系统	否	CentOS 7.7	MySQL 8.42	nginx 1.20.1	关键

2.3.2.5 终端设备

表 2-10 终端设备

序号	设备名称	是否虚拟设备	操作系统及版本	用途	重要程度
1	运维及管理终端-1	否	Windows 10 （版本 20H2（内部版本 19044.1889）	运维管理、系统管理	一般
2	业务终端-2	否	Windows 10 （版本 20H2（内部版本 19044.1889）	业务管理	一般
3	运维及管理终端-2	否	Windows 10 （版本 21H2（内部版本 19044.1889））	运维管理、系统管理	一般
4	业务终端-1	否	Windows 10 （版本 20H2（内部版本 19044.1889）	业务管理	一般

2.3.2.6 其他系统或设备

表 2-11 其他系统或设备

序号	设备名称	是否虚拟设备	系统及版本	用途	重要程度
/	/	/	/	/	/

注释：本次测评对象中不涉及专用移动互联终端等，不开展抽测。

2.3.2.7 系统管理软件/平台

表 2-12 系统管理软件/平台

序号	系统管理软件/平台名称	主要功能	版本	所在设备名称	重要程度
1	应用/数据库服务器-MySQL	数据生产、存储	8.42	应用/数据库服务器	关键
2	应用/数据库服务器-nginx	页面发布	1.20.1	应用/数据库服务器	关键

2.3.2.8 业务应用软件/平台

表 2-13 业务应用系统/平台

序号	业务应用软件/平台名称	主要功能	业务应用软件及版本	开发厂商	重要程度
1	招生信息网系统	招生信息网系统包括轮播图管理、文档列表管理、专题管理、单页管理、栏目管理、导航管理、内容模型管理、院系专业管理、招生计划、历年录取和自助查询等功能模块，招生信息网为学院提供一个招生信息发布平台，也为有就读意向的学生提供一个了解茂名职业技术学院的平台，通	V6.0	广东卓锐软件有限公司	关键

序号	业务应用软件/平台名称	主要功能	业务应用软件及版本	开发厂商	重要程度
		过招生网，为学院和学生建立一个相互了解的通道，同时也为学院的招生工作提供了一个更高效的方式。			

2.3.2.9 数据资源

表 2-14 数据资源

序号	数据类别	所属业务应用	安全防护需求	重要程度
1	重要个人信息	招生信息网系统	完整性、保密性	关键
2	重要业务数据	招生信息网系统	完整性、保密性	关键
3	鉴别数据	招生信息网系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性、保密性	关键
4	重要审计数据	招生信息网系统（安全管理中心）	完整性	重要
5	重要配置数据	招生信息网系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性	关键

注释：网络设备、安全设备、服务器、终端、系统管理软件/平台和业务应用系统等所涉及的鉴别数据和重要配置数据分别在各自测评对象中汇总测评证据后集中体现,包括数据完整性、数据保密性和备份恢复。重要审计数据在安全管理中心进行汇总测评证据，包括数据完整性。重要业务数据和重要个人信息分别在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。

2.3.2.10 安全相关人员

表 2-15 安全相关人员

序号	姓名	岗位/角色	联系方式	所属单位
1	龙恒	网络管理员	13377766618	茂名职业技术学院
2	吴国华	系统管理员	0668-2920122	茂名职业技术学院
3	龙恒	数据管理员	13377766618	茂名职业技术学院
4	杨云	资产管理员	0668-2920122	茂名职业技术学院
5	杨云	审计管理员	0668-2920122	茂名职业技术学院
6	叶永利	安全管理员	0668-2920122	茂名职业技术学院
7	吴国华	机房管理员	0668-2920122	茂名职业技术学院
8	龙恒	应用管理员	13377766618	茂名职业技术学院

2.3.2.11 安全管理文档

表 2-16 安全管理文档

序号	文档名称	主要内容
1	制度类文档-系统交付管理	关于单位交付工作管理制度文档
2	制度类文档-介质管理制度	关于单位介质安全管理工制度文档
3	制度类文档-授权和审批管理规定	关于单位授权审批、审批流程规范制度文档
4	制度类文档-设备安全管理制度	关于单位设备安全管理制度文档
5	制度类文档-办公环境管理制度	关于单位办公环境管理制度文档
6	制度类文档-信息系统外包运维管理制度	关于单位外包运维工作管理制度文档
7	制度类文档-制度制定、发布、评审和修订管理制度	关于单位制度制定、发布、评审和修订等管理文档
8	制度类文档-网络安全事件报告制度	关于单位网络安全事件管理报告文档
9	制度类文档-网络安全事件应急预案	关于单位网络安全事件应急处理、流程、培训等管理制度文档
10	制度类文档-安全漏洞管理制度	关于单位安全漏洞管理工作制度文档

序号	文档名称	主要内容
11	制度类文档-办公环境保密管理	关于单位办公环境管理制度文档
12	制度类文档-人员管理制度	关于单位人员录用、调岗、离岗管理制度文档
13	制度类文档-信息系统恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
14	制度类文档-备份与恢复管理制度	关于单位数据备份、恢复管理制度文档
15	制度类文档-应用安全管理规范	关于规定单位应用安全管理要求及规范的制度文档
16	制度类文档-外部人员访问管理制度	关于单位针对外来人员访问管控制度文档
17	制度类文档-应用系统业务用户密码设置规定	关于单位用户密码管理制度文档
18	制度类文档-物理安全管理规范	关于加强单位办公区域及电子计算机机房的管理和设备运行安全，规范办公区域及机房建设，使人员办公高效及机房设备安全、稳定运行的制度文档
19	制度类文档-变更控制管理制度	关于单位变更流程、控制管理制度文档
20	制度类文档-主机安全管理规范	关于规定单位主机系统安全管理要求规范，指导业务平台主机的安全配置和维护的制度文档
21	制度类文档-恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
22	制度类文档-组织安全结构和人员职责制度	关于单位组织结构、人员安排、人员职责制度文档
23	制度类文档-外包开发软件管理规定	关于单位外包项目管理工作制度文档
24	制度类文档-网络安全管理制度	关于单位网络安全工作管理制度文档
25	制度类文档-安全事件报告和处置	关于单位网络安全事件管理、处置、流程等报告制度文档
26	制度类文档-服务供应商选择安全管理制度	关于单位安全服务供应商管理规定制度文档
27	制度类文档-数据安全管理规范	关于保障关键数据安全，从数据库本身、数据加密、数据备份恢复三个方面对数据安全进行规范的制度文档
28	制度类文档-恶意代码防范管理制度	关于单位恶意代码防范工作制度文档
29	制度类文档-网络与信息系统安全设计规范	关于单位网络与信息化安全设计制度文档
30	制度类文档-外部接入受控网络访问系统管理规范	关于单位针对外部人员工作接入规范制度文档
31	制度类文档-信息安全奖惩办法	关于单位人员奖惩制度文档

序号	文档名称	主要内容
32	制度类文档-离岗人员工作交接规范	关于单位离岗交接工作规范制度文档
33	制度类文档-测试及验收方案	关于单位测试验收方案文档
34	制度类文档-外部服务人员管理规范	关于单位针对外部人员工作管理规范制度文档
35	制度类文档-安全管理组织规范	关于单位组织结构管理规范制度文档
36	制度类文档-安全审查和检查管理规范	关于单位安全检查、审查工作规范制度文档
37	制度类文档-工程实施管理制度	关于单位工程实施工作管理制度文档
38	制度类文档-信息安全总体策略	关于单位网络安全方针、策略制度文档
39	制度类文档-信息安全漏洞扫描规范	关于单位安全漏洞工作规范制度文档
40	制度类文档-系统及应用数据备份管理规范	关于单位数据备份、恢复管理制度文档
41	制度类文档-安全教育和培训制度	关于单位安全培训、安全交流工作制度文档
42	制度类文档-组织安全结构和人员职责制度	关于单位安全结构、人员职责
43	制度类文档-岗位安排及岗位职责	关于单位岗位职责、岗位安排制度文档
44	制度类文档-系统安全管理制度	关于单位系统安全管理、安全服务管理制度文档
45	制度类文档-机房安全管理制度	关于单位机房安全管理工作制度文档
46	制度类文档-员工考核管理制度	关于单位人员考核工作管理制度文档
47	制度类文档-网络安全管理规范	关于保障单位网络系统的安全稳定运行，抵御内部和外部各种形式的网络攻击或威胁制定的管理文档
48	制度类文档-工程测试验收管理	关于单位工程测试工作管理制度文档
49	操作类文档-设备操作规程	关于单位相关设备操作指导文档
50	操作类文档-数据备份策略	关于单位数据备份策略文件
51	操作类文档-设备及系统软件配置和操作手册	关于单位安全设备操作、Linux服务器配置手册、主机运维操作手册、软件操作手册、防火墙配置和操作手册、数据库日常运维操作手册等指导文档
52	操作类文档-软硬件日常维护管理规程	关于单位计算机网络系统使用、管理、信息安全、资源共享有所遵循,规范上网操作流程,提高网络系统安全性的指导文档
53	记录类文档-离场信息资料	关于人员离岗交接工作记录

序号	文档名称	主要内容
	交接表	
54	记录类文档-备份工作汇总表	关于单位数据备份工作总结表
55	记录类文档-机房维护日志	关于机房维护工作记录
56	记录类文档-安全管理制度评审记录	关于单位制度审计记录
57	记录类文档-接入受控网络申请表	关于外来人员接入工作记录
58	记录类文档-通用变更记录表	关于单位变更工作记录
59	记录类文档-离职员工物品交回登记表	关于人员离岗工物交接工作记录
60	记录类文档-设备操作维护记录	关于单位设备维护工作记录
61	记录类文档-软件交付清单	关于单位交付工作记录
62	记录类文档-信息系统存储介质销毁申请表	关于备份介质销毁申请工作记录
63	记录类文档-系统交付清单	关于单位交付工作记录
64	记录类文档-信息系统存储介质使用清单	关于备份介质存储使用清单
65	记录类文档-设备出入登记记录表	关于设备进出机房登记工作记录
66	记录类文档-机房设备维修记录表	关于单位机房设备维修工作记录
67	记录类文档-信息安全检查记录表	关于单位安全检查工作记录
68	记录类文档-信息管理系统漏洞检查表	关于单位安全漏洞工作检测记录表
69	记录类文档-技能培训记录	关于单位系统培训工作、考核工作记录
70	记录类文档-机房设备维护记录表	关于设备维护登记工作记录
71	记录类文档-存储介质目录清单	关于备份介质存储工作清单
72	记录类文档-机房巡检记录表	关于单位机房环境巡检记录
73	记录类文档-评审和修订记录	关于单位变更评审、修订工作记录
74	记录类文档-专家论证记录表	关于单位网络方案论证记录
75	记录类文档-外部人员访问申请表	关于外来人员访问申请流程工作记录
76	记录类文档-信息安全会议	关于单位安全培训、安全交流会议记录

序号	文档名称	主要内容
	记录	
77	记录类文档-机房出入登记表	关于人员进出机房登记工作记录
78	记录类文档-外部人员访问记录表	关于外来人员访问登记工作记录
79	记录类文档-网络信息安全事件记录表	关于单位网络安全事件工作记录
80	记录类文档-应急预案培训记录表	关于单位应急预案培训工作记录
81	记录类文档-人员入职考核记录	关于人员录用、考核工作记录
82	记录类文档-收发文登记记录	关于单位文档签发记录
83	记录类文档-数据恢复申请表	关于单位数据恢复工作申请表
84	记录类文档-数据备份记录表	关于单位数据备份工作记录
85	记录类文档-网络配置信息	关于单位配置信息登记工作记录
86	记录类文档-监理审批表	关于单位监理审核工作记录
87	记录类文档-外部会议文件和记录	关于单位外部联系、交流及会议工作记录
88	记录类文档-人员离岗申请表	关于人员离岗申请记录
89	记录类文档-访问记录表	关于人员访问工作记录
90	记录类文档-设备维修申请表	关于单位设备维护工作申请记录
91	记录类文档-人员培训及考核记录表	关于人员培训、考核等工作记录
92	记录类文档-漏洞检测报告	关于单位安全漏洞检测报告文档
93	记录类文档-重要操作审批表	关于单位审批工作记录
94	记录类文档-关键岗位人员考核记录	关于关键岗位考核工作记录
95	记录类文档-安全建设方案评审纪录	关于单位网络与信息化安全设计方案评审工作记录
96	记录类文档-备份介质使用记录	关于备份介质使用登记工作记录
97	证据类文档-外部联系表	关于单位内部联系及外部联系名单
98	证据类文档-定级备案	关于单位系统定级报告、备案证文件
99	证据类文档-安全职位人员	关于单位人员岗位安排名单
100	证据类文档-深信服安全采购合同	关于单位与安全厂家服务采购、产品选择合同文件

序号	文档名称	主要内容
101	证据类文档-网络安全系统设计方案	关于单位网络与信息化安全设计方案文档
102	证据类文档-网络安全等级保护测评服务合同	关于单位与安全服务商签定的安全服务合同文件
103	证据类文档-网络安全等级保护工作小组名单	关于单位网络安全等级保护工作小组人员名单文件
104	证据类文档-资产清单	关于单位信息系统资产清单统计表
105	证据类文档-信息安全事件分析报告表	关于单位安全事件分析报告
106	证据类文档-工程项目实施方案	关于单位工程实施方案文档

3 单项测评结果分析

3.1 安全物理环境

3.1.1 已有安全控制措施汇总分析

安全通用要求

物理位置选择	
a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；	
信息化机房	（1）机房和办公场地场所在建筑物具有建筑验收文档，包含对防震、防风和防雨能力的说明； （2）机房和办公场地未出严重的问题。
b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	
信息化机房	（1）机房未部署在易发生问题的位置； （2）机房对于空调设备的排水管等部位采取密封防漏处理； （3）机房对于楼板进行了防护措施。
防盗窃和防破坏	
a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识；	
信息化机房	（1）机房设备或主要部件都固定在机架上； （2）机房内对主要部件已绑定相应不易除去的标签； （3）重要机柜已进行上锁处理。
b) 应将通信线缆铺设在隐蔽安全处。	
信息化机房	（1）通信线缆铺设在下走线槽隐蔽处中； （2）通信线缆设有明显的源目的标识； （3）通信线缆均铺设整齐、规范。
防雷击	
应将各类机柜、设施和设备等通过接地系统安全接地。	

信息化机房	（1）机房设置专用地线； （2）机房内机柜、设施和设备等进行接地处理； （3）交流电源接地验收检测结果符合要求。
防火	
a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；	
信息化机房	（1）机房采用经消防检测部门检测合格并在有效期内的（如 七氟丙烷）气体自动灭火设备，火灾自动报警类型为烟感+红外； （2）自动消防系统工作状态正常，有定期巡检和维护记录《机房巡检记录表》； （3）建立机房消防的管理制度相关文档《机房安全管理制度》，按管理要求机房无人情况下气体灭火配置为自动模式，进入机房调整为手动模式，机房报警有7*24小时值班人员进行监控。
防水和防潮	
a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	
信息化机房	（1）机房不存在雨水渗透、破损等不合规情况； （2）机房不位于建筑的顶层、边缘区域。
b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。	
信息化机房	（1）机房区域范围已部署1台科华品牌（精密）空调，机房内分别配置1组温湿度传感器监控； （2）机房内空调下方已铺设安装好挡水和排水设施； （3）机房墙壁或楼板的管道采取必要的防渗防漏等防水保护措施； （4）机房安装检测设备（如：漏水检测绳）检测地下积水，及时处理机房水蒸气结露和地下积水的转移与渗透； （5）目前防水\防潮检测未发现异常情况，并且有防水防潮的运维记录《机房维护日志》。
温湿度控制	
应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。	
信息化机房	（1）机房范围已部署1组科华品牌精密空调进行温湿度调节； （2）机房范围已部署空调及加湿机进行温湿度调节； （3）温湿度自动调节设施运作正常，有运行和维护记录《机房维护日志》； （4）机房温度能保持在24摄氏度到28摄氏度之间； （5）机房湿度能保持在40%到65%之间。
电力供应	
a）应在机房供电线路上配置稳压器和过电压防护设备；	
信息化机房	（1）机房配备了稳压器和过电压防护设备； （2）稳压器和过电压防护设备正常工作； （3）机房具备电力供应安全设计，并在其中标明配备稳压器、过电压防护设备等要求。
b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。	
信息化机房	（1）机房配备了1组科华品牌UPS； （2）UPS正常工作，可满足主要设备断电情况下的至少1小时正常运行要求； （3）UPS有定期（至少每年）检查和维护，有运行和维护记录《机房巡检记录表》。

电磁防护	
电源线和通信线缆应隔离铺设，避免互相干扰。	
信息化机房	（1）通信线缆铺设采用独立的具有电磁屏蔽作用线槽； （2）电源线缆铺设采用独立的具有电磁屏蔽作用线槽； （3）弱电线缆隔离铺设，没有干扰。

3.1.2 主要安全问题汇总分析

安全通用要求

（1）机房出入口未配置电子门禁系统（如：信息化机房）。上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域,可能对系统的平稳运行造成影响。中风险。

（2）机房建设未完全采用符合耐火等级的建筑材料。机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级（如：信息化机房）。存在发生火情时助燃火灾的风险。 低风险。

（3）机房内缺乏防静电措施（如防静电地板或铺设防静电地毯 ）（如：信息化机房）。存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。 中风险。

3.2 安全通信网络

3.2.1 已有安全控制措施汇总分析

安全通用要求

网络架构	
b) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	
安全通信网络	(1)网络内重要网段未部署在网络边界处,且未直接连接外部信息系统; (2) 系统通过防火墙对重要网段采取访问控制策略; (3) 各安全域（子网）的出口唯一。
通信传输	
应采用校验技术保证通信过程中数据的完整性。	
安全通信网络	(1) 网络系统中未涉及完整性保障设备，但在安全计算环境方面网络设备采用SSH协议、安全设备采用HTTPS协议、操作系统采用SSH协议、应

	用系统采用HTTPS协议来保证通信过程中数据的完整性。

3.2.2 主要安全问题汇总分析

安全通用要求

（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况（如：安全通信网络）。上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变得更为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。 中风险。

（2）缺乏对通信设备可信验证方面的安全设计要求。现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况（如：安全通信网络）。缺乏对系统可执行程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致计算资源被干扰和破坏造成损失。 低风险。

3.3 安全区域边界

3.3.1 已有安全控制措施汇总分析

安全通用要求

边界防护	
应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络存在受保护的边界； （2）网络边界处部署了可提供访问控制功能的设备； （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。
访问控制	
a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	
办公网区域 外网边界区域	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备；

安全管理区域 服务器存储区域	（3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。
b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。
c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。
d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。
入侵防范	
应在关键网络节点处监视网络攻击行为。	
外网边界区域 服务器存储区域	（1）网络层部署支持对内部发起的攻击行为进行防范的设备； （2）现有的防范措施满足相应防护要求； （3）内部安全防范措施能检测相应攻击行为。
恶意代码和垃圾邮件防范	
应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	
外网边界区域 服务器存储区域	（1）在关键网络节点处部署合规的防恶意代码措施； （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试。
安全审计	
a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； （3）现有的审计措施满足相应的审计要求。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； （3）设备本地时间正常。
c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
办公网区域 外网边界区域 安全管理区域	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求；

服务器存储区域	（4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。

3.3.2 主要安全问题汇总分析

安全通用要求

（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为（如：办公网区域）。存在不能及时发现内部主机作为攻击跳板，或网络攻击行为而造成系统损坏/网络资源浪费的风险。中风险。

（2）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面（如：办公网区域）。无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。 中风险。

（3）缺乏对边界设备可信验证方面的安全设计要求。现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况（如：办公网区域）。缺乏对边界设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4 安全计算环境

3.4.1 网络设备

3.4.1.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
核心交换机 汇聚交换机	（1）设备对各登录模式均启用身份鉴别； （2）设备对登录管理的用户进行身份鉴别；

	（3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的全局密码策略； （6）设备配置加密的super认证。
b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
核心交换机 汇聚交换机	（1）设备配置合规的全局登录失败处理策略； （2）设备配置合规的操作超时退出措施。
c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
核心交换机 汇聚交换机	（1）设备配置合规的远程管理模式。
访问控制	
a）应对登录的用户分配账户和权限；	
核心交换机 汇聚交换机	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。
b）应重命名或删除默认账户，修改默认账户的默认口令；	
核心交换机 汇聚交换机	（1）设备不存在默认账户名； （2）设备账户口令设置合规。
c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
核心交换机 汇聚交换机	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。
d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	
核心交换机 汇聚交换机	（1）设备根据安全策略要求对特权用户进行分离； （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
核心交换机 汇聚交换机	（1）设备开启审计功能，审计进程正常； （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
核心交换机 汇聚交换机	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。
c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
核心交换机 汇聚交换机	（1）设备限制审计文件的访问控制权限，普通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效； （5）日志及审计记录保存大于6个月。

入侵防范	
a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	
核心交换机 汇聚交换机	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。
b) 应关闭不需要的系统服务、默认共享和高危端口；	
核心交换机 汇聚交换机	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。
c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
核心交换机 汇聚交换机	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
核心交换机 汇聚交换机	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
核心交换机 汇聚交换机	鉴别数据、重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； （2）设备对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
核心交换机 汇聚交换机	（1）设备定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。

3.4.1.2 主要安全问题汇总分析

安全通用要求

（1）设备不具备相关可信验证的技术措施（如：核心交换机）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.2 安全设备

3.4.2.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备对各登录模式均启用身份鉴别； （2）设备对登录管理的用户进行身份鉴别； （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。
b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备启用合规登录失败处理策略； （2）设备配置合规的操作超时退出措施。
c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备配置合规的远程管理模式； （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。
访问控制	
a）应对登录的用户分配账户和权限；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。
b）应重命名或删除默认账户，修改默认账户的默认口令；	

WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备不存在默认账户名； (2) 设备账户口令设置合规。
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备不存在多余或过期账户； (2) 设备管理员用户与账户之间一一对应。
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备根据安全策略要求对特权用户进行分离； (2) 设备不存在多个管理级别高的特权用户； (3) 设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备开启审计功能，审计进程正常； (2)设备的日志审计级别满足要求,审计覆盖所有用户操作审计和记录。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备日期、时间正常； (2) 设备审计记录内容基本完整。
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
WEB应用防火墙 上网行为管理系统 基线核查系统	(1) 设备限制审计文件的访问控制权限，普通用户不可删除及修改； (2) 设备针对日志、审计记录具备充足的存储容量； (3) 对审计记录进行定期存档备份，其备份策略有效；

运维安全管理系统 防火墙-1 防火墙-2	（4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。
日志审计系统	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）日志及审计记录保存大于6个月。
入侵防范	
a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。
b）应关闭不需要的系统服务、默认共享和高危端口；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。
c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 防火墙-1 防火墙-2	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
运维安全管理系统	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制。
d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备管理具备数据有效性检验功能； （2）设备管理的校验接口范围较全面。
e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
WEB应用防火墙	（1）设备已根据需要不定期地对已发布的新固件版本进行更新；

上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。
恶意代码防范	
应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	
WEB应用防火墙 防火墙-1 防火墙-2	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	鉴别数据、重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； （2）设备对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a）应提供重要数据的本地数据备份与恢复功能；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。

3.4.2.2 主要安全问题汇总分析

安全通用要求

（1）设备不具备相关可信验证的技术措施（如：WEB应用防火墙）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.3 服务器和终端

3.4.3.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统对登录系统的用户进行身份鉴别； （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； （5）用户属性策略未勾选“密码永不过期”。
应用/数据库服务器	（1）操作系统对登录系统的用户进行身份鉴别； （2）操作系统不存在空口令用户； （3）操作系统不存在默认信任的登录模式； （4）操作系统为登录用户设置的身份标识具有唯一性； （5）操作系统配置的一定的密码长度且定期更换； （6）操作系统配置一定的密码复杂度策略。
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统启用登录失败处理策略。 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略。
应用/数据库服务器	（1）操作系统启用pam_tally2模块的合规登录失败处理策略； （2）操作系统配置合规的操作超时锁定； （3）操作系统启用SSH的合规登录超时策略。
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS的管理。
应用/数据库服务器	（1）操作系统配置合规的远程管理模式； （2）操作系统远程端口使用情况合规； （3）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
访问控制	
a) 应对登录的用户分配账户和权限；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权

	限分配表情况一致。
应用/数据库服务器	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在所有用户均属于root组的情况。
b）应重命名或删除默认账户，修改默认账户的默认口令；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统针对默认账户采用相应的安全策略配置； （2）操作系统账户不存在弱口令或空口令。
应用/数据库服务器	（1）操作系统对多余帐户进行删除、锁定或禁止其登录； （2）操作系统账户口令设置合规。
c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。
d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统根据安全策略要求对特权用户进行分离； （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
应用/数据库服务器	（1）操作系统根据安全策略要求对特权用户进行分离； （2）操作系统不存在除root外的特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统开启审计策略，操作系统审计策略基本完整； （2）审计覆盖所有用户操作审计和记录。
应用/数据库服务器	（1）操作系统开启审计功能，审计进程正常； （2）操作系统开启审计范围及策略满足要求，审计覆盖所有用户操作审计和记录。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。
c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	

业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统采取对审计记录存储容量如下： 运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。
应用/数据库服务器	(1)操作系统限制审计文件的访问控制权限,普通用户不可删除及修改； （2）操作系统针对日志、审计记录具备充足的存储容量； （3）操作系统采取合规的日志文件权限策略； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。
入侵防范	
a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。
应用/数据库服务器	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。
b）应关闭不需要的系统服务、默认共享和高危端口；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统不存在多余的默认共享及其它文件共享； （2）操作系统关闭不必要端口； （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。
应用/数据库服务器	（1）操作系统关闭不必要端口； （2）操作系统禁用不必要服务； （3）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口； （4）漏洞扫描未发现高风险主机端口。
c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
应用/数据库服务器	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	

业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。
应用/数据库服务器	（1）操作系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。
恶意代码防范	
应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。
应用/数据库服务器	（1）操作系统安装深信服edr防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	鉴别数据、重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。
应用/数据库服务器	鉴别数据: （1）系统在通信传输过程中对鉴别数据采取完整性保护措施。 重要配置数据: （1）系统在通信传输过程中对重要配置数据采取完整性保护措施。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
业务终端-1 业务终端-2 应用/数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施: 安全选项“不显示上次的用户名”->启用

应用/数据库服务器	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统不保存过多终端历史记录。

3.4.3.2 主要安全问题汇总分析

安全通用要求

（1）缺乏对计算设备可信验证方面的安全设计要求。现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。现有的计算设备存在对系统运行过程中的可信检验不全面的情况。现有的可信验证存在部分告警、审计及联动措施不全面的情况(如：应用/数据库服务器）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.4 系统管理软件/平台

3.4.4.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
应用/数据库服务器-MySQL	（1）数据库系统启用合规登录失败处理策略； （2）数据库系统执行合规的锁定策略； （3）数据库系统配置合规的操作超时锁定。
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
应用/数据库服务器-MySQL	（1）数据库系统配置合规的远程管理模式。
访问控制	
a) 应对登录的用户分配账户和权限；	
应用/数据库服务器-MySQL	（1）登录数据库系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （2）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在多用户均与root用户权限一致的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。
应用/数据库服务器-nginx	（1）宿主系统可提供系统权限功能；

	（2）系统安装Nginx后产生的用户已对权限加以控制； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。
b）应重命名或删除默认账户，修改默认账户的默认口令；	
应用/数据库服务器-MySQL	（1）数据库系统对多余帐户进行删除、锁定或禁止其登录； （2）数据库系统账户口令设置合规。
应用/数据库服务器-nginx	（1）中间件不存在默认账户名； （2）中间件账户口令设置合规。
c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
应用/数据库服务器-MySQL	（1）数据库系统不存在多余或过期账户； （2）数据库系统管理员用户与账户之间一一对应。
应用/数据库服务器-nginx	（1）中间件不存在多余或过期账户； （2）中间件管理员用户与账户之间一一对应。
d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	
应用/数据库服务器-MySQL	（1）数据库系统根据安全策略要求对特权用户进行分离； （2）数据库系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限； （3）数据库账户和系统管理员账户未处于同一个用户组中； （4）宿主操作系统管理员与数据库管理员为不同的人员，且使用不同的帐户登录系统。
应用/数据库服务器-nginx	（1）中间件根据安全策略要求对特权用户及宿主管理用户进行分离； （2）中间件管理不存在多个管理级别高的特权用户； （3）Nginx中间件不采用root用户权限运行。
安全审计	
a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
应用/数据库服务器-MySQL	（1）数据库系统开启审计功能，审计进程正常。
应用/数据库服务器-nginx	（1）中间件开启审计功能，审计进程正常； （2）系统的日志审计级别满足要求。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
应用/数据库服务器-MySQL	（1）数据库宿主系统日期、时间正常； （2）数据库系统审计记录内容基本完整。
应用/数据库服务器-nginx	（1）中间件日期、时间正常； （2）中间件审计记录access.log及error.log内容基本完整。
c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
应用/数据库服务器-MySQL	（1）数据库系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）数据库系统针对日志、审计记录具备充足的存储容量； （3）日志及审计记录保存大于6个月。
应用/数据库服务器-nginx	（1）中间件限制审计文件的访问控制权限，普通用户不可删除及修改； （2）宿主系统针对中间件日志、审计记录具备充足的存储容量； （3）对中间件审计记录进行定期存档备份，其备份策略有效； （4）日志及审计记录可保存大于6个月。
入侵防范	
c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	

应用/数据库服务器-MySQL	（1）数据库系统设定有效的终端接入策略，对通过网络进行管理的终端进行限制； （2）核心交换机设备ACL策略有效限制访问本机的IP地址及管理模式。
e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
应用/数据库服务器-MySQL	（1）数据库系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）数据库宿主系统不存在启用未加控制的高危端口； （3）MYSQL分离默认安装的示例数据库； （4）数据库系统进行渗透及扫描未发现存在可造成高风险的漏洞。
应用/数据库服务器-nginx	（1）中间件已根据需要不定期地对已发布的版本进行更新； （2）中间件更新安装前进行安全性和兼容性测试； （3）在不影响业务系统正常运行情况下，对发现的中间件漏洞在确保安全的情况下进行修补； （4）中间件进行渗透及扫描未发现存在可造成高风险的漏洞。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
应用/数据库服务器-MySQL	鉴别数据、重要配置数据: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。
应用/数据库服务器-nginx	鉴别数据、重要配置数据: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a）应提供重要数据的本地数据备份与恢复功能；	
应用/数据库服务器-MySQL	（1）数据库系统定义了相关重要数据； （2）数据库系统定期完全依照备份策略，采用正确的配置进行本地备份； （3）系统的备份周期为：每天一次增量、每月一次全备； （4）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
应用/数据库服务器-nginx	（1）系统定义了相关需要备份的中间件重要数据； （2）宿主系统定期完全依照备份策略，采用正确的配置进行本地备份； （3）中间件相关数据的备份周期合理； （4）中间件开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	
应用/数据库服务器-MySQL	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）数据库系统不保存终端历史记录。
应用/数据库服务器-nginx	（1）宿主系统具有清除用户鉴别信息的功能； （2）经测试，宿主系统退出后无法访问先前中间件登录过的页面； （3）经测试，宿主系统关闭后无残留的中间件用户鉴别信息。
个人信息保护	
a）应仅采集和保存业务必需的用户个人信息；	
应用/数据库服务器-MySQL	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程；

	（2）数据库存储的用户个人信息均为业务应用必需的环节。
b）应禁止未授权访问和非法使用用户个人信息。	
应用/数据库服务器-MySQL	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； （2）数据库具备控制措施禁止未授权访问用户个人信息表单； （3）数据库具备控制措施禁止非法使用用户个人信息表单。

3.4.4.2 主要安全问题汇总分析

安全通用要求

（1）数据库系统配置不合规的密码有效周期策略（如：应用/数据库服务器-MySQL）。上述问题的存在，使恶意用户能够较为容易的访问数据库等资源并实施恶意操作，对相关系统的正常运行造成影响，存在系统被未授权访问、操作的可能性。 中风险。

（2）未能提供数据库系统重要数据的异地定时数据备份功能（如：应用/数据库服务器-MySQL）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供，使企业的经济利益或声誉受到损害。 中风险。

3.4.5 业务应用系统/平台

3.4.5.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
招生信息网系统	（1）系统对各登录模式均启用身份鉴别； （2）系统对登录管理的用户进行身份鉴别； （3）系统登录用户设置的身份标识具有唯一性； （4）系统不存在空口令用户； （5）设备配置合规的密码策略。
b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
招生信息网系统	（1）系统启用合规登录失败处理策略； （2）系统配置合规的操作超时退出措施。
c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
招生信息网系统	（1）应用系统的用户鉴别数据采用SHA-512算法在可控网络环境中传输；

	（2）系统配置合规的远程管理模式。
访问控制	
a）应对登录的用户分配账户和权限；	
招生信息网系统	（1）可提供系统权限分配表； （2）登录系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需分配不同的用户权限，不存在所有用户均属于管理级别、高权限的情况。
b）应重命名或删除默认账户，修改默认账户的默认口令；	
招生信息网系统	（1）系统禁用默认账户名； （2）系统账户口令设置合规。
c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
招生信息网系统	（1）系统不存在多余或过期账户； （2）系统管理员用户与账户之间一一对应。
d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	
招生信息网系统	（1）系统不存在多个管理级别高的特权用户； （2）系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
招生信息网系统	（1）系统开启审计功能，审计进程正常； （2）系统的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
招生信息网系统	（1）系统日期、时间正常； （2）系统审计记录内容基本完整。
c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
招生信息网系统	（1）系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）系统针对日志、审计记录具备充足的存储容量； （3）审计记录及日志保存大于6个月。
入侵防范	
c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
招生信息网系统	（1）系统自身设定有效的终端访问策略，通过访问措施进行管理地址的限制。
d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	
招生信息网系统	（1）系统具备数据有效性检验功能； （2）系统的校验接口范围较全面。
e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
招生信息网系统	（1）系统已根据需要不定期地对已发布的版本进行更新； （2）在系统上线或发生重大变更时测试并安装最新的版本或更新补丁； （3）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补。
数据完整性	

应采用校验技术保证重要数据在传输过程中的完整性。	
招生信息网系统	鉴别数据、重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； （2）系统对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
招生信息网系统	（1）系统定义了相关需要备份重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	
招生信息网系统	（1）系统具有清除用户鉴别信息的功能； （2）经测试，系统退出后无法访问先前登录过的页面； （3）经测试，系统关闭后无残留的用户鉴别信息。
个人信息保护	
a) 应仅采集和保存业务必需的用户个人信息；	
招生信息网系统	(1) 单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息； （3）系统采集的用户个人信息均为业务应用必需的环节。
b) 应禁止未授权访问和非法使用用户个人信息。	
招生信息网系统	（1）系统不采集和保存任何形式的用户个人信息； （2）系统对所有涉及个人信息的环节均有明确的授权同意过程； （3）系统具备控制措施禁止未授权访问用户个人信息； （4）系统具备控制措施禁止非法使用用户个人信息。

3.4.5.2 主要安全问题汇总分析

安全通用要求

（1）未能提供应用软件系统重要数据的异地定时数据备份功能（如：招生信息网系统）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

3.4.6 数据资源

3.4.6.1 已有安全控制措施汇总分析

安全通用要求

数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
重要业务数据 重要个人信息	（1）系统在通信传输过程中对相关数据采取完整性保护措施； （2）系统对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
重要业务数据 重要个人信息	（1）系统定义了相关需要备份重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
个人信息保护	
a) 应仅采集和保存业务必需的用户个人信息；	
重要个人信息	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息； （3）系统采集的用户个人信息均为业务应用必需的环节。
b) 应禁止未授权访问和非法使用用户个人信息。	
重要个人信息	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； （2）系统具备控制措施禁止未授权访问用户个人信息； （3）系统具备控制措施禁止非法使用用户个人信息。

3.4.6.2 主要安全问题汇总分析

安全通用要求

重要业务数据

（1）未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要业务数据）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

重要个人信息

（1）未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要个人信息）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

3.4.7 其他系统或设备

3.4.7.1 已有安全控制措施汇总分析

安全通用要求

无其他系统或设备，不涉及相关测评

3.4.7.2 主要安全问题汇总分析

安全通用要求

无其他系统或设备，不涉及相关测评

3.5 安全管理中心

3.5.1 已有安全控制措施汇总分析

安全通用要求

系统管理	
a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；	
管理中心	(1) 网络中部署运维安全管理系统实现集中的系统管理； (2) 系统对登录用户进行身份鉴别； (3) 系统用户标识具有唯一性； (4) 系统可实现对账户的身份鉴别数据进行保密性和完整性保护； (5) 系统管理操作模式具备控制措施； (6) 系统具备相应的管理操作审计措施。
审计管理	
a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；	
管理中心	(1) 网络中部署运维安全管理系统实现集中安全审计功能； (2) 审计系统对审计管理员进行身份鉴别； (3) 审计系统用户标识具有唯一性； (4) 审计系统管理操作模式具备控制措施； (5) 审计系统具备相应的管理操作审计措施。

b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	
管理中心	招生信息网系统: （1）审计管理员定期对审计记录进行分析，对发现的安全可疑事件及时处理； （2）单位具有安全审计策略文件，规范审计记录的存储、管理和查询要求； （3）审计管理员按规范要求对审计记录进行管理。 重要审计数据: 日志审计系统、运维安全管理系统: （1）设备在通信传输过程中对相关数据采取完整性保护措施； （2）设备对重要数据在传输过程中采取必要的完整性保护措施。

3.5.2 主要安全问题汇总分析

安全通用要求

（1）系统管理的资源、运行及配置管理不够全面（如：管理中心）。系统的资源和运行缺少统一的管理，将导致系统可能无法按规划实现基于资源配置、 系统加载、异常处理、及备份/恢复等的安全控制措施。 低风险。

3.6 安全管理制度

3.6.1 已有安全控制措施汇总分析

安全通用要求

安全策略	
应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。	
制度文件、执行/记录文件	（1）单位具有网络安全工作的总体方针和安全策略文件； （2）制度内容包括明确的单位安全工作要求； （3）管理文件详见《信息安全总体策略》。
管理制度	
a) 应对安全管理活动中的主要管理内容建立安全管理制度；	
制度文件、执行/记录文件	（1）单位有针对安全管理活动中的各类管理内容建立安全管理制度； （2）现有制度已覆盖管理活动的主要的方面； （3）制度详见：《信息安全总体策略》、《网络安全管理规范》、《组

	织安全结构和人员职责制度》、《人员管理制度》、《员工考核管理制度》。
b) 应对管理人员或操作人员执行的日常管理操作建立操作规程。	
制度文件、执行/记录文件	（1）单位针对相关业务日常管理的操作建立规程类管理制度； （2）现有制度已覆盖重要管理方面的系统维护手册和用户操作规程等； （3）管理文件详见《设备及系统软件配置和操作手册》。
制定和发布	
a) 应指定或授权专门的部门或人员负责安全管理制度的制定；	
制度文件、执行/记录文件	（1）单位针对安全管理制度的制定，指定教育信息与网络中心部主要负责； （2）在已制定的相关制度中可查阅到被授权制定管理制度的部门/人员信息； （3）管理文件详见《安全管理组织规范》。
b) 安全管理制度应通过正式、有效的方式发布，并进行版本控制。	
制度文件、执行/记录文件	（1）单位针对制度的制定和发布要求，制定管理规范文件； （2）管理规范文件对文件制定及发布定义了规范要求； （3）安全管理制度的收发登记记录有效； （4）管理文件详见《制度制定、发布、评审和修订管理制度》、《收发文登记记录》。
评审和修订	
应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	
制度文件、执行/记录文件	（1）单位针对制度的合理性和适用性需进行论证和审定及修订的要求，制定管理规范文件； （2）管理规范文件对制度的评审及修订定义了规范要求； （3）单位具有安全管理制度的审定或论证的过程记录； （4）单位对做过修订的制度，具备有修订版本的安全管理过程记录； （5）管理文件详见《制度制定、发布、评审和修订管理制度》及 《安全管理制度评审记录》。

3.6.2 主要安全问题汇总分析

安全通用要求

招生信息网系统针对安全管理制度层面的安全通用要求采取的安全措施比较完善，未发现不符合项。

3.7 安全管理机构

3.7.1 已有安全控制措施汇总分析

安全通用要求

岗位设置	
a) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；	
制度文件、执行/记录文件	（1）单位已明确网络安全管理工作的职能部门，并明确了各岗位职责； （2）单位各部门职责文档已明确网络安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备网络安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。
b) 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。	
制度文件、执行/记录文件	（1）单位已明确系统安全管理工作的职能部门，并明确了各岗位职责； （2）单位各部门职责文档已明确系统安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备系统安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。
人员配备	
应配备一定数量的系统管理员、审计管理员和安全管理员等。	
制度文件、执行/记录文件	（1）单位针对人员配备要求，制定了管理制度； （2）单位按要求配备一定数量的重要岗位管理人员； （3）单位针对各岗位人员，制定并维护人员档案； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。
授权和审批	
a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；	
制度文件、执行/记录文件	（1）单位在制度中用文字描述或在流程图中明确，对关键活动进行审批； （2）单位对审批过程明确审批权限，对各项信息系统的重要操作与变更明确审批部门和批准人； （3）管理文件详见《授权和审批管理规定》。
b) 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。	
制度文件、执行/记录文件	（1）单位针对各项业务操作及变更等建立了审批程序规定； （2）单位针对系统变更、系统接入、物理范围等事项已明确按审批程序执行，记录有批准人签字； （3）管理文件详见《授权和审批管理规定》。
沟通和合作	
a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；	
制度文件、执行/记录文件	（1）单位针对机构内部管理人员之间、部门之间的沟通与合作，制定了管理制度；

	（2）单位的管理制度规范了合作和沟通的方式和周期； （3）单位有组织机构内部人员联系表； （4）单位有定期召开信息安全会议，保存有会议纪要； （5）管理文件详见《安全教育和培训制度》、《技能培训记录》《外部联系表》。
b）应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；	
制度文件、执行/记录文件	（1）单位针对加强与外部单位的合作与沟通，制定了管理制度规定； （2）单位能按要求与相关单位保持沟通合作，并提供相关单位联系方式和交流会议纪要； （3）管理文件详见《安全教育和培训制度》、《技能培训记录》、《外部联系表》。
c）应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	
制度文件、执行/记录文件	（1）单位建立了完善的对外联单位的联系列表； （2）管理文件详见《外部联系表》。

3.7.2 主要安全问题汇总分析

安全通用要求

（1）单位开展的检查工作不够完善（如：制度文件、执行/记录文件）。检查工作开展不仔细，可能对存在或潜在的安全风险不能被及时发现并进行处理。 低风险。

3.8 安全管理人员

3.8.1 已有安全控制措施汇总分析

安全通用要求

人员录用	
a）应指定或授权专门的部门或人员负责人员录用；	
制度文件、执行/记录文件	（1）单位授权专门的部门负责人员录用工作，制定了管理制度规范； （2）由人力资源保障科负责人员录用工作； （3）管理文件详见《人员管理制度》。
b）应对被录用人员的身份、安全背景、专业资格或资质等进行审查。	
制度文件、执行/记录文件	（1）单位针对人员录用过程，制定了明确要求，并形成人员安全管理制度； （2）单位现有管理制度明确说明录用人员应具备的条件； （3）单位按规定执行人员录用的相关审查过程； （4）管理文件详见《人员管理制度》、《人员入职考核记录》。
人员离岗	
应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设	

备。	
制度文件、执行/记录文件	（1）单位针对离岗人员权限终止及取回机构提供的各种设施的要求，制定了管理制度； （2）单位按规范开展对离岗人员的相关管理工作； （3）管理文件详见《人员管理度》、《人员离岗申请表》、《离场信息资料交接表》。
安全意识教育和培训	
应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。	
制度文件、执行/记录文件	（1）单位针对人员安全培训及责任和惩戒措施，制定了管理制度； （2）单位已开展安全意识教育及岗位技能培训。 （3）管理文件详见《安全教育和培训制度》。
外部人员访问管理	
a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；	
制度文件、执行/记录文件	（1）单位针对外部人员物理访问，制定了外部人员访问管理文档； （2）单位具备有效的外部人员访问重要区域的书面申请文档； （3）单位具备外部人员访问重要区域的登记记录； （4）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。
b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；	
制度文件、执行/记录文件	（1）单位针对外部接入受控网络访问系统，制定了管理制度； （2）单位具备外部人员接入受控网络前的申请审批流程； （3）单位具备外部人员接入及访问系统的书面申请文档； （4）单位具备外部人员接入及访问系统的登记记录； （5）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。

3.8.2 主要安全问题汇总分析

安全通用要求

（1）单位未完全按管理规范开展人员离场后的清理工作（如：制度文件、执行/记录文件）。人员离场后的清理工作开展不规范，可能导致遗留外部人员访问受控区域的记录，存在被二次非法利用，造成泄密。 低风险。

3.9 安全建设管理

3.9.1 已有安全控制措施汇总分析

安全通用要求

定级和备案	
a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；	
制度文件、执行/记录文件	（1）单位的被测系统于2022年4月已完成备案； （2）系统备案相关文档（定级报告）中明确等级划分方法和理由，SAG三个方面的级别描述清晰； （3）管理文件详见《定级备案》。
b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；	
制度文件、执行/记录文件	(1)单位针对系统定级结果的审批及评审工作等要求,制定了管理制度; （2）现有系统的定级已具备合理性和正确性审定； （3）管理文件详见《定级备案》。
c) 应保证定级结果经过相关部门的批准；	
制度文件、执行/记录文件	（1）单位针对系统定级结果的上级批准要求，制定了管理制度； （2）现有系统的定级获得了相关部门的批准； （3）管理文件详见《定级备案》。
d) 应将备案材料报主管部门和相应公安机关备案。	
制度文件、执行/记录文件	（1）单位对被测系统的等级备案表、定级报告等备案材料已经报相应公安机关备案； （2）单位具备公安机关出具的备案号； （3）管理文件详见《定级备案》。
产品采购和使用	
a) 应确保网络安全产品采购和使用符合国家的有关规定；	
制度文件、执行/记录文件	（1）单位已建立安全产品管理的相关管理规定； （2）单位具备安全产品采购流程及相关实施文档； （3）被测系统使用的安全产品具备销售许可资质； （4）安全产品具均为国内产品； （5）管理文件详见《设备安全管理制度》。
b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。	
制度文件、执行/记录文件	（1）单位已建立密码产品与服务管理的相关管理制度； （2）系统未使用密码产品； （3）管理文件详见《设备安全管理制度》。
外包软件开发	
b) 应保证开发单位提供软件设计文档和使用指南。	
制度文件、执行/记录文件	（1）单位制定软件开发项目验收要求，明确开发单位的提交材料； （2）开发单位提供软件日常维护和使用所需的文档； （3）管理文件详见《外包开发软件管理规定》、《设备及系统软件配置和操作手册》。
工程实施	
a) 应指定或授权专门的部门或人员负责工程实施过程的管理；	
制度文件、执行/记录文件	（1）单位针对专门的部门负责工程实施过程的管理要求，制定管理度； （2）单位由专岗负责系统建设的工程实施，且按照实施方案的要求对进度和质量进行控制；

	（3）管理文件详见《工程实施管理制度》。
b）应制定安全工程实施方案控制工程实施过程。	
制度文件、执行/记录文件	（1）单位制定了详细的工程实施方案； （2）工程实施单位严格按照方案执行，并有过程记录； （3）管理文件详见《测试及验收方案》、《工程项目实施方案》。
系统交付	
a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；	
制度文件、执行/记录文件	（1）单位具备系统交付清单； （2）系统交付清单内容较详细； （3）单位的清点工作较合规； （4）管理文件详见《系统交付管理》、《资产清单》。
b）应对负责运行维护的技术人员进行相应的技能培训；	
制度文件、执行/记录文件	（1）单位已对负责系统运行维护的技术人员进行了技能培训； （2）具备运维人员的培训记录； （3）管理文件详见《系统交付管理》、《资产清单》、《系统交付清单》、《技能培训记录》。
c）应提供建设过程文档和运行维护文档。	
制度文件、执行/记录文件	（1）单位提供了系统建设过程中的文档； （2）单位提供了指导用户进行系统运维的文档和系统培训手册； （3）管理文件详见《系统交付管理》、《系统交付清单》、《设备及系统软件配置和操作手册》。
等级测评	
a）应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；	
制度文件、执行/记录文件	（1）单位针对系统等级测评要求，制定管理制度； （2）系统按要求开展首次测评工作； （3）管理文件详见《系统安全管理制度》。
b）应在发生重大变更或级别发生变化时进行等级测评；	
制度文件、执行/记录文件	（1）管理制度中已规定在系统发生变更时及时对系统进行等级测评； （2）系统未发生过重大变更，系统等级未发生变化； （3）管理文件详见《系统安全管理制度》。
c）应确保测评机构的选择符合国家有关规定。	
制度文件、执行/记录文件	（1）已选择在“全国等级保护测评机构推荐目录”中的测评单位进行等级测评； （2）管理文件详见《系统安全管理制度》、《网络安全等级保护测评服务合同》。
服务供应商选择	
a）应确保服务供应商的选择符合国家的有关规定；	
制度文件、执行/记录文件	（1）单位在管理制度内明确提出安全服务供应商选择的要求； （2）单位选择的安全服务商符合国家的有关规定，具备相应的安全服务资质； （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。
b）应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。	
制度文件、执行/记录文件	（1）单位的管理制度中已规定，需与安全服务商签订安全相关的协议并

	明确整个服务供应链各方需履行的网络安全相关义务； （2）单位已按规定与选定的安全服务商签订合规的协议； （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。

3.9.2 主要安全问题汇总分析

安全通用要求

（1）单位未具备适用于被测系统的安全规划设计方案（如：制度文件、执行/记录文件）。规划设计需求不全面，可能导致安全方案设计不完善，信息系统存在安全缺陷。低风险。

（2）单位未具备完整的安全设计方案相关的文档。单位相关方案的设计的内容不够完善（如：制度文件、执行/记录文件）。相关合规的规划配套文件缺失，可能导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。 中风险。

（3）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定。单位未对相关论证过程及内容进行完整的记录（如：制度文件、执行/记录文件）。未开展规范的审批过程，可能存在安全整体规划缺乏合理性和可行性，导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。 低风险。

（4）单位未在软件开发过程中对所有软件安全性进行测试。单位未在软件安装之前按要求对所有软件开展恶意代码检测（如：制度文件、执行/记录文件）。软件交付前恶意代码检测不规范，可能在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。 低风险。

（5）单位未完全根据测试验收方案组织相关部门和人员开展验收工作（如：制度文件、执行/记录文件）。可能由于验收测试不严谨，造成测试过程缺乏计划性及操作性，无法保证经过测试验收的系统达到既定的安全性等目标。 低风险。

(6)针对系统上线前的安全性测试工作存在问题(如:制度文件、执行/记录文件)。未按规定开展上线前测试，安全隐患可能在系统上线运行前未被发现并作出相应处理。低风险。

3.10 安全运维管理

3.10.1 已有安全控制措施汇总分析

安全通用要求

环境管理	
a) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；	
制度文件、执行/记录文件	（1）单位建立机房安全方面的管理制度，对有关运维方面的管理作出规定； （2）单位具备完整的机房出入登记记录； （3）单位具备完整的机房基础设施的维护记录； （4）管理文件详见《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。
b) 应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；	
制度文件、执行/记录文件	（1）单位建立机房安全方面的管理制度； （2）单位现有机房管理记录与制度相符； （3）制度详见：《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。
c) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	
制度文件、执行/记录文件	（1）单位机房安全管理制度已明确来访人员的接待区域的要求； （2）单位按规范要求开展人员来访接待； （3）单位办公环境未发现有随意放置含有敏感信息介质的情况； （4）制度详见：《机房安全管理制度》、《物理安全管理规范》、《办公环境保密管理》。
资产管理	
应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。	
制度文件、执行/记录文件	（1）单位已建立有效的资产清单； （2）单位现有资产清单内容较全面； （3）制度详见：《设备安全管理制度》、《资产清单》。
介质管理	
a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；	
制度文件、执行/记录文件	（1）介质按管理要求放置于受控的环境中（如：机房）；

	（2）介质管理具备较全面的记录； （3）制度详见：《设备安全管理制度》、《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。
b）应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。	
制度文件、执行/记录文件	（1）介质管理制度中对介质安全传输有明确规定； （2）存储重要信息的介质在物理传输过程，具备严格的环节控制，无重大环节疏漏； （3）对介质的归档和查询均具备记录； （4）制度详见：《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。
设备维护管理	
a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	
制度文件、执行/记录文件	（1）单位人员岗位职责相关文档已明确设备维护管理的责任部门； （2）单位对各类设施、设备进行定期维护； （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。
b）应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。	
制度文件、执行/记录文件	（1）单位建立了配套设施、软硬件维护管理方面的管理制度； （2）单位开展相关工作与制度相符，且保留记录； （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。
网络和系统安全管理	
a）应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；	
制度文件、执行/记录文件	（1）单位建立系统安全管理文档，对系统管理员的管理制定了要求； （2）单位对各类关键角色建立了相应的工作职责文档； （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。
b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	
制度文件、执行/记录文件	（1）单位制定管理制度，对系统账号进行管理； （2）单位按管理规范开展账号管理工作； （3）账户管理记录内容较完整； （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。
c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	
制度文件、执行/记录文件	（1）单位建立了网络和系统安全管理制度； （2）网络和系统安全管理制度内容较全面； （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。
d）应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；	

制度文件、执行/记录文件	（1）单位对重要设备、系统的配置和操作建立配置手册； （2）现有操作配置手册已明确操作步骤、参数配置； （3）制度详见：《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。
e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。	
制度文件、执行/记录文件	（1）单位制定日常运维管理的相关制度规范； （2）单位按制度规范开展日常运维管理工作； （3）单位具备合规的运维记录； （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》、《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。
恶意代码防范管理	
a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	
制度文件、执行/记录文件	（1）单位制定恶意代码防范管理制度，明确对外来计算机或存储设备接入系统前进行恶意代码检查； （2）单位按外来计算机接入恶意代码检查规范开展工作； （3）单位制定培训管理制度，明确需通过培训提升员工的防恶意代码意识； （4）单位按培训管理要求开展工作； （5）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申请表》、《信息管理系统漏洞检查表》。
b) 应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；	
制度文件、执行/记录文件	（1）建立恶意代码防范管理文档； （2）管理制度中覆盖防恶意代码软件的授权使用、恶意代码库升级、定期查杀等内容； （3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》。
配置管理	
应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。	
制度文件、执行/记录文件	（1）单位制定了基本配置信息管理的制度要求； （2）管理文件详见：《主机安全管理规范》、《网络安全管理规范》、《应用安全管理规范》、《网络配置信息》。
变更管理	
应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。	
制度文件、执行/记录文件	（1）单位建立了关于系统变更管理的制度文件； （2）现有变更管理制度覆盖了变更管理的各方面要求； （3）制度详见：《变更控制管理制度》、《通用变更记录表》。
备份与恢复管理	
a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；	
制度文件、执行/记录文件	（1）单位根据业务重要程度，制定了需要定期备份的重要业务信息列表或清单。清单内需要定期备份的重要数据已经过用户方确认； （2）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。

b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等；	
制度文件、执行/记录文件	(1) 单位建立了备份与恢复管理相关的安全管理制度； (2) 备份与恢复管理的相关要求比较明确； (3) 制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。
c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	
制度文件、执行/记录文件	(1) 单位现有管理制度，明确了数据备份策略和数据恢复策略，以及备份程序和恢复程序； (2) 单位可按策略要求实现重要数据的定期备份与恢复性测试； (3)单位现有的备份的数据均经过恢复性测试,可确保备份的数据可用； (4) 制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。
安全事件处置	
a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件；	
制度文件、执行/记录文件	(1)单位已在安全培训及宣传过程中告知用户在发现安全弱点和可疑事件时及时向安全管理部门报告； (2)单位在系统运维过程中对发现的安全弱点和可疑事件均编制了对应的报告或相关文档； (3) 单位现有安全弱点和可疑事件报告文档内容较详实； (4) 制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。
b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；	
制度文件、执行/记录文件	(1) 单位制定了安全事件报告和处置管理制度； (2) 现有安全事件管理制度内容较完整； (3) 制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。
c) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。	
制度文件、执行/记录文件	(1) 单位具备对安全事件的分析、处理、总结、防范等的报告／过程文档； (2) 单位提供的安全事件报告和响应处置记录内容较完整； (3) 制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。
应急预案管理	
a) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；	
制度文件、执行/记录文件	(1) 单位制定重要事件的应急预案； (2) 单位现有应急预案涉及的类型范围较全面； (3) 单位现有应急预案的内容较完整； (4) 制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。
b) 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。	
制度文件、执行/记录文件	(1) 单位定期对相关人员进行应急预案培训； (2) 单位根据不同的应急预案，按要求进行应急演练； (3) 单位具备近期应急预案工作开展的相关记录； (4) 单位提供的应急预案培训记录比较完整； (5) 单位提供的应急预案演练记录比较完整；

	（6）经检查单位目前一旦出现应急事件，可参照预案合理有序的进行应急事件处置过程； （7）制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。

3.10.2 主要安全问题汇总分析

安全通用要求

（1）单位未严格按规范开展漏洞及安全隐患检测工作（如：制度文件、执行/记录文件）。漏洞检测、修补工作不到位，可能存在未授权人员利用漏洞攻击信息系统的风险。 低风险。

（2）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作（如：制度文件、执行/记录文件）。可能导致系统恶意代码检测管理不到位，存在信息系统感染恶意代码，从而导致严重的信息安全风险。 低风险。

（3）单位不了解现有密码相关的国家标准和行业标准。单位缺乏密码管理要求的制度文档（如：制度文件、执行/记录文件）。密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不到位，存在违反国家政策的风险。 中风险。

3.11 其他安全要求指标

3.11.1 已有安全控制措施汇总分析

本次测评未涉及其他安全要求指标。

3.11.2 主要安全问题汇总分析

本次测评未涉及其他安全要求指标。

3.12 验证测试

验证测试包括漏洞扫描，渗透测试等，验证测试发现的安全问题对应到相应的测评项的结果记录中。详细验证测试报告见报告附录。

3.12.1 漏洞扫描

3.12.1.1 漏洞扫描结果统计

本次测评主要使用了[绿盟远程安全评估系统]对系统的设备进行了安全扫描，其所涉及的系统版本为：[V6.0R04F01SP06]，规则库版本为：[V6.0R02F01.2900]。扫描结果如下：

经分析统计，共发现各接入点存在3类漏洞，其中0类危险程度为高的漏洞，0类危害程度为中的漏洞，3类危害程度为低的漏洞。

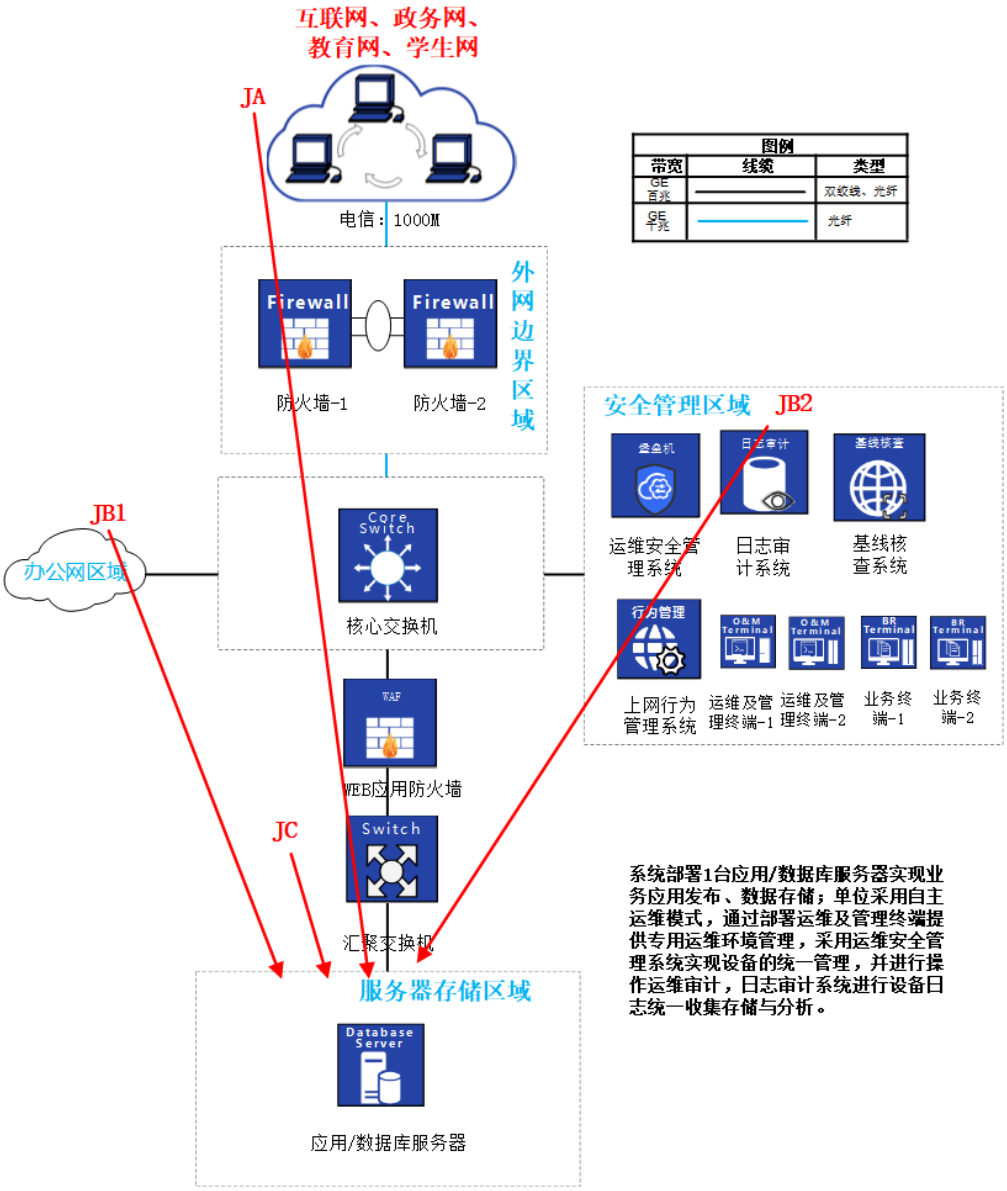


图 3-1 漏洞扫描工具接入测试示意图

接入点JA：在防火墙外侧接入，开展扫描/渗透主要目的是，探测对外服务功能区上各服务器、应用系统对外部网络边界暴露的安全漏洞情况，并根据漏洞扫描的结果接入渗透测试工具集，试图利用服务器、应用的安全漏洞入侵网络的行为。

接入点JB：在办公网区域VLAN段、安全管理区域VLAN段接入，开展扫描/渗透主要目的是，模拟外联单位/内部恶意用户发现操作系统、数据库、Web应用、第三方产品等安全漏洞的过程，并尝试利用以上漏洞实施诸如获取系统控制权（GetShell）、获得大量敏感信息（DragLibrary）等模拟攻击行为。

接入点JC：在系统所在VLAN的交换机接入，开展扫描/渗透主要目的是，直接测试对服务功能区上各服务器在最小化防御的基础上，对网络暴露的安全漏洞情况。

（1）接入点A漏洞扫描结果统计

根据在接入点A对14台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-1 接入点 A 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	0	0	0	0
2	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	0	0	0	0
3	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	0	0	0	0
4	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	0	0	0	0
5	172.16.1.14/上网行为管理系统	(安全设备)深信服AC12.0.26	0	0	0	0
6	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	0	0	0	0
7	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	0	0	0	0
8	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	0	0	0	0
9	192.168.33.11/业务终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
10	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
11	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
12	192.168.33.10/业务终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
13	10.1.4.10/应用/数据库服务器	(服务器存储设备)CentOS 7.7	0	0	0	0
14	https://w.mmpt.edu.cn/招生信息网系统	(业务应用软件平台) V6.0	0	0	0	0
安全漏洞数量小计			0	0	0	0

（2）接入点B漏洞扫描结果统计

根据在接入点B对14台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-2 接入点 B 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	1	0	0	1
2	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	1	0	0	1
3	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	1	0	0	1
4	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	2	0	0	2
5	172.16.1.14/上网行为管理系统	(安全设备)深信服AC12.0.26	1	0	0	1
6	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	1	0	0	1
7	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	1	0	0	1
8	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	1	0	0	1
9	192.168.33.11/业务终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
10	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
11	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10（版本 20H2（内部版本	0	0	0	0

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
		19044.1889)				
12	192.168.33.10/业务终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889)	0	0	0	0
13	10.1.4.10/应用/数据库服务器	(服务器存储设备)CentOS 7.7	3	0	0	3
14	https://w.mmpt.edu.cn/招生信息网系统	(业务应用软件平台) V6.0	0	0	0	0
安全漏洞数量小计			12	0	0	12

（3）接入点C漏洞扫描结果统计

根据在接入点C对14台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-3 接入点 C 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	1	0	0	1
2	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	1	0	0	1
3	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	1	0	0	1
4	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	2	0	0	2
5	172.16.1.14/上网行为管理系统	(安全设备)深信服 AC12.0.26	1	0	0	1
6	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	1	0	0	1
7	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	1	0	0	1
8	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	1	0	0	1
9	192.168.33.11/业务终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889)	0	0	0	0
10	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889)	0	0	0	0
11	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889)	0	0	0	0
12	192.168.33.10/业务终端-2	(终端设备) Windows 10	0	0	0	0

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
		（版本 20H2（内部版本 19044.1889）				
13	10.1.4.10/应用/数据库服务器	(服务器存储设备)CentOS 7.7	3	0	0	3
14	https://w.mmpt.edu.cn/招生信息网系统	(业务应用软件平台) V6.0	0	0	0	0
安全漏洞数量小计			12	0	0	12

3.12.1.2 漏洞扫描问题描述

通过对漏洞扫描结果进行分析,招生信息网系统存在的主要安全漏洞汇总如下表所示

表 3-4 主要安全漏洞汇总表

序号	安全漏洞名称	关联资产/域名	严重程度
1	OpenSSH CBC 模式信息泄露漏洞(CVE-2008-5161) 此类漏洞涉及服务器存储设备、网络设备。	10.1.4.10/应用/数据库服务器 172.16.1.2/核心交换机	低
2	允许Traceroute探测 此类漏洞涉及服务器存储设备、安全设备、网络设备。	10.1.4.10/应用/数据库服务器 10.2.1.4/运维安全管理系统 10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/上网行为管理系统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/汇聚交换机 172.16.1.2/核心交换机	低
3	SSH版本信息可被获取 此类漏洞涉及服务器存储设备。	10.1.4.10/应用/数据库服务器	低

3.12.2 渗透测试

经分析统计，共发现各接入点存在1类漏洞，其中0类危险程度为高的漏洞，0类危害程度为中的漏洞，1类危害程度为低的漏洞。

3.12.2.1 渗透测试过程说明

方案制定：

在得到委托单位的书面授权许可后，才进行渗透测试的实施。并且将实施范围、方法、时间、人员等具体的方案委托单位进行交流，并得到委托单位的认同。在测试实施之前，会做到让委托单位对渗透测试过程和风险的知晓，使随后的正式测试流程都在委托单位的管控下。

信息收集：

此阶段中，渗透测试人员对目标信息系统进行必要的信息收集，如操作系统类型、开放的端口和服务、中间件信息、后台数据库类型、web开发语言等，即收集有利于漏洞挖掘的相关信息，为渗透测试做准备。

漏洞挖掘方法：

此阶段中，渗透测试人员对目标信息系统开始进行渗透测试，利用已知信息和现有条件及技术进行漏洞挖掘，尽可能发现目标信息系统中存在的所有安全风险，并进行记录。

漏洞利用：

此阶段中，渗透测试人员对目标信息系统对上一阶段漏洞挖掘中发现的漏洞进行必要的利用以证明其危害性，再对渗透测试过程所产生的测试数据进行清除。

输出报告：

此阶段中，渗透测试人员把渗透测试记录、截图等相关信息进行整理，然后撰写渗透测试报告，最终提交给委托单位。

漏洞修复：

此阶段中，委托单位依据收到的渗透测试报告对其中所提出的漏洞进行整改，可参考报告中所提出的修复建议，整改完成后联系本单位相关人员准备回归测试。

回归测试：

此阶段中，渗透测试人员对整改后的目标信息系统进行复测，以确定报告中提出的漏洞是否已被修复，若已被修复，则进入下一阶段；否则，返回上一阶段。

测试工具：

序号	工具	工具用途
1	Burpsuite Pro	用于攻击Web应用程序的集成软件
2	Sqlmap	开源的自动化SQL注入工具
3	Nmap	开源的网络发现和安全审计工具
4	OWASP ZAP	自动化Web应用漏洞扫描工具
5	其他测试工具	根据信息系统的类别选择不同的工具（如自写脚本、目录扫描器、木马扫描器、其它开源工具等）

3.12.2.2 渗透测试问题描述

通过渗透测试发现，招生信息网系统存在的安全问题汇总如下表所示。

表 3-5 渗透测试结果汇总表

序号	安全问题	关联资产/域名	严重程度
1	缺少“Content-Security-Policy”响应头 此类漏洞涉及业务应用软件平台。	https://w.mmpt.edu.cn/招生信息网系统	低

3.13 单项测评小结

3.13.1 控制点符合情况汇总

根据单项测评结果汇总控制点符合情况如下表所示。（表格以不同颜色对测评结果进行区分，不符合的安全控制点采用红色标识，部分符合的采用黄色标识，不适用的采用蓝色标识且不做勾选。）

表 3-6 控制点符合情况汇总表

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
1	安全通用要求	安全物理环境	物理位置选择	√		
2			物理访问控制		√	
3			防盗窃和防破坏	√		
4			防雷击	√		
5			防火		√	
6			防水和防潮	√		
7			防静电			√
8			温湿度控制	√		
9			电力供应	√		
10			电磁防护	√		
11	安全通用要求	安全通信网络	网络架构		√	
12			通信传输	√		
13			可信验证			√
14	安全通用要求	安全区域边界	边界防护	√		
15			访问控制	√		
16			入侵防范		√	
17			恶意代码和垃圾邮件防范		√	
18			安全审计	√		
19			可信验证			√

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
20	安全通用要求	安全计算环境	身份鉴别		√	
21			访问控制	√		
22			安全审计	√		
23			入侵防范	√		
24			恶意代码防范	√		
25			可信验证			√
26			数据完整性	√		
27			数据备份恢复		√	
28			剩余信息保护	√		
29			个人信息保护	√		
30	安全通用要求	安全管理中心	系统管理		√	
31			审计管理	√		
32	安全通用要求	安全管理制度	安全策略	√		
33			管理制度	√		
34			制定和发布	√		
35			评审和修订	√		
36	安全通用要求	安全管理机构	岗位设置	√		
37			人员配备	√		
38			授权和审批	√		
39			沟通和合作	√		

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
40			审核和检查		√	
41	安全通用要求	安全管理人员	人员录用	√		
42			人员离岗	√		
43			安全意识教育和培训	√		
44			外部人员访问管理		√	
45	安全通用要求	安全建设管理	定级和备案	√		
46			安全方案设计			√
47			产品采购和使用	√		
48			自行软件开发			
49			外包软件开发		√	
50			工程实施	√		
51			测试验收		√	
52			系统交付	√		
53			等级测评	√		
54			服务供应商选择	√		
55	安全通用要求	安全运维管理	环境管理	√		
56			资产管理	√		
57			介质管理	√		
58			设备维护管理	√		
59			漏洞和风险管理			√

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
60			网络和系统安全管理	√		
61			恶意代码防范管理		√	
62			配置管理	√		
63			密码管理			√
64			变更管理	√		
65			备份与恢复管理	√		
66			安全事件处置	√		
67			应急预案管理	√		
68			外包运维管理			
安全通用要求控制点符合情况数量统计				46	13	7
控制点符合情况数量统计				46	13	7

3.13.2 安全问题汇总

针对单项测评结果中存在的部分符合和不符合项进行汇总，形成了安全问题如下表所示。

表 3-7 安全问题汇总表

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T1	（1）机房出入口未配置电子门禁系统。	信息化机房	安全通用要求	安全物理环境	物理访问控制	机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。
T2	（1）机房建设未完全采用符合耐火等级的建筑材料； （2）机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级。	信息化机房	安全通用要求	安全物理环境	防火	b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T3	（1）机房内缺乏防静电措施（如防静电地板或铺设防静电地毯 ）。	信息化机房	安全通用要求	安全物理环境	防静电	应采用防静电地板或地面并采用必要的接地防静电措施。
T4	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	安全通用要求	安全通信网络	网络架构	a）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
T5	（1）缺乏对通信设备可信验证方面的安全设计要求； （2）现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况。	安全通信网络	安全通用要求	安全通信网络	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T6	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	安全通用要求	安全区域边界	入侵防范	应在关键网络节点处监视网络攻击行为。
T7	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	安全通用要求	安全区域边界	恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。
T8	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	办公网区域 外网边界区域 安全管理区域 服务器存储区域	安全通用要求	安全区域边界	可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T9	（1）数据库系统配置不合规的密码有效周期策略。	应用/数据库服务器-MySQL	安全通用要求	安全计算环境	身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
T10	（1）设备不具备相关可信	WEB 应用防	安全通	安全计算	可信验证	可基于可信根对计算设

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
	验证的技术措施。	火墙 上网行为管理系统 基线核查系统 日志审计系统 核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2	用要求	环境		备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T11	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。	业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	安全通用要求	安全计算环境	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T12	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况； （3）现有的计算设备存在对系统运行过程中的可信检验不全面的情况； （4）现有的可信验证存在部分告警、审计及联动措施不全面的情况。	应用/数据库服务器	安全通用要求	安全计算环境	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T13	（1）未能提供数据库系统重要数据的异地定时数据备份功能。	应用/数据库服务器-MySQL	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T14	（1）未能提供中间件重要数据的异地定时数据备份功能。	应用/数据库服务器-nginx	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T15	（1）未能提供应用软件系	招生信息网系	安全通	安全计算	数据备份	b）应提供异地数据备

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
	统重要数据的异地定时数据备份功能。	统	用要求	环境	恢复	份功能，利用通信网络将重要数据定时批量传送至备用场地。
T16	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	重要业务数据重要个人信息	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T17	（1）系统管理的资源、运行及配置管理不够全面。	管理中心	安全通用要求	安全管理中心	系统管理	b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
T18	（1）单位开展的检查工作不够完善。	制度文件、执行/记录文件	安全通用要求	安全管理机构	审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。
T19	（1）单位未完全按管理规范开展人员离场后的清理工作。	制度文件、执行/记录文件	安全通用要求	安全管理人员	外部人员访问管理	c）外部人员离场后应及时清除其所有的访问权限。
T20	（1）单位未具备适用于被测系统的安全规划设计方案。	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
T21	（1）单位未具备完整的安全设计方案相关的文档； （2）单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	b）应根据保护对象的安全保护等级进行安全方案设计；
T22	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； （2）单位未对相关论证过程及内容进行完整的记录。	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	c）应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。
T23	（1）单位未在软件开发过程中对所有软件安全性进行测试； （2）单位未在软件安装之前按要求对所有软件开展	制度文件、执行/记录文件	安全通用要求	安全建设管理	外包软件开发	a）应在软件交付前检测其中可能存在的恶意代码；

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
	恶意代码检测。					
T24	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	安全通用要求	安全建设管理	测试验收	a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；
T25	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	安全通用要求	安全建设管理	测试验收	b）应进行上线前的安全性测试，并出具安全测试报告。
T26	（1）单位未严格按规范开展漏洞及安全隐患检测工作。	制度文件、执行/记录文件	安全通用要求	安全运维管理	漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。
T27	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	安全通用要求	安全运维管理	恶意代码防范管理	c）应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。
T28	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	制度文件、执行/记录文件	安全通用要求	安全运维管理	密码管理	a）应遵循密码相关国家标准和行业标准；

4 整体测评

从安全控制间、区域间和验证测试等方面对单元测评的结果进行验证、分析和整体评价。

具体内容参见《GB/T 28448-2019信息安全技术 网络安全等级保护测评要求》。

4.1 安全控制点间安全测评

安全控制间的安全测评主要考虑同一区域内、同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用。安全功能上的增强和补充可以使两个不同强度、不

同等级的安全控制发挥更强的综合效能,可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。

4.1.1 安全建设管理

4.1.1.1 安全通用要求

（T24）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。

单位未具备适用于被测系统的安全规划设计方案。安全方案设计不完善，导致规划设计需求不全面，信息系统存在安全缺陷。可升高单位未完全根据测试验收方案组织相关部门和人员开展验收工作的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

（T25）针对系统上线前的安全性测试工作存在问题。

单位未在软件交付之前按要求对所有软件开展恶意代码检测,导致在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。可升高针对系统上线前的安全性测试工作存在问题的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

4.1.2 安全运维管理

4.1.2.1 安全通用要求

（T27）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。

单位未严格按规范开展漏洞及安全隐患检测工作，漏洞检测工作不到位，导致存在未授权人员利用漏洞攻击信息系统的风险。可升高单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

4.2 区域间安全测评

区域间的安全测评主要考虑互连互通（包括物理上和逻辑上的互连互通等）的不同区域之间存在的安全功能增强、补充和削弱等关联作用，特别是有数据交换的两个不同区域。

4.2.1 安全物理环境

4.2.1.1 安全通用要求

（T1）机房出入口未配置电子门禁系统。

机房所在位置处于内部受控区域，非授权人员无法随意通过现有控制措施（如机械锁）进出机房，且具备相对完善的机房出入管理要求（具备《机房安全管理制度》），并实际执行措施效果良好（具备《机房出入登记表》），可降低机房出入口访问控制措施缺失的问题严重程度（如信息化机房）。根据整体测评分析，问题严重程度变化为降低。

4.2.2 安全通信网络

4.2.2.1 安全通用要求

（T4）关键的应用服务和数据库服务网段未独立进行子网划分的情况。

单位有完整的IP地址规范，对IP地址的使用、回收均有记录《资产清单》，且系统具备相对完善的设备自身访问控制策略管理要求（具备《网络安全管理规范》、《设备及系统软件配置和操作手册》），措施效果良好，有助于部分补充未划分子网的安全功能不足（如安全通信网络）。根据整体测评分析，问题严重程度变化为降低。

4.2.3 安全区域边界

4.2.3.1 安全通用要求

（T6）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。

网络环境划分了相应的安全区域，区域间具备有效的访问控制措施，区域内各主机设备部署深信服EDR单机版，策略库、规则库更新及时，能够对攻击行为进行检测、阻断或限制，实际措施效果良好，且系统具备相对完善的策略库、规则库更新/校准管理要求，管理措施效果良好且及时检查更新有效性（具备《漏洞检测报告》、《主机安全管理规范》），可降低外部网络攻击防御措施缺失的问题严重程度（如办公网区域、安全管理区域）。根据整体测评分析，问题严重程度变化为降低。

（T7）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。

系统部署于可控的网络环境内（具备有效的访问控制、入侵防护措施）限制相关主机对象访问非受控网络，操作系统层面配置防御策略（具备本地防火墙策略、核心交换机地址限制策略、部署深信服EDR单机版），恶意代码入侵的可能性相对较低，可降低恶意代码防范措施缺失的问题严重程度（如办公网区域、安全管理区域）。根据整体测评分析，问题严重程度变化为降低。

4.2.4 安全计算环境

4.2.4.1 安全通用要求

（T9）数据库系统配置不合规的密码有效周期策略。

单位管理制度中明确规定密码长度、复杂度及有效期要求《应用安全管理规范》、《设备及系统软件配置和操作手册》，且有按照管理规定对设备密码定期更换，减轻设备存在弱口令或相同口令的风险,综合考虑风险后可降低数据库系统配置不合规的密码长度及复杂度策略的问题严重程度（如应用/数据库服务器-MySQL）。根据整体测评分析，问题严重程度变化为降低。

4.3 整体测评结果汇总

经整体测评后安全问题严重程度变化情况如下表所示

表 4-1 整体测评结果汇总表

问题编号	安全问题描述	测评对象	整体测评描述	严重程度变化
T1	（1）机房出入口未配置电子门禁系统。	信息化机房	（1）机房所在位置处于内部受控区域，非授权人员无法随意通过现有控制措施（如机械锁）进出机房，且具备相对完善的机房出入管理要求（具备《机房安全管理制度》），并实际执行措施效果良好（具备《机房出入登记表》），可降低机房出入口访问控制措施缺失的问题严重程度。	□升高 ☑降低
T4	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	（1）单位有完整的IP地址规范，对IP地址的使用、回收均有记录《资产清单》，且系统具备相对完善的设备自身访问控制策略管理要求（具备《网络安全管理规范》、《设备及系统软件配置和操作手册》），措施效果良好，有助于部分补充未划分子网的安全功能不足。	□升高 ☑降低
T6	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	（1）网络环境划分了相应的安全区域，区域间具备有效的访问控制措施，区域内各主机设备部署深信服EDR单机版，策略库、规则库更新及时，能够对攻击行为进行检测、阻断或限制，实际措施效果良好，且系统具备相对完善的策略库、规则库更新/校准管理要求，管理措施效果良好且及时检查更新有效性（具备《漏洞检测报告》、《主机安全管理规范》），可降低外部网络攻击防御措施缺失的问题严重程度。	□升高 ☑降低
T7	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	（1）系统部署于可控的网络环境内（具备有效的访问控制、入侵防护措施）限制相关主机对象访问非受控网络，操作系统层面配置防御策略（具备本地防火墙策略、核心交	□升高 ☑降低

问题编号	安全问题描述	测评对象	整体测评描述	严重程度变化
			换机地址限制策略、部署深信服EDR单机版），恶意代码入侵的可能性相对较低，可降低恶意代码防范措施缺失的问题严重程度。	
T9	（1）数据库系统配置不合规的密码有效周期策略。	应用/数据库服务器-MySQL	（1）单位管理制度中明确规定密码长度、复杂度及有效期要求《应用安全管理规范》、《设备及系统软件配置和操作手册》，且有按照管理规定对设备密码定期更换，减轻设备存在弱口令或相同口令的风险，综合考虑风险后可降低数据库系统配置不合规的密码长度及复杂度策略的问题严重程度。	□升高 ☑降低
T24	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	（1）单位未具备适用于被测系统的安全规划设计方案。安全方案设计不完善，导致规划设计需求不全面，信息系统存在安全缺陷。可升高单位未完全根据测试验收方案组织相关部门和人员开展验收工作的问题严重程度。	☑升高 □降低
T25	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	（1）单位未在软件交付之前按要求对所有软件开展恶意代码检测，导致在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。可升高针对系统上线前的安全性测试工作存在问题的问题严重程度。	☑升高 □降低
T27	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	（1）单位未严格按规范开展漏洞及安全隐患检测工作，漏洞检测工作不到位，导致存在未授权人员利用漏洞攻击信息系统的风险。可升高单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作的问题严重程度。	☑升高 □降低

5 安全问题风险分析

针对等级测评结果中存在的所有安全问题，结合关联资产和威胁分别分析安全问题可能产生的危害结果，找出可能对系统、单位、社会及国家造成的最大安全危害（损失），

并根据最大安全危害(损失)的严重程度进一步确定安全问题的风险等级,结果为“高”、“中”或“低”。最大安全危害（损失）结果应结合安全问题所影响业务的重要程度、相关系统组件的重要程度、安全问题严重程度以及安全事件影响范围等进行综合分析。

表 5-1 安全问题风险分析

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
1	安全物理环境	（1）机房出入口未配置电子门禁系统。	信息化机房	物理攻击	（1）上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域，可能对系统的平稳运行造成影响。	中风险
2	安全物理环境	（1）机房建设未完全采用符合耐火等级的建筑材料; （2）机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级。	信息化机房	物理环境影响	（1）存在发生火情时助燃火灾的风险。	低风险
3	安全物理环境	（1）机房内缺乏防静电措施(如防静电地板或铺设防静电地毯 ）。	信息化机房	软硬件故障	（1）存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。	中风险
4	安全通信网络	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	恶意攻击	（1）上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变得更为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。	中风险
5	安全通信网络	（1）缺乏对通信设备可信验证方面的安全设计要求; （2）现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况。	安全通信网络	恶意攻击	（1）缺乏对系统可执行程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致计算资源被干扰和破坏造成损失。	低风险
6	安全区域	（1）网络层部署防火墙,	办公网区域	恶意	（1）存在不能及时发现内	中风

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
	边界	防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	安全管理区域	攻击	部主机作为攻击跳板，或网络攻击行为而造成系统损坏/网络资源浪费的风险。	险
7	安全区域边界	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	恶意攻击	（1）无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。	中风险
8	安全区域边界	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	办公网区域 外网边界区域 安全管理区域 服务器存储区域	恶意攻击	（1）缺乏对边界设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险
9	安全计算环境	（1）数据库系统配置不合规的密码有效周期策略。	应用/数据库服务器-MySQL	恶意攻击	（1）上述问题的存在，使恶意用户能够较为容易的访问数据库等资源并实施恶意操作，对相关系统的正常运行造成影响，存在系统被未授权访问、操作的可能性。	中风险
10	安全计算环境	（1）设备不具备相关可信验证的技术措施。	WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2	恶意攻击	（1）缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险
11	安全计算环境	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。	业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	恶意攻击	（1）缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险
12	安全计算	（1）缺乏对计算设备可	应用/数据库服务	恶意	（1）缺乏对计算设备的相	低风

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
	环境	信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况； （3）现有的计算设备存在对系统运行过程中的可信检验不全面的情况； （4）现有的可信验证存在部分告警、审计及联动措施不全面的情况。	器	攻击	关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	险
13	安全计算环境	（1）未能提供数据库系统重要数据的异地定时数据备份功能。	应用/数据库服务器-MySQL	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供，使企业的经济利益或声誉受到损害。	中风险
14	安全计算环境	（1）未能提供中间件重要数据的异地定时数据备份功能。	应用/数据库服务器-nginx	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。	中风险
15	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	招生信息网系统	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。	中风险
16	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	重要业务数据 重要个人信息	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。	中风险
17	安全管理中心	（1）系统管理的资源、运行及配置管理不够全面。	管理中心	恶意攻击	（1）系统的资源和运行缺少统一的管理，将导致系统可能无法按规划实现基于资源配置、 系统加载、异常处理、及备份/恢复等的安全控制措施。	低风险
18	安全管理机构	（1）单位开展的检查工作不够完善。	制度文件、执行/记录文件	管理不到	（1）检查工作开展不仔细，可能对存在或潜在的	低风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
				位	安全风险不能被及时发现并进行处理。	
19	安全管理人员	（1）单位未完全按管理规范开展人员离场后的清理工作。	制度文件、执行/记录文件	管理不到位	（1）人员离场后的清理工作开展不规范，可能导致遗留外部人员访问受控区域的记录，存在被二次非法利用，造成泄密。	低风险
20	安全建设管理	（1）单位未具备适用于被测系统的安全规划设计方案。	制度文件、执行/记录文件	管理不到位	（1）规划设计需求不全面，可能导致安全方案设计不完善，信息系统存在安全缺陷。	低风险
21	安全建设管理	（1）单位未具备完整的安全设计方案相关的文档； （2）单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	管理不到位	（1）相关合规的规划配套文件缺失，可能导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。	中风险
22	安全建设管理	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； （2）单位未对相关论证过程及内容进行完整的记录。	制度文件、执行/记录文件	管理不到位	（1）未开展规范的审批过程，可能存在安全整体规划缺乏合理性和可行性，导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。	低风险
23	安全建设管理	（1）单位未在软件开发过程中对所有软件安全性进行测试； （2）单位未在软件安装之前按要求对所有软件开展恶意代码检测。	制度文件、执行/记录文件	管理不到位	（1）软件交付前恶意代码检测不规范，可能在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。	低风险
24	安全建设管理	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	管理不到位	（1）可能由于验收测试不严谨，造成测试过程缺乏计划性及操作性，无法保证经过测试验收的系统达到既定的安全性等目标。	低风险
25	安全建设管理	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	管理不到位	（1）未按规定开展上线前测试，安全隐患可能在系统上线运行前未被发现并作出相应处理。	低风险
26	安全运维管理	（1）单位未严格按规范开展漏洞及安全隐患检测工作。	制度文件、执行/记录文件	管理不到位	（1）漏洞检测、修补工作不到位，可能存在未授权人员利用漏洞攻击信息系	低风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
					统的风险。	
27	安全运维管理	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	管理不到位	（1）可能导致系统恶意代码检测管理不到位，存在信息系统感染恶意代码，从而导致严重的信息安全风险。	低风险
28	安全运维管理	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	制度文件、执行/记录文件	管理不到位	（1）密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不到位，存在违反国家政策的风险。	中风险

6 等级测评结论

等级测评结论由安全问题风险分析结果和综合得分共同确定，判定依据如下表所示。

表 6-1 等级测评结论判别依据

测评结论	判别依据
优	被测对象中存在安全问题，但不会导致被测对象面临中、高等级安全风险，且系统综合得分 90 分以上（含90 分）。
良	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分 80分以上（含 80分）。
中	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分 70分以上（含 70分）
差	被测对象中存在安全问题，而且会导致被测对象面临高等级安全风险，或被测对象综合得分低于 70 分。

综合得分计算方法如下：

设M为被测对象的综合得分，$M = V_t + V_m$，V_t和V_m根据下列公式计算。

$$V_t = \begin{cases} 100 \cdot y - \sum_{k=1}^{t} f(\omega_k) \cdot (1 - x_k) \cdot S, & V_t > 0 \\ 0, & V_t \leq 0 \end{cases}$$

$$V_m = \begin{cases} 100 \cdot (1-y) - \sum_{k=1}^{m} f(\omega_k) \cdot (1-x_k) \cdot S, & V_m > 0 \\ 0, & V_m \le 0 \end{cases}$$

$$0 \le x_k \le 1,\ S = 100 \cdot \frac{1}{n},\ f(\omega_k) = \begin{cases} 1, & \omega_k = \text{一般} \\ 2, & \omega_k = \text{重要} \\ 3, & \omega_k = \text{关键} \end{cases}$$

其中，y为关注系数，取值在0至1之间，由等级保护工作管理部门给出，默认值为0.5。n为被测对象涉及的总测评项数（不含不适用项，下同），t为技术方面对应的总测评项数，V_t为技术方面的得分，m为管理方面对应的总测评项数，V_m为管理方面的得分，ω_k为测评项k的重要程度（分为一般、重要和关键），x_k为测评项k的得分，如果测评项k涉及多测评项对象，则x_k取值为多测评对象得分的算术平均值。

x_k的得分计算如下：

测评项k涉及对象 / 测评项k定性判定	只涉及单个对象	涉及多个对象
符合	1	1
部分符合	0.5	计算测评对象平均分，取值在0至1之间
不符合	0	0

注：当测评项k涉及多个对象时，针对每个对象的得分取值为1、0.5和0。

根据第5章安全问题风险分析结果统计高、中、低风险安全问题的数量，利用综合得分计算公式计算出被测对象的综合得分，并将相关结果填入下表。

表 6-2 安全问题统计和综合得分

被测对象名称	安全问题数量			综合得分
	高风险	中风险	低风险	
招生信息网系统	0	12	16	73.8

依据 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》和GB/T 28448—2019《信息安全技术 网络安全等级保护测评要求》的第二级要求，经对招生信息网系统的安全保护状况进行综合分析评价，等级测评结论如下：

招生信息网系统本次等级测评的综合得分为73.8，且不存在高等级安全风险，等级测评结论为中。

7 安全问题整改建议

表 7-1 安全问题整改建议

序号	安全类	安全问题	关联资产	整改建议
1	安全物理环境	(1)机房出入口未配置电子门禁系统。	信息化机房	(1) 采用电子门禁系统严格控制机房其他出入口的进出，或安排专人值守； (2) 采用电子门禁系统，对机房所有人员出入进行登记记录，并保存。
2	安全物理环境	(1)机房建设未完全采用符合耐火等级的建筑材料； (2)机房建设不具备防火设计/验收文档,或机房验收文档未明确相关建筑材料的耐火等级。	信息化机房	(1) 机房及相关的工作房间和辅助房采用具有耐火等级的建筑材料； (2) 机房建设采用符合相关耐火等级（二级）的建筑材料。（内外墙壁均应采用具有防火涂料、隔热板、铝板、钢板等阻燃或不燃的材料）； (3) 机房耐火等级建筑材料有相关合格证，并留存机房验收文档。
3	安全物理环境	(1)机房内缺乏防静电措施（如防静电地板或铺设防静电地毯）。	信息化机房	(1) 机房铺设防静电地板或铺设防静电地毯； (2) 机房房静电设计可依据GB50174-2008和GB50314-2006相关规定进行机房设计和验收。
4	安全通信网络	(1)关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	(1) 建议独立划分出应用服务器网段、数据库服务器网段。
5	安全通信网络	(1)缺乏对通信设备可信验证方面的安全设计要求；	安全通信网络	(1) 建议在管理规范文档内对通信设备可信验证方面的安全设计提出要求；

序号	安全类	安全问题	关联资产	整改建议
		(2)现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况。		（2）建议系统实现对所有可执行环节进行可信验证，包括： 运行过程中的可信检验： ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■通信应用连接过程。
6	安全区域边界	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	（1）建议网络层部署的防火墙配置对内部发起的攻击行为实现防范功能策略，实现检测、防止或限制从内部发起的网络攻击行为； （2）内部安全防范措施能检测以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、碎片攻击、网络蠕虫攻击、应用漏洞攻击。
7	安全区域边界	(1)现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	（1）建议现有部署的恶意代码防范措施网络边界覆盖全面，及时对恶意代码及逆行检测和清除。
8	安全区域边界	(1)缺乏对边界设备可信验证方面的安全设计要求； (2)现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）建议对边界设备系统程序的可信验证设计并保存设计文件； （2）建议系统实现对所有可执行环节进行可信验证。
9	安全计算环境	(1)数据库系统配置不合规的密码有效周期策略。	应用/数据库服务器-MySQL	（1）建议数据库配置‘default_password_lifetime‘；默认密码有效期不为0（具体有效期视业务需求定，一般情况可参考设为90-180天）。
10	安全计算环境	(1)设备不具备相关可信验证的技术措施。	WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2	（1）建议通过设备的启动过程和运行过程中对预装软件（包括系统引导程序、系统程序、相关应用程序和重要配置参数）的完整性验证或检测，确保对系统引导程序、系统程序、重要配置参数和关键应用程序可信根验证； （2）建议设备启用在检测到其可信性受到破坏后进行报警的相关功能。
11	安全计算	(1)缺乏对计算设备可信验	业务终端-1	（1）建议对计算设备系统程序的可信

序号	安全类	安全问题	关联资产	整改建议
	环境	证方面的安全设计要求； (2)现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。	业务终端-2 运维及管理终端-1 运维及管理终端-2	验证设计并保存设计文件； （2）建议系统实现对所有可执行环节进行可信验证。
12	安全计算环境	(1)缺乏对计算设备可信验证方面的安全设计要求； (2)现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况； (3)现有的计算设备存在对系统运行过程中的可信检验不全面的情况； (4)现有的可信验证存在部分告警、审计及联动措施不全面的情况。	应用/数据库服务器	（1）建议对计算设备系统程序的可信验证设计并保存设计文件； （2）建议系统实现对所有可执行环节进行可信验证。
13	安全计算环境	(1)未能提供数据库系统重要数据的异地定时数据备份功能。	应用/数据库服务器-MySQL	（1）建议设置异地灾备机房，并利用通信网络将重要数据定时备份至备份场地； （2）异地备份的数据范围（不限于）包括系统的： ■配置数据 ■重要业务数据。
14	安全计算环境	(1)未能提供中间件重要数据的异地定时数据备份功能。	应用/数据库服务器-nginx	（1）建议设置异地灾备机房，并利用通信网络将中间件重要数据定时备份至备份场地； （2）异地备份的中间件数据范围（不限于）包括系统的： ■配置数据 ■重要日志数据。
15	安全计算环境	(1)未能提供应用软件系统重要数据的异地定时数据备份功能。	招生信息网系统	（1）建议设置异地灾备机房，并利用通信网络将应用软件系统重要数据定时备份至备份场地； （2）异地备份的应用软件系统数据范围（不限于）包括系统的：配置数据、重要日志数据，业务数据。
16	安全计算环境	(1)未能提供应用软件系统重要数据的异地定时数据备份功能。	重要业务数据 重要个人信息	（1）建议设置异地灾备机房，并利用通信网络将应用软件系统重要数据定时备份至备份场地。
17	安全管理中心	（1）系统管理的资源、运行及配置管理不够全面。	管理中心	（1）需实现系统包括对可信证书管理、可信基准库的管理。

序号	安全类	安全问题	关联资产	整改建议
18	安全管理机构	(1)单位开展的检查工作不够完善。	制度文件、执行/记录文件	(1) 建议单位按要求提供安全检查报告。
19	安全管理人员	(1)单位未完全按管理规范开展人员离场后的清理工作。	制度文件、执行/记录文件	(1) 建议单位按管理规范开展人员离场后的清理工作。至少包括：保留清理记录、及时清除离场后的所有访问权限、记录访问权限清除时间。
20	安全建设管理	(1)单位未具备适用于被测系统的安全规划设计方案。	制度文件、执行/记录文件	(1) 建议单位根据等保要求进行过全面的自查或对比，根据系统的安全级别选择基本安全措施； (2) 建议规划方案需根据风险分析结果对系统安全措施进行补充和整，并在系统建设\\整改方案中有详细描述。
21	安全建设管理	(1)单位未具备完整的安全设计方案相关的文档； (2)单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	(1) 建议单位根据信息系统的等级划分情况，准备安全设计方案、安全管理策略、安全建设规划文档等； (2) 建议相关文档内容应完善，包括统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、密码技术要求、总体建设规划和详细设计方案，并形成一致性的配套文件。
22	安全建设管理	(1) 单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； (2)单位未对相关论证过程及内容进行完整的记录。	制度文件、执行/记录文件	(1) 建议单位组织相关部门和安全技术专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定； (2) 保存论证和审定记录，记录包括批准时间、批准人员签字； (3) 文件经过批准后，才能正式实施。
23	安全建设管理	(1)单位未在软件开发过程中对所有软件安全性进行测试； (2)单位未在软件安装之前按要求对所有软件开展恶意代码检测。	制度文件、执行/记录文件	(1) 建议开发商提供软件源代码，软件安装前检测软件中的恶意代码； (2) 输出检测报告（或提供第三方检测报告），内容包括测试时间、测试地点、测试对象、测试结论、测试人员。
24	安全建设管理	(1)单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	(1) 建议根据测试验收过程记录与结果，形成测试验收报告。
25	安全建设管理	(1)针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	(1) 建议系统建设完成后，委托第三方测试单位对系统进行安全性测试，并出具安全性测试报告； (2) 测试报告内容至少包括测试时间、测试地点、测试人、测试对象、测试方法、测试过程、测试发现的安全问题、

序号	安全类	安全问题	关联资产	整改建议
				整改建议、测试结论，并有第三方测试机构的签字盖章。
26	安全运维管理	(1)单位未严格按规范开展漏洞及安全隐患检测工作。	制度文件、执行/记录文件	（1）建议单位定期开展漏洞扫描，对发现的安全漏洞和隐患进行及时修补评估； （2）对必需修补的安全漏洞和隐患进行加固测试，测试无误后，备份系统数据，再从生产环境进行修补； （3）对于剩余安全漏洞和隐患进行残余风险分析，明确安全风险整改原则。
27	安全运维管理	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	（1）建议单位按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。包括;定期对相关产品的恶意代码库进行升级；对相关设备升级情况进行记录；对各类防病毒产品上截获的恶意代码进行分析并汇总上报； （2）单位需保留完整的恶意代码检测/升级的记录。至少具备：执行人、升级结果/检测结果、处理方式、负责人签字 。
28	安全运维管理	(1)单位不了解现有密码相关的国家标准和行业标准； (2)单位缺乏密码管理要求的制度文档。	制度文件、执行/记录文件	（1）建议单位学习现有密码相关的国家标准和行业标准。建立密码管理要求的制度文档。

漏洞安全问题整改建议

序号	安全类	安全问题	关联资产	整改建议
1	安全计算环境	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161) 此类漏洞涉及服务器存储设备、网络设备。	10.1.4.10/应用/数据库服务器 172.16.1.2/核心交换机	临时解决方法：* 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://downloads.ssh.com/ 对于具体Linux发行版中使用的版本，可以参考如下链接,确认系统是否受该漏洞影响: Redhat ------- https://rhn.redhat.com/errata/RHSA-2009-1287.html Suse -------

序号	安全类	安全问题	关联资产	整改建议
				http://support.novell.com/security/cve/CVE-2008-5161.html Ubuntu ------- http://people.canonical.com/~ubuntu-security/cve/2008/CVE-2008-5161.html
2	安全计算环境	允许Traceroute探测 此类漏洞涉及服务器存储设备、安全设备、网络设备。	10.1.4.10/应用/数据库服务器 10.2.1.4/运维安全管理系统 10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/ 上网行为管理系统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/ 汇聚交换机 172.16.1.2/核心交换机	在防火墙出站规则中禁用echo-reply（type 0）、time-exceeded（type 11）、destination-unreachable（type 3）类型的ICMP包。
3	安全计算环境	SSH版本信息可被获取 此类漏洞涉及服务器存储设备。	10.1.4.10/应用/数据库服务器	NSFOCUS建议您采取以下措施以降低威胁： * 修改源代码或者配置文件改变SSH服务的缺省banner。
4	安全计算环境	缺少“Content-Security-Policy”响应头 此类漏洞涉及业务应用软件平台。	https://w.mmpt.edu.cn/招生信息网系统	在服务器中配置Content-Security-Policy响应头为“default-src 'self’ ”。

【正文结束】

附录A 被测对象资产

A.1 物理机房

附录A 表- 1物理机房

序号	机房名称	物理位置	重要程度
1	信息化机房	茂名市茂南区文明北路232号大院大楼	关键

A.2 网络设备

附录A 表- 2网络设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度	备注
1	核心交换机	否	H3C version 7.1.070, Release 7585P07	H3C S7500E-X	核心数据交换、访问控制	关键	
2	汇聚交换机	否	H3C version 7.1.070, Release 6126P20	H3C S5560X-30C-EI	数据交换	重要	

A.3 安全设备

附录A 表- 3安全设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度	备注
1	防火墙-1	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键	
2	运维安全管理系统	否	深信服V3.0.6	深信服AC-1000-D603-PT	运维审计	重要	
3	WEB应用防火墙	否	深信服AF 8.0.9	深信服WAF-2000-H642	应用防护、入侵防范、病毒防护	重要	
4	基线核查系统	否	深信服V3.0.3	深信服AC-1000-D602-PT	漏洞扫描	重要	
5	日志审计系统	否	深信服LAS 3.0.5	深信服AC-1000-D601-PT	日志审计	重要	
6	上网行为管理系统	否	深信服AC12.0.26	深信服AC-1000-D600-PT	上网行为管理及终端准入控制	重要	
7	防火墙-2	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键	

A.4 服务器

附录A 表-4服务器

序号	设备名称	所属业务应用系统/平台名称	是否虚拟设备	操作系统及版本	数据库管理系统及版本	中间件及版本	重要程度	备注
1	应用/数据库服务器	招生信息网系统	否	CentOS 7.7	MySQL 8.42	nginx 1.20.1	关键	

A.5 终端设备

附录A 表-5终端设备

序号	设备名称	是否虚拟设备	操作系统/控制软件及版本	用途	重要程度	备注
1	运维及管理终端-1	否	Windows 10（版本20H2（内部版本19044.1889）	运维管理、系统管理	一般	
2	业务终端-2	否	Windows 10（版本20H2（内部版本19044.1889）	业务管理	一般	
3	运维及管理终端-2	否	Windows 10（版本21H2（内部版本19044.1889））	运维管理、系统管理	一般	
4	业务终端-1	否	Windows 10（版本20H2（内部版本19044.1889）	业务管理	一般	

A.6 其他系统或设备

附录A 表-6其他系统或设备

序号	设备名称	是否虚拟设备	操作系统/控制软件及版本	用途	重要程度	备注
/	/	/	/	/	/	/

注释：本次测评对象中不涉及专用移动互联终端等，不开展抽测。

A.7 系统管理软件/平台

附录A 表-7系统管理软件/平台

序号	系统管理软件/平台名称	所在设备名称	版本	主要功能	重要程度	备注
1	应用/数据库服务器-MySQL	应用/数据库服务器	8.42	数据生产、存储	关键	

序号	系统管理软件/平台名称	所在设备名称	版本	主要功能	重要程度	备注
2	应用/数据库服务器-nginx	应用/数据库服务器	1.20.1	页面发布	关键	

A.8 业务应用软件/平台

附录A 表- 8业务应用系统/平台

序号	业务应用系统/平台名称	主要功能	业务应用软件及版本	开发厂商	重要程度
1	招生信息网系统	招生信息网系统包括轮播图管理、文档列表管理、专题管理、单页管理、栏目管理、导航管理、内容模型管理、院系专业管理、招生计划、历年录取和自助查询等功能模块，招生信息网为学院提供一个招生信息发布平台，也为有就读意向的学生提供一个了解茂名职业技术学院的平台，通过招生网，为学院和学生建立一个相互了解的通道，同时也为学院的招生工作提供了一个更高效的方式。	V6.0	广东卓锐软件有限公司	关键

A.9 数据资源

附录A 表- 9数据资源

序号	数据类别	所属业务应用	安全防护需求	重要程度
1	重要个人信息	招生信息网系统	完整性、保密性	关键
2	重要业务数据	招生信息网系统	完整性、保密性	关键
3	鉴别数据	招生信息网系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性、保密性	关键
4	重要审计数据	招生信息网系统（安全管理中心)	完整性	重要
5	重要配置数据	招生信息网系统(网络设备、安全设备、服务器存储设备、终端设备、系统	完整性	关键

序号	数据类别	所属业务应用	安全防护需求	重要程度
		管理软件平台、业务应用软件/平台)		

注释：网络设备、安全设备、服务器、终端、系统管理软件/平台和业务应用系统等所涉及的鉴别数据和重要配置数据分别在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。重要审计数据在安全管理中心进行汇总测评证据，包括数据完整性。重要业务数据和重要个人信息分别在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。

A.10 密码产品

附录A 表- 10密码产品

序号	产品/模块名称	生成厂商	商密型号	密码算法	用途	重要程度
/	/	/	/	/	/	/

注释：本次测评不存在加密机等密码产品。

A.11 安全相关人员

附录A 表- 11安全相关人员

序号	姓名	岗位/角色	联系方式	所属单位
1	龙恒	网络管理员	13377766618	茂名职业技术学院
2	吴国华	系统管理员	0668-2920122	茂名职业技术学院
3	龙恒	数据管理员	13377766618	茂名职业技术学院
4	杨云	资产管理员	0668-2920122	茂名职业技术学院
5	杨云	审计管理员	0668-2920122	茂名职业技术学院
6	叶永利	安全管理员	0668-2920122	茂名职业技术学院
7	吴国华	机房管理员	0668-2920122	茂名职业技术学院
8	龙恒	应用管理员	13377766618	茂名职业技术学院

A.12 安全管理文档

附录A 表- 12安全管理文档

序号	文档名称	主要内容
1	制度类文档-系统交付管理	关于单位交付工作管理制度文档
2	制度类文档-介质管理制度	关于单位介质安全管理工制度文档
3	制度类文档-授权和审批管理规定	关于单位授权审批、审批流程规范制度文档
4	制度类文档-设备安全管理制度	关于单位设备安全管理制度文档
5	制度类文档-办公环境管理制度	关于单位办公环境管理制度文档
6	制度类文档-信息系统外包运维管理制度	关于单位外包运维工作管理制度文档
7	制度类文档-制度制定、发布、评审和修订管理制度	关于单位制度制定、发布、评审和修订等管理文档
8	制度类文档-网络安全事件报告制度	关于单位网络安全事件管理报告文档
9	制度类文档-网络安全事件应急预案	关于单位网络安全事件应急处理、流程、培训等管理制度文档
10	制度类文档-安全漏洞管理制度	关于单位安全漏洞管理工作制度文档
11	制度类文档-办公环境保密管理	关于单位办公环境管理制度文档
12	制度类文档-人员管理制度	关于单位人员录用、调岗、离岗管理制度文档
13	制度类文档-信息系统恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
14	制度类文档-备份与恢复管理制度	关于单位数据备份、恢复管理制度文档
15	制度类文档-应用安全管理规范	关于规定单位应用安全管理要求及规范的制度文档
16	制度类文档-外部人员访问管理制度	关于单位针对外来人员访问管控制度文档
17	制度类文档-应用系统业务用户密码设置规定	关于单位用户密码管理制度文档
18	制度类文档-物理安全管理规范	关于加强单位办公区域及电子计算机机房的管理和设备运行安全，规范办公区域及机房建设，使人员办公高效及机房设备安全、稳定运行的制度文档
19	制度类文档-变更控制管理制度	关于单位变更流程、控制管理制度文档

序号	文档名称	主要内容
20	制度类文档-主机安全管理规范	关于规定单位主机系统安全管理要求规范，指导业务平台主机的安全配置和维护的制度文档
21	制度类文档-恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
22	制度类文档-组织安全结构和人员职责制度	关于单位组织结构、人员安排、人员职责制度文档
23	制度类文档-外包开发软件管理规定	关于单位外包项目管理工作制度文档
24	制度类文档-网络安全管理制度	关于单位网络安全工作管理制度文档
25	制度类文档-安全事件报告和处置	关于单位网络安全事件管理、处置、流程等报告制度文档
26	制度类文档-服务供应商选择安全管理制度	关于单位安全服务供应商管理规定制度文档
27	制度类文档-数据安全管理规范	关于保障关键数据安全，从数据库本身、数据加密、数据备份恢复三个方面对数据安全进行规范的制度文档
28	制度类文档-恶意代码防范管理制度	关于单位恶意代码防范工作制度文档
29	制度类文档-网络与信息系统安全设计规范	关于单位网络与信息化安全设计制度文档
30	制度类文档-外部接入受控网络访问系统管理规范	关于单位针对外部人员工作接入规范制度文档
31	制度类文档-信息安全奖惩办法	关于单位人员奖惩制度文档
32	制度类文档-离岗人员工作交接规范	关于单位离岗交接工作规范制度文档
33	制度类文档-测试及验收方案	关于单位测试验收方案文档
34	制度类文档-外部服务人员管理规范	关于单位针对外部人员工作管理规范制度文档
35	制度类文档-安全管理组织规范	关于单位组织结构管理规范制度文档
36	制度类文档-安全审查和检查管理规范	关于单位安全检查、审查工作规范制度文档
37	制度类文档-工程实施管理制度	关于单位工程实施工作管理制度文档
38	制度类文档-信息安全总体策略	关于单位网络安全方针、策略制度文档
39	制度类文档-信息安全漏洞扫描规范	关于单位安全漏洞工作规范制度文档
40	制度类文档-系统及应用数据备份管理规范	关于单位数据备份、恢复管理制度文档

序号	文档名称	主要内容
41	制度类文档-安全教育和培训制度	关于单位安全培训、安全交流工作制度文档
42	制度类文档-组织安全结构和人员职责制度	关于单位安全结构、人员职责
43	制度类文档-岗位安排及岗位职责	关于单位岗位职责、岗位安排制度文档
44	制度类文档-系统安全管理制度	关于单位系统安全管理、安全服务管理制度文档
45	制度类文档-机房安全管理制度	关于单位机房安全管理工作制度文档
46	制度类文档-员工考核管理制度	关于单位人员考核工作管理制度文档
47	制度类文档-网络安全管理规范	关于保障单位网络系统的安全稳定运行，抵御内部和外部各种形式的网络攻击或威胁制定的管理文档
48	制度类文档-工程测试验收管理	关于单位工程测试工作管理制度文档
49	操作类文档-设备操作规程	关于单位相关设备操作指导文档
50	操作类文档-数据备份策略	关于单位数据备份策略文件
51	操作类文档-设备及系统软件配置和操作手册	关于单位安全设备操作、Linux服务器配置手册、主机运维操作手册、软件操作手册、防火墙配置和操作手册、数据库日常运维操作手册等指导文档
52	操作类文档-软硬件日常维护管理规程	关于单位计算机网络系统使用、管理、信息安全、资源共享有所遵循,规范上网操作流程,提高网络系统安全性的指导文档
53	记录类文档-离场信息资料交接表	关于人员离岗交接工作记录
54	记录类文档-备份工作汇总表	关于单位数据备份工作总结表
55	记录类文档-机房维护日志	关于机房维护工作记录
56	记录类文档-安全管理制度评审记录	关于单位制度审计记录
57	记录类文档-接入受控网络申请表	关于外来人员接入工作记录
58	记录类文档-通用变更记录表	关于单位变更工作记录
59	记录类文档-离职员工物品交回登记表	关于人员离岗工物交接工作记录
60	记录类文档-设备操作维护记录	关于单位设备维护工作记录
61	记录类文档-软件交付清单	关于单位交付工作记录

序号	文档名称	主要内容
62	记录类文档-信息系统存储介质销毁申请表	关于备份介质销毁申请工作记录
63	记录类文档-系统交付清单	关于单位交付工作记录
64	记录类文档-信息系统存储介质使用清单	关于备份介质存储使用清单
65	记录类文档-设备出入登记记录表	关于设备进出机房登记工作记录
66	记录类文档-机房设备维修记录表	关于单位机房设备维修工作记录
67	记录类文档-信息安全检查记录表	关于单位安全检查工作记录
68	记录类文档-信息管理系统漏洞检查表	关于单位安全漏洞工作检测记录表
69	记录类文档-技能培训记录	关于单位系统培训工作、考核工作记录
70	记录类文档-机房设备维护记录表	关于设备维护登记工作记录
71	记录类文档-存储介质目录清单	关于备份介质存储工作清单
72	记录类文档-机房巡检记录表	关于单位机房环境巡检记录
73	记录类文档-评审和修订记录	关于单位变更评审、修订工作记录
74	记录类文档-专家论证记录表	关于单位网络方案论证记录
75	记录类文档-外部人员访问申请表	关于外来人员访问申请流程工作记录
76	记录类文档-信息安全会议记录	关于单位安全培训、安全交流会议记录
77	记录类文档-机房出入登记表	关于人员进出机房登记工作记录
78	记录类文档-外部人员访问记录表	关于外来人员访问登记工作记录
79	记录类文档-网络信息安全事件记录表	关于单位网络安全事件工作记录
80	记录类文档-应急预案培训记录表	关于单位应急预案培训工作记录
81	记录类文档-人员入职考核记录	关于人员录用、考核工作记录
82	记录类文档-收发文登记记录	关于单位文档签发记录
83	记录类文档-数据恢复	关于单位数据恢复工作申请表

序号	文档名称	主要内容
	申请表	
84	记录类文档-数据备份记录表	关于单位数据备份工作记录
85	记录类文档-网络配置信息	关于单位配置信息登记工作记录
86	记录类文档-监理审批表	关于单位监理审核工作记录
87	记录类文档-外部会议文件和记录	关于单位外部联系、交流及会议工作记录
88	记录类文档-人员离岗申请表	关于人员离岗申请记录
89	记录类文档-访问记录表	关于人员访问工作记录
90	记录类文档-设备维修申请表	关于单位设备维护工作申请记录
91	记录类文档-人员培训及考核记录表	关于人员培训、考核等工作记录
92	记录类文档-漏洞检测报告	关于单位安全漏洞检测报告文档
93	记录类文档-重要操作审批表	关于单位审批工作记录
94	记录类文档-关键岗位人员考核记录	关于关键岗位考核工作记录
95	记录类文档-安全建设方案评审纪录	关于单位网络与信息化安全设计方案评审工作记录
96	记录类文档-备份介质使用记录	关于备份介质使用登记工作记录
97	证据类文档-外部联系表	关于单位内部联系及外部联系名单
98	证据类文档-定级备案	关于单位系统定级报告、备案证文件
99	证据类文档-安全职位人员	关于单位人员岗位安排名单
100	证据类文档-深信服安全采购合同	关于单位与安全厂家服务采购、产品选择合同文件
101	证据类文档-网络安全系统设计方案	关于单位网络与信息化安全设计方案文档
102	证据类文档-网络安全等级保护测评服务合同	关于单位与安全服务商签定的安全服务合同文件
103	证据类文档-网络安全等级保护工作小组名单	关于单位网络安全等级保护工作小组人员名单文件
104	证据类文档-资产清单	关于单位信息系统资产清单统计表

序号	文档名称	主要内容
105	证据类文档-信息安全事件分析报告表	关于单位安全事件分析报告
106	证据类文档-工程项目实施方案	关于单位工程实施方案文档

附录B 上次测评问题整改情况说明

此次为招生信息网系统初次等级测评，之前未实施过等级保护测评工作。

附录B 表- 1上次测评问题整改情况

序号	主要安全问题	整改情况	情况说明
/	/	□已整改 □未整改	/

附录C 单项测评结果汇总

C.1 安全物理环境

附录 C 表-1 安全物理环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			物理位置选择	物理访问控制	防盗窃和防破坏	防雷击	防火	防水和防潮	防静电	温湿度控制	电力供应	电磁防护
1	信息化机房	符合	2	0	2	1	1	2	0	1	2	1
		部分符合	0	1	0	0	0	0	0	0	0	0
		不符合	0	0	0	0	1	0	1	0	0	0
		不适用	0	0	0	0	0	0	0	0	0	0

附录 C 表-2 安全物理环境单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.2 安全通信网络

附录 C 表-3 安全通信网络单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求		
			网络架构	通信传输	可信验证
1	安全通信网络	符合	1	1	0
		部分符合	1	0	0
		不符合	0	0	1
		不适用	0	0	0

附录 C 表-4 安全通信网络单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.3 安全区域边界

附录 C 表-5 安全区域边界单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求					
			边界防护	访问控制	入侵防范	恶意代码和垃圾邮件防范	安全审计	可信验证
1	外网边界区域	符合	1	4	1	1	3	0
		部分符合	0	0	0	0	0	0
		不符合	0	0	0	0	0	1
		不适用	0	0	0	0	0	0
2	安全管理区域	符合	1	4	0	0	3	0
		部分符合	0	0	0	1	0	0
		不符合	0	0	1	0	0	1
		不适用	0	0	0	0	0	0
3	服务器存储区域	符合	1	4	1	1	3	0
		部分符合	0	0	0	0	0	0
		不符合	0	0	0	0	0	1
		不适用	0	0	0	0	0	0
4	办公网区域	符合	1	4	0	0	3	0
		部分符合	0	0	0	1	0	0
		不符合	0	0	1	0	0	1
		不适用	0	0	0	0	0	0

附录 C 表-6 安全区域边界单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.4 安全计算环境

C.4.1 网络设备

附录 C 表-7 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	汇聚交换机	符合	3	4	3	4	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	1	0	0	1	1	--
2	核心交换机	符合	3	4	3	4	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	1	0	0	1	1	--

C.4.2 安全设备

附录 C 表-8 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	基线核查系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
2	上网行为管理系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
3	WEB应用防火墙	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
4	防火墙-1	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
5	防火墙-2	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
6	日志	符合	3	4	3	5	0	0	1	1	0	--

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
	审计系统	部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
7	运维安全管理系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--

C.4.3 服务器和终端

附录 C 表-9 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	应用/数据库服务器	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
2	业务终端-2	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
3	业务终端-1	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
4	运维及管理终端-2	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
5	运维及管理终端-1	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
		不适用	0	0	0	1	0	0	0	1	0	--

C.4.4 系统管理软件/平台

附录 C 表-10 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	应用/数据库服务器-nginx	符合	0	4	3	1	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	3	0	0	4	1	1	0	0	0	--
2	应用/数据库服务器-MySQL	符合	2	4	3	2	0	0	1	1	1	--
		部分符合	1	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	0	0	0	3	1	1	0	0	0	--

C.4.5 业务应用系统/平台

附录 C 表-11 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	招生信息网系统	符合	3	4	3	3	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	0	0	0	2	1	1	0	0	0	--

C.4.6 数据资源

附录 C 表-12 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	重要个人	符合	--	--	--	--	--	--	1	1	0	2
		部分符	--	--	--	--	--	--	0	0	0	0

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
	信息	合										
		不符合	--	--	--	--	--	--	0	1	0	0
		不适用	--	--	--	--	--	--	0	0	1	0
2	重要业务数据	符合	--	--	--	--	--	--	1	1	0	0
		部分符合	--	--	--	--	--	--	0	0	0	0
		不符合	--	--	--	--	--	--	0	1	0	0
		不适用	--	--	--	--	--	--	0	0	1	2

C.4.7 其他系统或设备

附录 C 表-13 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	--	符合	--	--	--	--	--	--	--	--	--	--
		部分符合	--	--	--	--	--	--	--	--	--	--
		不符合	--	--	--	--	--	--	--	--	--	--
		不适用	--	--	--	--	--	--	--	--	--	--

C.5 安全管理中心

附录 C 表-14 安全管理中心单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求	
			系统管理	审计管理
1	管理中心	符合	1	2
		部分符合	0	0
		不符合	1	0
		不适用	0	0

附录 C 表-15 安全管理中心单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.6 安全管理制度

附录 C 表-16 安全管理制度单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求			
			安全策略	管理制度	制定和发布	评审和修订
1	制度文件、执行/记录文件	符合	1	2	2	1
		部分符合	0	0	0	0
		不符合	0	0	0	0
		不适用	0	0	0	0

C.7 安全管理机构

附录 C 表-17 安全管理机构单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求				
			岗位设置	人员配备	授权和审批	沟通和合作	审核和检查
1	制度文件、执行/记录文件	符合	2	1	2	3	0
		部分符合	0	0	0	0	1
		不符合	0	0	0	0	0
		不适用	0	0	0	0	0

C.8 安全管理人员

附录 C 表-18 安全管理人员单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求			
			人员录用	人员离岗	安全意识教育和培训	外部人员访问管理
1	制度文件、执行/记录文件	符合	2	1	1	2
		部分符合	0	0	0	0
		不符合	0	0	0	1
		不适用	0	0	0	0

C.9 安全建设管理

附录 C 表-19 安全建设管理单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			定级和备案	安全方案设计	产品采购和使用	自行软件开发	外包软件开发	工程实施	测试验收	系统交付	等级测评	服务供应商选择
1	制度文件、执行/记录文件	符合	4	0	2	0	1	2	0	3	3	2
		部分符合	0	0	0	0	0	0	1	0	0	0
		不符合	0	3	0	0	1	0	1	0	0	0
		不适用	0	0	0	2	0	0	0	0	0	0

附录 C 表-20 安全建设管理单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.10 安全运维管理

附录 C 表-21 安全运维管理单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求													
			环境管理	资产管理	介质管理	设备维护管理	漏洞和风险管理	网络和系统安全管理	恶意代码防范管理	配置管理	密码管理	变更管理	备份与恢复管理	安全事件处置	应急预案管理	外包运维管理
1	制度文件、执行/记录文件	符合	3	1	2	2	0	5	2	1	0	1	3	3	2	0
		部分符合	0	0	0	0	0	0	1	0	0	0	0	0	0	0
		不符合	0	0	0	0	1	0	0	0	1	0	0	0	0	0
		不适用	0	0	0	0	0	0	0	0	1	0	0	0	0	2

附录 C 表-22 安全运维管理单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.11 其他安全要求指标

附录 C 表-23 其他指标单项测评结果汇总表

序号	测评对象	符合情况
本报告不涉及		

附录D 单项测评结果记录

D.1 安全物理环境

D.1.1 安全通用要求

D.1.1.1 信息化机房

安全控制点	测评指标	结果结论	符合程度
物理位置选择	a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；	（1）机房和办公场地场所在建筑物具有建筑验收文档，包含对防震、防风和防雨能力的说明； ■机房建设地址为：茂名市茂南区文明北路232号大院大楼 （2）机房和办公场地未出严重的问题。 ■无雨水渗透痕迹 ■无因风导致的较严重尘土 ■无屋顶、墙体、地面等破损开裂	符合
	b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	（1）机房未部署在易发生问题的位置； （2）机房对于空调设备的排水管等部位采取密封防漏处理； （3）机房对于楼板进行了防护措施。	符合
物理访问控制	机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。	（1）制定了《机房安全管理制度》，内容包含机房出入方面的管理规定； （2）对未配置电子门禁系统的出入口指定专人7*24小时负责机房出入，对出入的人员进行身份鉴别和登记，可查出入记录，且出入有专人陪同； （3）机房存在未配置门禁系统的开放出入口。	部分符合
防盗窃和防破坏	a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识；	（1）机房设备或主要部件都固定在机架上； （2）机房内对主要部件已绑定相应不易除去的标签； ■包括网络设备 ■包括安全设备 ■包括服务器 ■包括网络线缆 （3）重要机柜已进行上锁处理。	符合
	b) 应将通信线缆铺设在隐蔽安全处。	（1）通信线缆铺设在下走线槽隐蔽处中； （2）通信线缆设有明显的源目的标识； （3）通信线缆均铺设整齐、规范。	符合
防雷击	应将各类机柜、设施和设备等通过接地系统安全接地。	（1）机房设置专用地线； （2）机房内机柜、设施和设备等进行接地处理； （3）交流电源接地验收检测结果符合要求。	符合
防火	a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭	（1）机房采用经消防检测部门检测合格并在有效期内的（如 七氟丙烷）气体自动灭火设备，火灾自动报警类型为烟感+红外；	符合

安全控制点	测评指标	结果结论	符合程度
	火；	（2）自动消防系统工作状态正常，有定期巡检和维护记录《机房巡检记录表》； （3）建立机房消防的管理制度相关文档《机房安全管理制度》，按管理要求机房无人情况下气体灭火配置为自动模式，进入机房调整为手动模式，机房报警有7*24小时值班人员进行监控。	
	b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。	（1）机房及相关的工作房间和辅助房没有采用具有耐火等级的建筑材料； （2）缺乏机房防火设计文档； （3）缺乏机房防火验收文档。	不符合
防水和防潮	a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	（1）机房不存在雨水渗透、破损等不合规情况； （2）机房不位于建筑的顶层、边缘区域。	符合
	b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。	（1）机房区域范围已部署1台科华品牌（精密）空调，机房内分别配置1组温湿度传感器监控； （2）机房内空调下方已铺设安装好挡水和排水设施； （3）机房墙壁或楼板的管道采取必要的防渗防漏等防水保护措施； （4）机房安装检测设备（如：漏水检测绳）检测地下积水，及时处理机房水蒸气结露和地下积水的转移与渗透； （5）目前防水\防潮检测未发现异常情况，并且有防水防潮的运维记录《机房维护日志》。	符合
防静电	应采用防静电地板或地面并采用必要的接地防静电措施。	（1）对机房内设备（可导电金属线槽）采用了接地静电泄放措施； （2）机房未采用防静电地板或铺设防静电地毯。	不符合
温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。	（1）机房范围已部署1组科华品牌精密空调进行温湿度调节； （2）机房范围已部署空调及加湿机进行温湿度调节； （3）温湿度自动调节设施运作正常，有运行和维护记录《机房维护日志》； （4）机房温度能保持在24摄氏度到28摄氏度之间； （5）机房湿度能保持在40%到65%之间。	符合
电力供应	a）应在机房供电线路上配置稳压器和过电压防护设备；	（1）机房配备了稳压器和过电压防护设备； （2）稳压器和过电压防护设备正常工作； （3）机房具备电力供应安全设计，并在其中标明配备稳压器、过电压防护设备等要求。	符合
	b）应提供短期的备用电力	（1）机房配备了1组科华品牌UPS；	符合

安全控制点	测评指标	结果结论	符合程度
	供应，至少满足设备在断电情况下的正常运行要求。	（2）UPS正常工作，可满足主要设备断电情况下的至少1小时正常运行要求； （3）UPS有定期（至少每年）检查和维护，有运行和维护记录《机房巡检记录表》。	
电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。	（1）通信线缆铺设采用独立的具有电磁屏蔽作用线槽； （2）电源线缆铺设采用独立的具有电磁屏蔽作用线槽； （3）弱电线缆隔离铺设，没有干扰。	符合

D.2 安全通信网络

D.2.1 安全通用要求

D.2.1.1 安全通信网络

安全控制点	测评指标	结果结论	符合程度
网络架构	a）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；	（1）已对网络地址划分，且便于管理和控制； （2）网络地址划分采用核心交换机实现外网边界区域、服务器存储区域等的划分； （3）重要核心网络区域与非重要网络在同一网段； （4）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	部分符合
	b）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	（1）网络内重要网段未部署在网络边界处，且未直接连接外部信息系统； （2）系统通过防火墙对重要网段采取访问控制策略； （3）各安全域（子网）的出口唯一。	符合
通信传输	应采用校验技术保证通信过程中数据的完整性。	（1）网络系统中未涉及完整性保障设备，但在安全计算环境方面网络设备采用SSH协议、安全设备采用HTTPS协议、操作系统采用SSH协议、应用系统采用HTTPS协议来保证通信过程中数据的完整性。	符合
可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对通信设备可信验证方面的安全设计要求； （2）现有的通信设备存在未能实现操作系统到上层应用的信任链的情况，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■通信应用连接过程	不符合

D.3 安全区域边界

D.3.1 安全通用要求

D.3.1.1 办公网区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■办公网区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	符合
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问	符合

安全控制点	测评指标	结果结论	符合程度
		的能力。	
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略,无法检测、防止或限制从内部发起的网络攻击行为。	不符合
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试； （4）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	部分符合
安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备	（1）缺乏对边界设备可信验证方面的安全设	不符合

安全控制点	测评指标	结果结论	符合程度
	的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	

D.3.1.2 外网边界区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■外网边界区域 （2）网络边界处部署了可提供访问控制功能的设备； ■防火墙 ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	符合
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■防火墙 ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址	符合

安全控制点	测评指标	结果结论	符合程度
		■源端口 ■目的端口 ■协议	
	d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制,能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署支持对内部发起的攻击行为进行防范的设备； ■防火墙(带入侵防御模块) ■WEB应用防火墙 （2）现有的防范措施满足相应防护要求； ■所有关键网络边界均有检测措施 ■设备的规则库及时更新 ■检测(模块)符合国家相关产品检测要求 ■其安全策略有效 (3)内部安全防范措施能检测相应攻击行为。 ■端口扫描 ■强力攻击 ■木马后门攻击 ■拒绝服务攻击 ■缓冲区溢出攻击 ■碎片攻击 ■网络蠕虫攻击 ■应用漏洞攻击	符合
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试。	符合
安全审计	a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块)	符合

安全控制点	测评指标	结果结论	符合程度
		■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.3.1.3 安全管理区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■安全管理区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设	符合

安全控制点	测评指标	结果结论	符合程度
		备通过非法无线热点接入内部网络。	
访问控制	a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	不符合
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容	部分符合

安全控制点	测评指标	结果结论	符合程度
		性进行测试； （4）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	
安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.3.1.4 服务器存储区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和	（1）网络存在受保护的边界；	符合

安全控制点	测评指标	结果结论	符合程度
	数据流通过边界设备提供的受控接口进行通信。	■服务器存储区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■WEB应用防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视	（1）网络层部署支持对内部发起的攻击行为	符合

安全控制点	测评指标	结果结论	符合程度
	网络攻击行为。	进行防范的设备； ■WEB应用防火墙 （2）现有的防范措施满足相应防护要求； ■所有关键网络边界均有检测措施 ■设备的规则库及时更新 ■检测(模块)符合国家相关产品检测要求 ■其安全策略有效 （3）内部安全防范措施能检测相应攻击行为。 ■端口扫描 ■强力攻击 ■木马后门攻击 ■拒绝服务攻击 ■缓冲区溢出攻击 ■碎片攻击 ■网络蠕虫攻击 ■应用漏洞攻击	
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■WEB应用防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试。	符合
安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■WEB应用防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c）应对审计记录进行保	（1）网络层部署日志审计系统，统一接收及	符合

安全控制点	测评指标	结果结论	符合程度
	护，定期备份，避免受到未预期的删除、修改或覆盖等。	保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.4 安全计算环境

D.4.1 安全通用要求

D.4.1.1 网络设备

D.4.1.1.1 核心交换机

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括VTY认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的全局密码策略； ■Password control:Enabled ■Password aging:Enabled (180 days) ■Password length:Enabled (8 characters) ■Password composition:Enabled (4 types, 1 characters per type) （6）设备配置加密的super认证。	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备配置合规的全局登录失败处理策略； ■Password control: Enabled ■Maximum login attempts: 5 ■Action for exceeding login attempts: Lock user for 5 minutes	符合

安全控制点	测评指标	结果结论	符合程度
		（2）设备配置合规的操作超时退出措施。 ■VTY配置idle-timeout 15 0	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式。 ■未启用TELNET ■启用SSH	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； ■Information Center: Enabled ■Console: Enabled ■Monitor: Enabled ■Log host: Enabled 10.2.1.2 ■Security log file: Enabled （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间	符合

安全控制点	测评指标	结果结论	符合程度
		■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制； ■对ssh 登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）网络层相关设备不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的交换功能，不具备恶意代码防范模块，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配	（1）网络层设备不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	前得到完全清除。		
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.1.2 汇聚交换机

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括VTY认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的全局密码策略； ■Password control:Enabled ■Password aging:Enabled (180 days) ■Password length:Enabled (8 characters) ■Password composition:Enabled (4 types, 1 characters per type) （6）设备配置加密的super认证。	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备配置合规的全局登录失败处理策略； ■Password control: Enabled ■Maximum login attempts: 5 ■Action for exceeding login attempts: Lock user for 5 minutes （2）设备配置合规的操作超时退出措施。 ■VTY配置idle-timeout 15 0	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式。 ■未启用TELNET ■启用SSH	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令	符合

安全控制点	测评指标	结果结论	符合程度
		■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； ■Information Center: Enabled ■Console: Enabled ■Monitor: Enabled ■Log host: Enabled 10.2.1.2 ■Security log file: Enabled （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效；	符合

安全控制点	测评指标	结果结论	符合程度
		（5）日志及审计记录保存大于6个月。	
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制； ■对ssh 登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）网络层相关设备不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的交换功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要	符合

安全控制点	测评指标	结果结论	符合程度
		的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2 安全设备

D.4.1.2.1 WEB应用防火墙

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有	符合

安全控制点	测评指标	结果结论	符合程度
		唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，	（1）设备开启审计功能，审计进程正常；	符合

安全控制点	测评指标	结果结论	符合程度
	审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请	符合

安全控制点	测评指标	结果结论	符合程度
		表》。	
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.2 上网行为管理系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合

安全控制点	测评指标	结果结论	符合程度
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要	符合

安全控制点	测评指标	结果结论	符合程度
		的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.3 基线核查系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性；	符合

安全控制点	测评指标	结果结论	符合程度
		（4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆	符合

安全控制点	测评指标	结果结论	符合程度
	重要的用户行为和重要安全事件进行审计；	盖所有用户操作审计和记录。	
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成	符合

安全控制点	测评指标	结果结论	符合程度
		高风险的漏洞。	
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的基线核查功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要	不适用

安全控制点	测评指标	结果结论	符合程度
	数据定时批量传送至备用场地。	求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.4 日志审计系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合

安全控制点	测评指标	结果结论	符合程度
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 (2)设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合

安全控制点	测评指标	结果结论	符合程度
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施；	符合

安全控制点	测评指标	结果结论	符合程度
		■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.5 运维安全管理系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合

安全控制点	测评指标	结果结论	符合程度
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； (2)登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 (2)设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期	符合

安全控制点	测评指标	结果结论	符合程度
	他与审计相关的信息；	■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制。 ■对Web登录配置管理地址，限制登录范围	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备	（1）设备不具备相关可信验证的技术措施；	不符合

安全控制点	测评指标	结果结论	符合程度
	的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.6 防火墙-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合

安全控制点	测评指标	结果结论	符合程度
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方	（1）设备通过核心交换机的访问控制策略，	符合

安全控制点	测评指标	结果结论	符合程度
	式或网络地址范围对通过网络进行管理的管理终端进行限制；	通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要	符合

安全控制点	测评指标	结果结论	符合程度
		的完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.7 防火墙-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会	（1）设备启用合规登录失败处理策略； ■启用登录失败策略	符合

安全控制点	测评指标	结果结论	符合程度
	话、限制非法登录次数和当登录连接超时自动退出等相关措施；	■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型	符合

安全控制点	测评指标	结果结论	符合程度
		■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合

安全控制点	测评指标	结果结论	符合程度
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配	（1）网络层设备不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	前得到完全清除。		
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.3 服务器和终端

D.4.1.3.1 应用/数据库服务器

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）操作系统不存在空口令用户； ■etc/passwd文件中各用户的第二字段处不为空 ■/etc/shadow文件中各用户密码字段处不为空 （3）操作系统不存在默认信任的登录模式； （4）操作系统为登录用户设置的身份标识具有唯一性； ■UID具有唯一性 ■UID=0只能root用户 （5）操作系统配置的一定的密码长度且定期更换； ■PASS_MAX_DAYS 180 ■PASS_MIN_DAYS 1 ■PASS_MIN_LEN 8 ■PASS_WARN_AGE 28 （6）操作系统配置一定的密码复杂度策略。 ■minlen=8 ■ucredit=-2 ■lcredit=-1 ■dcredit=-4 ■ocredit=-1	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用pam_tally2模块的合规登录失败处理策略； auth required /lib/security/pam_tally.so onerr=fail no_magic_root和 account required /lib/security/pam_tally.so deny=10 no_magic_root reset （2）操作系统配置合规的操作超时锁定； ■配置具备以下措施：	符合

安全控制点	测评指标	结果结论	符合程度
		/etc/profile设置TMOUT=300 （3）操作系统启用SSH的合规登录超时策略。 ■配置具备以下措施： /sshd_config设置 ClientAliveInterval 60 ClientAliveCountMax 3	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）操作系统配置合规的远程管理模式； ■启用SSH （2）操作系统远程端口使用情况合规； ■21（FTP）未启用 ■23（Telnet）未启用 （3）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在所有用户均属于root组的情况。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统对多余帐户进行删除、锁定或禁止其登录； （2）操作系统账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； （2）操作系统不存在除root外的特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计功能，审计进程正常； ■rsyslog：loaded ■auditctl：enabled=1 （2）操作系统开启审计范围及策略满足要求，审计覆盖所有用户操作审计和记录。 ■rsyslog： *.info;mail.none;news.none;authpriv.none;cron.none /var/log/messages	符合

安全控制点	测评指标	结果结论	符合程度
		■auditctl： 关键目录、文件的审计行为采用 perm=rwxa	
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）操作系统针对日志、审计记录具备充足的存储容量； （3）操作系统采取合规的日志文件权限策略； ■/var/log/messages：640 ■/var/log/secure：640 ■/var/log/audit/audit.log：640 对审计记录进行定期存档备份，其备份策略有效 （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统关闭不必要端口； （2）操作系统禁用不必要服务； （3）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口； （4）漏洞扫描未发现高风险主机端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服edr防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证； ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序 （3）现有的可信验证缺乏以下措施。 ■对可信性破坏报警 ■将可信性验证结果形成审计记录 ■对可信性审计的动态关联感知	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对鉴别数据采取完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）系统在通信传输过程中对重要配置数据采取完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确	符合

安全控制点	测评指标	结果结论	符合程度
		的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为服务器设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统不保存过多终端历史记录。 ■通过echo $HISTSIZE查看history保留数目为30	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）本设备不存在此部分的控制需求，故此项不适用	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）本设备不存在此部分的控制需求，故此项不适用	不适用

D.4.1.3.2 业务终端-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟	符合

安全控制点	测评指标	结果结论	符合程度
	等相关措施；	■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败	符合

安全控制点	测评指标	结果结论	符合程度
		■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下：运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略	符合

安全控制点	测评指标	结果结论	符合程度
	进行限制；	要求下，统一集中管理远程登录地址。	
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据	符合

安全控制点	测评指标	结果结论	符合程度
		（2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.3 业务终端-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用	符合

安全控制点	测评指标	结果结论	符合程度
		户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户	（1）操作系统根据安全策略要求对特权用户进行分离；	符合

安全控制点	测评指标	结果结论	符合程度
	的权限分离。	■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1)操作系统采取对审计记录存储容量如下:运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用	符合

安全控制点	测评指标	结果结论	符合程度
		必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整	鉴别数据: （1）系统在通信传输过程中对相关数据采取	符合

安全控制点	测评指标	结果结论	符合程度
	性。	完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必	（1）操作系统不存在此部分的控制需求，不	不适用

安全控制点	测评指标	结果结论	符合程度
	需的用户个人信息；	适用。	
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.4 运维及管理终端-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 (5)用户属性策略未勾选“密码永不过期”。	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户	符合

安全控制点	测评指标	结果结论	符合程度
		权限分配表，系统现状与权限分配表情况一致。	
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到	(1)操作系统采取对审计记录存储容量如下:运维审计和日志记录 应用日志 1G、安全日	符合

安全控制点	测评指标	结果结论	符合程度
	未预期的删除、修改或覆盖等。	志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备；	符合

安全控制点	测评指标	结果结论	符合程度
		（5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施： 安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.5 运维及管理终端-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超	符合

安全控制点	测评指标	结果结论	符合程度
		时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败	符合

安全控制点	测评指标	结果结论	符合程度
		■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下：运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入	（1）操作系统不存在此部分的控制需求，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	的内容符合系统设定要求；		
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能	符合

安全控制点	测评指标	结果结论	符合程度
		发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.4 系统管理软件/平台

D.4.1.4.1 应用/数据库服务器-MySQL

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）数据库系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）数据库系统不存在弱口令用户； ■MySQL数据库已修改默认root口令 ■MySQL数据库不存在空口令用户 （3）数据库系统不存在默认信任的登录模式； ■MySQL数据库登录未设置skip-grant-tables （4）数据库系统为登录用户设置的身份标识	部分符合

安全控制点	测评指标	结果结论	符合程度
		具有唯一性； （5）数据库系统配置合规的密码长度及复杂度策略； ■MySQL 数据库系统启用“validate_password” ■validate_password_length 8 ■validate_password_mixed_case_count 1 ■validate_password_number_count 1 ■validate_password_special_char_count 1 （6）不存在空口令或弱口令帐户； （7）数据库系统配置合规的密码有效周期策略。 ■MySQL 数据库配置未合理的“password_lifetime”参数	
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）数据库系统启用合规登录失败处理策略； ■MySQL 数据库系统启用“connection_control” （2）数据库系统执行合规的锁定策略； ■Connection_control_failed_connections_threshold 3 ■Connection_control_min_connection_delay 1000 （3）数据库系统配置合规的操作超时锁定。 ■interactive_timeout 1800	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）数据库系统配置合规的远程管理模式。 ■MySQL 数据库系统have_openssl为YES	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）登录数据库系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （2）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在多用户均与root用户权限一致的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）数据库系统对多余帐户进行删除、锁定或禁止其登录； ■数据库系统账户禁用不常用的默认用户 （2）数据库系统账户口令设置合规。 ■数据库系统各用户未使用空口令 ■数据库系统未使用弱口令或默认与用户名相同的口令	符合

安全控制点	测评指标	结果结论	符合程度
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）数据库系统不存在多余或过期账户； （2）数据库系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）数据库系统根据安全策略要求对特权用户进行分离； （2）数据库系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限； （3）数据库账户和系统管理员账户未处于同一个用户组中； （4）宿主操作系统管理员与数据库管理员为不同的人员，且使用不同的帐户登录系统。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）数据库系统开启审计功能，审计进程正常。 ■MySQL 数据库系统log_bin=ON	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）数据库宿主系统日期、时间正常； （2）数据库系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括重要用户行为 ■包括系统资源的异常使用情况 ■包括重要系统命令的使用 ■包括重要的安全相关事件	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）数据库系统限制审计文件的访问控制权限，普通用户不可删除及修改； ■MySQL数据库系统日志文件安装路径下的log文件 用户权限为640 （2）数据库系统针对日志、审计记录具备充足的存储容量； （3）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）数据库系统设定有效的终端接入策略，对通过网络进行管理的终端进行限制； ■数据库系统对帐号进行IP限制，host ≠ % （2）核心交换机设备ACL策略有效限制访问本机的IP地址及管理模式。	符合
	d) 应提供数据有效性检验	（1）数据库系统不存在此部分的控制需求，	不适用

安全控制点	测评指标	结果结论	符合程度
	功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	不适用。	
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）数据库系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）数据库宿主系统不存在启用未加控制的高危端口； （3）MYSQL分离默认安装的示例数据库； （4）数据库系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■使用数据库内置的SSL协议加密 重要配置数据: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■使用数据库内置的SSL协议加密	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）数据库系统定义了相关重要数据； ■包括鉴别数据 ■包括重要配置数据 ■包括重要审计数据 （2）数据库系统定期完全依照备份策略，采用正确的配置进行本地备份；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）系统的备份周期为：每天一次增量、每月一次全备； （4）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）数据库系统未能提供异地数据备份功能。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）数据库系统不保存终端历史记录。	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）数据库存储的用户个人信息均为业务应用必需的环节。	符合
	b）应禁止未授权访问和非法使用用户个人信息。	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； ■包括信息采集 ■包括信息保存 ■包括信息访问 ■包括信息使用 （2）数据库具备控制措施禁止未授权访问用户个人信息表单； （3）数据库具备控制措施禁止非法使用用户个人信息表单。	符合

D.4.1.4.2 应用/数据库服务器-nginx

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）Nginx中间件的身份鉴别功能由宿主操作系统实现，不适用。	不适用
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）Nginx中间件的身份鉴别功能由宿主操作系统实现，不适用。	不适用
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃	（1）Nginx中间件的远程管理功能由宿主操作系统实现，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	听。		
访问控制	a) 应对登录的用户分配账户和权限；	（1）宿主系统可提供系统权限功能； （2）系统安装Nginx后产生的用户已对权限加以控制； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）中间件不存在默认账户名； （2）中间件账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）中间件不存在多余或过期账户； （2）中间件管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）中间件根据安全策略要求对特权用户及宿主管理用户进行分离； （2）中间件管理不存在多个管理级别高的特权用户； （3）Nginx中间件不采用root用户权限运行。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）中间件开启审计功能，审计进程正常； ■设置日志记录文件标签为main的log_format格式 ■设置记录内容文件标签为main的log_format格式 ■设置记录格式内容文件标签，添加标签为main的log_format格式 （2）系统的日志审计级别满足要求。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）中间件日期、时间正常； （2）中间件审计记录access.log及error.log内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括结果	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）中间件限制审计文件的访问控制权限，普通用户不可删除及修改； （2）宿主系统针对中间件日志、审计记录具备充足的存储容量； （3）对中间件审计记录进行定期存档备份，其备份策略有效； （4）日志及审计记录可保存大于6个月。	符合

安全控制点	测评指标	结果结论	符合程度
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）中间件系统不存在此部分的安装控制需求，不适用。	不适用
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）Nginx中间件的管理地址限制功能由宿主操作系统实现，故该项不适用。	不适用
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）中间件已根据需要不定期地对已发布的版本进行更新； （2）中间件更新安装前进行安全性和兼容性测试； （3）在不影响业务系统正常运行情况下，对发现的中间件漏洞在确保安全的情况下进行修补； （4）中间件进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输 ■宿主系统使用SSH加密协议进行传输	符合

安全控制点	测评指标	结果结论	符合程度
		重要配置数据: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输 ■宿主系统使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份的中间件重要数据； ■包括鉴别数据 ■包括重要配置数据 ■包括重要审计数据 （2）宿主系统定期完全依照备份策略，采用正确的配置进行本地备份； （3）中间件相关数据的备份周期合理； ■每天增量一次 ■每月全备一次 （4）中间件开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）宿主系统具有清除用户鉴别信息的功能； （2）经测试，宿主系统退出后无法访问先前中间件登录过的页面； （3）经测试，宿主系统关闭后无残留的中间件用户鉴别信息。	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用

D.4.1.5 业务应用系统/平台

D.4.1.5.1 招生信息网系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）系统对各登录模式均启用身份鉴别； ■包括管理后台认证 （2）系统对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码	符合

安全控制点	测评指标	结果结论	符合程度
		（3）系统登录用户设置的身份标识具有唯一性； （4）系统不存在空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）系统启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）系统配置合规的操作超时退出措施。 ■管理后台配置超时15分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）应用系统的用户鉴别数据采用SHA-512算法在可控网络环境中传输； （2）系统配置合规的远程管理模式。 ■启用HTTPS	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供系统权限分配表； （2）登录系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需分配不同的用户权限，不存在所有用户均属于管理级别、高权限的情况。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）系统禁用默认账户名； （2）系统账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）系统不存在多余或过期账户； （2）系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）系统不存在多个管理级别高的特权用户； （2）系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）系统开启审计功能，审计进程正常； （2）系统的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其	（1）系统日期、时间正常； （2）系统审计记录内容基本完整。 ■包括事件的日期	符合

安全控制点	测评指标	结果结论	符合程度
	他与审计相关的信息；	■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）系统针对日志、审计记录具备充足的存储容量； （3）审计记录及日志保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）应用软件系统不存在此部分的安装控制需求，不适用。	不适用
	b) 应关闭不需要的系统服务、默认共享和高危端口；	(1)应用软件系统不存在此部分的控制需求，不适用。	不适用
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）系统自身设定有效的终端访问策略，通过访问措施进行管理地址的限制。 ■系统管理页面仅能内网登录	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）系统具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）系统的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）系统已根据需要不定期地对已发布的版本进行更新； （2）在系统上线或发生重大变更时测试并安装最新的版本或更新补丁； （3）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	(1)应用软件系统不存在此部分的控制需求，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证	(1)应用软件系统不存在此部分的控制需求，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	结果形成审计记录送至安全管理中心。		
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）系统具有清除用户鉴别信息的功能； （2）经测试，系统退出后无法访问先前登录过的页面； （3）经测试，系统关闭后无残留的用户鉴别信息。	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）系统采集的用户个人信息均为业务应用必需的环节。	
	b）应禁止未授权访问和非法使用用户个人信息。	（1）系统不采集和保存任何形式的用户个人信息； （2）系统对所有涉及个人信息的环节均有明确的授权同意过程； ■包括信息采集 ■包括信息保存 ■包括信息访问 ■包括信息使用 （3）系统具备控制措施禁止未授权访问用户个人信息； （4）系统具备控制措施禁止非法使用用户个人信息。	符合

D.4.1.6 数据资源

D.4.1.6.1 重要业务数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	（1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要业务数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份重要数据； ■包括重要业务数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）该测评项测评对象鉴别数据，已在安全计算环境层面其他对象判定，此项不适用。	不适用
个人信息保护	a）应仅采集和保存业务必	（1）该测评项测评对象为重要个人信息的内	不适用

安全控制点	测评指标	结果结论	符合程度
	需的用户个人信息；	容，已在安全计算环境层面其他对象判定，该项不适用。	
	b）应禁止未授权访问和非法使用用户个人信息。	（1）该测评项测评对象为重要个人信息的内容，已在安全计算环境层面其他对象判定，该项不适用。	不适用

D.4.1.6.2 重要个人信息

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	（1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要个人信息 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份重要数据； ■包括重要个人信息 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）该测评项测评对象鉴别数据，已在安全计算环境层面其他对象判定，此项不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息； （3）系统采集的用户个人信息均为业务应用必需的环节。	符合
	b）应禁止未授权访问和非法使用用户个人信息。	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； ■包括信息采集 ■包括信息保存	符合

安全控制点	测评指标	结果结论	符合程度
		■包括信息访问 ■包括信息使用 （2）系统具备控制措施禁止未授权访问用户个人信息； （3）系统具备控制措施禁止非法使用用户个人信息。	

D.4.1.6.3 鉴别数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	业务终端-1、业务终端-2、运维及管理终端-1、运维及管理终端-2: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 应用/数据库服务器-MySQL: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■使用数据库内置的SSL协议加密 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 应用/数据库服务器-nginx: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）中间件对重要数据在传输过程中采取必	符合

安全控制点	测评指标	结果结论	符合程度
		要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输 ■宿主系统使用SSH加密协议进行传输 招生信息网系统: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输 应用/数据库服务器: （1）系统在通信传输过程中对鉴别数据采取完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	该测评项在各系统及设备已做判定,数据资源针对鉴别数据不做判定	不适用
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	该测评项在各系统及设备已做判定,数据资源针对鉴别数据不做判定，不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	应用/数据库服务器-nginx: （1）宿主系统具有清除用户鉴别信息的功能； （2）经测试，宿主系统退出后无法访问先前中间件登录过的页面； （3）经测试，宿主系统关闭后无残留的中间件用户鉴别信息。 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）网络层设备不适用。 业务终端-1、业务终端-2、运维及管理终端-1、运维及管理终端-2: （1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用 应用/数据库服务器: （1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统不保存过多终端历史记录。 ■通过echo $HISTSIZE查看history保留数目为30	符合

安全控制点	测评指标	结果结论	符合程度
		招生信息网系统: （1）系统具有清除用户鉴别信息的功能； （2）经测试，系统退出后无法访问先前登录过的页面； （3）经测试，系统关闭后无残留的用户鉴别信息。 应用/数据库服务器-MySQL: （1）身份鉴别信息释放或清除机制正常且满足要求； （2）数据库系统不保存终端历史记录。	
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	鉴别数据不存在此部分的控制需求,故此项不适用	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	鉴别数据不存在此部分的控制需求,故此项不适用	不适用

D.4.1.6.4 重要配置数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	招生信息网系统: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输 应用/数据库服务器-MySQL: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■使用数据库内置的SSL协议加密 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 业务终端-1、业务终端-2、运维及管理终端-1、运维及管理终端-2:	符合

安全控制点	测评指标	结果结论	符合程度
		（1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 应用/数据库服务器-nginx: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■站点使用HTTPS加密协议进行传输 ■宿主系统使用SSH加密协议进行传输 应用/数据库服务器: （1）系统在通信传输过程中对重要配置数据采取完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	应用/数据库服务器-nginx: （1）系统定义了相关需要备份的中间件重要数据； ■包括重要配置数据 （2）宿主系统定期完全依照备份策略，采用正确的配置进行本地备份； （3）中间件相关数据的备份周期合理； ■每天增量一次 ■每月全备一次 （4）中间件开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）设备定义了相关重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确	符合

安全控制点	测评指标	结果结论	符合程度
		的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 业务终端-1、业务终端-2、应用/数据库服务器、运维及管理终端-1、运维及管理终端-2: （1）操作系统定义了相关重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 招生信息网系统: （1）系统定义了相关需要备份重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 应用/数据库服务器-MySQL: （1）数据库系统定义了相关重要数据； ■包括重要配置数据 （2）数据库系统定期完全依照备份策略，采用正确的配置进行本地备份； （3）系统的备份周期为：每天一次增量、每月一次全备； （4）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用	WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、运维安全管理系统、防火墙-1、防火墙-2:	不符合

安全控制点	测评指标	结果结论	符合程度
	场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 应用/数据库服务器-MySQL: （1）数据库系统未能提供异地数据备份功能。 应用/数据库服务器-nginx、招生信息网系统: （1）单位未能提供异地数据备份措施。 业务终端-1、业务终端-2、运维及管理终端-1、运维及管理终端-2: （1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 应用/数据库服务器: （1）设备为服务器设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 核心交换机、汇聚交换机: （1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	重要配置数据不存在此部分的控制需求,故此项不适用	不适用
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息;	重要配置数据不存在此部分的控制需求,故此项不适用	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	重要配置数据不存在此部分的控制需求,故此项不适用	不适用

D.4.1.7 其他系统或设备

无

D.5 安全管理中心

D.5.1 安全通用要求

D.5.1.1 管理中心

安全控制点	测评指标	结果结论	符合程度

安全控制点	测评指标	结果结论	符合程度
系统管理	a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；	（1）网络中部署运维安全管理系统实现集中的系统管理； （2）系统对登录用户进行身份鉴别； ■包括合规的用户名 ■包括合规的口令策略 （3）系统用户标识具有唯一性； ■不存在多人共享 ■增加、删除用户或权限变更需经过审批 （4）系统可实现对账户的身份鉴别数据进行保密性和完整性保护； （5）系统管理操作模式具备控制措施； ■只允许系统管理员登录 ■具备特定的登录命令 ■具备特定的登录操作界面 （6）系统具备相应的管理操作审计措施。 ■可实现对系统管理操作进行审计 ■审计范围覆盖所有用户 ■操作审计不可被删除	符合
	b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。	（1）系统管理员对系统的资源和运行进行配置、控制和管理； ■包括用户身份管理 ■包括资源配置管理 ■包括系统加载和启动管理 ■包括系统运行的异常处理管理 ■包括数据和设备的备份与恢复管理 （2）系统的资源、运行及配置管理不够全面。 ■缺乏可信证书管理 ■缺乏可信基准库管理	不符合
审计管理	a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；	（1）网络中部署运维安全管理系统实现集中安全审计功能； （2）审计系统对审计管理员进行身份鉴别； ■包括合规的用户名 ■包括合规的口令策略 （3）审计系统用户标识具有唯一性； ■不存在多人共享 ■增加、删除用户或权限变更需经过审批 （4）审计系统管理操作模式具备控制措施； ■只允许审计管理员登录 ■具备特定的登录命令 ■具备特定的登录操作界面 （5）审计系统具备相应的管理操作审计措施。 ■可实现对安全审计操作进行审计 ■审计范围覆盖所有审计管理用户	符合

安全控制点	测评指标	结果结论	符合程度
		■操作审计不可被删除	
	b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	招生信息网系统: （1）审计管理员定期对审计记录进行分析，对发现的安全可疑事件及时处理； （2）单位具有安全审计策略文件，规范审计记录的存储、管理和查询要求； （3）审计管理员按规范要求对审计记录进行管理。 ■审计记录不可随意删除/修改 ■定期备份、存储审计记录 ■审计记录存储周期满足6个月要求 重要审计数据: 日志审计系统、运维安全管理系统: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要审计数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■网络设备、安全设备使用rsyslog协议进行传输 ■Linux操作系统使用rsyslog协议进行传输 ■Windows操作系统使用插件+SSL协议进行传输	符合

D.6 安全管理制度

D.6.1 安全通用要求

D.6.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。	（1）单位具有网络安全工作的总体方针和安全策略文件； ■具备独立的网络安全总体方针文件 ■具备涵盖网络安全总体方针策略要求的相关管理文件 ■具备安全策略文件 (2)制度内容包括明确的单位安全工作要求； ■安全目标 ■安全范围 ■安全原则 ■安全框架 ■各类安全策略 （3）管理文件详见《信息安全总体策略》。	符合

安全控制点	测评指标	结果结论	符合程度
管理制度	a) 应对安全管理活动中的主要管理内容建立安全管理制度；	（1）单位有针对安全管理活动中的各类管理内容建立安全管理制度； （2）现有制度已覆盖管理活动的主要的方面； ■具备文件控制管理 ■具备安全检查管理 ■具备人力资源及培训 ■具备设备管理 ■具备软件开发/外包开发项目管理 ■具备机房安全管理 ■具备信息分类及管理 ■具备网络安全管理 ■具备系统安全管理 ■具备恶意代码管理 ■具备变更控制 ■具备备份及介质管理 ■具备事件管理 ■具备应急预案 （3）制度详见：《信息安全总体策略》、《网络安全管理规范》、《组织安全结构和人员职责制度》、《人员管理制度》、《员工考核管理制度》。	符合
	b) 应对管理人员或操作人员执行的日常管理操作建立操作规程。	（1）单位针对相关业务日常管理的操作建立规程类管理制度； （2）现有制度已覆盖重要管理方面的系统维护手册和用户操作规程等； ■具备网络/安全管理 ■具备服务器管理 ■具备数据库管理 ■具备机房硬件设施管理 ■具备业务应用管理 （3）管理文件详见《设备及系统软件配置和操作手册》。	符合
制定和发布	a) 应指定或授权专门的部门或人员负责安全管理制度的制定；	（1）单位针对安全管理制度的制定，指定教育信息与网络中心部主要负责； （2）在已制定的相关制度中可查阅到被授权制定管理制度的部门/人员信息； （3）管理文件详见《安全管理组织规范》。	符合
	b) 安全管理制度应通过正式、有效的方式发布，并进行版本控制。	（1）单位针对制度的制定和发布要求，制定管理规范文件； （2）管理规范文件对文件制定及发布定义了规范要求； ■包括安全管理制度的制定和发布程序 ■包括格式要求	符合

安全控制点	测评指标	结果结论	符合程度
		■包括版本编号要求 （3）安全管理制度的收发登记记录有效； ■具备通过正式、有效的方式收发 ■具备正式发文 ■具备领导签署、单位盖章等 （4）管理文件详见《制度制定、发布、评审和修订管理制度》、《收发文登记记录》。	
评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	（1）单位针对制度的合理性和适用性需进行论证和审定及修订的要求，制定管理规范文件； （2）管理规范文件对制度的评审及修订定义了规范要求； （3）单位具有安全管理制度的审定或论证的过程记录； （4）单位对做过修订的制度，具备有修订版本的安全管理过程记录； （5）管理文件详见《制度制定、发布、评审和修订管理制度》及 《安全管理制度评审记录》。	符合

D.7 安全管理机构

D.7.1 安全通用要求

D.7.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
岗位设置	a) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；	（1）单位已明确网络安全管理工作的职能部门，并明确了各岗位职责； ■已设置机房管理员 ■已设置网络管理员 ■已设置安全管理员 （2）单位各部门职责文档已明确网络安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备网络安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	符合
	b) 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。	（1）单位已明确系统安全管理工作的职能部门，并明确了各岗位职责； ■已设置系统管理员 ■已设置数据管理员 ■已设置审计管理员 ■已设置应用管理员 （2）单位各部门职责文档已明确系统安全管理工作的职能部门和各负责人职责；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）单位各岗位职责文档已具备系统安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	
人员配备	应配备一定数量的系统管理员、审计管理员和安全管理员等。	（1）单位针对人员配备要求，制定了管理制度； （2）单位按要求配备一定数量的重要岗位管理人员； （3）单位针对各岗位人员，制定并维护人员档案； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	符合
授权和审批	a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；	（1）单位在制度中用文字描述或在流程图中明确，对关键活动进行审批； ■具备部门职责文档明确各部门审批事项 ■具备岗位职责文档明确各岗位审批事项 （2）单位对审批过程明确审批权限，对各项信息系统的重要操作与变更明确审批部门和批准人； （3）管理文件详见《授权和审批管理规定》。	符合
	b）应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。	（1）单位针对各项业务操作及变更等建立了审批程序规定； ■包括系统变更 ■包括重要操作 ■包括物理访问 ■包括系统接入 （2）单位针对系统变更、系统接入、物理范围等事项已明确按审批程序执行,记录有批准人签字； （3）管理文件详见《授权和审批管理规定》。	符合
沟通和合作	a）应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；	（1）单位针对机构内部管理人员之间、部门之间的沟通与合作，制定了管理制度； （2）单位的管理制度规范了合作和沟通的方式和周期； （3）单位有组织机构内部人员联系表； （4）单位有定期召开信息安全会议，保存有会议纪要； （5）管理文件详见《安全教育和培训制度》、《技能培训记录》《外部联系表》。	符合
	b）应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；	（1）单位针对加强与外部单位的合作与沟通，制定了管理制度规定； ■包括公安机关 ■包括网络安全职能部门	符合

安全控制点	测评指标	结果结论	符合程度
		■包括职能监管机构 ■包括各类供应商 ■包括业界专家 ■包括安全组织 （2）单位能按要求与相关单位保持沟通合作，并提供相关单位联系方式和交流会议纪要； （3）管理文件详见《安全教育和培训制度》、《技能培训记录》、《外部联系表》。	
	c）应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	（1）单位建立了完善的对外联单位的联系列表； ■记录单位名称 ■记录合作内容 ■记录联系人 ■记录联系方式 （2）管理文件详见《外部联系表》。	符合
审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。	（1）单位针对定期开展常规安全检查，制定了管理制度； （2）单位对检查工作的范围、过程、要求等管理的比较完善； ■系统日常运行 ■系统漏洞 ■数据备份 ■包括敏感系统检查人员 （3）单位已按要求由安全管理员定期检查，检查内容需覆盖系统运行相关的管理活动，并能提供安全检查报告； （4）管理文件详见《安全审查和检查管理规范》； （5）单位开展的检查工作不够完善。 ■未定期检查	部分符合

D.8 安全管理人员

D.8.1 安全通用要求

D.8.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
人员录用	a）应指定或授权专门的部门或人员负责人员录用；	（1）单位授权专门的部门负责人员录用工作，制定了管理制度规范； （2）由人力资源保障科负责人员录用工作； （3）管理文件详见《人员管理制度》。	符合
	b）应对被录用人员的身份、安全背景、专业资格或资质等进行审查。	（1）单位针对人员录用过程，制定了明确要求，并形成人员安全管理制度； （2）单位现有管理制度明确说明录用人员应	符合

安全控制点	测评指标	结果结论	符合程度
		具备的条件； ■包括学历/学位要求 ■包括技术人员的专业技术要求 ■包括管理人员的安全管理要求 （3）单位按规定执行人员录用的相关审查过程； ■包括录用人身份 ■包括安全背景 ■包括专业资格 ■包括资质 （4）管理文件详见《人员管理制度》、《人员入职考核记录》。	
人员离岗	应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。	（1）单位针对离岗人员权限终止及取回机构提供的各种设施的要求，制定了管理制度； （2）单位按规范开展对离岗人员的相关管理工作； ■明确负责部门 ■及时终止其访问权限 ■交还身份证件 ■交还软硬件设备 （3）管理文件详见《人员管理度》、《人员离岗申请表》、《离场信息资料交接表》。	符合
安全意识教育和培训	应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。	（1）单位针对人员安全培训及责任和惩戒措施，制定了管理制度； （2）单位已开展安全意识教育及岗位技能培训 ■具备明确培训周期 ■具备有效的培训方式 ■具备清晰的培训内容 ■具备考核要求 （3）管理文件详见《安全教育和培训制度》。	符合
外部人员访问管理	a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；	（1）单位针对外部人员物理访问，制定了外部人员访问管理文档； ■明确允许外部人员访问的范围 ■明确外部人员进入的条件 ■明确外部人员进入的访问控制措施 （2）单位具备有效的外部人员访问重要区域的书面申请文档； ■具有申请人 ■具有申请原因 ■具有范围 ■具有日期 ■具有批准人签字	符合

安全控制点	测评指标	结果结论	符合程度
		（3）单位具备外部人员访问重要区域的登记记录； ■记录进入时间、 ■记录离开时间 ■记录访问区域 ■记录陪同人信息 （4）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。	
	b）应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；	（1）单位针对外部接入受控网络访问系统，制定了管理制度； （2）单位具备外部人员接入受控网络前的申请审批流程； （3）单位具备外部人员接入及访问系统的书面申请文档； ■具有申请人 ■具有申请原因 ■具有访问权限 ■具有日期 ■具有批准人签字 （4）单位具备外部人员接入及访问系统的登记记录； ■记录访问权限 ■记录访问时限 ■记录账户 （5）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。	符合
	c）外部人员离场后应及时清除其所有的访问权限。	（1）单位针对人员离场后的清理工作，制定了管理制度； （2）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》； （3）单位未完全按管理规范开展人员离场后的清理工作。 ■缺乏清理记录 ■未及时清除离场后的所有访问权限 ■未记录访问权限清除时间	不符合

D.9 安全建设管理

D.9.1 安全通用要求

D.9.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
定级和备案	a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；	（1）单位的被测系统于2022年4月已完成备案； （2）系统备案相关文档（定级报告）中明确等级划分方法和理由，SAG三个方面的级别描述清晰； （3）管理文件详见《定级备案》。	符合
	b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；	（1）单位针对系统定级结果的审批及评审工作等要求，制定了管理制度； （2）现有系统的定级已具备合理性和正确性审定； ■具备单位部门审定 （3）管理文件详见《定级备案》。	符合
	c) 应保证定级结果经过相关部门的批准；	（1）单位针对系统定级结果的上级批准要求，制定了管理制度； （2）现有系统的定级获得了相关部门的批准； （3）管理文件详见《定级备案》。	符合
	d) 应将备案材料报主管部门和相应公安机关备案。	（1）单位对被测系统的等级备案表、定级报告等备案材料已经报相应公安机关备案； （2）单位具备公安机关出具的备案号； （3）管理文件详见《定级备案》。	符合
安全方案设计	a) 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；	（1）单位未具备适用于被测系统的安全规划设计方案； （2）现有方案文档未能完全按照规范要求选择安全措施。 ■缺乏安全保护等级的要求 ■缺乏风险分析结果的要求 ■缺乏实际安全需求	不符合
	b) 应根据保护对象的安全保护等级进行安全方案设计；	（1）单位未具备完整的安全设计方案相关的文档。 ■缺乏总体规划 ■缺乏安全设计方案 ■缺乏相关配套文件 ■缺乏保护对象的安全保护等级要求	不符合
	c) 应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； ■缺乏安全整体规划 ■缺乏安全设计方案 ■缺乏安全配套文件 （2）单位未对相关论证过程及内容进行完整的记录。	不符合
产品采购和使用	a) 应确保网络安全产品采购和使用符合国家的有关	（1）单位已建立安全产品管理的相关管理规定；	符合

安全控制点	测评指标	结果结论	符合程度
	规定；	■包括采购要求 ■包括使用要求 （2）单位具备安全产品采购流程及相关实施文档； （3）被测系统使用的安全产品具备销售许可资质； （4）安全产品具均为国内产品； （5）管理文件详见《设备安全管理制度》。	
	b）应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。	（1）单位已建立密码产品与服务管理的相关管理制度； ■包括采购要求 ■包括使用要求 （2）系统未使用密码产品； （3）管理文件详见《设备安全管理制度》。	符合
自行软件开发	a）应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。	不适用
	b）应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。	不适用
外包软件开发	a）应在软件交付前检测其中可能存在的恶意代码；	（1）单位针对软件交付前测试恶意代码的要求，制定了管理制度； （2）管理文件详见《外包开发软件管理规定》； （3）单位未在软件交付之前按要求对所有软件开展恶意代码检测。 ■缺乏恶意代码检测报告	不符合
	b）应保证开发单位提供软件设计文档和使用指南。	（1）单位制定软件开发项目验收要求，明确开发单位的提交材料； （2）开发单位提供软件日常维护和使用所需的文档； ■包括需求分析说明书 ■包括软件设计说明书 ■包括软件操作手册 （3）管理文件详见《外包开发软件管理规定》、《设备及系统软件配置和操作手册》。	符合
工程实施	a）应指定或授权专门的部门或人员负责工程实施过程的管理；	（1）单位针对专门的部门负责工程实施过程的管理要求，制定管理度； （2）单位由专岗负责系统建设的工程实施，且按照实施方案的要求对进度和质量进行控制； （3）管理文件详见《工程实施管理制度》。	符合
	b）应制定安全工程实施方	（1）单位制定了详细的工程实施方案；	符合

安全控制点	测评指标	结果结论	符合程度
	案控制工程实施过程。	■包括工程时间限制 ■包括进度控制 ■包括质量控制 （2）工程实施单位严格按照方案执行，并有过程记录； （3）管理文件详见《测试及验收方案》、《工程项目实施方案》。	
测试验收	a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；	（1）单位可提供被测系统的合规测试验收方案； ■包括测试人员 ■包括测试验收内容 ■包括现场操作过程 （2）管理文件详见《测试及验收方案》、《工程项目实施方案》； （3）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。 ■缺乏验收报告 ■缺乏报告审定意见	部分符合
	b）应进行上线前的安全性测试，并出具安全测试报告。	（1）单位对系统上线前需开展安全性测试的要求，制定管理制度； （2）管理文件详见《外包开发软件管理规定》、《系统交付管理》； （3）针对系统上线前的安全性测试工作存在问题。 ■缺乏测试报告	不符合
系统交付	a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；	（1）单位具备系统交付清单； （2）系统交付清单内容较详细； ■包括设备 ■包括软件 ■包括文档 （3）单位的清点工作较合规； ■已依据交付清单开展清点工作 （4）管理文件详见《系统交付管理》、《资产清单》。	符合
	b）应对负责运行维护的技术人员进行相应的技能培训；	（1）单位已对负责系统运行维护的技术人员进行了技能培训； （2）具备运维人员的培训记录； ■包括培训时间 ■包括培训地点 ■包括培训对象 ■包括培训内容 ■包括培训参与人员签字 （3）管理文件详见《系统交付管理》、《资	符合

安全控制点	测评指标	结果结论	符合程度
		产清单》、《系统交付清单》、《技能培训记录》。	
	c) 应提供建设过程文档和运行维护文档。	（1）单位提供了系统建设过程中的文档； （2）单位提供了指导用户进行系统运维的文档和系统培训手册； （3）管理文件详见《系统交付管理》、《系统交付清单》、《设备及系统软件配置和操作手册》。	符合
等级测评	a) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；	（1）单位针对系统等级测评要求，制定管理制度； （2）系统按要求开展首次测评工作； （3）管理文件详见《系统安全管理制度》。	符合
	b) 应在发生重大变更或级别发生变化时进行等级测评；	（1）管理制度中已规定在系统发生变更时及时对系统进行等级测评； （2）系统未发生过重大变更，系统等级未发生变化； （3）管理文件详见《系统安全管理制度》。	符合
	c) 应确保测评机构的选择符合国家有关规定。	（1）已选择在“全国等级保护测评机构推荐目录”中的测评单位进行等级测评； （2）管理文件详见《系统安全管理制度》、《网络安全等级保护测评服务合同》。	符合
服务供应商选择	a) 应确保服务供应商的选择符合国家的有关规定；	（1）单位在管理制度内明确提出安全服务供应商选择的要求； （2）单位选择的安全服务商符合国家的有关规定，具备相应的安全服务资质； （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。	符合
	b) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。	（1）单位的管理制度中已规定，需与安全服务商签订安全相关的协议并明确整个服务供应链各方需履行的网络安全相关义务； （2）单位已按规定与选定的安全服务商签订合规的协议； ■明确整个服务供应链各方需履行的网络安全相关义务 ■包括保密范围 ■包括安全责任 ■包括违约责任 ■包括协议的有效期限 ■包括责任人签字 （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。	符合

D.10 安全运维管理

D.10.1 安全通用要求

D.10.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
环境管理	a) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；	（1）单位建立机房安全方面的管理制度，对有关运维方面的管理作出规定； ■指定教育信息与网络中心部门负责管理 ■包括出入管理要求 ■包括定期维护要求 ■包括空调要求 ■包括供配电设备要求 ■包括消防设施要求 ■包括温湿度控制要求 （2）单位具备完整的机房出入登记记录； ■记录来访人员 ■记录来访时间 ■记录离开时间 ■记录携带物品 （3）单位具备完整的机房基础设施的维护记录； ■记录维护日期 ■记录维护人 ■记录维护设备 ■记录故障原因 ■记录维护结果 （4）管理文件详见《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。	符合
	b) 应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；	（1）单位建立机房安全方面的管理制度； ■包括物理访问管理 ■包括物品进出管理 ■包括环境安全管理 （2）单位现有机房管理记录与制度相符； ■具备物理访问记录 ■具备物品进出记录 ■具备环境安全相关记录 （3）制度详见：《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。	符合
	c) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	（1）单位机房安全管理制度已明确来访人员的接待区域的要求； （2）单位按规范要求开展人员来访接待； ■划分来访人员的接待区域 ■记录来访人员的情况	符合

安全控制点	测评指标	结果结论	符合程度
		（3）单位办公环境未发现有随意放置含有敏感信息介质的情况； ■无纸档文件 ■无移动介质 （4）制度详见：《机房安全管理制度》、《物理安全管理规范》、《办公环境保密管理》。	
资产管理	应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。	（1）单位已建立有效的资产清单； （2）单位现有资产清单内容较全面； ■包括设备设施类别 ■包括软件类别 ■包括文档类别 ■包括资产责任人 ■包括所属级别 ■包括所处位置 ■包括所处部门 （3）制度详见：《设备安全管理制度》、《资产清单》。	符合
介质管理	a）应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；	（1）介质按管理要求放置于受控的环境中（如：机房）； （2）介质管理具备较全面的记录； ■包括介质归档 ■包括使用情况 ■包括定期盘点记录 （3）制度详见：《设备安全管理制度》、《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。	符合
	b）应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。	（1）介质管理制度中对介质安全传输有明确规定； ■包括人员选择 ■包括打包要求 ■包括交付要求 （2）存储重要信息的介质在物理传输过程，具备严格的环节控制，无重大环节疏漏； （3）对介质的归档和查询均具备记录； （4）制度详见：《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。	符合
设备维护管理	a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	（1）单位人员岗位职责相关文档已明确设备维护管理的责任部门； （2）单位对各类设施、设备进行定期维护； （3）制度详见：《设备安全管理制度》、《设	符合

安全控制点	测评指标	结果结论	符合程度
		备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。	
	b) 应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。	（1）单位建立了配套设施、软硬件维护管理方面的管理制度； ■包括维护人员的责任 ■包括维修和服务的审批 ■包括维修过程的监督控制 （2）单位开展相关工作与制度相符，且保留记录； ■包括维修和服务审批 ■包括维修过程记录 （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。	符合
漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。	（1）单位制定管理制度，规范对安全漏洞和隐患的检测、识别及评估修补要求； （2）制度详见：《恶意代码防范管理制度》； （3）单位未严格按规范开展漏洞及安全隐患检测工作。 ■未定期开展漏洞扫描	不符合
网络和系统安全管理	a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；	（1）单位建立系统安全管理文档，对系统管理员的管理制定了要求； ■包括角色划分 ■包括角色的责任 ■包括角色权限 （2）单位对各类关键角色建立了相应的工作职责文档； ■包括安全管理员 ■包括网络管理员 ■包括系统管理员 ■包括数据管理员 ■包括审计管理员 （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	符合
	b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	（1）单位制定管理制度，对系统账号进行管理； ■指定专人 ■包括申请账户管理 ■包括建立账户管理 ■包括删除账户管理 （2）单位按管理规范开展账号管理工作； ■具备相关审批流程 ■具备相关审批记录	符合

安全控制点	测评指标	结果结论	符合程度
		■具备管理登记记录 （3）账户管理记录内容较完整； ■包括变更日期 ■包括变更时间 ■包括变更人 ■包括变更设备/系统 ■包括变更结果 （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	
	c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	（1）单位建立了网络和系统安全管理制度； （2）网络和系统安全管理制度内容较全面； ■包括安全策略要求 ■包括账户管理 ■包括配置文件的生成及备份 ■包括变更审批管理 ■包括授权访问 ■包括最小服务控制 ■包括升级与打补丁管理 ■包括审计日志管理 ■包括口令管理 （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	符合
	d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；	（1）单位对重要设备、系统的配置和操作建立配置手册； ■包括操作系统 ■包括数据库 ■包括网络设备 ■包括安全设备 ■包括应用和组件 （2）现有操作配置手册已明确操作步骤、参数配置； （3）制度详见：《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。	符合
	e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。	(1)单位制定日常运维管理的相关制度规范； (2)单位按制度规范开展日常运维管理工作； （3）单位具备合规的运维记录； ■包括日常巡检记录 ■包括运行维护记录 ■包括参数的设置记录 ■包括参数的修改记录 （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》、《设备及系统软件配置和操作手册》、《软硬	符合

安全控制点	测评指标	结果结论	符合程度
		件日常维护管理规程》。	
恶意代码防范管理	a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	（1）单位制定恶意代码防范管理制度，明确对外来计算机或存储设备接入系统前进行恶意代码检查； （2）单位按外来计算机接入恶意代码检查规范开展工作； ■对外来计算机接入进行恶意代码检查 ■具备合规的检测记录 （3）单位制定培训管理制度，明确需通过培训提升员工的防恶意代码意识； （4）单位按培训管理要求开展工作； ■定期对员工开展防恶意代码意识培训 ■具备合规的培训记录 （5）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申请表》、《信息管理系统漏洞检查表》。	符合
	b) 应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；	（1）建立恶意代码防范管理文档； （2）管理制度中覆盖防恶意代码软件的授权使用、恶意代码库升级、定期查杀等内容； （3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》。	符合
	c) 应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。	（1）单位指定专门的部门负责定期验证防范恶意代码攻击的技术措施的有效性； （2）单位近期未发生过严重的恶意代码攻击事件； （3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申请表》、《信息管理系统漏洞检查表》； （4）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。 ■未定期对相关产品的恶意代码库进行升级 ■未对所有防病毒产品上截获的恶意代码进行分析并汇总上报	部分符合
配置管理	应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。	（1）单位制定了基本配置信息管理的制度要求； ■包括网络拓扑结构 ■包括设备安装的软件组件 ■包括软件组件的版本 （2）管理文件详见：《主机安全管理规范》、《网络安全管理规范》、《应用安全管理规范》、《网络配置信息》。	符合
密码管理	a) 应遵循密码相关国家标	（1）单位不了解现有密码相关的国家标准和	不符合

安全控制点	测评指标	结果结论	符合程度
	准和行业标准；	行业标准； （2）单位缺乏密码管理要求的制度文档。	
	b）应使用国家密码管理主管部门认证核准的密码技术和产品。	（1）单位未采购涉及密码技术的产品，不适用。	不适用
变更管理	应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。	（1）单位建立了关于系统变更管理的制度文件； （2）现有变更管理制度覆盖了变更管理的各方面要求； ■包括变更管理要求 ■包括整体变更管理流程 ■包括变更内容分析与论证 ■包括变更方案审批流程 ■包括变更后通报 （3）制度详见：《变更控制管理制度》、《通用变更记录表》。	符合
备份与恢复管理	a）应识别需要定期备份的重要业务信息、系统数据及软件系统等；	（1）单位根据业务重要程度，制定了需要定期备份的重要业务信息列表或清单。清单内需要定期备份的重要数据已经过用户方确认； （2）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。	符合
	b）应规定备份信息的备份方式、备份频度、存储介质、保存期等；	（1）单位建立了备份与恢复管理相关的安全管理制度； （2）备份与恢复管理的相关要求比较明确； ■规定备份方式 ■规定备份频度 ■规定存储介质 ■规定保存期 （3）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。	符合
	c）应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	（1）单位现有管理制度，明确了数据备份策略和数据恢复策略，以及备份程序和恢复程序； （2）单位可按策略要求实现重要数据的定期备份与恢复性测试； （3）单位现有的备份的数据均经过恢复性测试，可确保备份的数据可用； （4）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份	符合

安全控制点	测评指标	结果结论	符合程度
		与恢复管理制度》、《系统及应用数据备份管理规范》。	
安全事件处置	a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件；	（1）单位已在安全培训及宣传过程中告知用户在发现安全弱点和可疑事件时及时向安全管理部门报告； （2）单位在系统运维过程中对发现的安全弱点和可疑事件均编制了对应的报告或相关文档； （3）单位现有安全弱点和可疑事件报告文档内容较详实； （4）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	符合
	b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；	（1）单位制定了安全事件报告和处置管理制度； （2）现有安全事件管理制度内容较完整； ■包括安全事件类型分类 ■包括安全事件有关的工作职责 ■包括安全事件的报告 ■包括安全事件的处置 ■包括安全事件的响应流程 （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	符合
	c) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。	（1）单位具备对安全事件的分析、处理、总结、防范等的报告／过程文档； （2）单位提供的安全事件报告和响应处置记录内容较完整； ■记录引发安全事件的原因 ■记录事件的证据 ■记录处置过程 ■包括经验教训 ■提出补救措施 （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	符合
应急预案管理	a) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；	（1）单位制定重要事件的应急预案； （2）单位现有应急预案涉及的类型范围较全面； ■包括针对机房的预案 ■包括针对网络传输的预案 ■包括针对网络设备的预案 ■包括针对操作系统的预案 ■包括针对数据库的预案 ■包括针对安全漏洞攻击的预案 ■包括针对恶意代码的预案	符合

安全控制点	测评指标	结果结论	符合程度
		■包括针对数据泄露的预案 （3）单位现有应急预案的内容较完整； ■明确重要事件的应急处理流程 ■明确系统恢复流程等内容 （4）制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。	
	b）应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。	（1）单位定期对相关人员进行应急预案培训； （2）单位根据不同的应急预案，按要求进行应急演练； （3）单位具备近期应急预案工作开展的相关记录； ■具备培训记录 ■具备演练记录 （4）单位提供的应急预案培训记录比较完整； ■明确培训对象 ■明确培训内容 ■明确培训结果 （5）单位提供的应急预案演练记录比较完整； ■记录演练时间 ■记录主要操作内容 ■记录演练结果 （6）经检查单位目前一旦出现应急事件，可参照预案合理有序的进行应急事件处置过程； （7）制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。	符合
外包运维管理	a）应确保外包运维服务商的选择符合国家的有关规定；	（1）单位目前未涉及任何外包运维服务情况，不适用。	不适用
	b）应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。	（1）单位目前未涉及任何外包运维服务情况，不适用。	不适用

D.11 其他安全要求

本次测评不涉及其他安全要求指标。

附录E 漏洞扫描结果记录

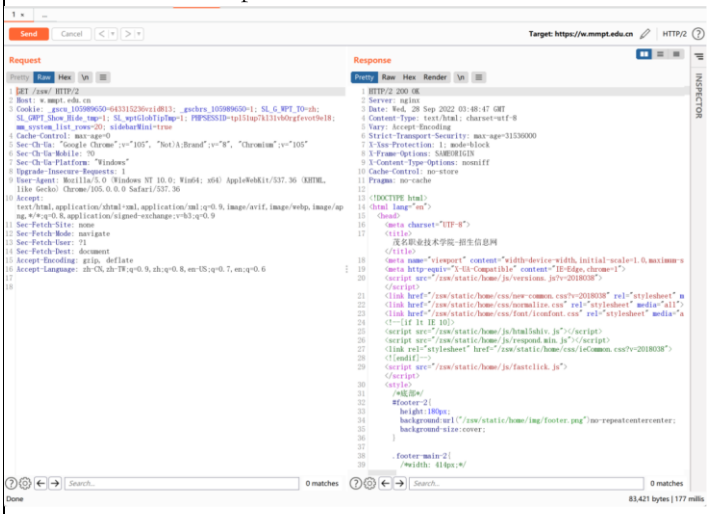
附录E表-1漏洞扫描主要安全漏洞

序号	危险程度	漏洞名称	影响IP
1	低	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161) 此类漏洞涉及服务器存储设备、网络设备。	10.1.4.10/应用/数据库服务器 172.16.1.2/核心交换机
2	低	允许Traceroute探测 此类漏洞涉及服务器存储设备、安全设备、	10.1.4.10/应用/数据库服务器 10.2.1.4/运维安全管理系统

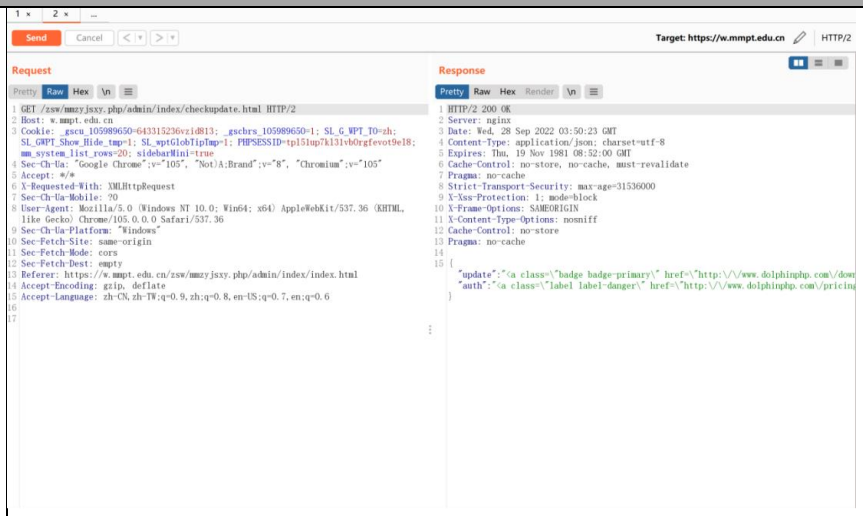
序号	危险程度	漏洞名称	影响IP
		网络设备。	10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/上网行为管理系统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/汇聚交换机 172.16.1.2/核心交换机
3	低	SSH版本信息可被获取 此类漏洞涉及服务器存储设备。	10.1.4.10/应用/数据库服务器

附录F 渗透测试结果记录

F.1 业务应用软件平台 缺少“Content-Security-Policy”响应头

缺少“Content-Security-Policy”响应头	
危险程度	低
渗透位置	JA,JB,JC
影响URL实体	https://w.mmpt.edu.cn/zsw
渗透详情	渗透方法：使用BurpSuite抓包查看响应头未包含Content-Security-Policy字段 采用的工具：BurpSuite 测试过程：使用BurpSuite抓包查看响应头未包含Content-Security-Policy字段 

缺少“Content-Security-Policy”响应头	
危险程度	低
渗透位置	JA,JB,JC
影响URL实体	https://w.mmpt.edu.cn/zsw/mmzyjsxy.php/admin/index/checkupdate.html
渗透详情	渗透方法：使用BurpSuite抓包查看响应头未包含Content-Security-Policy字段： 采用的工具：BurpSuite 测试过程：使用BurpSuite抓包查看响应头未包含Content-Security-Policy字段：

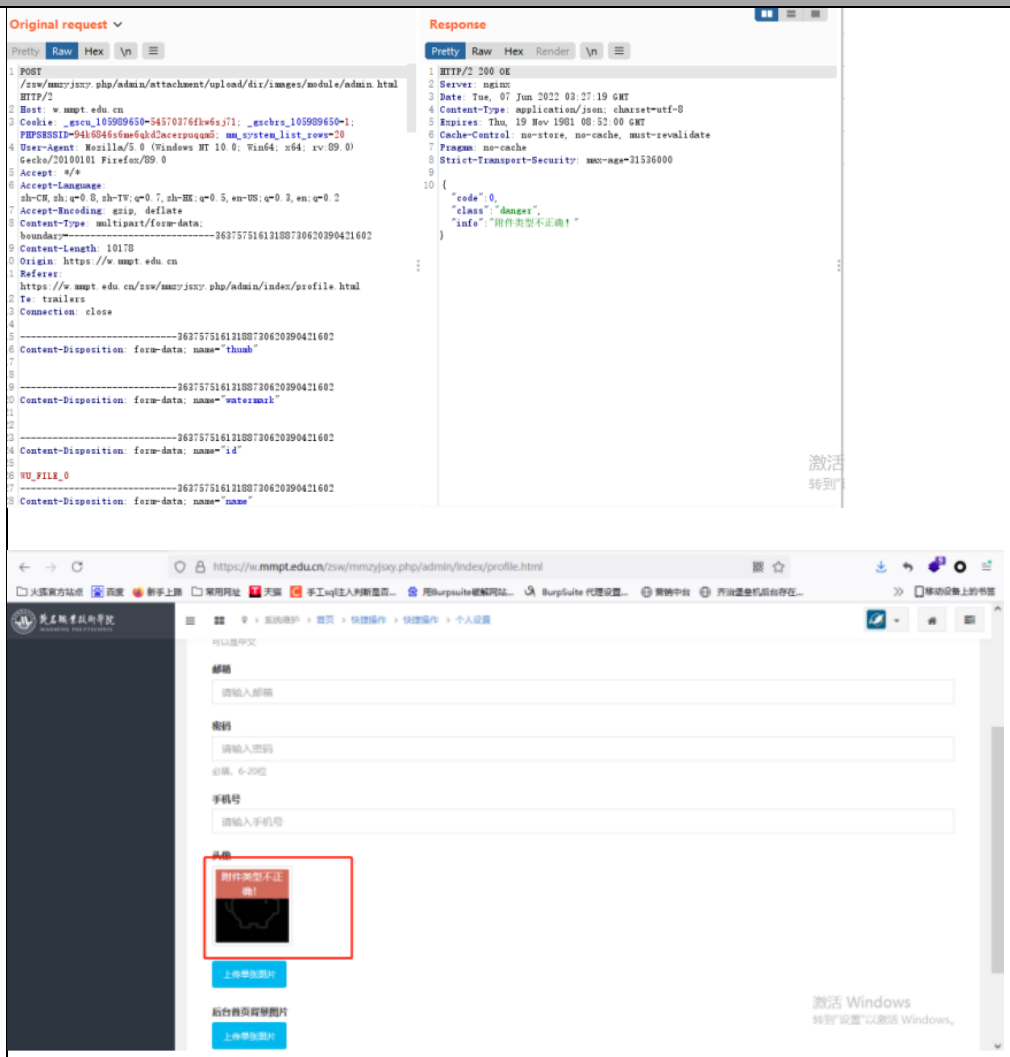
缺少“Content-Security-Policy”响应头	
	

F.2 业务应用软件平台 弱口令漏洞

弱口令漏洞	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：通过手工测试/暴力破解对登录接口测试是否存在弱口令 采用的工具：/ 测试过程：发现登录模块使用有效的图形验证码。 

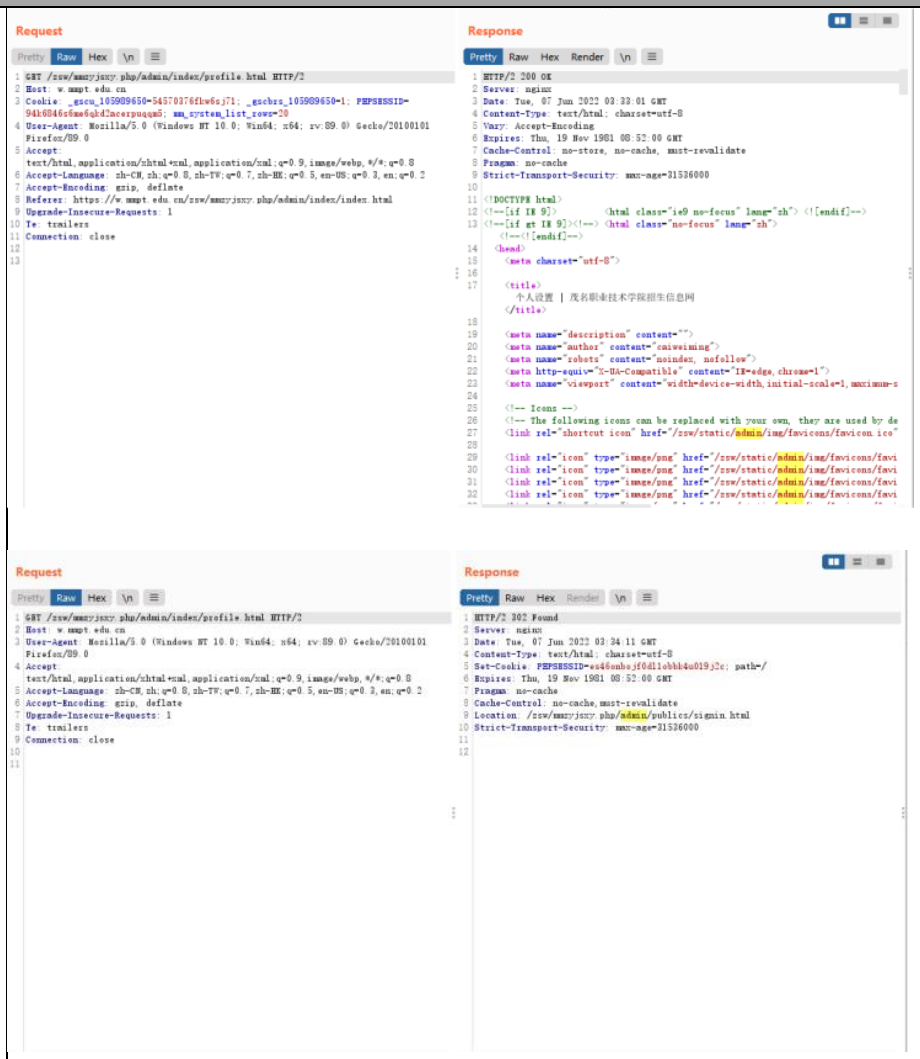
F.3 业务应用软件平台 任意文件上传

任意文件上传	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：测试能否成功上传含有恶意代码的脚本文件或其他可执行文件 采用的工具：Burpsuite 测试过程：通过数据包修改文件后缀，发现系统对文件上传格式做限制。

任意文件上传	
	

F.4 业务应用软件平台　　未授权访问

未授权访问	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：测试能否在系统未登录的状态下进行登录后功能访问或操作。 采用的工具：测试能否在系统未登录的状态下进行登录后功能访问或操作。 测试过程：在未登录的情况下无法访问用户管理信息。

未授权访问


附录G 威胁列表

附录G 表- 1威胁列表

序号	威胁列表	描述
1	恶意攻击	利用工具和技术对信息系统进行攻击和入侵。威胁行为包括：恶意代码、邮件勒索、网络攻击等。
2	软硬件故障	对业务实施或系统运行产生影响的设备硬件故障、通讯链路中断、系统本身或软件缺陷造等问题。威胁行为包括：设备故障、软件故障等。
3	管理不到位	由于制度缺失、不完善等原因导致安全管理无法落实或者不到位。威胁行为包括：管理不到位、媒体负面报道等。
4	无作为或操作失误	应该执行而没有执行相应的操作，或者无意执行了错误的操作。威胁行为包括：操作失误、维护错误等。
5	敏感信息泄漏	敏感信息泄露给不应了解的他人。威胁行为包括：内部信息泄露、外部信息泄露等。
6	物理环境影响	对信息系统正常运行造成影响的物理环境问题和自然

序号	威胁列表	描述
		灾害。威胁行为包括：物理损害等。
7	越权或滥用	越权访问本来无权访问的资源，或者滥用自己的权限破坏信息系统。威胁行为包括：未授权的设备使用、权限滥用、权限伪造等。
8	物理攻击	通过物理的接触造成对软件、硬件和数据的破坏。威胁行为包括：设备失效等。
9	篡改	非法修改信息，破坏信息的完整性使系统的安全性降低或信息不可用。威胁行为包括：硬件篡改、数据篡改等。
10	抵赖	否认所做的操作。威胁行为包括：行为否认（抵赖）、媒体负面报道等。

报告编号：44090243008-00002-22-0163-01

网络安全等级保护
智慧校园系统等级测评报告

委托单位：茂名职业技术学院

测评单位：广东南方信息安全研究院

报告时间：2022年10月30日

网络安全等级测评基本信息表

被测对象				
被测对象名称	智慧校园系统		安全保护等级	第二级（S2A2）
备案证明编号	44090243008-00002			
被测单位				
单位名称	茂名职业技术学院			
单位地址	广东省茂名市茂南区文明北路232号大院		邮政编码	525000
联系人	姓名	龙恒	职务/职称	教师
	所属部门	教育信息与网络中心	办公电话	0668-2920122
	移动电话	13377766618	电子邮件	372383968@qq.com
测评单位				
单位名称	广东南方信息安全研究院		机构代码	SC202127130010163
单位地址	广州市科学城彩频路9号B座12楼1202		邮政编码	510663
联系人	姓名	谢若雨	职务/职称	助理
	所属部门	办公室	办公电话	020-32290702
	移动电话	18819149895	电子邮件	office@cybersec-gd.cn
审核批准	编制人	林炯彦	编制日期	2022.10.30
	审核人	李	审核日期	2022.10.30
	批准人	陈	批准日期	2022.10.30

声明

本报告是智慧校园系统的等级测评报告。

本报告测评结论的有效性建立在被测评单位提供相关证据的真实性基础之上。

本报告中给出的测评结论仅对被测对象当时的安全状态有效。当测评工作完成后，由于被测对象发生变更而涉及到的系统构成组件（或子系统）本报告不再适用。

本报告中给出的测评结论不能作为对被测对象内部部署的相关系统构成组件（或产品）的测评结论。

在任何情况下，若需引用本报告中的测评结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。

单位名称：广东南方信息安全研究院

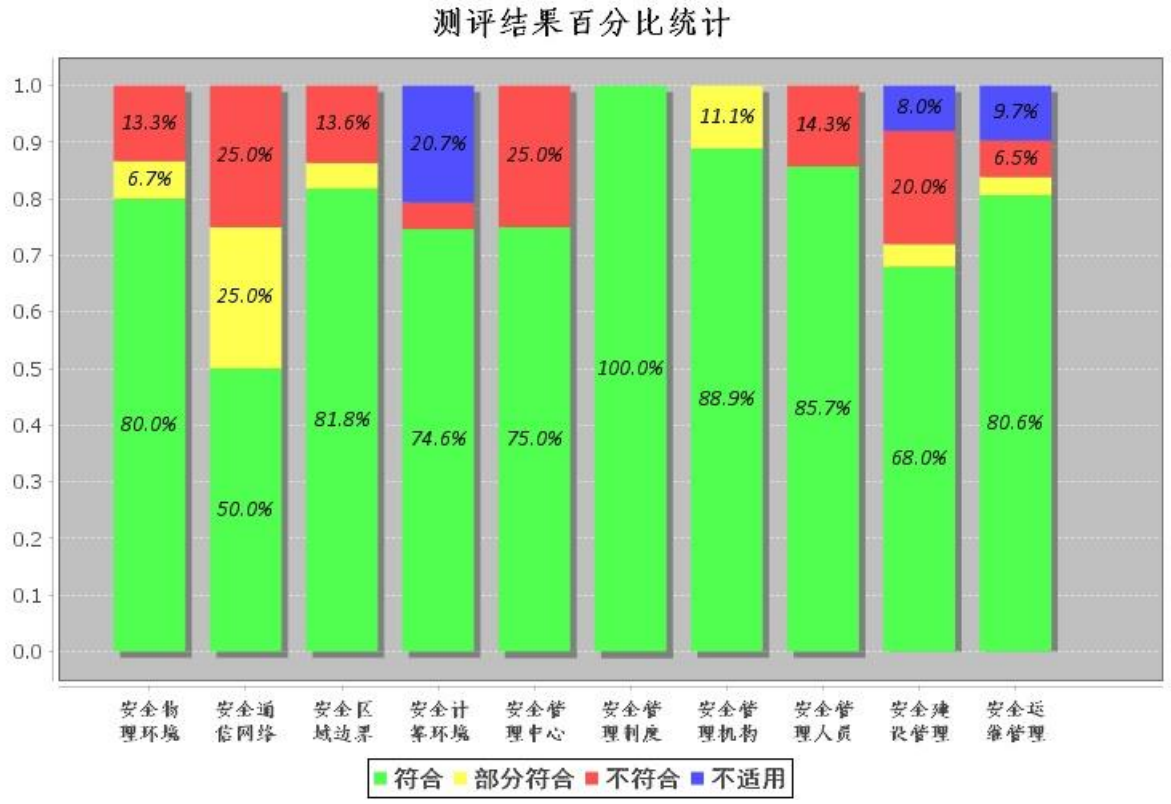
2022年10月30日

等级测评结论

测评结论和综合得分			
被测对象名称	智慧校园系统	安全保护等级	第二级（S2A2）
扩展要求应用情况	□云计算 □移动互联 □物联网 □工业控制系统 □大数据		
被测对象描述	智慧校园系统是由茂名职业技术学院统一组织规划建设，由江苏金智教育信息股份有限公司负责开发，于2021年1月正式投入运行，由教育信息与网络中心负责运行维护。茂名职业技术学院是该信息系统的业务主管部门，茂名职业技术学院为该信息系统定级的责任单位。 智慧校园系统网络主要分为4个区域，分别为外网边界区域、安全管理区域、服务器存储区域、办公网区域，主要由网络设备、安全设备组成，对互联网提供业务访问。智慧校园系统为B/S结构，主要由Linux平台的操作系统，Oracle平台的数据库系统，及Weblogic中间件系统组成。单位采用自主运维模式，通过部署运维及管理终端提供专用运维环境管理，采用运维安全管理系统实现设备的统一管理，并进行操作运维审计，日志审计系统进行设备日志统一收集存储与分析。 智慧校园系统包括校园移动应用、统一身份认证、服务能力开放、主数据管理、网上办事大厅等基础支撑模块，形成一体化的信息化整体架构，解决信息系统分别建立带来的数据孤岛和流程割裂问题，打通各部门的信息壁垒，为业务整合和流程整合提供技术支持。建立全校性的主数据平台，涵盖学院信息标准与数据规范的定义，共享数据目录的管理，数据的采集、共享和交换等。		
安全状况描述	智慧校园系统通信传输具备一定的保护措施，安全区域边界较清晰，网络层具备访问控制、安全审计的相应技术措施。各设备在身份鉴别、访问控制、安全审计、入侵防范方面具备控制措施。重要数据在数据完整性、个人信息保护方面具备保护措施。在安全管理制度层面较为完善。在网络架构不够完整，网络层在入侵防范、恶意代码和垃圾邮件防范的技术措施存在不足。重要数据在数据备份恢复方面存在不足。 智慧校园系统在本次测评中总共出现27类问题，其中0类高风险问题，11类中风险问题，16类低风险问题。在本次测评通过扫描及渗透发现4类漏洞问题，其中0类危险程度为高的漏洞，0类危险程度为中的漏洞，4类危险程度为低的漏洞。 智慧校园系统本次等级测评的综合得分为73.85，且不存在高等级安全风险，等级测评结论为中。		
等级测评结论	中	综合得分	73.85

总体评价

通过对信息系统基本安全保护状态的分析，茂名职业技术学院针对智慧校园系统面临的主要安全威胁采取了相应的安全机制，基本达到保护信息系统重要资产的作用。智慧校园系统在本次测评中采用了GB/T 22239-2019，其中安全通用要求135项，不适用5项。



在安全物理环境方面，针对安全通用要求，基础设施在防雷击、电磁防护、防水和防潮、物理位置选择、电力供应、防盗窃和防破坏、温湿度控制等方面较为完善（如：信息化机房）。在物理访问控制、防静电等方面还不够完善（如：信息化机房），机房出入口未配置电子门禁系统，机房内缺乏防静电措施（如防静电地板或铺设防静电地毯）。

在安全通信网络方面,针对安全通用要求,网络环境在通信传输等方面较为完善(如:安全通信网络)。在网络架构等方面还不够完善（如：安全通信网络），关键的应用服务和数据库服务网段未独立进行子网划分的情况。

在安全区域边界方面，针对安全通用要求，网络环境在边界防护、安全审计、访问控制等方面较为完善（如：外网边界区域，安全管理区域，服务器存储区域等）。在入侵防范、恶意代码和垃圾邮件防范等方面还不够完善(如:安全管理区域,办公网区域)，网络层部署防火墙,防火墙未配置对内部发起的攻击行为实现防范功能策略,无法检测、防止或限制从内部发起的网络攻击行为,现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。

在安全计算环境方面，针对安全通用要求，计算环境在个人信息保护、安全审计、数据完整性、访问控制、入侵防范、恶意代码防范、身份鉴别、剩余信息保护等方面较为完善。在主机方面，在可信验证等方面还不够完善（如：业务终端-2，业务终端-1，运维及管理终端-2等），缺乏对计算设备可信验证方面的安全设计要求，现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。在应用方面，在数据备份恢复等方面还不够完善（如：应用服务器-Weblogic），未能提供中间件重要数据的异地定时数据备份功能。在网络及安全设备方面，在可信验证等方面还不够完善（如：基线核查系统，上网行为管理系统，WEB应用防火墙等），设备不具备相关可信验证的技术措施。在数据保护方面，在数据备份恢复等方面还不够完善（如：重要个人信息，重要业务数据），未能提供应用软件系统重要数据的异地定时数据备份功能。

在安全管理中心方面，针对安全通用要求，安全控制措施在审计管理等方面较为完善（如：管理中心）。在系统管理等方面还不够完善（如：管理中心），系统管理的资源、运行及配置管理不够全面。

在安全管理制度方面,针对安全通用要求,管理制度体系在制定和发布、安全策略、管理制度、评审和修订等方面较为完善（如：制度文件、执行/记录文件）。

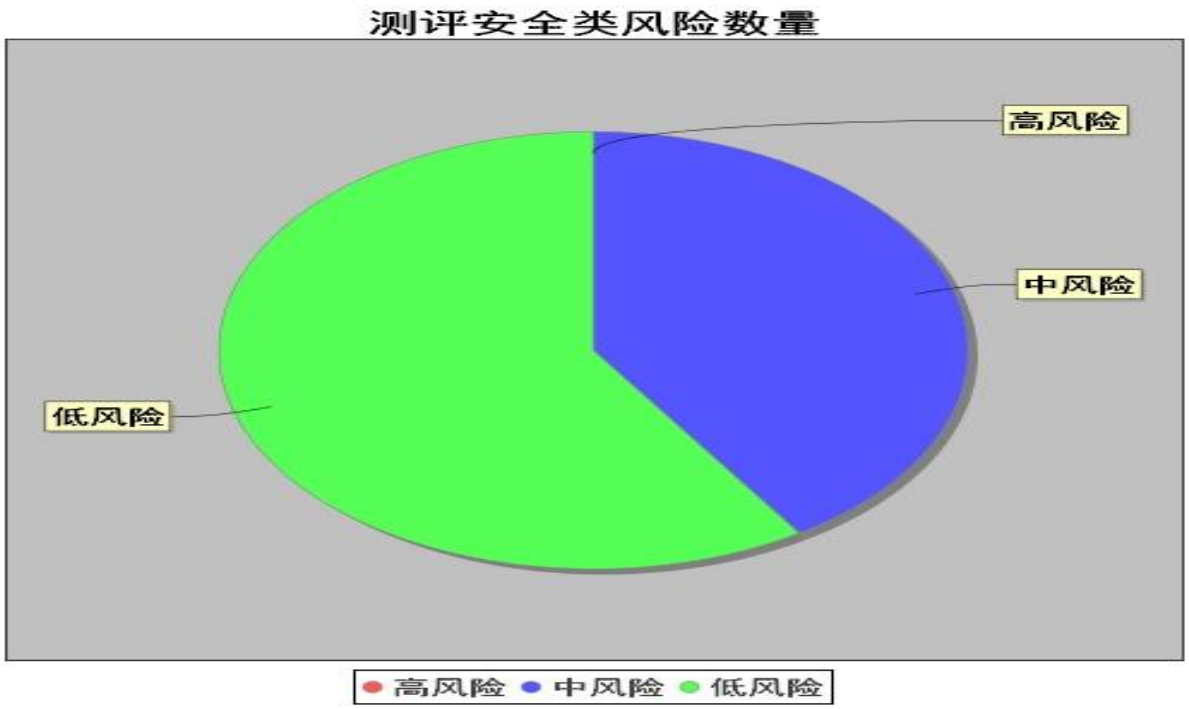
在安全管理机构方面，针对安全通用要求，机构建设在人员配备、沟通和合作、授权和审批、岗位设置等方面较为完善（如：制度文件、执行/记录文件）。在审核和检查等方面还不够完善（如：制度文件、执行/记录文件），单位开展的检查工作不够完善。

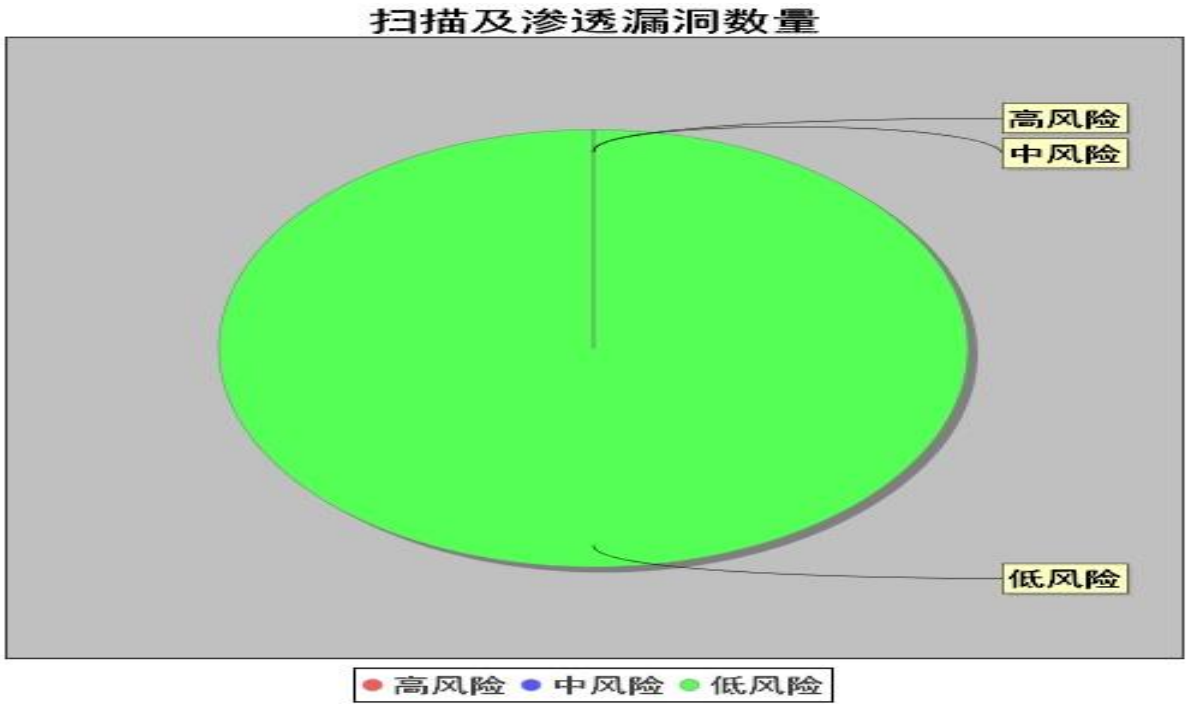
在安全管理人员方面,针对安全通用要求,人员在人员录用、安全意识教育和培训、人员离岗等方面较为完善（如：制度文件、执行/记录文件）。在外部人员访问管理等方面还不够完善（如：制度文件、执行/记录文件），单位未完全按管理规范开展人员离场后的清理工作。

在安全建设管理方面，针对安全通用要求，系统建设在定级和备案、工程实施、等级测评、产品采购和使用、服务供应商选择、系统交付等方面较为完善（如：制度文件、执行/记录文件）。在安全方案设计等方面还不够完善（如：制度文件、执行/记录文件），单位未具备完整的安全设计方案相关的文档，单位相关方案的设计的内容不够完善。

在安全运维管理方面，针对安全通用要求，系统运维在介质管理、设备维护管理、网络和系统安全管理、备份与恢复管理、资产管理、应急预案管理、环境管理、配置管理、安全事件处置、变更管理等方面较为完善（如：制度文件、执行/记录文件）。在密码管理等方面还不够完善（如：制度文件、执行/记录文件），单位不了解现有密码相关的国家标准和行业标准，单位缺乏密码管理要求的制度文档。

智慧校园系统在本次测评中总共出现27类问题，其中0类高风险问题,11类中风险问题，16类低风险问题。在本次测评通过扫描及渗透发现4类漏洞问题，其中0类危险程度为高的漏洞，0类危险程度为中的漏洞，4类危险程度为低的漏洞。





智慧校园系统本次等级测评的综合得分为73.85，且不存在高等级安全风险，等级测评结论为中。

主要安全问题及整改建议

一、安全物理环境

安全通用要求

(1)中风险 机房出入口未配置电子门禁系统（如：信息化机房）。 上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域,可能对系统的平稳运行造成影响。

建议安排专人7*24小时负责机房出入，对出入的人员进行身份鉴别和登记，且出入有专人陪同或在机房出入口配置电子门禁系统，控制、鉴别和记录进入的人员。

(2)中风险 机房内缺乏防静电措施（如防静电地板或铺设防静电地毯 ）（如：信息化机房）。 存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。

建议采用防静电地板或地面并采用必要的接地防静电措施。

二、安全通信网络

安全通用要求

(1)中风险 关键的应用服务和数据库服务网段未独立进行子网划分的情况（如：安全通信网络）。 上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变得更为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。

建议独立划分出应用服务器网段、数据库服务器网段。

三、安全区域边界

安全通用要求

(1)中风险 网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为（如：办公网区域）。 存在不

能及时发现内部主机作为攻击跳板，或网络攻击行为而造成系统损坏/网络资源浪费的风险。

建议网络层部署的防火墙配置对内部发起的攻击行为实现防范功能策略，实现检测、防止或限制从内部发起的网络攻击行为。

(2)中风险 现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面（如：办公网区域）。 无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。

建议现有部署的恶意代码防范措施网络边界覆盖全面，及时对恶意代码及逆行检测和清除。

四、安全计算环境

1、网络设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

2、安全设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

3、服务器和终端

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

4、系统管理软件/平台

安全通用要求

(1)中风险 未能提供中间件重要数据的异地定时数据备份功能（如：应用服务器

-Weblogic)。异地备份策略不完善/执行不到位,在发生地震或其他灾祸的极端情况下,会影响到业务服务的持续提供。

建议利用通信网络将中间件关键数据定时批量传送至备用场地,实现异地数据异地备份。

5、业务应用系统/平台

安全通用要求

(1)中风险 未能提供应用软件系统重要数据的异地定时数据备份功能（如：智慧校园系统）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。

建议利用通信网络将应用软件系统关键数据定时批量传送至备用场地,实现异地数据异地备份。

6、数据资源

安全通用要求

重要业务数据

(1)中风险 未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要业务数据）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。

建议利用通信网络将应用软件系统关键数据定时批量传送至备用场地,实现异地数据异地备份。

重要个人信息

(1)中风险 未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要个人信息）。 异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会

影响到业务服务的持续提供。

建议利用通信网络将应用软件系统关键数据定时批量传送至备用场地，实现异地数据异地备份。

7、其他系统或设备

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

五、安全管理中心

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

六、安全管理制度

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

七、安全管理机构

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

八、安全管理人员

安全通用要求

该层面不存在中、高风险问题，详细安全问题见3.13.2。

九、安全建设管理

安全通用要求

(1)中风险 单位未具备完整的安全设计方案相关的文档。单位相关方案的设计的内容不够完善（如：制度文件、执行/记录文件）。 相关合规的规划配套文件缺失，可能导

致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。

建议根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件。

十、安全运维管理

安全通用要求

(1)中风险 **单位不了解现有密码相关的国家标准和行业标准。单位缺乏密码管理要求的制度文档（如：制度文件、执行/记录文件）。 密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不到位，存在违反国家政策的风险。**

建议单位学习现有密码相关的国家标准和行业标准。建立密码管理要求的制度文档。

目录

网络安全等级测评基本信息表 I
声明 II
等级测评结论 III
总体评价 IV
主要安全问题及整改建议 VIII
一、安全物理环境 VIII
安全通用要求 VIII
二、安全通信网络 VIII
安全通用要求 VIII
三、安全区域边界 VIII
安全通用要求 VIII
四、安全计算环境 IX
1、网络设备 IX
安全通用要求 IX
2、安全设备 IX
安全通用要求 IX
3、服务器和终端 IX
安全通用要求 IX
4、系统管理软件/平台 IX
安全通用要求 IX
5、业务应用系统/平台 X
安全通用要求 X
6、数据资源 X
安全通用要求 X
7、其他系统或设备 XI
安全通用要求 XI
五、安全管理中心 XI
安全通用要求 XI
六、安全管理制度 XI
安全通用要求 XI
七、安全管理机构 XI
安全通用要求 XI
八、安全管理人员 XI
安全通用要求 XI
九、安全建设管理 XI
安全通用要求 XI
十、安全运维管理 XII
安全通用要求 XII

目录.....XIII
1 测评项目概述.....1
1.1 测评目的.....1
1.2 测评依据.....1
1.3 测评过程.....2
1.4 报告分发范围.....5
2 被测对象描述.....5
2.1 被测对象概述.....5
2.1.1 定级结果.....5
2.1.2 业务和采用的技术.....5
2.1.3 网络结构.....5
2.2 测评指标.....7
2.2.1 安全通用要求指标.....7
2.2.2 安全扩展要求指标.....9
2.2.3 其他安全要求指标.....10
2.2.4 不适用安全要求指标.....10
2.3 测评对象.....10
2.3.1 测评对象选择方法.....10
2.3.2 测评对象选择结果.....11
2.3.2.1 物理机房.....12
2.3.2.2 网络设备.....12
2.3.2.3 安全设备.....12
2.3.2.4 服务器.....13
2.3.2.5 终端设备.....13
2.3.2.6 其他系统或设备.....13
2.3.2.7 系统管理软件/平台.....14
2.3.2.8 业务应用软件/平台.....14
2.3.2.9 数据资源.....15
2.3.2.10 安全相关人员.....15
2.3.2.11 安全管理文档.....16
3 单项测评结果分析.....21
3.1 安全物理环境.....21
3.1.1 已有安全控制措施汇总分析.....21
3.1.2 主要安全问题汇总分析.....23
3.2 安全通信网络.....23
3.2.1 已有安全控制措施汇总分析.....23
3.2.2 主要安全问题汇总分析.....24
3.3 安全区域边界.....24
3.3.1 已有安全控制措施汇总分析.....24
3.3.2 主要安全问题汇总分析.....26
3.4 安全计算环境.....26
3.4.1 网络设备.....26

3.4.1.1 已有安全控制措施汇总分析 26
3.4.1.2 主要安全问题汇总分析 28
3.4.2 安全设备 29
3.4.2.1 已有安全控制措施汇总分析 29
3.4.2.2 主要安全问题汇总分析 32
3.4.3 服务器和终端 32
3.4.3.1 已有安全控制措施汇总分析 33
3.4.3.2 主要安全问题汇总分析 37
3.4.4 系统管理软件/平台 37
3.4.4.1 已有安全控制措施汇总分析 37
3.4.4.2 主要安全问题汇总分析 40
3.4.5 业务应用系统/平台 41
3.4.5.1 已有安全控制措施汇总分析 41
3.4.5.2 主要安全问题汇总分析 43
3.4.6 数据资源 43
3.4.6.1 已有安全控制措施汇总分析 43
3.4.6.2 主要安全问题汇总分析 44
3.4.7 其他系统或设备 44
3.4.7.1 已有安全控制措施汇总分析 44
3.4.7.2 主要安全问题汇总分析 44
3.5 安全管理中心 44
3.5.1 已有安全控制措施汇总分析 44
3.5.2 主要安全问题汇总分析 45
3.6 安全管理制度 46
3.6.1 已有安全控制措施汇总分析 46
3.6.2 主要安全问题汇总分析 47
3.7 安全管理机构 47
3.7.1 已有安全控制措施汇总分析 47
3.7.2 主要安全问题汇总分析 48
3.8 安全管理人员 48
3.8.1 已有安全控制措施汇总分析 49
3.8.2 主要安全问题汇总分析 50
3.9 安全建设管理 50
3.9.1 已有安全控制措施汇总分析 50
3.9.2 主要安全问题汇总分析 52
3.10 安全运维管理 53
3.10.1 已有安全控制措施汇总分析 53
3.10.2 主要安全问题汇总分析 57
3.11 其他安全要求指标 58
3.11.1 已有安全控制措施汇总分析 58
3.11.2 主要安全问题汇总分析 58
3.12 验证测试 58
3.12.1 漏洞扫描 58
3.12.1.1 漏洞扫描结果统计 58

3.12.1.2 漏洞扫描问题描述 62
3.12.2 渗透测试 63
3.12.2.1 渗透测试过程说明 63
3.12.2.2 渗透测试问题描述 65
3.13 单项测评小结 65
3.13.1 控制点符合情况汇总 65
3.13.2 安全问题汇总 69
4 整体测评 73
4.1 安全控制点间安全测评 73
4.1.1 安全建设管理 73
4.1.1.1 安全通用要求 73
4.1.2 安全运维管理 74
4.1.2.1 安全通用要求 74
4.2 区域间安全测评 74
4.2.1 安全物理环境 74
4.2.1.1 安全通用要求 74
4.2.2 安全通信网络 75
4.2.2.1 安全通用要求 75
4.2.3 安全区域边界 75
4.2.3.1 安全通用要求 75
4.3 整体测评结果汇总 76
5 安全问题风险分析 77
6 等级测评结论 82
7 安全问题整改建议 84
附录A 被测对象资产 90
A.1 物理机房 90
A.2 网络设备 90
A.3 安全设备 90
A.4 服务器 91
A.5 终端设备 91
A.6 其他系统或设备 91
A.7 系统管理软件/平台 91
A.8 业务应用软件/平台 92
A.9 数据资源 92
A.10 密码产品 93
A.11 安全相关人员 93
A.12 安全管理文档 93
附录B 上次测评问题整改情况说明 99
附录C 单项测评结果汇总 99
C.1 安全物理环境 99

C.2 安全通信网络 99
C.3 安全区域边界 100
C.4 安全计算环境 100
C.4.1 网络设备 100
C.4.2 安全设备 101
C.4.3 服务器和终端 102
C.4.4 系统管理软件/平台 103
C.4.5 业务应用系统/平台 103
C.4.6 数据资源 103
C.4.7 其他系统或设备 104
C.5 安全管理中心 104
C.6 安全管理制度 104
C.7 安全管理机构 105
C.8 安全管理人员 105
C.9 安全建设管理 105
C.10 安全运维管理 106
C.11 其他安全要求指标 106

附录D 单项测评结果记录 107

D.1 安全物理环境 107
D.1.1 安全通用要求 107
D.1.1.1 信息化机房 107
D.2 安全通信网络 109
D.2.1 安全通用要求 109
D.2.1.1 安全通信网络 109
D.3 安全区域边界 109
D.3.1 安全通用要求 109
D.3.1.1 办公网区域 110
D.3.1.2 外网边界区域 112
D.3.1.3 安全管理区域 114
D.3.1.4 服务器存储区域 116
D.4 安全计算环境 119
D.4.1 安全通用要求 119
D.4.1.1 网络设备 119
D.4.1.2 安全设备 126
D.4.1.3 服务器和终端 151
D.4.1.4 系统管理软件/平台 177
D.4.1.5 业务应用系统/平台 184
D.4.1.6 数据资源 188
D.4.1.7 其他系统或设备 196
D.5 安全管理中心 196
D.5.1 安全通用要求 196
D.5.1.1 管理中心 196
D.6 安全管理制度 197
D.6.1 安全通用要求 197

D.6.1.1 制度文件、执行/记录文件 197
D.7 安全管理机构 199
D.7.1 安全通用要求 199
D.7.1.1 制度文件、执行/记录文件 199
D.8 安全管理人员 201
D.8.1 安全通用要求 201
D.8.1.1 制度文件、执行/记录文件 202
D.9 安全建设管理 204
D.9.1 安全通用要求 204
D.9.1.1 制度文件、执行/记录文件 204
D.10 安全运维管理 208
D.10.1 安全通用要求 208
D.10.1.1 制度文件、执行/记录文件 208
D.11 其他安全要求 216
附录E 漏洞扫描结果记录 216
附录F 渗透测试结果记录 216
附录G 威胁列表 219

1 测评项目概述

1.1 测评目的

安全等级测评的目标是通过对目标系统在安全技术及管理方面的测评,对目标系统的安全技术状态及安全管理状况做出初步判断,给出目标系统在安全技术及安全管理方面与其相应安全等级保护要求之间的差距。测评结论作为委托方进一步完善系统安全策略及安全技术防护措施依据。

项目背景是为进一步提高信息系统的保障能力,根据《信息安全等级保护管理办法》（公通字2007【43】号）的精神，茂名职业技术学院委托广东南方信息安全研究院（SC202127130010163）对智慧校园系统实施等级测评，以期发现信息系统和等级保护标准的差距以及存在的安全隐患，为后续的安全整改工作提供参考依据。

1.2 测评依据

测评过程中主要依据的标准:

测评标准

（1）GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》

（2）GB/T 28448-2019 《信息安全技术 网络安全等级保护测评要求》

测评参考标准

（1）GB 17859-1999 《计算机信息系统 安全保护等级划分准则》

（2）GB/T 28449-2018 《信息安全技术 网络安全等级保护测评过程指南》

（3）GB/T 20984-2007 《信息安全技术 信息安全风险评估规范》

（4）GB/T 25058-2019 《信息安全技术 网络安全等级保护实施指南》

测评参考法律法规

（1）《中华人民共和国网络安全法》

（2）《中华人民共和国密码法》

（3）《中华人民共和国数据安全法》

1.3 测评过程

本次等级测评分为四个过程：测评准备活动、方案编制活动、测评实施活动、报告编制活动。具体如图 1-1 所示。其中，各阶段的时间安排如下：

⑴ 测评准备活动

测评准备活动的目标是顺利启动测评项目,收集定级对象相关资料,准备测评所需资料,为编制测评方案打下良好的基础。测评准备活动包括工作启动、信息收集和分析、工具和表单准备三项主要任务。

（2）方案编制活动

方案编制活动的目标是整理测评准备活动中获取的定级对象相关资料,为现场测评活动提供最基本的文档和指导方案。方案编制活动包括测评对象确定、测评指标确定、测评内容确定、工具测试方法确定、测评指导书开发及测评方案编制六项主要任务。

（3）现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调,为现场测评的顺利开展打下良好基础,依据测评方案实施现场测评工作,将测评方案和测评方法等内容具体落实到现场测评活动中。现场测评工作应取得报告编制活动所需的、足够的证据和资料。现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

（4）报告编制活动

在现场测评工作结束后,测评机构应对现场测评获得的测评结果(或称测评证据)进行汇总分析,形成等级测评结论,并编制测评报告。测评人员在初步判定单项测评结果后,还需进行单元测评结果判定、整体测评、系统安全保障评估,经过整体测评后,有的单项

测评结果可能会有所变化,需进一步修订单项测评结果,而后针对安全问题进行风险评估,形成等级测评结论。分析与报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、系统安全保障评估、安全问题风险评估、等级测评结论形成及测评报告编制七项主要任务。

各阶段完成的关键任务：

序号	阶段	任务	对象	开始日期	结束日期
1	测评准备活动	工作启动	项目甲乙双方	2022年8月15日	2022年8月19日
2		信息收集与分析	调研表	2022年8月22日	2022年8月25日
3		工具和表单准备	测评工具、测评授权书、文档交接单	2022年8月25日	2022年8月30日
4	方案编制活动	测评对象确认	测评方案-对象列表	2022年8月31日	2022年8月31日
5		测评指标确认	测评方案-指标列表	2022年8月31日	2022年8月31日
6		测评内容确认	测评方案-内容列表	2022年9月1日	2022年9月1日
7		工具测试方法确认	测评方案-工具测试方法列表	2022年9月1日	2022年9月1日
8		测评指导书开发	测评作业指导书	2022年9月2日	2022年9月2日
9		测评方案编制	测评方案	2022年9月5日	2022年9月5日
10	现场测评活动	现场测评准备	工具、人员、表单准备	2022年9月28日	2022年9月28日
11		现场测评和结果记录	安全管理访谈	2022年9月28日	2022年9月28日
12			安全管理文档检查	2022年9月28日	2022年9月28日
13			安全物理环境测评	2022年9月28日	2022年9月28日
14			安全通信网络	2022年9月28日	2022年9月29日
15			安全区域边界	2022年9月28日	2022年9月29日
16			安全计算环境	2022年9月28日	2022年9月29日
17			工具测试	2022年9月29日	2022年10月9日
18		结果确认和资料归还	检测人员出入场确认单、测评现场服务评价单	2022年10月8日	2022年10月9日
19	报告编制活动	单项测评结果	测评报告	2022年10月9日	2022年10月12日

序号	阶段	任务	对象	开始日期	结束日期
		判定			
20		单元测评结果判定		2022年10月9日	2022年10月17日
21		整体测评		2022年10月9日	2022年10月17日
22		系统安全保障评估		2022年10月9日	2022年10月17日
23		安全问题风险分析		2022年10月9日	2022年10月17日
24		等级测评结论形成		2022年10月17日	2022年10月30日
25		测评报告编制		2022年10月17日	2022年10月30日

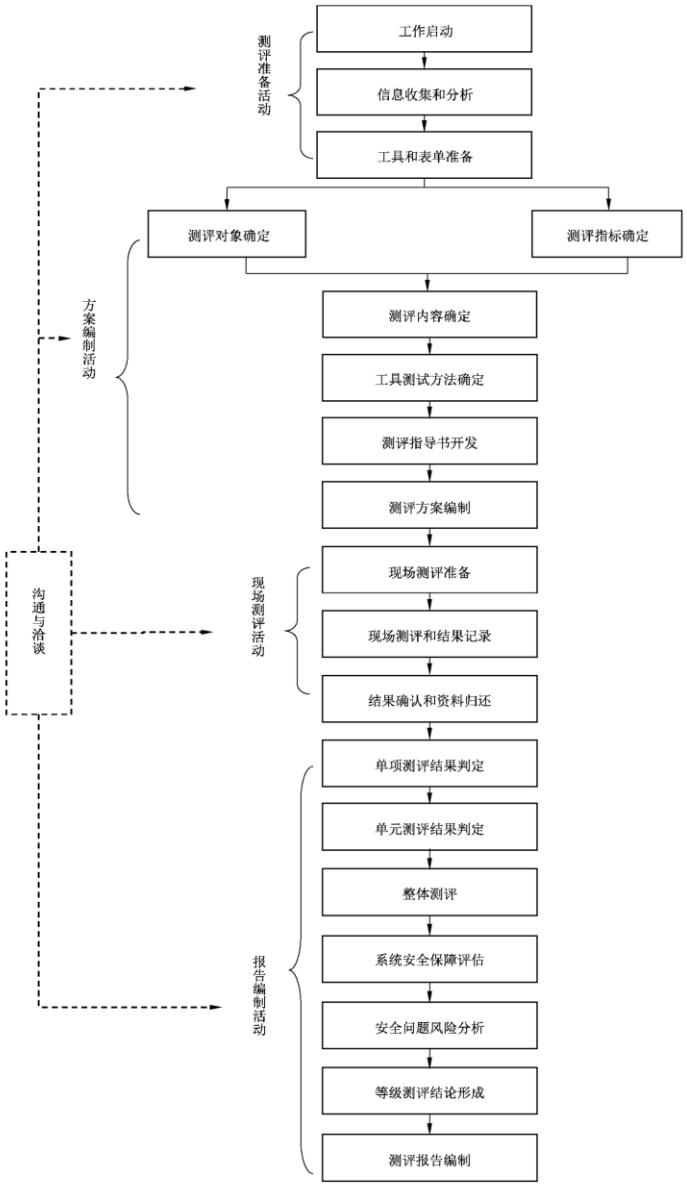


图 1-1 等级保护测评工作流程图

其中，于项目前期召开了项目启动会议，确定了工作方案及项目人员名单；于现场测评完成后召开了项目末次会议，确认了测评发现的问题；于2022年10月30日在对系统的整改情况进行了复核确认后，完成报告编制。

1.4 报告分发范围

等级测评报告正本一式3份，其中茂名职业技术学院1份，广东南方信息安全研究院1份，受理备案的公安机关1份。

2 被测对象描述

2.1 被测对象概述

2.1.1 定级结果

表 2-1定级结果

被测对象名称	安全保护等级	业务信息安全等级	系统服务安全等级
智慧校园系统	2	2	2

2.1.2 业务和采用的技术

智慧校园系统包括校园移动应用、统一身份认证、服务能力开放、主数据管理、网上办事大厅等基础支撑模块，形成一体化的信息化整体架构，解决信息系统分别建立带来的数据孤岛和流程割裂问题，打通各部门的信息壁垒，为业务整合和流程整合提供技术支持。建立全校性的主数据平台，涵盖学院信息标准与数据规范的定义，共享数据目录的管理，数据的采集、共享和交换等。

被测对象未采用云计算/移动互联/物联网/工业控制/大数据等技术情况。

2.1.3 网络结构

智慧校园系统主要是对互联网提供服务，相关设备部署在信息化机房当中,其简要拓扑如下:

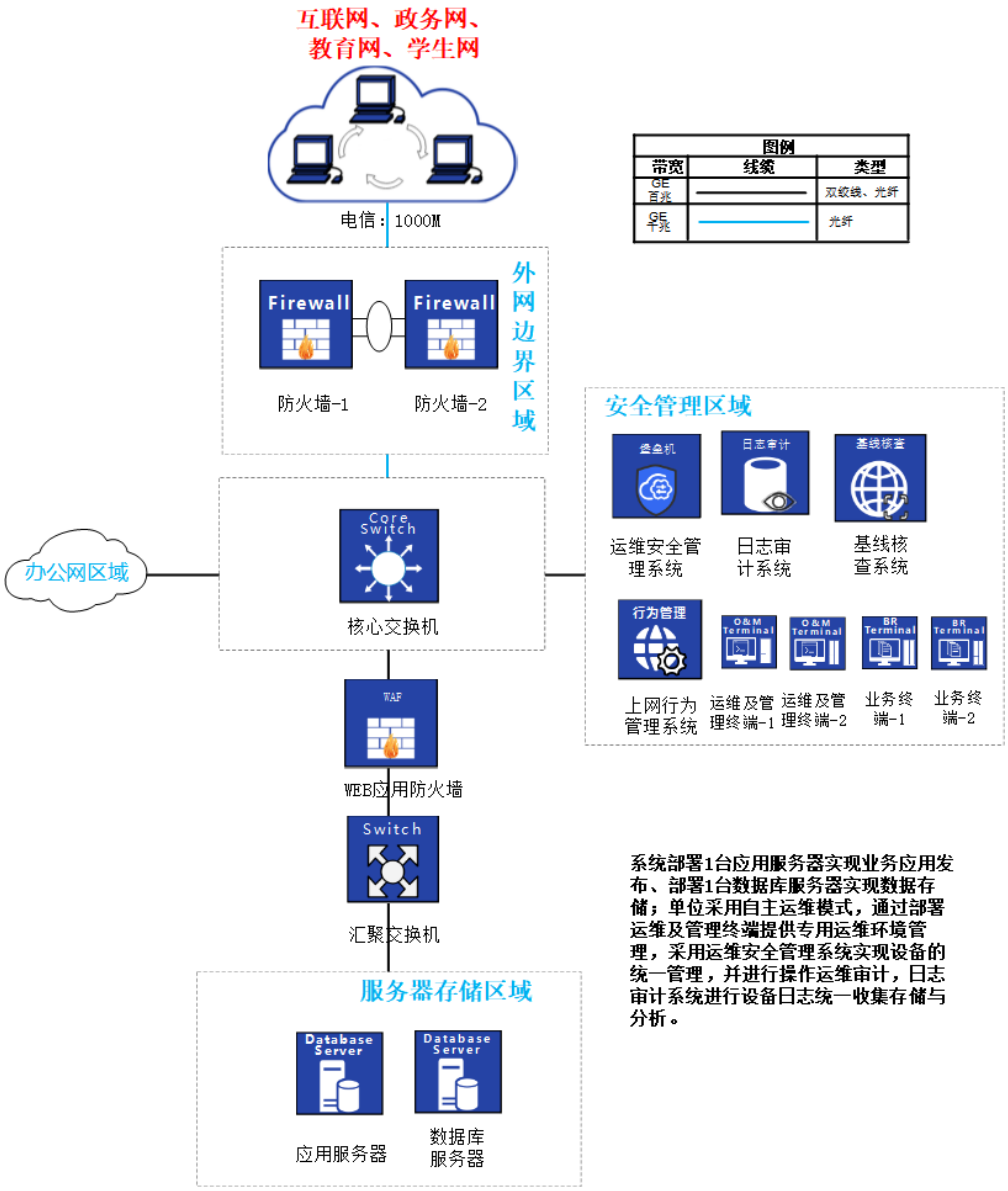


图 2-1 智慧校园系统网络拓扑图

如图2-1智慧校园系统网络拓扑图所示，智慧校园系统网络安全域划分为4个，分别为外网边界区域、安全管理区域、服务器存储区域、办公网区域。

1、外网边界区域：

外网边界区域网络主要包括智慧校园系统的业务服务和信息交换应用，是安全管理区域、服务器存储区域、办公网区域的出口边界；其链路接入为光纤线，带宽为1000mb。通过部署核心交换机、防火墙等设备实施网络访问控制，防火墙（入侵防御模块）实现网络入侵攻击行为防御。

2、办公网区域：

办公网区域网络主要包括智慧校园系统与办公区域的信息交换应用，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、防火墙、上网行为管理系统等设备实施网络访问控制、防火墙（入侵防御模块）实现网络入侵攻击行为防御。

3、安全管理区域：

安全管理区域网络主要包括日志审计系统、运维安全管理系统、上网行为管理系统，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、上网行为管理系统等设备实施网络访问控制。

4、服务器存储区域：

服务器存储区域网络主要包括智慧校园系统的应用服务器、数据库服务器，其链路接入为双绞线，带宽为100mb。通过部署核心交换机、上网行为管理系统等设备实现一定的网络访问控制。

5、服务器部署情况：

智慧校园系统由1台应用服务器实现应用发布；1台数据库服务器实现数据处理、存储、维护。

6、灾备及冗余

智慧校园系统无异地备份机房，未实现异地备份数据定时传输功能。系统重要数据根据需求采用每天增量、每月全备到本地信息化机房。

智慧校园系统未实现冗余措施。

2.2 测评指标

2.2.1 安全通用要求指标

表 2-2 安全通用要求指标

安全类	安全控制点	测评项数
安全物理环境	物理位置选择	2
	物理访问控制	1
	防盗窃和防破坏	2
	防雷击	1
	防火	2
	防水和防潮	2
	防静电	1
	温湿度控制	1
	电力供应	2
	电磁防护	1
安全通信网络	网络架构	2
	通信传输	1
	可信验证	1
安全区域边界	边界防护	1
	访问控制	4
	入侵防范	1
	恶意代码和垃圾邮件防范	1
	安全审计	3
	可信验证	1
安全计算环境	身份鉴别	3
	访问控制	4
	安全审计	3
	入侵防范	5
	恶意代码防范	1
	可信验证	1
	数据完整性	1
	数据备份恢复	2
	剩余信息保护	1
	个人信息保护	2
安全管理中心	系统管理	2
	审计管理	2
安全管理制度	安全策略	1
	管理制度	2
	制定和发布	2
	评审和修订	1
安全管理机构	岗位设置	2
	人员配备	1
	授权和审批	2
	沟通和合作	3

安全类	安全控制点	测评项数
	审核和检查	1
安全管理人员	人员录用	2
	人员离岗	1
	安全意识教育和培训	1
	外部人员访问管理	3
安全建设管理	定级和备案	4
	安全方案设计	3
	产品采购和使用	2
	自行软件开发	2
	外包软件开发	2
	工程实施	2
	测试验收	2
	系统交付	3
	等级测评	3
	服务供应商选择	2
安全运维管理	环境管理	3
	资产管理	1
	介质管理	2
	设备维护管理	2
	漏洞和风险管理	1
	网络和系统安全管理	5
	恶意代码防范管理	3
	配置管理	1
	密码管理	2
	变更管理	1
	备份与恢复管理	3
	安全事件处置	3
	应急预案管理	2
	外包运维管理	2
安全通用要求指标数量统计		135

2.2.2 安全扩展要求指标

表 2-3 安全扩展要求指标

扩展类型	安全类	安全控制点	测评项数
本次测评不涉及安全扩展要求指标			

2.2.3 其他安全要求指标

表 2-4 其他安全要求指标

安全类	安全控制点	测评项数
本次测评不涉及其他安全要求指标		

2.2.4 不适用安全要求指标

表 2-5-1 不适用安全要求指标

安全类	安全控制点	不适用项	不适用原因
安全建设管理	自行软件开发	a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。
安全建设管理	自行软件开发	b) 应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。	（1）单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员，本测评项目不适用。
安全运维管理	密码管理	b) 应使用国家密码管理主管部门认证核准的密码技术和产品。	（1）单位未采购涉及密码技术的产品，不适用。
安全运维管理	外包运维管理	a) 应确保外包运维服务商的选择符合国家的有关规定；	（1）单位目前未涉及任何外包运维服务情况，不适用。
安全运维管理	外包运维管理	b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。	（1）单位目前未涉及任何外包运维服务情况，不适用。

表 2-5-2 其他不适用安全要求指标

安全类	安全控制点	不适用项	不适用原因
本次测评不涉及其他安全要求指标			

2.3 测评对象

2.3.1 测评对象选择方法

智慧校园系统等级测评的测评对象种类上基本覆盖、数量进行抽样，重点抽查主要的设备、设施、人员和文档等。结合智慧校园系统的网络拓扑结构和业务情况，本次等级测评的测评对象在抽样时主要考虑以下几个方面：

（1） 主机房（包括其环境、设备和设施等）和灾备机房；

（2） 存储被测系统重要数据的介质的存放环境；

（3） 办公场地；

（4） 整个系统的网络拓扑结构；

（5） 安全设备，包括防火墙等；

（6） 边界网络设备，包括路由器、楼层交换机等；

（7） 对整个信息系统或其局部的安全性起作用的网络互联设备，如核心交换机、路由器等；

（8） 承载业务处理系统主要业务或数据的服务器（包括其操作系统和数据库）；

（9） 管理终端和主要应用系统终端；

（10） 能够完成系统不同业务使命的业务应用系统；

（11） 业务备份系统；

（12） 信息安全主管人员、各方面的负责人员、具体负责安全管理的当事人、业务负责人；

（13） 涉及到信息系统安全的所有管理制度和记录。

抽样原则：在等级测评时，业务处理系统中配置相同的安全设备、边界网络设备、网络互联设备、服务器、终端以及备份设备，每类至少抽查两台作为测评对象。

2.3.2 测评对象选择结果

2.3.2.1 物理机房

表 2-6 物理机房

序号	机房名称	物理位置	重要程度
1	信息化机房	茂名市茂南区文明北路232号大院大楼	关键

2.3.2.2 网络设备

表 2-7 网络设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度
1	核心交换机	否	H3C version 7.1.070, Release 7585P07	H3C S7500E-X	核心数据交换、访问控制	关键
2	汇聚交换机	否	H3C version 7.1.070, Release 6126P20	H3C S5560X-30C-EI	数据交换	重要

2.3.2.3 安全设备

表 2-8 安全设备

序号	设备名称	是否虚拟设备	系统及版本	品牌型号	用途	重要程度
1	WEB应用防火墙	否	深信服AF 8.0.9	深信服WAF-2000-H642	应用防护、入侵防范、病毒防护	重要
2	日志审计系统	否	深信服LAS 3.0.5	深信服AC-1000-D601-PT	日志审计	重要
3	防火墙-2	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键
4	防火墙-1	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键
5	基线核查系统	否	深信服V3.0.3	深信服AC-1000-D602-PT	漏洞扫描	重要
6	运维安全管理系统	否	深信服V3.0.6	深信服AC-1000-D603-	运维审计	重要

序号	设备名称	是否虚拟设备	系统及版本	品牌型号	用途	重要程度
				PT		
7	上网行为管理系统	否	深信服AC12.0.26	深信服AC-1000-D600-PT	上网行为管理及终端准入控制	重要

2.3.2.4 服务器

表 2-9 服务器

序号	设备名称	所属业务应用系统/平台	是否虚拟设备	操作系统及版本	数据库管理系统及版本	中间件及版本	重要程度
1	应用服务器	智慧校园系统	否	CentOS 7.7	/	Weblogic 11g	关键
2	数据库服务器	智慧校园系统	否	CentOS 7.7	Oracle 11.2.0.1.0	/	关键

2.3.2.5 终端设备

表 2-10 终端设备

序号	设备名称	是否虚拟设备	操作系统及版本	用途	重要程度
1	运维及管理终端-1	否	Windows 10 （版本 20H2（内部版本 19044.1889）	运维管理、系统管理	一般
2	业务终端-2	否	Windows 10 （版本 20H2（内部版本 19044.1889）	业务管理	一般
3	运维及管理终端-2	否	Windows 10 （版本 21H2（内部版本 19044.1889））	运维管理、系统管理	一般
4	业务终端-1	否	Windows 10 （版本 20H2（内部版本 19044.1889）	业务管理	一般

2.3.2.6 其他系统或设备

表 2-11 其他系统或设备

序号	设备名称	是否虚拟设备	系统及版本	用途	重要程度
/	/	/	/	/	/

注释：本次测评对象中不涉及专用移动互联终端等，不开展抽测。

2.3.2.7 系统管理软件/平台

表 2-12 系统管理软件/平台

序号	系统管理软件/平台名称	主要功能	版本	所在设备名称	重要程度
1	数据库服务器-Oracle	数据生产、存储	11.2.0.1.0	应用/数据库服务器	关键
2	应用服务器-Weblogic	页面发布	11C	应用/数据库服务器	关键

2.3.2.8 业务应用软件/平台

表 2-13 业务应用系统/平台

序号	业务应用软件/平台名称	主要功能	业务应用软件及版本	开发厂商	重要程度
1	智慧校园系统	茂名职业技术学院智慧校园系统包括校园移动应用、统一身份认证、服务能力开放、主数据管理、网上办事大厅等基础支撑模块，形成一体化的信息化整体架构，解决信息系统分别建立带来的数据孤岛和流程割裂问题，打通各部门的信息壁垒，为业务整合和流程整合提供技术支持。建立	V6.0	江苏金智教育信息股份有限公司	关键

序号	业务应用软件/平台名称	主要功能	业务应用软件及版本	开发厂商	重要程度
		全校性的主数据平台，涵盖学院信息标准与数据规范的定义，共享数据目录的管理，数据的采集、共享和交换等。			

2.3.2.9 数据资源

表 2-14 数据资源

序号	数据类别	所属业务应用	安全防护需求	重要程度
1	重要个人信息	智慧校园系统	完整性、保密性	关键
2	重要业务数据	智慧校园系统	完整性、保密性	关键
3	鉴别数据	智慧校园系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性、保密性	关键
4	重要审计数据	智慧校园系统（安全管理中心）	完整性	重要
5	重要配置数据	智慧校园系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性	关键

注释：网络设备、安全设备、服务器、终端、系统管理软件/平台和业务应用系统等所涉及的鉴别数据和重要配置数据分别在各自测评对象中汇总测评证据后集中体现,包括数据完整性、数据保密性和备份恢复。重要审计数据在安全管理中心进行汇总测评证据，包括数据完整性。重要业务数据和重要个人信息分别在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。

2.3.2.10 安全相关人员

表 2-15 安全相关人员

序号	姓名	岗位/角色	联系方式	所属单位
1	吴国华	机房管理员	0668-2920122	茂名职业技术学院
2	叶永利	安全管理员	0668-2920122	茂名职业技术学院
3	杨云	审计管理员	0668-2920122	茂名职业技术学院
4	龙恒	应用管理员	13377766618	茂名职业技术学院
5	龙恒	网络管理员	13377766618	茂名职业技术学院
6	吴国华	系统管理员	0668-2920122	茂名职业技术学院
7	杨云	资产管理员	0668-2920122	茂名职业技术学院
8	龙恒	数据管理员	13377766618	茂名职业技术学院

2.3.2.11 安全管理文档

表 2-16 安全管理文档

序号	文档名称	主要内容
1	制度类文档-员工考核管理制度	关于单位人员考核工作管理制度文档
2	制度类文档-岗位安排及岗位职责	关于单位岗位职责、岗位安排制度文档
3	制度类文档-工程测试验收管理	关于单位工程测试工作管理制度文档
4	制度类文档-外部服务人员管理规范	关于单位针对外部人员工作管理规范制度文档
5	制度类文档-机房安全管理制度	关于单位机房安全管理工作制度文档
6	制度类文档-数据安全管理规范	关于保障关键数据安全，从数据库本身、数据加密、数据备份恢复三个方面对数据安全进行规范的制度文档
7	制度类文档-系统及应用数据备份管理规范	关于单位数据备份、恢复管理制度文档
8	制度类文档-服务供应商选择安全管理制度	关于单位安全服务供应商管理规定制度文档
9	制度类文档-主机安全管理规范	关于规定单位主机系统安全管理要求规范，指导业务平台主机的安全配置和维护的制度文档

序号	文档名称	主要内容
10	制度类文档-介质管理制度	关于单位介质安全管理工制度文档
11	制度类文档-安全事件报告和处置	关于单位网络安全事件管理、处置、流程等报告制度文档
12	制度类文档-备份与恢复管理制度	关于单位数据备份、恢复管理制度文档
13	制度类文档-系统安全管理制度	关于单位系统安全管理、安全服务管理制度文档
14	制度类文档-办公环境管理制度	关于单位办公环境管理制度文档
15	制度类文档-信息安全奖惩办法	关于单位人员奖惩制度文档
16	制度类文档-安全漏洞管理制度	关于单位安全漏洞管理工作制度文档
17	制度类文档-信息安全总体策略	关于单位网络安全方针、策略制度文档
18	制度类文档-办公环境保密管理	关于单位办公环境管理制度文档
19	制度类文档-设备安全管理制度	关于单位设备安全管理制度文档
20	制度类文档-网络安全管理制度	关于单位网络安全工作管理制度文档
21	制度类文档-信息安全漏洞扫描规范	关于单位安全漏洞工作规范制度文档
22	制度类文档-安全教育和培训制度	关于单位安全培训、安全交流工作制度文档
23	制度类文档-网络与信息系统安全设计规范	关于单位网络与信息化安全设计制度文档
24	制度类文档-组织安全结构和人员职责制度	关于单位安全结构、人员职责
25	制度类文档-外部人员访问管理制度	关于单位针对外来人员访问管控制度文档
26	制度类文档-信息系统恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
27	制度类文档-恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
28	制度类文档-物理安全管理规范	关于加强单位办公区域及电子计算机机房的管理和设备运行安全，规范办公区域及机房建设，使人员办公高效及机房设备安全、稳定运行的制度文档
29	制度类文档-网络安全事件报告制度	关于单位网络安全事件管理报告文档
30	制度类文档-离岗人员工作交接规范	关于单位离岗交接工作规范制度文档

序号	文档名称	主要内容
31	制度类文档-制度制定、发布、评审和修订管理制度	关于单位制度制定、发布、评审和修订等管理文档
32	制度类文档-安全管理组织规范	关于单位组织结构管理规范制度文档
33	制度类文档-安全审查和检查管理规范	关于单位安全检查、审查工作规范制度文档
34	制度类文档-外部接入受控网络访问系统管理规范	关于单位针对外部人员工作接入规范制度文档
35	制度类文档-信息系统外包运维管理制度	关于单位外包运维工作管理制度文档
36	制度类文档-测试及验收方案	关于单位测试验收方案文档
37	制度类文档-应用系统业务用户密码设置规定	关于单位用户密码管理制度文档
38	制度类文档-外包开发软件管理规定	关于单位外包项目管理工作制度文档
39	制度类文档-人员管理制度	关于单位人员录用、调岗、离岗管理制度文档
40	制度类文档-应用安全管理规范	关于规定单位应用安全管理要求及规范的制度文档
41	制度类文档-工程实施管理制度	关于单位工程实施工作管理制度文档
42	制度类文档-网络安全管理规范	关于保障单位网络系统的安全稳定运行，抵御内部和外部各种形式的网络攻击或威胁制定的管理文档
43	制度类文档-系统交付管理	关于单位交付工作管理制度文档
44	制度类文档-授权和审批管理规定	关于单位授权审批、审批流程规范制度文档
45	制度类文档-网络安全事件应急预案	关于单位网络安全事件应急处理、流程、培训等管理制度文档
46	制度类文档-恶意代码防范管理制度	关于单位恶意代码防范工作制度文档
47	制度类文档-变更控制管理制度	关于单位变更流程、控制管理制度文档
48	制度类文档-组织安全结构和人员职责制度	关于单位组织结构、人员安排、人员职责制度文档
49	操作类文档-设备及系统软件配置和操作手册	关于单位安全设备操作、Linux服务器配置手册、主机运维操作手册、软件操作手册、防火墙配置和操作手册、数据库日常运维操作手册等指导文档
50	操作类文档-数据备份策略	关于单位数据备份策略文件
51	操作类文档-软硬件日常维护管理规程	关于单位计算机网络系统使用、管理、信息安全、资源共享有所遵循,规范上网操作流程,提高网络系统安全性的指导文档
52	操作类文档-设备操作规程	关于单位相关设备操作指导文档
53	记录类文档-系统交付清单	关于单位交付工作记录

序号	文档名称	主要内容
54	记录类文档-应急预案培训记录表	关于单位应急预案培训工作记录
55	记录类文档-软件交付清单	关于单位交付工作记录
56	记录类文档-通用变更记录表	关于单位变更工作记录
57	记录类文档-接入受控网络申请表	关于外来人员接入工作记录
58	记录类文档-人员培训及考核记录表	关于人员培训、考核等工作记录
59	记录类文档-漏洞检测报告	关于单位安全漏洞检测报告文档
60	记录类文档-关键岗位人员考核记录	关于关键岗位考核工作记录
61	记录类文档-重要操作审批表	关于单位审批工作记录
62	记录类文档-信息安全检查记录表	关于单位安全检查工作记录
63	记录类文档-设备维修申请表	关于单位设备维护工作申请记录
64	记录类文档-人员入职考核记录	关于人员录用、考核工作记录
65	记录类文档-访问记录表	关于人员访问工作记录
66	记录类文档-数据恢复申请表	关于单位数据恢复工作申请表
67	记录类文档-外部人员访问申请表	关于外来人员访问申请流程工作记录
68	记录类文档-监理审批表	关于单位监理审核工作记录
69	记录类文档-离场信息资料交接表	关于人员离岗交接工作记录
70	记录类文档-信息安全会议记录	关于单位安全培训、安全交流会议记录
71	记录类文档-存储介质目录清单	关于备份介质存储工作清单
72	记录类文档-数据备份记录表	关于单位数据备份工作记录
73	记录类文档-外部会议文件和记录	关于单位外部联系、交流及会议工作记录
74	记录类文档-备份介质使用记录	关于备份介质使用登记工作记录
75	记录类文档-信息管理系统漏洞检查表	关于单位安全漏洞工作检测记录表
76	记录类文档-设备操作维护记录	关于单位设备维护工作记录

序号	文档名称	主要内容
77	记录类文档-离职员工物品交回登记表	关于人员离岗工物交接工作记录
78	记录类文档-机房出入登记表	关于人员进出机房登记工作记录
79	记录类文档-安全管理制度评审记录	关于单位制度审计记录
80	记录类文档-专家论证记录表	关于单位网络方案论证记录
81	记录类文档-备份工作汇总表	关于单位数据备份工作总结表
82	记录类文档-安全建设方案评审纪录	关于单位网络与信息化安全设计方案评审工作记录
83	记录类文档-机房设备维修记录表	关于单位机房设备维修工作记录
84	记录类文档-机房设备维护记录表	关于设备维护登记工作记录
85	记录类文档-收发文登记记录	关于单位文档签发记录
86	记录类文档-网络信息安全事件记录表	关于单位网络安全事件工作记录
87	记录类文档-网络配置信息	关于单位配置信息登记工作记录
88	记录类文档-信息系统存储介质销毁申请表	关于备份介质销毁申请工作记录
89	记录类文档-机房维护日志	关于机房维护工作记录
90	记录类文档-设备出入登记记录表	关于设备进出机房登记工作记录
91	记录类文档-评审和修订记录	关于单位变更评审、修订工作记录
92	记录类文档-机房巡检记录表	关于单位机房环境巡检记录
93	记录类文档-信息系统存储介质使用清单	关于备份介质存储使用清单
94	记录类文档-外部人员访问记录表	关于外来人员访问登记工作记录
95	记录类文档-技能培训记录	关于单位系统培训工作、考核工作记录
96	记录类文档-人员离岗申请表	关于人员离岗申请记录
97	证据类文档-深信服安全采购合同	关于单位与安全厂家服务采购、产品选择合同文件
98	证据类文档-网络安全等级保护工作小组名单	关于单位网络安全等级保护工作小组人员名单文件
99	证据类文档-网络安全系统	关于单位网络与信息化安全设计方案文档

序号	文档名称	主要内容
	设计方案	
100	证据类文档-定级备案	关于单位系统定级报告、备案证文件
101	证据类文档-信息安全事件分析报告表	关于单位安全事件分析报告
102	证据类文档-安全职位人员	关于单位人员岗位安排名单
103	证据类文档-网络安全等级保护测评服务合同	关于单位与安全服务商签定的安全服务合同文件
104	证据类文档-资产清单	关于单位信息系统资产清单统计表
105	证据类文档-外部联系表	关于单位内部联系及外部联系名单
106	证据类文档-工程项目实施方案	关于单位工程实施方案文档

3 单项测评结果分析

3.1 安全物理环境

3.1.1 已有安全控制措施汇总分析

安全通用要求

物理位置选择	
a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；	
信息化机房	（1）机房和办公场地场所在建筑物具有建筑验收文档，包含对防震、防风和防雨能力的说明； （2）机房和办公场地未出严重的问题。
b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	
信息化机房	（1）机房未部署在易发生问题的位置； （2）机房对于空调设备的排水管等部位采取密封防漏处理； （3）机房对于楼板进行了防护措施。
防盗窃和防破坏	
a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识；	
信息化机房	（1）机房设备或主要部件都固定在机架上； （2）机房内对主要部件已绑定相应不易除去的标签； （3）重要机柜已进行上锁处理。
b) 应将通信线缆铺设在隐蔽安全处。	
信息化机房	（1）通信线缆铺设在下走线槽隐蔽处中； （2）通信线缆设有明显的源目的标识； （3）通信线缆均铺设整齐、规范。
防雷击	
应将各类机柜、设施和设备等通过接地系统安全接地。	

信息化机房	（1）机房设置专用地线； （2）机房内机柜、设施和设备等进行接地处理； （3）交流电源接地验收检测结果符合要求。
防火	
a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；	
信息化机房	（1）机房采用经消防检测部门检测合格并在有效期内的（如 七氟丙烷）气体自动灭火设备，火灾自动报警类型为烟感+红外； （2）自动消防系统工作状态正常，有定期巡检和维护记录《机房巡检记录表》； （3）建立机房消防的管理制度相关文档《机房安全管理制度》，按管理要求机房无人情况下气体灭火配置为自动模式，进入机房调整为手动模式，机房报警有7*24小时值班人员进行监控。
防水和防潮	
a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	
信息化机房	（1）机房不存在雨水渗透、破损等不合规情况； （2）机房不位于建筑的顶层、边缘区域。
b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。	
信息化机房	（1）机房区域范围已部署1台科华品牌（精密）空调，机房内分别配置1组温湿度传感器监控； （2）机房内空调下方已铺设安装好挡水和排水设施； （3）机房墙壁或楼板的管道采取必要的防渗防漏等防水保护措施； （4）机房安装检测设备（如：漏水检测绳）检测地下积水，及时处理机房水蒸气结露和地下积水的转移与渗透； （5）目前防水\防潮检测未发现异常情况，并且有防水防潮的运维记录《机房维护日志》。
温湿度控制	
应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。	
信息化机房	（1）机房范围已部署1组科华品牌精密空调进行温湿度调节； （2）机房范围已部署空调及加湿机进行温湿度调节； （3）温湿度自动调节设施运作正常，有运行和维护记录《机房维护日志》； （4）机房温度能保持在24摄氏度到28摄氏度之间； （5）机房湿度能保持在40%到65%之间。
电力供应	
a）应在机房供电线路上配置稳压器和过电压防护设备；	
信息化机房	（1）机房配备了稳压器和过电压防护设备； （2）稳压器和过电压防护设备正常工作； （3）机房具备电力供应安全设计，并在其中标明配备稳压器、过电压防护设备等要求。
b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。	
信息化机房	（1）机房配备了1组科华品牌UPS； （2）UPS正常工作，可满足主要设备断电情况下的至少1小时正常运行要求； （3）UPS有定期（至少每年）检查和维护，有运行和维护记录《机房巡检记录表》。

电磁防护	
电源线和通信线缆应隔离铺设，避免互相干扰。	
信息化机房	（1）通信线缆铺设采用独立的具有电磁屏蔽作用线槽； （2）电源线缆铺设采用独立的具有电磁屏蔽作用线槽； （3）弱电线缆隔离铺设，没有干扰。

3.1.2 主要安全问题汇总分析

安全通用要求

（1）机房出入口未配置电子门禁系统（如：信息化机房）。上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域,可能对系统的平稳运行造成影响。中风险。

（2）机房建设未完全采用符合耐火等级的建筑材料。机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级（如：信息化机房）。存在发生火情时助燃火灾的风险。 低风险。

（3）机房内缺乏防静电措施（如防静电地板或铺设防静电地毯 ）（如：信息化机房）。存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。 中风险。

3.2 安全通信网络

3.2.1 已有安全控制措施汇总分析

安全通用要求

网络架构	
b) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	
安全通信网络	(1)网络内重要网段未部署在网络边界处,且未直接连接外部信息系统; (2) 系统通过防火墙对重要网段采取访问控制策略; (3) 各安全域（子网）的出口唯一。
通信传输	
应采用校验技术保证通信过程中数据的完整性。	
安全通信网络	（1）网络系统中未涉及完整性保障设备，但在安全计算环境方面网络设备采用SSH协议、安全设备采用HTTPS协议、操作系统采用SSH协议、应

	用系统采用HTTPS协议来保证通信过程中数据的完整性。

3.2.2 主要安全问题汇总分析

安全通用要求

（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况（如：安全通信网络）。上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变得更为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。 中风险。

（2）缺乏对通信设备可信验证方面的安全设计要求。现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况（如：安全通信网络）。缺乏对系统可执行程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致计算资源被干扰和破坏造成损失。 低风险。

3.3 安全区域边界

3.3.1 已有安全控制措施汇总分析

安全通用要求

边界防护	
应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络存在受保护的边界； （2）网络边界处部署了可提供访问控制功能的设备； （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。
访问控制	
a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	
办公网区域 外网边界区域	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备；

安全管理区域 服务器存储区域	（3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。
b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。
c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。
d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。
入侵防范	
应在关键网络节点处监视网络攻击行为。	
外网边界区域 服务器存储区域	（1）网络层部署支持对内部发起的攻击行为进行防范的设备； （2）现有的防范措施满足相应防护要求； （3）内部安全防范措施能检测相应攻击行为。
恶意代码和垃圾邮件防范	
应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	
外网边界区域 服务器存储区域	（1）在关键网络节点处部署合规的防恶意代码措施； （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试。
安全审计	
a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； （3）现有的审计措施满足相应的审计要求。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
办公网区域 外网边界区域 安全管理区域 服务器存储区域	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； （3）设备本地时间正常。
c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
办公网区域 外网边界区域 安全管理区域	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求；

服务器存储区域	(4) 日志及审计记录的保存能力可超过6个月; (5) 定期收集日志记录并定期备份。

3.3.2 主要安全问题汇总分析

安全通用要求

(1)网络层部署防火墙,防火墙未配置对内部发起的攻击行为实现防范功能策略,无法检测、防止或限制从内部发起的网络攻击行为（如：办公网区域）。存在不能及时发现内部主机作为攻击跳板，或网络攻击行为而造成系统损坏/网络资源浪费的风险。中风险。

(2)现有部署的恶意代码防范措施存在不合规的问题,网络边界覆盖不全面(如:办公网区域）。无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。 中风险。

(3) 缺乏对边界设备可信验证方面的安全设计要求。现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况（如：办公网区域）。缺乏对边界设备的相关程序的可信性验证,无法保证系统始终运行于可信环境中,运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4 安全计算环境

3.4.1 网络设备

3.4.1.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换;	
核心交换机 汇聚交换机	(1) 设备对各登录模式均启用身份鉴别; (2) 设备对登录管理的用户进行身份鉴别;

	（3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的全局密码策略； （6）设备配置加密的super认证。
b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
核心交换机 汇聚交换机	（1）设备配置合规的全局登录失败处理策略； （2）设备配置合规的操作超时退出措施。
c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
核心交换机 汇聚交换机	（1）设备配置合规的远程管理模式。
访问控制	
a）应对登录的用户分配账户和权限；	
核心交换机 汇聚交换机	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。
b）应重命名或删除默认账户，修改默认账户的默认口令；	
核心交换机 汇聚交换机	（1）设备不存在默认账户名； （2）设备账户口令设置合规。
c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
核心交换机 汇聚交换机	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。
d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	
核心交换机 汇聚交换机	（1）设备根据安全策略要求对特权用户进行分离； （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
核心交换机 汇聚交换机	（1）设备开启审计功能，审计进程正常； （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
核心交换机 汇聚交换机	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。
c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
核心交换机 汇聚交换机	（1）设备限制审计文件的访问控制权限，普通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效； （5）日志及审计记录保存大于6个月。

入侵防范	
a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	
核心交换机 汇聚交换机	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。
b) 应关闭不需要的系统服务、默认共享和高危端口；	
核心交换机 汇聚交换机	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。
c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
核心交换机 汇聚交换机	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
核心交换机 汇聚交换机	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
核心交换机 汇聚交换机	鉴别数据、重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； （2）设备对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
核心交换机 汇聚交换机	（1）设备定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。

3.4.1.2 主要安全问题汇总分析

安全通用要求

（1）设备不具备相关可信验证的技术措施（如：核心交换机）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.2 安全设备

3.4.2.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备对各登录模式均启用身份鉴别； （2）设备对登录管理的用户进行身份鉴别； （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。
b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备启用合规登录失败处理策略； （2）设备配置合规的操作超时退出措施。
c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备配置合规的远程管理模式； （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。
访问控制	
a）应对登录的用户分配账户和权限；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。
b）应重命名或删除默认账户，修改默认账户的默认口令；	

WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备不存在默认账户名； (2) 设备账户口令设置合规。
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备不存在多余或过期账户； (2) 设备管理员用户与账户之间一一对应。
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备根据安全策略要求对特权用户进行分离； (2) 设备不存在多个管理级别高的特权用户； (3) 设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备开启审计功能，审计进程正常； (2)设备的日志审计级别满足要求,审计覆盖所有用户操作审计和记录。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	(1) 设备日期、时间正常； (2) 设备审计记录内容基本完整。
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
WEB应用防火墙 上网行为管理系统 基线核查系统	(1) 设备限制审计文件的访问控制权限，普通用户不可删除及修改； (2) 设备针对日志、审计记录具备充足的存储容量； (3) 对审计记录进行定期存档备份，其备份策略有效；

运维安全管理系统 防火墙-1 防火墙-2	（4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。
日志审计系统	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）日志及审计记录保存大于6个月。
入侵防范	
a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。
b）应关闭不需要的系统服务、默认共享和高危端口；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。
c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 防火墙-1 防火墙-2	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
运维安全管理系统	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制。
d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备管理具备数据有效性检验功能； （2）设备管理的校验接口范围较全面。
e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
WEB应用防火墙	（1）设备已根据需要不定期地对已发布的新固件版本进行更新；

上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。
恶意代码防范	
应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	
WEB应用防火墙 防火墙-1 防火墙-2	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	鉴别数据、重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； （2）设备对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a）应提供重要数据的本地数据备份与恢复功能；	
WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 运维安全管理系统 防火墙-1 防火墙-2	（1）设备定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。

3.4.2.2 主要安全问题汇总分析

安全通用要求

（1）设备不具备相关可信验证的技术措施（如：WEB应用防火墙）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.3 服务器和终端

3.4.3.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统对登录系统的用户进行身份鉴别； （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； （5）用户属性策略未勾选“密码永不过期”。
应用服务器 数据库服务器	（1）操作系统对登录系统的用户进行身份鉴别； （2）操作系统不存在空口令用户； （3）操作系统不存在默认信任的登录模式； （4）操作系统为登录用户设置的身份标识具有唯一性； （5）操作系统配置的一定的密码长度且定期更换； （6）操作系统配置一定的密码复杂度策略。
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统启用登录失败处理策略。 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略。
应用服务器 数据库服务器	（1）操作系统启用pam_tally2模块的合规登录失败处理策略； （2）操作系统配置合规的操作超时锁定； （3）操作系统启用SSH的合规登录超时策略。
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS的管理。
应用服务器 数据库服务器	（1）操作系统配置合规的远程管理模式； （2）操作系统远程端口使用情况合规； （3）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
访问控制	
a) 应对登录的用户分配账户和权限；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权

	限分配表情况一致。
应用服务器 数据库服务器	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在所有用户均属于root组的情况。
b）应重命名或删除默认账户，修改默认账户的默认口令；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统针对默认账户采用相应的安全策略配置； （2）操作系统账户不存在弱口令或空口令。
应用服务器 数据库服务器	（1）操作系统对多余帐户进行删除、锁定或禁止其登录； （2）操作系统账户口令设置合规。
c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
业务终端-1 业务终端-2 应用服务器 数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。
d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统根据安全策略要求对特权用户进行分离； （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
应用服务器 数据库服务器	（1）操作系统根据安全策略要求对特权用户进行分离； （2）操作系统不存在除root外的特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统开启审计策略，操作系统审计策略基本完整； （2）审计覆盖所有用户操作审计和记录。
应用服务器 数据库服务器	（1）操作系统开启审计功能，审计进程正常； （2）操作系统开启审计范围及策略满足要求，审计覆盖所有用户操作审计和记录。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
业务终端-1 业务终端-2 应用服务器 数据库服务器 运维及管理终端-1	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。

运维及管理终端-2	
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统采取对审计记录存储容量如下： 运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。
应用服务器 数据库服务器	(1)操作系统限制审计文件的访问控制权限,普通用户不可删除及修改； （2）操作系统针对日志、审计记录具备充足的存储容量； （3）操作系统采取合规的日志文件权限策略； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。
入侵防范	
a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。
应用服务器 数据库服务器	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。
b) 应关闭不需要的系统服务、默认共享和高危端口；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统不存在多余的默认共享及其它文件共享； （2）操作系统关闭不必要端口； （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。
应用服务器 数据库服务器	（1）操作系统关闭不必要端口； （2）操作系统禁用不必要服务； （3）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口； （4）漏洞扫描未发现高风险主机端口。
c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。
应用服务器 数据库服务器	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程

	登录地址。
e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。
应用服务器 数据库服务器	（1）操作系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。
恶意代码防范	
应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。
应用服务器 数据库服务器	（1）操作系统安装深信服edr防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	鉴别数据、重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。
应用服务器 数据库服务器	鉴别数据: （1）系统在通信传输过程中对鉴别数据采取完整性保护措施。 重要配置数据: （1）系统在通信传输过程中对重要配置数据采取完整性保护措施。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
业务终端-1 业务终端-2 应用服务器 数据库服务器 运维及管理终端-1 运维及管理终端-2	（1）操作系统定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	
业务终端-1 业务终端-2	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：

运维及管理终端-1 运维及管理终端-2	安全选项“不显示上次的用户名”->启用
应用服务器 数据库服务器	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统不保存过多终端历史记录。

3.4.3.2 主要安全问题汇总分析

安全通用要求

（1）缺乏对计算设备可信验证方面的安全设计要求。现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。现有的计算设备存在对系统运行过程中的可信检验不全面的情况。现有的可信验证存在部分告警、审计及联动措施不全面的情况(如：应用服务器）。缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。 低风险。

3.4.4 系统管理软件/平台

3.4.4.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
应用服务器-Weblogic	（1）WebLogic中间件对各登录模式均启用身份鉴别； （2）对登录管理的中间件用户进行身份鉴别； （3）WebLogic中间件登录用户设置的身份标识具有唯一性； （4）WebLogic中间件不存在弱口令用户； （5）WebLogic中间件配置合规的密码长度策略。
数据库服务器-Oracle	（1）数据库系统对登录系统的用户进行身份鉴别； （2）数据库系统不存在弱口令用户； （3）数据库系统为登录用户设置的身份标识具有唯一性； （4）数据库系统配置合规的密码长度及复杂度策略； （5）数据库系统配置合规的密码有效周期策略。
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
应用服务器-Weblogic	（1）WebLogic中间件web管理控制台仅内部授权网段可访问； （2）WebLogic中间件合规登录失败处理策略；

	（3）WebLogic中间件配置空闲连接超时。
数据库服务器-Oracle	（1）数据库系统启用合规登录失败处理策略； （2）数据库系统执行合规的锁定策略。
c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
应用服务器-Weblogic	（1）WebLogic中间件管理控制台开启了SSL监听端口。
数据库服务器-Oracle	（1）数据库系统配置合规的远程管理模式。
访问控制	
a）应对登录的用户分配账户和权限；	
应用服务器-Weblogic	（1）WebLogic中间件可提供管理控制台权限功能； （2）对应不同的账户均按需分配不同的用户权限，不存在中间件用户均属于管理级别、高权限的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。
数据库服务器-Oracle	（1）登录数据库系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （2）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在多用户均与sys、DBA用户权限一致的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。
b）应重命名或删除默认账户，修改默认账户的默认口令；	
应用服务器-Weblogic	（1）中间件不存在除如默认账户名； （2）中间件账户口令设置合规。
数据库服务器-Oracle	（1）数据库系统对多余帐户进行删除、锁定或禁止其登录； （2）数据库系统账户口令设置合规。
c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
应用服务器-Weblogic	（1）中间件不存在多余或过期账户； （2）中间件管理员用户与账户之间一一对应。
数据库服务器-Oracle	（1）数据库系统不存在多余或过期账户； （2）数据库系统管理员用户与账户之间一一对应。
d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	
应用服务器-Weblogic	（1）中间件根据安全策略要求对特权用户及宿主管理用户进行分离； （2）中间件管理不存在多个管理级别高的特权用户； （3）中间件管理按不同用户分配了不同的角色并且授予的角色是管理用户所需的最小权限。
数据库服务器-Oracle	（1）数据库系统根据安全策略要求对特权用户进行分离； （2）数据库系统用户权限合理，非管理员未设置过大权限； （3）数据库系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
应用服务器-Weblogic	（1）中间件开启审计功能，审计进程正常； （2）系统的日志审计级别满足要求； （3）审计记录覆盖所有用户。
数据库服务器-Oracle	（1）数据库系统开启审计功能，审计进程正常；

	（2）ORACLE数据库系统启动数据库日志模式和自动归档； （3）审计覆盖所有用户操作审计和记录。
b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	
应用服务器-Weblogic	（1）中间件日期、时间正常； （2）宿主系统启用NTP服务，服务端的地址配置正确； （3）中间件审计记录开启审核策略且日志级别正常。
数据库服务器-Oracle	（1）数据库宿主系统日期、时间正常； （2）数据库系统审计记录内容基本完整。
c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
应用服务器-Weblogic	（1）中间件限制审计文件的访问控制权限，普通用户不可删除及修改； （2）宿主系统针对中间件日志、审计记录具备充足的存储容量； （3）对中间件审计记录进行定期存档备份，其备份策略有效； （4）日志及审计记录保存大于6个月。
数据库服务器-Oracle	（1）数据库系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）数据库系统针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）日志及审计记录保存大于6个月。
入侵防范	
c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
数据库服务器-Oracle	（1）网络设备ACL策略有效限制访问本机的IP地址及管理模式。
d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	
应用服务器-Weblogic	（1）中间件管理具备数据有效性检验功能； （2）中间件管理的校验接口范围较全面。
e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
应用服务器-Weblogic	（1）中间件已根据需要不定期地对已发布的版本进行更新； （2）中间件更新安装前进行安全性和兼容性测试； （3）在系统上线或发生重大变更时测试并安装最新的中间件版本或更新补丁； （4）在不影响业务系统正常运行情况下，对发现的中间件漏洞在确保安全的情况下进行修补； （5）中间件进行渗透及扫描未发现存在可造成高风险的漏洞。
数据库服务器-Oracle	（1）数据库系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）数据库宿主系统不存在启用未加控制的高危端口； （3）MY_SQL分离默认安装的示例数据库； （4）数据库系统进行渗透及扫描未发现存在可造成高风险的漏洞。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
应用服务器-Weblogic	鉴别数据、重要配置数据： （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。
数据库服务器-Oracle	鉴别数据、重要配置数据： （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施；

	（2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a）应提供重要数据的本地数据备份与恢复功能；	
应用服务器-Weblogic	（1）系统定义了相关需要备份的中间件重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）宿主系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）中间件相关数据的备份周期合理； （5）中间件开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
数据库服务器-Oracle	（1）数据库系统定义了相关重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）数据库系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	
应用服务器-Weblogic	（1）宿主系统具有清除用户鉴别信息的功能； （2）经测试，宿主系统退出后无法访问先前中间件登录过的页面； （3）经测试，宿主系统关闭后无残留的中间件用户鉴别信息。
数据库服务器-Oracle	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）数据库系统不保存终端历史记录。
个人信息保护	
a）应仅采集和保存业务必需的用户个人信息；	
数据库服务器-Oracle	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）数据库存储的用户个人信息均为业务应用必需的环节。
b）应禁止未授权访问和非法使用用户个人信息。	
数据库服务器-Oracle	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； （2）数据库具备控制措施禁止未授权访问用户个人信息表单； （3）数据库具备控制措施禁止非法使用用户个人信息表单。

3.4.4.2 主要安全问题汇总分析

安全通用要求

（1）未能提供中间件重要数据的异地定时数据备份功能（如：应用服务器-Weblogic）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

3.4.5 业务应用系统/平台

3.4.5.1 已有安全控制措施汇总分析

安全通用要求

身份鉴别	
a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	
智慧校园系统	（1）系统对各登录模式均启用身份鉴别； （2）系统对登录管理的用户进行身份鉴别； （3）系统登录用户设置的身份标识具有唯一性； （4）系统不存在空口令用户； （5）设备配置合规的密码策略。
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	
智慧校园系统	（1）系统启用合规登录失败处理策略； （2）系统配置合规的操作超时退出措施。
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	
智慧校园系统	(1)应用系统的用户鉴别数据采用SHA-512算法在可控网络环境中传输； （2）系统配置合规的远程管理模式。
访问控制	
a) 应对登录的用户分配账户和权限；	
智慧校园系统	（1）可提供系统权限分配表； （2）登录系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需分配不同的用户权限，不存在所有用户均属于管理级别、高权限的情况。
b) 应重命名或删除默认账户，修改默认账户的默认口令；	
智慧校园系统	（1）系统禁用默认账户名； （2）系统账户口令设置合规。
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	
智慧校园系统	（1）系统不存在多余或过期账户； （2）系统管理员用户与账户之间一一对应。
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	
智慧校园系统	（1）系统不存在多个管理级别高的特权用户； （2）系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。
安全审计	
a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	
智慧校园系统	（1）系统开启审计功能，审计进程正常； (2)系统的日志审计级别满足要求,审计覆盖所有用户操作审计和记录。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	

智慧校园系统	（1）系统日期、时间正常； （2）系统审计记录内容基本完整。
c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	
智慧校园系统	（1）系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）系统针对日志、审计记录具备充足的存储容量； （3）审计记录及日志保存大于6个月。
入侵防范	
c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	
智慧校园系统	（1）系统自身设定有效的终端访问策略，通过访问措施进行管理地址的限制。
d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	
智慧校园系统	（1）系统具备数据有效性检验功能； （2）系统的校验接口范围较全面。
e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	
智慧校园系统	（1）系统已根据需要不定期地对已发布的版本进行更新； （2）在系统上线或发生重大变更时测试并安装最新的版本或更新补丁； （3）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补。
数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
智慧校园系统	鉴别数据、重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； （2）系统对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a）应提供重要数据的本地数据备份与恢复功能；	
智慧校园系统	（1）系统定义了相关需要备份重要数据； （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
剩余信息保护	
应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	
智慧校园系统	（1）系统具有清除用户鉴别信息的功能； （2）经测试，系统退出后无法访问先前登录过的页面； （3）经测试，系统关闭后无残留的用户鉴别信息。
个人信息保护	
a）应仅采集和保存业务必需的用户个人信息；	
智慧校园系统	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息； （3）系统采集的用户个人信息均为业务应用必需的环节。

b) 应禁止未授权访问和非法使用用户个人信息。	
智慧校园系统	(1) 系统不采集和保存任何形式的用户个人信息； (2) 系统对所有涉及个人信息的环节均有明确的授权同意过程； (3) 系统具备控制措施禁止未授权访问用户个人信息； (4) 系统具备控制措施禁止非法使用用户个人信息。

3.4.5.2 主要安全问题汇总分析

安全通用要求

（1）未能提供应用软件系统重要数据的异地定时数据备份功能（如：智慧校园系统）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

3.4.6 数据资源

3.4.6.1 已有安全控制措施汇总分析

安全通用要求

数据完整性	
应采用校验技术保证重要数据在传输过程中的完整性。	
重要业务数据 重要个人信息	(1) 系统在通信传输过程中对相关数据采取完整性保护措施； (2) 系统对重要数据在传输过程中采取必要的完整性保护措施。
数据备份恢复	
a) 应提供重要数据的本地数据备份与恢复功能；	
重要业务数据 重要个人信息	(1) 系统定义了相关需要备份重要数据； (2) 单位具备合理的重要数据的备份策略规范； (3) 系统定期完全依照备份策略，采用正确的配置进行本地备份； (4) 系统的备份周期合理：每天增量一次、每月全备一次； (5) 系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。
个人信息保护	
a) 应仅采集和保存业务必需的用户个人信息；	
重要个人信息	(1) 单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； (2) 系统按管理规范，仅最小化采集必需的用户个人信息； (3) 系统采集的用户个人信息均为业务应用必需的环节。
b) 应禁止未授权访问和非法使用用户个人信息。	
重要个人信息	(1) 系统对所有涉及个人信息的环节均有明确的授权同意过程；

	(2) 系统具备控制措施禁止未授权访问用户个人信息; (3) 系统具备控制措施禁止非法使用用户个人信息。

3.4.6.2 主要安全问题汇总分析

安全通用要求

重要业务数据

(1) 未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要业务数据）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

重要个人信息

(1) 未能提供应用软件系统重要数据的异地定时数据备份功能（如：重要个人信息）。异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。 中风险。

3.4.7 其他系统或设备

3.4.7.1 已有安全控制措施汇总分析

安全通用要求

无其他系统或设备，不涉及相关测评

3.4.7.2 主要安全问题汇总分析

安全通用要求

无其他系统或设备，不涉及相关测评

3.5 安全管理中心

3.5.1 已有安全控制措施汇总分析

安全通用要求

系统管理	
a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；	
管理中心	（1）网络中部署运维安全管理系统实现集中的系统管理； （2）系统对登录用户进行身份鉴别； （3）系统用户标识具有唯一性； （4）系统可实现对账户的身份鉴别数据进行保密性和完整性保护； （5）系统管理操作模式具备控制措施； （6）系统具备相应的管理操作审计措施。
审计管理	
a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；	
管理中心	（1）网络中部署运维安全管理系统实现集中安全审计功能； （2）审计系统对审计管理员进行身份鉴别； （3）审计系统用户标识具有唯一性； （4）审计系统管理操作模式具备控制措施； （5）审计系统具备相应的管理操作审计措施。
b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	
管理中心	智慧校园系统: （1）审计管理员定期对审计记录进行分析，对发现的安全可疑事件及时处理； （2）单位具有安全审计策略文件，规范审计记录的存储、管理和查询要求； （3）审计管理员按规范要求对审计记录进行管理。 重要审计数据: 日志审计系统、运维安全管理系统: （1）设备在通信传输过程中对相关数据采取完整性保护措施； （2）设备对重要数据在传输过程中采取必要的完整性保护措施。

3.5.2 主要安全问题汇总分析

安全通用要求

（1）系统管理的资源、运行及配置管理不够全面（如：管理中心）。系统的资源和运行缺少统一的管理，将导致系统可能无法按规划实现基于资源配置、 系统加载、异常处理、及备份/恢复等的安全控制措施。 低风险。

3.6 安全管理制度

3.6.1 已有安全控制措施汇总分析

安全通用要求

安全策略	
应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。	
制度文件、执行/记录文件	（1）单位具有网络安全工作的总体方针和安全策略文件； （2）制度内容包括明确的单位安全工作要求； （3）管理文件详见《信息安全总体策略》。
管理制度	
a) 应对安全管理活动中的主要管理内容建立安全管理制度；	
制度文件、执行/记录文件	（1）单位有针对安全管理活动中的各类管理内容建立安全管理制度； （2）现有制度已覆盖管理活动的主要的方面； （3）制度详见：《信息安全总体策略》、《网络安全管理规范》、《组织安全结构和人员职责制度》、《人员管理制度》、《员工考核管理制度》。
b) 应对管理人员或操作人员执行的日常管理操作建立操作规程。	
制度文件、执行/记录文件	（1）单位针对相关业务日常管理的操作建立规程类管理制度； （2）现有制度已覆盖重要管理方面的系统维护手册和用户操作规程等； （3）管理文件详见《设备及系统软件配置和操作手册》。
制定和发布	
a) 应指定或授权专门的部门或人员负责安全管理制度的制定；	
制度文件、执行/记录文件	（1）单位针对安全管理制度的制定，指定教育信息与网络中心部主要负责； （2）在已制定的相关制度中可查阅到被授权制定管理制度的部门/人员信息； （3）管理文件详见《安全管理组织规范》。
b) 安全管理制度应通过正式、有效的方式发布，并进行版本控制。	
制度文件、执行/记录文件	（1）单位针对制度的制定和发布要求，制定管理规范文件； （2）管理规范文件对文件制定及发布定义了规范要求； （3）安全管理制度的收发登记记录有效； （4）管理文件详见《制度制定、发布、评审和修订管理制度》、《收发文登记记录》。
评审和修订	
应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	
制度文件、执行/记录文件	（1）单位针对制度的合理性和适用性需进行论证和审定及修订的要求，制定管理规范文件； （2）管理规范文件对制度的评审及修订定义了规范要求； （3）单位具有安全管理制度的审定或论证的过程记录；

	（4）单位对做过修订的制度，具备有修订版本的安全管理过程记录； （5）管理文件详见《制度制定、发布、评审和修订管理制度》及 《安全管理制度评审记录》。

3.6.2 主要安全问题汇总分析

安全通用要求

智慧校园系统针对安全管理制度层面的安全通用要求采取的安全措施比较完善，未发现不符合项。

3.7 安全管理机构

3.7.1 已有安全控制措施汇总分析

安全通用要求

岗位设置	
a) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；	
制度文件、执行/记录文件	（1）单位已明确网络安全管理工作的职能部门，并明确了各岗位职责； （2）单位各部门职责文档已明确网络安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备网络安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。
b) 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。	
制度文件、执行/记录文件	（1）单位已明确系统安全管理工作的职能部门，并明确了各岗位职责； （2）单位各部门职责文档已明确系统安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备系统安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。
人员配备	
应配备一定数量的系统管理员、审计管理员和安全管理员等。	
制度文件、执行/记录文件	（1）单位针对人员配备要求，制定了管理制度； （2）单位按要求配备一定数量的重要岗位管理人员； （3）单位针对各岗位人员，制定并维护人员档案； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员

	职责制度》。
授权和审批	
a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；	
制度文件、执行/记录文件	（1）单位在制度中用文字描述或在流程图中明确，对关键活动进行审批； （2）单位对审批过程明确审批权限，对各项信息系统的重要操作与变更明确审批部门和批准人； （3）管理文件详见《授权和审批管理规定》。
b) 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。	
制度文件、执行/记录文件	（1）单位针对各项业务操作及变更等建立了审批程序规定； （2）单位针对系统变更、系统接入、物理范围等事项已明确按审批程序执行，记录有批准人签字； （3）管理文件详见《授权和审批管理规定》。
沟通和合作	
a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；	
制度文件、执行/记录文件	（1）单位针对机构内部管理人员之间、部门之间的沟通与合作，制定了管理制度； （2）单位的管理制度规范了合作和沟通的方式和周期； （3）单位有组织机构内部人员联系表； （4）单位有定期召开信息安全会议，保存有会议纪要； （5）管理文件详见《安全教育和培训制度》、《技能培训记录》《外部联系表》。
b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；	
制度文件、执行/记录文件	（1）单位针对加强与外部单位的合作与沟通，制定了管理制度规定； （2）单位能按要求与相关单位保持沟通合作，并提供相关单位联系方式和交流会议纪要； （3）管理文件详见《安全教育和培训制度》、《技能培训记录》、《外部联系表》。
c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	
制度文件、执行/记录文件	（1）单位建立了完善的对外联单位的联系列表； （2）管理文件详见《外部联系表》。

3.7.2 主要安全问题汇总分析

安全通用要求

（1）单位开展的检查工作不够完善（如：制度文件、执行/记录文件）。检查工作开展不仔细，可能对存在或潜在的安全风险不能被及时发现并进行处理。 低风险。

3.8 安全管理人员

3.8.1 已有安全控制措施汇总分析

安全通用要求

人员录用	
a) 应指定或授权专门的部门或人员负责人员录用；	
制度文件、执行/记录文件	（1）单位授权专门的部门负责人员录用工作，制定了管理制度规范； （2）由人力资源保障科负责人员录用工作； （3）管理文件详见《人员管理制度》。
b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查。	
制度文件、执行/记录文件	（1）单位针对人员录用过程，制定了明确要求，并形成人员安全管理制度； （2）单位现有管理制度明确说明录用人员应具备的条件； （3）单位按规定执行人员录用的相关审查过程； （4）管理文件详见《人员管理制度》、《人员入职考核记录》。
人员离岗	
应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。	
制度文件、执行/记录文件	（1）单位针对离岗人员权限终止及取回机构提供的各种设施的要求，制定了管理制度； （2）单位按规范开展对离岗人员的相关管理工作； （3）管理文件详见《人员管理度》、《人员离岗申请表》、《离场信息资料交接表》。
安全意识教育和培训	
应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。	
制度文件、执行/记录文件	（1）单位针对人员安全培训及责任和惩戒措施，制定了管理制度； （2）单位已开展安全意识教育及岗位技能培训。 （3）管理文件详见《安全教育和培训制度》。
外部人员访问管理	
a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；	
制度文件、执行/记录文件	（1）单位针对外部人员物理访问，制定了外部人员访问管理文档； （2）单位具备有效的外部人员访问重要区域的书面申请文档； （3）单位具备外部人员访问重要区域的登记记录； （4）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。
b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；	
制度文件、执行/记录文件	（1）单位针对外部接入受控网络访问系统，制定了管理制度； （2）单位具备外部人员接入受控网络前的申请审批流程； （3）单位具备外部人员接入及访问系统的书面申请文档； （4）单位具备外部人员接入及访问系统的登记记录； （5）管理文件详见《外部人员访问管理制度》、《外部服务人员管理规

	范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。

3.8.2 主要安全问题汇总分析

安全通用要求

（1）单位未完全按管理规范开展人员离场后的清理工作（如：制度文件、执行/记录文件）。人员离场后的清理工作开展不规范，可能导致遗留外部人员访问受控区域的记录，存在被二次非法利用，造成泄密。 低风险。

3.9 安全建设管理

3.9.1 已有安全控制措施汇总分析

安全通用要求

定级和备案	
a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；	
制度文件、执行/记录文件	（1）单位的被测系统于2022年4月已完成备案； （2）系统备案相关文档（定级报告）中明确等级划分方法和理由，SAG三个方面的级别描述清晰； （3）管理文件详见《定级备案》。
b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；	
制度文件、执行/记录文件	(1)单位针对系统定级结果的审批及评审工作等要求,制定了管理制度; （2）现有系统的定级已具备合理性和正确性审定； （3）管理文件详见《定级备案》。
c) 应保证定级结果经过相关部门的批准；	
制度文件、执行/记录文件	（1）单位针对系统定级结果的上级批准要求，制定了管理制度； （2）现有系统的定级获得了相关部门的批准； （3）管理文件详见《定级备案》。
d) 应将备案材料报主管部门和相应公安机关备案。	
制度文件、执行/记录文件	（1）单位对被测系统的等级备案表、定级报告等备案材料已经报相应公安机关备案； （2）单位具备公安机关出具的备案号； （3）管理文件详见《定级备案》。
产品采购和使用	
a) 应确保网络安全产品采购和使用符合国家的有关规定；	
制度文件、执行/记录文件	（1）单位已建立安全产品管理的相关管理规定； （2）单位具备安全产品采购流程及相关实施文档；

	（3）被测系统使用的安全产品具备销售许可资质； （4）安全产品具均为国内产品； （5）管理文件详见《设备安全管理制度》。
b）应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。	
制度文件、执行/记录文件	（1）单位已建立密码产品与服务管理的相关管理制度； （2）系统未使用密码产品； （3）管理文件详见《设备安全管理制度》。
外包软件开发	
b）应保证开发单位提供软件设计文档和使用指南。	
制度文件、执行/记录文件	（1）单位制定软件开发项目验收要求，明确开发单位的提交材料； （2）开发单位提供软件日常维护和使用所需的文档； （3）管理文件详见《外包开发软件管理规定》、《设备及系统软件配置和操作手册》。
工程实施	
a）应指定或授权专门的部门或人员负责工程实施过程的管理；	
制度文件、执行/记录文件	（1）单位针对专门的部门负责工程实施过程的管理要求，制定管理度； （2）单位由专岗负责系统建设的工程实施，且按照实施方案的要求对进度和质量进行控制； （3）管理文件详见《工程实施管理制度》。
b）应制定安全工程实施方案控制工程实施过程。	
制度文件、执行/记录文件	（1）单位制定了详细的工程实施方案； （2）工程实施单位严格按照方案执行，并有过程记录； （3）管理文件详见《测试及验收方案》、《工程项目实施方案》。
系统交付	
a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；	
制度文件、执行/记录文件	（1）单位具备系统交付清单； （2）系统交付清单内容较详细； （3）单位的清点工作较合规； （4）管理文件详见《系统交付管理》、《资产清单》。
b）应对负责运行维护的技术人员进行相应的技能培训；	
制度文件、执行/记录文件	（1）单位已对负责系统运行维护的技术人员进行了技能培训； （2）具备运维人员的培训记录； （3）管理文件详见《系统交付管理》、《资产清单》、《系统交付清单》、《技能培训记录》。
c）应提供建设过程文档和运行维护文档。	
制度文件、执行/记录文件	（1）单位提供了系统建设过程中的文档； （2）单位提供了指导用户进行系统运维的文档和系统培训手册； （3）管理文件详见《系统交付管理》、《系统交付清单》、《设备及系统软件配置和操作手册》。
等级测评	
a）应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；	
制度文件、执行/记录文件	（1）单位针对系统等级测评要求，制定管理制度； （2）系统按要求开展首次测评工作； （3）管理文件详见《系统安全管理制度》。

b) 应在发生重大变更或级别发生变化时进行等级测评；	
制度文件、执行/记录文件	（1）管理制度中已规定在系统发生变更时及时对系统进行等级测评； （2）系统未发生过重大变更，系统等级未发生变化； （3）管理文件详见《系统安全管理制度》。
c) 应确保测评机构的选择符合国家有关规定。	
制度文件、执行/记录文件	（1）已选择在“全国等级保护测评机构推荐目录”中的测评单位进行等级测评； （2）管理文件详见《系统安全管理制度》、《网络安全等级保护测评服务合同》。
服务供应商选择	
a) 应确保服务供应商的选择符合国家的有关规定；	
制度文件、执行/记录文件	（1）单位在管理制度内明确提出安全服务供应商选择的要求； （2）单位选择的安全服务商符合国家的有关规定，具备相应的安全服务资质； （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。
b) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。	
制度文件、执行/记录文件	（1）单位的管理制度中已规定，需与安全服务商签订安全相关的协议并明确整个服务供应链各方需履行的网络安全相关义务； （2）单位已按规定与选定的安全服务商签订合规的协议； （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。

3.9.2 主要安全问题汇总分析

安全通用要求

（1）单位未具备适用于被测系统的安全规划设计方案（如：制度文件、执行/记录文件）。规划设计需求不全面，可能导致安全方案设计不完善，信息系统存在安全缺陷。低风险。

（2）单位未具备完整的安全设计方案相关的文档。单位相关方案的设计的内容不够完善（如：制度文件、执行/记录文件）。相关合规的规划配套文件缺失，可能导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。 中风险。

（3）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定。单位未对相关论证过程及内容进行完整的记录（如：制度文件、执行/记录文件）。未开展规范

的审批过程，可能存在安全整体规划缺乏合理性和可行性，导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。 低风险。

（4）单位未在软件开发过程中对所有软件安全性进行测试。单位未在软件安装之前按要求对所有软件开展恶意代码检测（如：制度文件、执行/记录文件）。软件交付前恶意代码检测不规范，可能在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。 低风险。

（5）单位未完全根据测试验收方案组织相关部门和人员开展验收工作（如：制度文件、执行/记录文件）。可能由于验收测试不严谨，造成测试过程缺乏计划性及操作性，无法保证经过测试验收的系统达到既定的安全性等目标。 低风险。

(6)针对系统上线前的安全性测试工作存在问题(如:制度文件、执行/记录文件)。未按规定开展上线前测试，安全隐患可能在系统上线运行前未被发现并作出相应处理。低风险。

3.10 安全运维管理

3.10.1 已有安全控制措施汇总分析

安全通用要求

环境管理	
a) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；	
制度文件、执行/记录文件	（1）单位建立机房安全方面的管理制度，对有关运维方面的管理作出规定； （2）单位具备完整的机房出入登记记录； （3）单位具备完整的机房基础设施的维护记录； （4）管理文件详见《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。
b) 应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；	
制度文件、执行/记录文件	（1）单位建立机房安全方面的管理制度； （2）单位现有机房管理记录与制度相符；

	（3）制度详见：《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。
c）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	
制度文件、执行/记录文件	（1）单位机房安全管理制度已明确来访人员的接待区域的要求； （2）单位按规范要求开展人员来访接待； （3）单位办公环境未发现有随意放置含有敏感信息介质的情况； （4）制度详见：《机房安全管理制度》、《物理安全管理规范》、《办公环境保密管理》。
资产管理	
应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。	
制度文件、执行/记录文件	（1）单位已建立有效的资产清单； （2）单位现有资产清单内容较全面； （3）制度详见：《设备安全管理制度》、《资产清单》。
介质管理	
a）应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；	
制度文件、执行/记录文件	（1）介质按管理要求放置于受控的环境中（如：机房）； （2）介质管理具备较全面的记录； （3）制度详见：《设备安全管理制度》、《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。
b）应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。	
制度文件、执行/记录文件	（1）介质管理制度中对介质安全传输有明确规定； （2）存储重要信息的介质在物理传输过程，具备严格的环节控制，无重大环节疏漏； （3）对介质的归档和查询均具备记录； （4）制度详见：《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。
设备维护管理	
a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	
制度文件、执行/记录文件	（1）单位人员岗位职责相关文档已明确设备维护管理的责任部门； （2）单位对各类设施、设备进行定期维护； （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。
b）应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。	
制度文件、执行/记录文件	（1）单位建立了配套设施、软硬件维护管理方面的管理制度； （2）单位开展相关工作与制度相符，且保留记录； （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。
网络和系统安全管理	

a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；	
制度文件、执行/记录文件	（1）单位建立系统安全管理文档，对系统管理员的管理制定了要求； （2）单位对各类关键角色建立了相应的工作职责文档； （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。
b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	
制度文件、执行/记录文件	（1）单位制定管理制度，对系统账号进行管理； （2）单位按管理规范开展账号管理工作； （3）账户管理记录内容较完整； （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。
c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	
制度文件、执行/记录文件	（1）单位建立了网络和系统安全管理制度； （2）网络和系统安全管理制度内容较全面； （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。
d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；	
制度文件、执行/记录文件	（1）单位对重要设备、系统的配置和操作建立配置手册； （2）现有操作配置手册已明确操作步骤、参数配置； （3）制度详见：《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。
e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。	
制度文件、执行/记录文件	（1）单位制定日常运维管理的相关制度规范； （2）单位按制度规范开展日常运维管理工作； （3）单位具备合规的运维记录； （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》、《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。
恶意代码防范管理	
a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	
制度文件、执行/记录文件	（1）单位制定恶意代码防范管理制度，明确对外来计算机或存储设备接入系统前进行恶意代码检查； （2）单位按外来计算机接入恶意代码检查规范开展工作； （3）单位制定培训管理制度，明确需通过培训提升员工的防恶意代码意识； （4）单位按培训管理要求开展工作； （5）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申请表》、《信息管理系统漏洞检查表》。
b) 应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；	
制度文件、执行/记录文件	（1）建立恶意代码防范管理文档； （2）管理制度中覆盖防恶意代码软件的授权使用、恶意代码库升级、定期查杀等内容；

	（3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》。
配置管理	
应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。	
制度文件、执行/记录文件	（1）单位制定了基本配置信息管理的制度要求； （2）管理文件详见：《主机安全管理规范》、《网络安全管理规范》、《应用安全管理规范》、《网络配置信息》。
变更管理	
应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。	
制度文件、执行/记录文件	（1）单位建立了关于系统变更管理的制度文件； （2）现有变更管理制度覆盖了变更管理的各方面要求； （3）制度详见：《变更控制管理制度》、《通用变更记录表》。
备份与恢复管理	
a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；	
制度文件、执行/记录文件	（1）单位根据业务重要程度，制定了需要定期备份的重要业务信息列表或清单。清单内需要定期备份的重要数据已经过用户方确认； （2）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。
b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等；	
制度文件、执行/记录文件	（1）单位建立了备份与恢复管理相关的安全管理制度； （2）备份与恢复管理的相关要求比较明确； （3）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。
c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	
制度文件、执行/记录文件	（1）单位现有管理制度，明确了数据备份策略和数据恢复策略，以及备份程序和恢复程序； （2）单位可按策略要求实现重要数据的定期备份与恢复性测试； （3）单位现有的备份的数据均经过恢复性测试，可确保备份的数据可用； （4）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。
安全事件处置	
a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件；	
制度文件、执行/记录文件	（1）单位已在安全培训及宣传过程中告知用户在发现安全弱点和可疑事件时及时向安全管理部门报告； （2）单位在系统运维过程中对发现的安全弱点和可疑事件均编制了对应的报告或相关文档； （3）单位现有安全弱点和可疑事件报告文档内容较详实； （4）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。
b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；	
制度文件、执行/记录文件	（1）单位制定了安全事件报告和处置管理制度； （2）现有安全事件管理制度内容较完整； （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。

c) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。	
制度文件、执行/记录文件	（1）单位具备对安全事件的分析、处理、总结、防范等的报告／过程文档； （2）单位提供的安全事件报告和响应处置记录内容较完整； （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。
应急预案管理	
a) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；	
制度文件、执行/记录文件	（1）单位制定重要事件的应急预案； （2）单位现有应急预案涉及的类型范围较全面； （3）单位现有应急预案的内容较完整； （4）制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。
b) 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。	
制度文件、执行/记录文件	（1）单位定期对相关人员进行应急预案培训； （2）单位根据不同的应急预案，按要求进行应急演练； （3）单位具备近期应急预案工作开展的相关记录； （4）单位提供的应急预案培训记录比较完整； （5）单位提供的应急预案演练记录比较完整； （6）经检查单位目前一旦出现应急事件，可参照预案合理有序的进行应急事件处置过程； （7）制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。

3.10.2 主要安全问题汇总分析

安全通用要求

（1）单位未严格按规范开展漏洞及安全隐患检测工作（如：制度文件、执行/记录文件）。漏洞检测、修补工作不到位，可能存在未授权人员利用漏洞攻击信息系统的风险。 低风险。

（2）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作（如：制度文件、执行/记录文件）。可能导致系统恶意代码检测管理不到位，存在信息系统感染恶意代码，从而导致严重的信息安全风险。 低风险。

（3）单位不了解现有密码相关的国家标准和行业标准。单位缺乏密码管理要求的制度文档（如：制度文件、执行/记录文件）。密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不到位，存在违反国家政策的风险。 中风险。

3.11 其他安全要求指标

3.11.1 已有安全控制措施汇总分析

本次测评未涉及其他安全要求指标。

3.11.2 主要安全问题汇总分析

本次测评未涉及其他安全要求指标。

3.12 验证测试

验证测试包括漏洞扫描，渗透测试等，验证测试发现的安全问题对应到相应的测评项的结果记录中。详细验证测试报告见报告附录。

3.12.1 漏洞扫描

3.12.1.1 漏洞扫描结果统计

本次测评主要使用了[绿盟远程安全评估系统]对系统的设备进行了安全扫描，其所涉及的系统版本为：[V6.0R04F01SP06]，规则库版本为：[V6.0R02F01.2900]。扫描结果如下：

经分析统计，共发现各接入点存在3类漏洞，其中0类危险程度为高的漏洞，0类危害程度为中的漏洞，3类危害程度为低的漏洞。

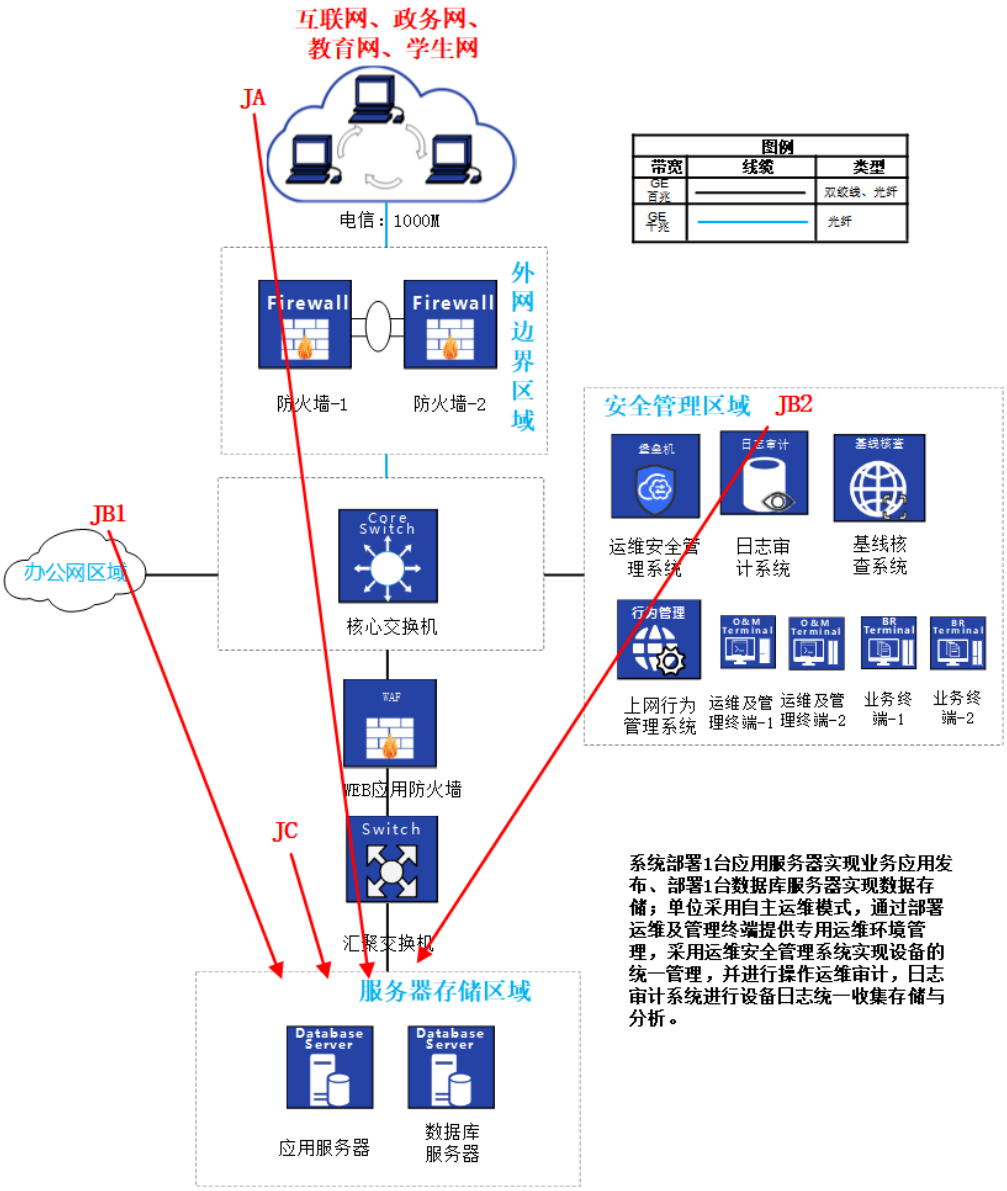


图 3-1 漏洞扫描工具接入测试示意图

接入点JA：在防火墙外侧接入，开展扫描/渗透主要目的是，探测对外服务功能区上各服务器、应用系统对外部网络边界暴露的安全漏洞情况，并根据漏洞扫描的结果接入渗透测试工具集，试图利用服务器、应用的安全漏洞入侵网络的行为。

接入点JB：在办公网区域VLAN段、安全管理区域VLAN段接入，开展扫描/渗透主要目的是，模拟外联单位/内部恶意用户发现操作系统、数据库、Web应用、第三方产品等安全漏洞的过程，并尝试利用以上漏洞实施诸如获取系统控制权（GetShell）、获得大量敏感信息（DragLibrary）等模拟攻击行为。

接入点JC：在系统所在VLAN的交换机接入，开展扫描/渗透主要目的是，直接测试对服务功能区上各服务器在最小化防御的基础上，对网络暴露的安全漏洞情况。

（1）接入点A漏洞扫描结果统计

根据在接入点A对15台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-1 接入点 A 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	0	0	0	0
2	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	0	0	0	0
3	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	0	0	0	0
4	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	0	0	0	0
5	172.16.1.14/上网行为管理系统	(安全设备)深信服AC12.0.26	0	0	0	0
6	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	0	0	0	0
7	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	0	0	0	0
8	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	0	0	0	0
9	192.168.33.11/业务终端-1	(终端设备) Windows 10（版本 20H2（内部版本19044.1889）	0	0	0	0
10	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10（版本 20H2（内部版本19044.1889）	0	0	0	0
11	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10（版本 20H2（内部版本19044.1889）	0	0	0	0
12	192.168.33.10/业务终端-2	(终端设备) Windows 10（版本 20H2（内部版本19044.1889）	0	0	0	0
13	10.1.8.10/数据库服务器	(服务器存储设备)CentOS 7.7	0	0	0	0
14	10.1.8.17/应用服务器	(服务器存储设备)CentOS 7.7	0	0	0	0
15	https://ehall.mmpt.edu.cn/智慧校园系统	(业务应用软件平台) V6.0	0	0	0	0
安全漏洞数量小计			0	0	0	0

（2）接入点B漏洞扫描结果统计

根据在接入点B对15台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-2 接入点 B 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	1	0	0	1
2	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	1	0	0	1
3	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	1	0	0	1
4	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	2	0	0	2
5	172.16.1.14/上网行为管理系统	(安全设备)深信服 AC12.0.26	1	0	0	1
6	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	1	0	0	1
7	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	1	0	0	1
8	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	1	0	0	1
9	192.168.33.11/业务终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
10	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
11	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
12	192.168.33.10/业务终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
13	10.1.8.10/数据库服务器	(服务器存储设备)CentOS 7.7	2	0	0	2
14	10.1.8.17/应用服务器	(服务器存储设备)CentOS 7.7	2	0	0	2
15	https://ehall.mmpt.edu.cn/智慧校园系统	(业务应用软件平台) V6.0	0	0	0	0
安全漏洞数量小计			11	0	0	11

（3）接入点C漏洞扫描结果统计

根据在接入点C对15台被测设备的漏洞扫描结果，汇总统计如下表：

表 3-3 接入点 C 漏洞扫描结果汇总表

序号	设备名称或IP地址	系统及版本	安全漏洞数量			
			低	中	高	小计
1	10.2.1.4/运维安全管理系统	(安全设备)深信服V3.0.6	1	0	0	1
2	10.2.1.2/日志审计系统	(安全设备)深信服LAS 3.0.5	1	0	0	1
3	10.2.1.3/基线核查系统	(安全设备)深信服V3.0.3	1	0	0	1
4	172.16.1.2/核心交换机	(网络设备)H3C version 7.1.070, Release 7585P07	2	0	0	2
5	172.16.1.14/上网行为管理系统	(安全设备)深信服 AC12.0.26	1	0	0	1
6	172.16.1.18/WEB应用防火墙	(安全设备)深信服AF 8.0.9	1	0	0	1
7	172.16.1.1/防火墙-2,防火墙-1	(安全设备)深信服AF 8.0.23	1	0	0	1
8	172.16.1.19/汇聚交换机	(网络设备)H3C version 7.1.070, Release 6126P20	1	0	0	1
9	192.168.33.11/业务终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
10	192.168.0.2/运维及管理终端-1	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
11	192.168.0.1/运维及管理终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
12	192.168.33.10/业务终端-2	(终端设备) Windows 10（版本 20H2（内部版本 19044.1889）	0	0	0	0
13	10.1.8.10/数据库服务器	(服务器存储设备)CentOS 7.7	2	0	0	2
14	10.1.8.17/应用服务器	(服务器存储设备)CentOS 7.7	2	0	0	2
15	https://ehall.mmpt.edu.cn/智慧校园系统	(业务应用软件平台) V6.0	0	0	0	0
安全漏洞数量小计			11	0	0	11

3.12.1.2 漏洞扫描问题描述

通过对漏洞扫描结果进行分析,智慧校园系统存在的主要安全漏洞汇总如下表所示

表 3-4 主要安全漏洞汇总表

序号	安全漏洞名称	关联资产/域名	严重程度
1	SSH版本信息可被获取 此类漏洞涉及服务器存储设备。	10.1.8.10/数据库服务器 10.1.8.17/应用服务器	低
2	允许Traceroute探测 此类漏洞涉及网络设备、安全设备、服务器存储设备。	10.1.8.17/应用服务器 10.1.8.10/数据库服务器 10.2.1.4/运维安全管理系统 10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/上网行为管理系统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/汇聚交换机 172.16.1.2/核心交换机	低
3	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161) 此类漏洞涉及网络设备。	172.16.1.2/核心交换机	低

3.12.2 渗透测试

经分析统计，共发现各接入点存在1类漏洞，其中0类危险程度为高的漏洞，0类危害程度为中的漏洞，1类危害程度为低的漏洞。

3.12.2.1 渗透测试过程说明

方案制定：

在得到委托单位的书面授权许可后，才进行渗透测试的实施。并且将实施范围、方法、时间、人员等具体的方案委托单位进行交流，并得到委托单位的认同。在测试实施之前，会做到让委托单位对渗透测试过程和风险的知晓，使随后的正式测试流程都在委托单位的管控下。

信息收集：

此阶段中，渗透测试人员对目标信息系统进行必要的信息收集，如操作系统类型、开放的端口和服务、中间件信息、后台数据库类型、web开发语言等，即收集有利于漏洞挖掘的相关信息，为渗透测试做准备。

漏洞挖掘方法：

此阶段中，渗透测试人员对目标信息系统开始进行渗透测试，利用已知信息和现有条件及技术进行漏洞挖掘，尽可能发现目标信息系统中存在的所有安全风险，并进行记录。

漏洞利用：

此阶段中，渗透测试人员对目标信息系统对上一阶段漏洞挖掘中发现的漏洞进行必要的利用以证明其危害性，再对渗透测试过程所产生的测试数据进行清除。

输出报告：

此阶段中，渗透测试人员把渗透测试记录、截图等相关信息进行整理，然后撰写渗透测试报告，最终提交给委托单位。

漏洞修复：

此阶段中，委托单位依据收到的渗透测试报告对其中所提出的漏洞进行整改，可参考报告中所提出的修复建议，整改完成后联系本单位相关人员准备回归测试。

回归测试：

此阶段中，渗透测试人员对整改后的目标信息系统进行复测，以确定报告中提出的漏洞是否已被修复，若已被修复，则进入下一阶段；否则，返回上一阶段。

测试工具：

序号	工具	工具用途
1	Burpsuite Pro	用于攻击Web应用程序的集成软件
2	Sqlmap	开源的自动化SQL注入工具

序号	工具	工具用途
3	Nmap	开源的网络发现和安全审计工具
4	OWASP ZAP	自动化Web应用漏洞扫描工具
5	其他测试工具	根据信息系统的类别选择不同的工具（如自写脚本、目录扫描器、木马扫描器、其它开源工具等）

3.12.2.2 渗透测试问题描述

通过渗透测试发现，智慧校园系统存在的安全问题汇总如下表所示。

表 3-5 渗透测试结果汇总表

序号	安全问题	关联资产/域名	严重程度
1	缺少“Content-Security-Policy”响应头 此类漏洞涉及业务应用软件平台。	https://ehall.mmpt.edu.cn/ 智慧校园系统	低

3.13 单项测评小结

3.13.1 控制点符合情况汇总

根据单项测评结果汇总控制点符合情况如下表所示。（表格以不同颜色对测评结果进行区分，不符合的安全控制点采用红色标识，部分符合的采用黄色标识，不适用的采用蓝色标识且不做勾选。）

表 3-6 控制点符合情况汇总表

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
1	安全通用要求	安全物理环境	物理位置选择	√		
2			物理访问控制		√	
3			防盗窃和防破坏	√		
4			防雷击	√		
5			防火		√	
6			防水和防潮	√		

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
7			防静电			√
8			温湿度控制	√		
9			电力供应	√		
10			电磁防护	√		
11	安全通用要求	安全通信网络	网络架构		√	
12			通信传输	√		
13			可信验证			√
14	安全通用要求	安全区域边界	边界防护	√		
15			访问控制	√		
16			入侵防范		√	
17			恶意代码和垃圾邮件防范		√	
18			安全审计	√		
19			可信验证			√
20	安全通用要求	安全计算环境	身份鉴别	√		
21			访问控制	√		
22			安全审计	√		
23			入侵防范	√		
24			恶意代码防范	√		
25			可信验证			√
26			数据完整性	√		

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
27			数据备份恢复		√	
28			剩余信息保护	√		
29			个人信息保护	√		
30	安全通用要求	安全管理中心	系统管理		√	
31			审计管理	√		
32	安全通用要求	安全管理制度	安全策略	√		
33			管理制度	√		
34			制定和发布	√		
35			评审和修订	√		
36	安全通用要求	安全管理机构	岗位设置	√		
37			人员配备	√		
38			授权和审批	√		
39			沟通和合作	√		
40			审核和检查		√	
41	安全通用要求	安全管理人员	人员录用	√		
42			人员离岗	√		
43			安全意识教育和培训	√		
44			外部人员访问管理		√	
45	安全通用要求	安全建设管理	定级和备案	√		
46			安全方案设计			√

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
47			产品采购和使用	√		
48			自行软件开发			
49			外包软件开发		√	
50			工程实施	√		
51			测试验收		√	
52			系统交付	√		
53			等级测评	√		
54			服务供应商选择	√		
55	安全通用要求	安全运维管理	环境管理	√		
56			资产管理	√		
57			介质管理	√		
58			设备维护管理	√		
59			漏洞和风险管理			√
60			网络和系统安全管理	√		
61			恶意代码防范管理		√	
62			配置管理	√		
63			密码管理			√
64			变更管理	√		
65			备份与恢复管理	√		
66			安全事件处置	√		

序号	通用/扩展	安全类	安全控制点	符合情况		
				符合	部分符合	不符合
67			应急预案管理	√		
68			外包运维管理			
安全通用要求控制点符合情况数量统计				47	12	7
控制点符合情况数量统计				47	12	7

3.13.2 安全问题汇总

针对单项测评结果中存在的部分符合和不符合项进行汇总，形成了安全问题如下表所示。

表 3-7 安全问题汇总表

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T1	（1）机房出入口未配置电子门禁系统。	信息化机房	安全通用要求	安全物理环境	物理访问控制	机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。
T2	（1）机房建设未完全采用符合耐火等级的建筑材料； （2）机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级。	信息化机房	安全通用要求	安全物理环境	防火	b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。
T3	（1）机房内缺乏防静电措施（如防静电地板或铺设防静电地毯）。	信息化机房	安全通用要求	安全物理环境	防静电	应采用防静电地板或地面并采用必要的接地防静电措施。
T4	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	安全通用要求	安全通信网络	网络架构	a）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
T5	（1）缺乏对通信设备可信验证方面的安全设计要求； （2）现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况。	安全通信网络	安全通用要求	安全通信网络	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
						形成审计记录送至安全管理中心。
T6	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	安全通用要求	安全区域边界	入侵防范	应在关键网络节点处监视网络攻击行为。
T7	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	安全通用要求	安全区域边界	恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。
T8	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	办公网区域 外网边界区域 安全管理区域 服务器存储区域	安全通用要求	安全区域边界	可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T9	（1）设备不具备相关可信验证的技术措施。	WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2	安全通用要求	安全计算环境	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T10	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。	业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	安全通用要求	安全计算环境	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
						中心。
T11	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况； （3）现有的计算设备存在对系统运行过程中的可信检验不全面的情况； （4）现有的可信验证存在部分告警、审计及联动措施不全面的情况。	应用服务器 数据库服务器	安全通用要求	安全计算环境	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
T12	（1）未能提供中间件重要数据的异地定时数据备份功能。	应用服务器-Weblogic	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T13	（1）未能提供数据库系统重要数据的异地定时数据备份功能。	数据库服务器-Oracle	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T14	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	智慧校园系统	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T15	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	重要业务数据 重要个人信息	安全通用要求	安全计算环境	数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
T16	（1）系统管理的资源、运行及配置管理不够全面。	管理中心	安全通用要求	安全管理中心	系统管理	b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
T17	（1）单位开展的检查工作不够完善。	制度文件、执行/记录文件	安全通用要求	安全管理机构	审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T18	（1）单位未完全按管理规范开展人员离场后的清理工作。	制度文件、执行/记录文件	安全通用要求	安全管理人员	外部人员访问管理	c）外部人员离场后应及时清除其所有的访问权限。
T19	（1）单位未具备适用于被测系统的安全规划设计方案。	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
T20	（1）单位未具备完整的安全设计方案相关的文档； （2）单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	b）应根据保护对象的安全保护等级进行安全方案设计；
T21	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； （2）单位未对相关论证过程及内容进行完整的记录。	制度文件、执行/记录文件	安全通用要求	安全建设管理	安全方案设计	c）应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。
T22	（1）单位未在软件开发过程中对所有软件安全性进行测试； （2）单位未在软件安装之前按要求对所有软件开展恶意代码检测。	制度文件、执行/记录文件	安全通用要求	安全建设管理	外包软件开发	a）应在软件交付前检测其中可能存在的恶意代码；
T23	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	安全通用要求	安全建设管理	测试验收	a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；
T24	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	安全通用要求	安全建设管理	测试验收	b）应进行上线前的安全性测试，并出具安全测试报告。
T25	（1）单位未严格按规范开展漏洞及安全隐患检测工作。	制度文件、执行/记录文件	安全通用要求	安全运维管理	漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。
T26	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	安全通用要求	安全运维管理	恶意代码防范管理	c）应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。
T27	（1）单位不了解现有密码相关的国家标准和行业标	制度文件、执行/记录文件	安全通用要求	安全运维管理	密码管理	a）应遵循密码相关国家标准和行业标准；

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
	准； （2）单位缺乏密码管理要求的制度文档。					

4 整体测评

从安全控制间、区域间和验证测试等方面对单元测评的结果进行验证、分析和整体评价。

具体内容参见《GB/T 28448-2019信息安全技术 网络安全等级保护测评要求》。

4.1 安全控制点间安全测评

安全控制间的安全测评主要考虑同一区域内、同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用。安全功能上的增强和补充可以使两个不同强度、不同等级的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。

4.1.1 安全建设管理

4.1.1.1 安全通用要求

（T23）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。

单位未具备适用于被测系统的安全规划设计方案。安全方案设计不完善，导致规划设计需求不全面，信息系统存在安全缺陷。可升高单位未完全根据测试验收方案组织相关部门和人员开展验收工作的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

（T24）针对系统上线前的安全性测试工作存在问题。

单位未在软件交付之前按要求对所有软件开展恶意代码检测，导致在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。可升高针对系统上线前的安全性测试工作存在问题的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

4.1.2 安全运维管理

4.1.2.1 安全通用要求

（T26）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。

单位未严格按规范开展漏洞及安全隐患检测工作，漏洞检测工作不到位，导致存在未授权人员利用漏洞攻击信息系统的风险。可升高单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作的问题严重程度（如制度文件、执行/记录文件）。根据整体测评分析，问题严重程度变化为升高。

4.2 区域间安全测评

区域间的安全测评主要考虑互连互通（包括物理上和逻辑上的互连互通等）的不同区域之间存在的安全功能增强、补充和削弱等关联作用，特别是有数据交换的两个不同区域。

4.2.1 安全物理环境

4.2.1.1 安全通用要求

（T1）机房出入口未配置电子门禁系统。

机房所在位置处于内部受控区域，非授权人员无法随意通过现有控制措施（如机械锁）进出机房，且具备相对完善的机房出入管理要求（具备《机房安全管理制度》），并实际执行措施效果良好（具备《机房出入登记表》），可降低机房出入口访问控制措

施缺失的问题严重程度（如信息化机房）。根据整体测评分析，问题严重程度变化为降低。

4.2.2 安全通信网络

4.2.2.1 安全通用要求

（T4）关键的应用服务和数据库服务网段未独立进行子网划分的情况。

单位有完整的IP地址规范，对IP地址的使用、回收均有记录《资产清单》，且系统具备相对完善的设备自身访问控制策略管理要求（具备《网络安全管理规范》、《设备及系统软件配置和操作手册》），措施效果良好，有助于部分补充未划分子网的安全功能不足（如安全通信网络）。根据整体测评分析，问题严重程度变化为降低。

4.2.3 安全区域边界

4.2.3.1 安全通用要求

（T6）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。

网络环境划分了相应的安全区域，区域间具备有效的访问控制措施，区域内各主机设备部署深信服EDR单机版，策略库、规则库更新及时，能够对攻击行为进行检测、阻断或限制，实际措施效果良好，且系统具备相对完善的策略库、规则库更新/校准管理要求，管理措施效果良好且及时检查更新有效性（具备《漏洞检测报告》、《主机安全管理规范》），可降低外部网络攻击防御措施缺失的问题严重程度（如办公网区域、安全管理区域）。根据整体测评分析，问题严重程度变化为降低。

（T7）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。

系统部署于可控的网络环境内（具备有效的访问控制、入侵防护措施）限制相关主机对象访问非受控网络，操作系统层面配置防御策略（具备本地防火墙策略、核心交换

机地址限制策略、部署深信服EDR单机版），恶意代码入侵的可能性相对较低，可降低恶意代码防范措施缺失的问题严重程度（如办公网区域、安全管理区域）。根据整体测评分析，问题严重程度变化为降低。

4.3 整体测评结果汇总

经整体测评后安全问题严重程度变化情况如下表所示

表 4-1 整体测评结果汇总表

问题编号	安全问题描述	测评对象	整体测评描述	严重程度变化
T1	（1）机房出入口未配置电子门禁系统。	信息化机房	（1）机房所在位置处于内部受控区域，非授权人员无法随意通过现有控制措施（如机械锁）进出机房，且具备相对完善的机房出入管理要求（具备《机房安全管理制度》），并实际执行措施效果良好（具备《机房出入登记表》），可降低机房出入口访问控制措施缺失的问题严重程度。	□升高 ☑降低
T4	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	（1）单位有完整的IP地址规范，对IP地址的使用、回收均有记录《资产清单》，且系统具备相对完善的设备自身访问控制策略管理要求（具备《网络安全管理规范》、《设备及系统软件配置和操作手册》），措施效果良好，有助于部分补充未划分子网的安全功能不足。	□升高 ☑降低
T6	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	（1）网络环境划分了相应的安全区域，区域间具备有效的访问控制措施，区域内各主机设备部署深信服EDR单机版，策略库、规则库更新及时，能够对攻击行为进行检测、阻断或限制，实际措施效果良好，且系统具备相对完善的策略库、规则库更新/校准管理要求，管理措施效果良好且及时检查更新有效性（具备《漏洞检测报告》、《主机安全管理规范》），可降低外部网络攻击防御措施缺失的问题严重程	□升高 ☑降低

问题编号	安全问题描述	测评对象	整体测评描述	严重程度变化
			度。	
T7	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域安全管理区域	（1）系统部署于可控的网络环境内（具备有效的访问控制、入侵防护措施）限制相关主机对象访问非受控网络，操作系统层面配置防御策略（具备本地防火墙策略、核心交换机地址限制策略、部署深信服EDR单机版），恶意代码入侵的可能性相对较低，可降低恶意代码防范措施缺失的问题严重程度。	□升高 ☑降低
T23	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	（1）单位未具备适用于被测系统的安全规划设计方案。安全方案设计不完善，导致规划设计需求不全面，信息系统存在安全缺陷。可升高单位未完全根据测试验收方案组织相关部门和人员开展验收工作的问题严重程度。	☑升高 □降低
T24	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	（1）单位未在软件交付之前按要求对所有软件开展恶意代码检测，导致在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。可升高针对系统上线前的安全性测试工作存在问题的问题严重程度。	☑升高 □降低
T26	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	（1）单位未严格按规范开展漏洞及安全隐患检测工作，漏洞检测工作不到位，导致存在未授权人员利用漏洞攻击信息系统的风险。可升高单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作的问题严重程度。	☑升高 □降低

5 安全问题风险分析

针对等级测评结果中存在的所有安全问题，结合关联资产和威胁分别分析安全问题可能产生的危害结果，找出可能对系统、单位、社会及国家造成的最大安全危害（损失），并根据最大安全危害（损失）的严重程度进一步确定安全问题的风险等级，结果为“高”、

“中”或“低”。最大安全危害（损失）结果应结合安全问题所影响业务的重要程度、相关系统组件的重要程度、安全问题严重程度以及安全事件影响范围等进行综合分析。

表 5-1 安全问题风险分析

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
1	安全物理环境	（1）机房出入口未配置电子门禁系统。	信息化机房	物理攻击	（1）上述问题的存在，使未授权用户可以更为容易的访问机房等敏感物理区域，可能对系统的平稳运行造成影响。	中风险
2	安全物理环境	（1）机房建设未完全采用符合耐火等级的建筑材料； （2）机房建设不具备防火设计/验收文档，或机房验收文档未明确相关建筑材料的耐火等级。	信息化机房	物理环境影响	（1）存在发生火情时助燃火灾的风险。	低风险
3	安全物理环境	（1）机房内缺乏防静电措施（如防静电地板或铺设防静电地毯 ）。	信息化机房	软硬件故障	（1）存在因静电过大，或静电积累而得不到释放造成设备损坏的风险。	中风险
4	安全通信网络	（1）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	恶意攻击	（1）上述问题的存在，使广播风暴、恶意代码的传播、网络攻击的开展都变得更为容易，且使管理者为不同业务区域部署相应的安全策略变得更为艰难，不利于对信息系统的安全运维，最终会对信息系统的稳定运行造成影响。	中风险
5	安全通信网络	（1）缺乏对通信设备可信验证方面的安全设计要求； （2）现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况。	安全通信网络	恶意攻击	（1）缺乏对系统可执行程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致计算资源被干扰和破坏造成损失。	低风险
6	安全区域边界	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范	办公网区域 安全管理区域	恶意攻击	（1）存在不能及时发现内部主机作为攻击跳板，或网络攻击行为而造成系统	中风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
		功能策略，无法检测、防止或限制从内部发起的网络攻击行为。			损坏/网络资源浪费的风险。	
7	安全区域边界	（1）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	恶意攻击	（1）无法有效对潜在的/新出现的恶意代码进行检测防护，可能会造成恶意代码流入系统造成破坏的风险。	中风险
8	安全区域边界	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	办公网区域 外网边界区域 安全管理区域 服务器存储区域	恶意攻击	（1）缺乏对边界设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险
9	安全计算环境	（1）设备不具备相关可信验证的技术措施。	WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2	恶意攻击	（1）缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险
10	安全计算环境	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。	业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	恶意攻击	（1）缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险
11	安全计算环境	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况； （3）现有的计算设备存在对系统运行过程中的可信检验不全面的情况；	应用服务器 数据库服务器	恶意攻击	（1）缺乏对计算设备的相关程序的可信性验证，无法保证系统始终运行于可信环境中，运行不可信程序将导致边界防护措施被干扰和破坏造成风险。	低风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
		（4）现有的可信验证存在部分告警、审计及联动措施不全面的情况。				
12	安全计算环境	（1）未能提供中间件重要数据的异地定时数据备份功能。	应用服务器-Weblogic	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。	中风险
13	安全计算环境	（1）未能提供数据库系统重要数据的异地定时数据备份功能。	数据库服务器-Oracle	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供，使企业的经济利益或声誉受到损害。	中风险
14	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	智慧校园系统	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。	中风险
15	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	重要业务数据 重要个人信息	软硬件故障	（1）异地备份策略不完善/执行不到位，在发生地震或其他灾祸的极端情况下，会影响到业务服务的持续提供。	中风险
16	安全管理中心	（1）系统管理的资源、运行及配置管理不够全面。	管理中心	恶意攻击	（1）系统的资源和运行缺少统一的管理，将导致系统可能无法按规划实现基于资源配置、 系统加载、异常处理、及备份/恢复等的安全控制措施。	低风险
17	安全管理机构	（1）单位开展的检查工作不够完善。	制度文件、执行/记录文件	管理不到位	（1）检查工作开展不仔细，可能对存在或潜在的安全风险不能被及时发现并进行处理。	低风险
18	安全管理人员	（1）单位未完全按管理规范开展人员离场后的清理工作。	制度文件、执行/记录文件	管理不到位	（1）人员离场后的清理工作开展不规范，可能导致遗留外部人员访问受控区域的记录，存在被二次非法利用，造成泄密。	低风险
19	安全建设管理	（1）单位未具备适用于被测系统的安全规划设	制度文件、执行/记录文件	管理不到	（1）规划设计需求不全面，可能导致安全方案设	低风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
		计方案。		位	计不完善，信息系统存在安全缺陷。	
20	安全建设管理	（1）单位未具备完整的安全设计方案相关的文档； （2）单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	管理不到位	（1）相关合规的规划配套文件缺失，可能导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。	中风险
21	安全建设管理	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； （2）单位未对相关论证过程及内容进行完整的记录。	制度文件、执行/记录文件	管理不到位	（1）未开展规范的审批过程，可能存在安全整体规划缺乏合理性和可行性，导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。	低风险
22	安全建设管理	（1）单位未在软件开发过程中对所有软件安全性进行测试； （2）单位未在软件安装之前按要求对所有软件开展恶意代码检测。	制度文件、执行/记录文件	管理不到位	（1）软件交付前恶意代码检测不规范，可能在上线前无法发现软件BUG和恶意代码，对组织的信息系统及声誉造成风险。	低风险
23	安全建设管理	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	管理不到位	（1）可能由于验收测试不严谨，造成测试过程缺乏计划性及操作性，无法保证经过测试验收的系统达到既定的安全性等目标。	低风险
24	安全建设管理	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	管理不到位	（1）未按规定开展上线前测试，安全隐患可能在系统上线运行前未被发现并作出相应处理。	低风险
25	安全运维管理	（1）单位未严格按规范开展漏洞及安全隐患检测工作。	制度文件、执行/记录文件	管理不到位	（1）漏洞检测、修补工作不到位，可能存在未授权人员利用漏洞攻击信息系统的风险。	低风险
26	安全运维管理	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	管理不到位	（1）可能导致系统恶意代码检测管理不到位，存在信息系统感染恶意代码，从而导致严重的信息安全风险。	低风险
27	安全运维管理	（1）单位不了解现有密码相关的国家标准和行业标准；	制度文件、执行/记录文件	管理不到位	（1）密码管理不足，导致信息系统所使用的密码、密钥及密码设备等管理不	中风险

序号	安全类	安全问题	关联资产	关联威胁	危害分析结果	风险等级
		（2）单位缺乏密码管理要求的制度文档。			到位，存在违反国家政策的风险。	

6 等级测评结论

等级测评结论由安全问题风险分析结果和综合得分共同确定,判定依据如下表所示。

表 6-1 等级测评结论判别依据

测评结论	判别依据
优	被测对象中存在安全问题，但不会导致被测对象面临中、高等级安全风险，且系统综合得分 90 分以上（含90 分）。
良	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分 80分以上（含 80分）。
中	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分 70分以上（含 70分）
差	被测对象中存在安全问题，而且会导致被测对象面临高等级安全风险，或被测对象综合得分低于 70 分。

综合得分计算方法如下:

设M为被测对象的综合得分，$M = V_t + V_m$，V_t和V_m根据下列公式计算。

$$V_t = \begin{cases} 100 \cdot y - \sum_{k=1}^{t} f(\omega_k) \cdot (1 - x_k) \cdot S, & V_t > 0 \\ 0, & V_t \le 0 \end{cases}$$

$$V_m = \begin{cases} 100 \cdot (1 - y) - \sum_{k=1}^{m} f(\omega_k) \cdot (1 - x_k) \cdot S, & V_m > 0 \\ 0, & V_m \le 0 \end{cases}$$

$$0 \le x_k \le 1,\ S = 100 \cdot \frac{1}{n},\ f(\omega_k) = \begin{cases} 1, & \omega_k = \text{一般} \\ 2, & \omega_k = \text{重要} \\ 3, & \omega_k = \text{关键} \end{cases}$$

其中，y为关注系数，取值在0至1之间，由等级保护工作管理部门给出，默认值为0.5。n为被测对象涉及的总测评项数（不含不适用项，下同），t为技术方面对应的总测评项数，V_t为技术方面的得分，m为管理方面对应的总测评项数，V_m为管理方面的得分，ω_k为测评项k的重要程度（分为一般、重要和关键），x_k为测评项k的得分，如果测评项k涉及多测评项对象，则x_k取值为多测评对象得分的算术平均值。

x_k的得分计算如下：

测评项k涉及对象 / 测评项k定性判定	只涉及单个对象	涉及多个对象
符合	1	1
部分符合	0.5	计算测评对象平均分，取值在0至1之间
不符合	0	0

注：当测评项k涉及多个对象时，针对每个对象的得分取值为1、0.5和0。

根据第5章安全问题风险分析结果统计高、中、低风险安全问题的数量，利用综合得分计算公式计算出被测对象的综合得分，并将相关结果填入下表。

表 6-2 安全问题统计和综合得分

被测对象名称	安全问题数量			综合得分
	高风险	中风险	低风险	
智慧校园系统	0	11	16	73.85

依据 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》和GB/T 28448—2019《信息安全技术 网络安全等级保护测评要求》的第二级要求，经对智慧校园系统的安全保护状况进行综合分析评价，等级测评结论如下：

智慧校园系统本次等级测评的综合得分为73.85，且不存在高等级安全风险，等级测评结论为中。

7 安全问题整改建议

表 7-1 安全问题整改建议

序号	安全类	安全问题	关联资产	整改建议
1	安全物理环境	(1)机房出入口未配置电子门禁系统。	信息化机房	(1) 采用电子门禁系统严格控制机房其他出入口的进出，或安排专人值守； (2) 采用电子门禁系统，对机房所有人员出入进行登记记录，并保存。
2	安全物理环境	(1)机房建设未完全采用符合耐火等级的建筑材料； (2)机房建设不具备防火设计/验收文档,或机房验收文档未明确相关建筑材料的耐火等级。	信息化机房	(1) 机房及相关的工作房间和辅助房采用具有耐火等级的建筑材料； (2) 机房建设采用符合相关耐火等级（二级）的建筑材料。（内外墙壁均应采用具有防火涂料、隔热板、铝板、钢板等阻燃或不燃的材料）； (3) 机房耐火等级建筑材料有相关合格证，并留存机房验收文档。
3	安全物理环境	(1)机房内缺乏防静电措施（如防静电地板或铺设防静电地毯）。	信息化机房	(1) 机房铺设防静电地板或铺设防静电地毯； (2) 机房房静电设计可依据GB50174-2008和GB50314-2006相关规定进行机房设计和验收。
4	安全通信网络	(1)关键的应用服务和数据库服务网段未独立进行子网划分的情况。	安全通信网络	(1) 建议独立划分出应用服务器网段、数据库服务器网段。
5	安全通信网络	(1)缺乏对通信设备可信验证方面的安全设计要求； (2)现有的通信设备存在对系统运行过程中的可信检验完全缺失的情况。	安全通信网络	(1) 建议在管理规范文档内对通信设备可信验证方面的安全设计提出要求； (2) 建议系统实现对所有可执行环节进行可信验证，包括： 运行过程中的可信检验： ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■通信应用连接过程。
6	安全区域边界	(1) 网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	办公网区域 安全管理区域	(1) 建议网络层部署的防火墙配置对内部发起的攻击行为实现防范功能策略，实现检测、防止或限制从内部发起的网络攻击行为； (2) 内部安全防范措施能检测以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、碎片攻击、网络蠕虫攻击、应用漏

序号	安全类	安全问题	关联资产	整改建议
				洞攻击。
7	安全区域边界	(1)现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	办公网区域 安全管理区域	(1) 建议现有部署的恶意代码防范措施网络边界覆盖全面，及时对恶意代码及逆行检测和清除。
8	安全区域边界	(1)缺乏对边界设备可信验证方面的安全设计要求； (2)现有的边界设备存在对系统运行过程中的可信检验完全缺失的情况。	办公网区域 外网边界区域 安全管理区域 服务器存储区域	(1) 建议对边界设备系统程序的可信验证设计并保存设计文件； (2) 建议系统实现对所有可执行环节进行可信验证。
9	安全计算环境	(1)设备不具备相关可信验证的技术措施。	WEB应用防火墙 上网行为管理系统 基线核查系统 日志审计系统 核心交换机 汇聚交换机 运维安全管理系统 防火墙-1 防火墙-2	(1) 建议通过设备的启动过程和运行过程中对预装软件（包括系统引导程序、系统程序、相关应用程序和重要配置参数）的完整性验证或检测，确保对系统引导程序、系统程序、重要配置参数和关键应用程序可信根验证； (2) 建议设备启用在检测到其可信性受到破坏后进行报警的相关功能。
10	安全计算环境	(1)缺乏对计算设备可信验证方面的安全设计要求； (2)现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况。	业务终端-1 业务终端-2 运维及管理终端-1 运维及管理终端-2	(1) 建议对计算设备系统程序的可信验证设计并保存设计文件； (2) 建议系统实现对所有可执行环节进行可信验证。
11	安全计算环境	(1)缺乏对计算设备可信验证方面的安全设计要求； (2)现有的计算设备存在对系统运行过程中的可信检验完全缺失的情况； (3)现有的计算设备存在对系统运行过程中的可信检验不全面的情况； (4)现有的可信验证存在部分告警、审计及联动措施不全面的情况。	应用服务器 数据库服务器	(1) 建议对计算设备系统程序的可信验证设计并保存设计文件； (2) 建议系统实现对所有可执行环节进行可信验证。
12	安全计算环境	(1)未能提供中间件重要数据的异地定时数据备份功能。	应用服务器-Weblogic	(1) 建议设置异地灾备机房，并利用通信网络将中间件重要数据定时备份至备份场地；

序号	安全类	安全问题	关联资产	整改建议
				（2）异地备份的中间件数据范围（不限于）包括系统的： ■重要配置数据。
13	安全计算环境	（1）未能提供数据库系统重要数据的异地定时数据备份功能。	数据库服务器-Oracle	（1）建议设置异地灾备机房，并利用通信网络将重要数据定时备份至备份场地； （2）异地备份的数据范围（不限于）包括系统的： ■配置数据 ■重要业务数据。
14	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	智慧校园系统	（1）建议设置异地灾备机房，并利用通信网络将应用软件系统重要数据定时备份至备份场地； （2）异地备份的应用软件系统数据范围（不限于）包括系统的：配置数据、重要日志数据，业务数据。
15	安全计算环境	（1）未能提供应用软件系统重要数据的异地定时数据备份功能。	重要业务数据 重要个人信息	（1）建议设置异地灾备机房，并利用通信网络将应用软件系统重要数据定时备份至备份场地。
16	安全管理中心	（1）系统管理的资源、运行及配置管理不够全面。	管理中心	（1）需实现系统包括对可信证书管理、可信基准库的管理。
17	安全管理机构	（1）单位开展的检查工作不够完善。	制度文件、执行/记录文件	（1）建议单位按要求提供安全检查报告。
18	安全管理人员	（1）单位未完全按管理规范开展人员离场后的清理工作。	制度文件、执行/记录文件	（1）建议单位按管理规范开展人员离场后的清理工作。至少包括：保留清理记录、及时清除离场后的所有访问权限、记录访问权限清除时间。
19	安全建设管理	（1）单位未具备适用于被测系统的安全规划设计方案。	制度文件、执行/记录文件	（1）建议单位根据等保要求进行过全面的自查或对比，根据系统的安全级别选择基本安全措施； （2）建议规划方案需根据风险分析结果对系统安全措施进行补充和整，并在系统建设\\整改方案中有详细描述。
20	安全建设管理	（1）单位未具备完整的安全设计方案相关的文档； （2）单位相关方案的设计的内容不够完善。	制度文件、执行/记录文件	（1）建议单位根据信息系统的等级划分情况，准备安全设计方案、安全管理策略、安全建设规划文档等； （2）建议相关文档内容应完善，包括统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、密码技术要求、总体建设规划和详细设计方案，并形成一致性的配套文件。

序号	安全类	安全问题	关联资产	整改建议
21	安全建设管理	（1）单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； （2）单位未对相关论证过程及内容进行完整的记录。	制度文件、执行/记录文件	（1）建议单位组织相关部门和安全技术专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定； （2）保存论证和审定记录，记录包括批准时间、批准人员签字； （3）文件经过批准后，才能正式实施。
22	安全建设管理	（1）单位未在软件开发过程中对所有软件安全性进行测试； （2）单位未在软件安装之前按要求对所有软件开展恶意代码检测。	制度文件、执行/记录文件	（1）建议开发商提供软件源代码，软件安装前检测软件中的恶意代码； （2）输出检测报告（或提供第三方检测报告），内容包括测试时间、测试地点、测试对象、测试结论、测试人员。
23	安全建设管理	（1）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。	制度文件、执行/记录文件	（1）建议根据测试验收过程记录与结果，形成测试验收报告。
24	安全建设管理	（1）针对系统上线前的安全性测试工作存在问题。	制度文件、执行/记录文件	（1）建议系统建设完成后，委托第三方测试单位对系统进行安全性测试，并出具安全性测试报告； （2）测试报告内容至少包括测试时间、测试地点、测试人、测试对象、测试方法、测试过程、测试发现的安全问题、整改建议、测试结论，并有第三方测试机构的签字盖章。
25	安全运维管理	（1）单位未严格按规范开展漏洞及安全隐患检测工作。	制度文件、执行/记录文件	（1）建议单位定期开展漏洞扫描，对发现的安全漏洞和隐患进行及时修补评估； （2）对必需修补的安全漏洞和隐患进行加固测试，测试无误后，备份系统数据，再从生产环境进行修补； （3）对于剩余安全漏洞和隐患进行残余风险分析，明确安全风险整改原则。
26	安全运维管理	（1）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。	制度文件、执行/记录文件	（1）建议单位按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工作。包括;定期对相关产品的恶意代码库进行升级；对相关设备升级情况进行记录；对各类防病毒产品上截获的恶意代码进行分析并汇总上报； （2）单位需保留完整的恶意代码检测/升级的记录。至少具备：执行人、升级结果/检测结果、处理方式、负责人签字 。

序号	安全类	安全问题	关联资产	整改建议
27	安全运维管理	(1)单位不了解现有密码相关的国家标准和行业标准； (2)单位缺乏密码管理要求的制度文档。	制度文件、执行/记录文件	（1）建议单位学习现有密码相关的国家标准和行业标准。建立密码管理要求的制度文档。

漏洞安全问题整改建议

序号	安全类	安全问题	关联资产	整改建议
1	安全计算环境	SSH版本信息可被获取 此类漏洞涉及服务器存储设备。	10.1.8.10/ 数据库服务器 10.1.8.17/ 应用服务器	NSFOCUS建议您采取以下措施以降低威胁： * 修改源代码或者配置文件改变SSH服务的缺省banner。
2	安全计算环境	允许Traceroute探测 此类漏洞涉及网络设备、安全设备、服务器存储设备。	10.1.8.17/ 应用服务器 10.1.8.10/ 数据库服务器 10.2.1.4/运维安全管理系统 10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/ 上网行为管理系统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/ 汇聚交换机 172.16.1.2/核心交换机	在防火墙出站规则中禁用echo-reply（type 0）、time-exceeded（type 11）、destination-unreachable（type 3）类型的ICMP包。
3	安全计算环境	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161) 此类漏洞涉及网络设备。	172.16.1.2/核心交换机	临时解决方法：* 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://downloads.ssh.com/ 对于具体

序号	安全类	安全问题	关联资产	整改建议
				Linux发行版中使用的版本，可以参考如下链接,确认系统是否受该漏洞影响: Redhat ------- https://rhn.redhat.com/errata/RHSA-2009-1287.html Suse ------- http://support.novell.com/security/cve/CVE-2008-5161.html Ubuntu ------- http://people.canonical.com/~ubuntu-security/cve/2008/CVE-2008-5161.html
4	安全计算环境	缺少“Content-Security-Policy”响应头 此类漏洞涉及业务应用软件平台。	https://ehall.mmpt.edu.cn/ 智慧校园系统	在服务器中配置Content-Security-Policy响应头为“default-src 'self’”。

【正文结束】

附录A 被测对象资产

A.1 物理机房

附录A 表- 1物理机房

序号	机房名称	物理位置	重要程度
1	信息化机房	茂名市茂南区文明北路232号大院大楼	关键

A.2 网络设备

附录A 表- 2网络设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度	备注
1	核心交换机	否	H3C version 7.1.070, Release 7585P07	H3C S7500E-X	核心数据交换、访问控制	关键	
2	汇聚交换机	否	H3C version 7.1.070, Release 6126P20	H3C S5560X-30C-EI	数据交换	重要	

A.3 安全设备

附录A 表- 3安全设备

序号	设备名称	是否虚拟设备	系统及版本	品牌及型号	用途	重要程度	备注
1	WEB应用防火墙	否	深信服AF 8.0.9	深信服WAF-2000-H642	应用防护、入侵防范、病毒防护	重要	
2	日志审计系统	否	深信服LAS 3.0.5	深信服AC-1000-D601-PT	日志审计	重要	
3	防火墙-2	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键	
4	防火墙-1	否	深信服AF 8.0.23	深信服AF-2000-H642	访问控制、入侵防范、病毒防护	关键	
5	基线核查系统	否	深信服V3.0.3	深信服AC-1000-D602-PT	漏洞扫描	重要	
6	运维安全管理系统	否	深信服V3.0.6	深信服AC-1000-D603-PT	运维审计	重要	
7	上网行为管理系统	否	深信服AC12.0.26	深信服AC-1000-D600-PT	上网行为管理及终端准入控制	重要	

A.4 服务器

附录A 表-4服务器

序号	设备名称	所属业务应用系统/平台名称	是否虚拟设备	操作系统及版本	数据库管理系统及版本	中间件及版本	重要程度	备注
1	应用服务器	智慧校园系统	否	CentOS 7.7	/	Weblogic 11g	关键	
2	数据库服务器	智慧校园系统	否	CentOS 7.7	Oracle 11.2.0.1.0	/	关键	

A.5 终端设备

附录A 表-5终端设备

序号	设备名称	是否虚拟设备	操作系统/控制软件及版本	用途	重要程度	备注
1	运维及管理终端-1	否	Windows 10（版本20H2（内部版本19044.1889）	运维管理、系统管理	一般	
2	业务终端-2	否	Windows 10（版本20H2（内部版本19044.1889）	业务管理	一般	
3	运维及管理终端-2	否	Windows 10（版本21H2（内部版本19044.1889））	运维管理、系统管理	一般	
4	业务终端-1	否	Windows 10（版本20H2（内部版本19044.1889）	业务管理	一般	

A.6 其他系统或设备

附录A 表-6其他系统或设备

序号	设备名称	是否虚拟设备	操作系统/控制软件及版本	用途	重要程度	备注
/	/	/	/	/	/	/

注释：本次测评对象中不涉及专用移动互联终端等，不开展抽测。

A.7 系统管理软件/平台

附录A 表-7系统管理软件/平台

序号	系统管理软件/平台名称	所在设备名称	版本	主要功能	重要程度	备注

序号	系统管理软件/平台名称	所在设备名称	版本	主要功能	重要程度	备注
1	数据库服务器-Oracle	应用/数据库服务器	11.2.0.1.0	数据生产、存储	关键	
2	应用服务器-Weblogic	应用/数据库服务器	11C	页面发布	关键	

A.8 业务应用软件/平台

附录A 表- 8业务应用系统/平台

序号	业务应用系统/平台名称	主要功能	业务应用软件及版本	开发厂商	重要程度
1	智慧校园系统	茂名职业技术学院智慧校园系统包括校园移动应用、统一身份认证、服务能力开放、主数据管理、网上办事大厅等基础支撑模块，形成一体化的信息化整体架构，解决信息系统分别建立带来的数据孤岛和流程割裂问题，打通各部门的信息壁垒，为业务整合和流程整合提供技术支持。建立全校性的主数据平台，涵盖学院信息标准与数据规范的定义，共享数据目录的管理，数据的采集、共享和交换等。	V6.0	江苏金智教育信息股份有限公司	关键

A.9 数据资源

附录A 表- 9数据资源

序号	数据类别	所属业务应用	安全防护需求	重要程度
1	重要个人信息	智慧校园系统	完整性、保密性	关键
2	重要业务数据	智慧校园系统	完整性、保密性	关键
3	鉴别数据	智慧校园系统(网络设备、安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)	完整性、保密性	关键
4	重要审计数据	智慧校园系统（安全管理中心)	完整性	重要
5	重要配置数据	智慧校园系统(网络设备、	完整性	关键

序号	数据类别	所属业务应用	安全防护需求	重要程度
		安全设备、服务器存储设备、终端设备、系统管理软件平台、业务应用软件/平台)		

注释：网络设备、安全设备、服务器、终端、系统管理软件/平台和业务应用系统等所涉及的鉴别数据和重要配置数据分别在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。重要审计数据在安全管理中心进行汇总测评证据，包括数据完整性。重要业务数据和重要个人信息分别在各自测评对象中汇总测评证据后集中体现，包括数据完整性、数据保密性和备份恢复。

A.10 密码产品

附录A 表- 10密码产品

序号	产品/模块名称	生成厂商	商密型号	密码算法	用途	重要程度
/	/	/	/	/	/	/

注释：本次测评不存在加密机等密码产品。

A.11 安全相关人员

附录A 表- 11安全相关人员

序号	姓名	岗位/角色	联系方式	所属单位
1	吴国华	机房管理员	0668-2920122	茂名职业技术学院
2	叶永利	安全管理员	0668-2920122	茂名职业技术学院
3	杨云	审计管理员	0668-2920122	茂名职业技术学院
4	龙恒	应用管理员	13377766618	茂名职业技术学院
5	龙恒	网络管理员	13377766618	茂名职业技术学院
6	吴国华	系统管理员	0668-2920122	茂名职业技术学院
7	杨云	资产管理员	0668-2920122	茂名职业技术学院
8	龙恒	数据管理员	13377766618	茂名职业技术学院

A.12 安全管理文档

附录A 表- 12安全管理文档

序号	文档名称	主要内容
1	制度类文档-员工考核管理制度	关于单位人员考核工作管理制度文档
2	制度类文档-岗位安排及岗位职责	关于单位岗位职责、岗位安排制度文档
3	制度类文档-工程测试验收管理	关于单位工程测试工作管理制度文档
4	制度类文档-外部服务人员管理规范	关于单位针对外部人员工作管理规范制度文档
5	制度类文档-机房安全管理制度	关于单位机房安全管理工作制度文档
6	制度类文档-数据安全管理规范	关于保障关键数据安全，从数据库本身、数据加密、数据备份恢复三个方面对数据安全进行规范的制度文档
7	制度类文档-系统及应用数据备份管理规范	关于单位数据备份、恢复管理制度文档
8	制度类文档-服务供应商选择安全管理制度	关于单位安全服务供应商管理规定制度文档
9	制度类文档-主机安全管理规范	关于规定单位主机系统安全管理要求规范，指导业务平台主机的安全配置和维护的制度文档
10	制度类文档-介质管理制度	关于单位介质安全管理工制度文档
11	制度类文档-安全事件报告和处置	关于单位网络安全事件管理、处置、流程等报告制度文档
12	制度类文档-备份与恢复管理制度	关于单位数据备份、恢复管理制度文档
13	制度类文档-系统安全管理制度	关于单位系统安全管理、安全服务管理制度文档
14	制度类文档-办公环境管理制度	关于单位办公环境管理制度文档
15	制度类文档-信息安全奖惩办法	关于单位人员奖惩制度文档
16	制度类文档-安全漏洞管理制度	关于单位安全漏洞管理工作制度文档
17	制度类文档-信息安全总体策略	关于单位网络安全方针、策略制度文档
18	制度类文档-办公环境保密管理	关于单位办公环境管理制度文档
19	制度类文档-设备安全管理制度	关于单位设备安全管理制度文档
20	制度类文档-网络安全管理制度	关于单位网络安全工作管理制度文档
21	制度类文档-信息安全漏洞扫描规范	关于单位安全漏洞工作规范制度文档

序号	文档名称	主要内容
22	制度类文档-安全教育和培训制度	关于单位安全培训、安全交流工作制度文档
23	制度类文档-网络与信息系统安全设计规范	关于单位网络与信息化安全设计制度文档
24	制度类文档-组织安全结构和人员职责制度	关于单位安全结构、人员职责
25	制度类文档-外部人员访问管理制度	关于单位针对外来人员访问管控制度文档
26	制度类文档-信息系统恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
27	制度类文档-恶意代码防范管理制度	关于单位恶意代码工作管理制度文档
28	制度类文档-物理安全管理规范	关于加强单位办公区域及电子计算机机房的管理和设备运行安全，规范办公区域及机房建设，使人员办公高效及机房设备安全、稳定运行的制度文档
29	制度类文档-网络安全事件报告制度	关于单位网络安全事件管理报告文档
30	制度类文档-离岗人员工作交接规范	关于单位离岗交接工作规范制度文档
31	制度类文档-制度制定、发布、评审和修订管理制度	关于单位制度制定、发布、评审和修订等管理文档
32	制度类文档-安全管理组织规范	关于单位组织结构管理规范制度文档
33	制度类文档-安全审查和检查管理规范	关于单位安全检查、审查工作规范制度文档
34	制度类文档-外部接入受控网络访问系统管理规范	关于单位针对外部人员工作接入规范制度文档
35	制度类文档-信息系统外包运维管理制度	关于单位外包运维工作管理制度文档
36	制度类文档-测试及验收方案	关于单位测试验收方案文档
37	制度类文档-应用系统业务用户密码设置规定	关于单位用户密码管理制度文档
38	制度类文档-外包开发软件管理规定	关于单位外包项目管理工作制度文档
39	制度类文档-人员管理制度	关于单位人员录用、调岗、离岗管理制度文档
40	制度类文档-应用安全管理规范	关于规定单位应用安全管理要求及规范的制度文档

序号	文档名称	主要内容
41	制度类文档-工程实施管理制度	关于单位工程实施工作管理制度文档
42	制度类文档-网络安全管理规范	关于保障单位网络系统的安全稳定运行，抵御内部和外部各种形式的网络攻击或威胁制定的管理文档
43	制度类文档-系统交付管理	关于单位交付工作管理制度文档
44	制度类文档-授权和审批管理规定	关于单位授权审批、审批流程规范制度文档
45	制度类文档-网络安全事件应急预案	关于单位网络安全事件应急处理、流程、培训等管理制度文档
46	制度类文档-恶意代码防范管理制度	关于单位恶意代码防范工作制度文档
47	制度类文档-变更控制管理制度	关于单位变更流程、控制管理制度文档
48	制度类文档-组织安全结构和人员职责制度	关于单位组织结构、人员安排、人员职责制度文档
49	操作类文档-设备及系统软件配置和操作手册	关于单位安全设备操作、Linux服务器配置手册、主机运维操作手册、软件操作手册、防火墙配置和操作手册、数据库日常运维操作手册等指导文档
50	操作类文档-数据备份策略	关于单位数据备份策略文件
51	操作类文档-软硬件日常维护管理规程	关于单位计算机网络系统使用、管理、信息安全、资源共享有所遵循,规范上网操作流程,提高网络系统安全性的指导文档
52	操作类文档-设备操作规程	关于单位相关设备操作指导文档
53	记录类文档-系统交付清单	关于单位交付工作记录
54	记录类文档-应急预案培训记录表	关于单位应急预案培训工作记录
55	记录类文档-软件交付清单	关于单位交付工作记录
56	记录类文档-通用变更记录表	关于单位变更工作记录
57	记录类文档-接入受控网络申请表	关于外来人员接入工作记录
58	记录类文档-人员培训及考核记录表	关于人员培训、考核等工作记录
59	记录类文档-漏洞检测报告	关于单位安全漏洞检测报告文档
60	记录类文档-关键岗位人员考核记录	关于关键岗位考核工作记录
61	记录类文档-重要操作审批表	关于单位审批工作记录

序号	文档名称	主要内容
62	记录类文档-信息安全检查记录表	关于单位安全检查工作记录
63	记录类文档-设备维修申请表	关于单位设备维护工作申请记录
64	记录类文档-人员入职考核记录	关于人员录用、考核工作记录
65	记录类文档-访问记录表	关于人员访问工作记录
66	记录类文档-数据恢复申请表	关于单位数据恢复工作申请表
67	记录类文档-外部人员访问申请表	关于外来人员访问申请流程工作记录
68	记录类文档-监理审批表	关于单位监理审核工作记录
69	记录类文档-离场信息资料交接表	关于人员离岗交接工作记录
70	记录类文档-信息安全会议记录	关于单位安全培训、安全交流会议记录
71	记录类文档-存储介质目录清单	关于备份介质存储工作清单
72	记录类文档-数据备份记录表	关于单位数据备份工作记录
73	记录类文档-外部会议文件和记录	关于单位外部联系、交流及会议工作记录
74	记录类文档-备份介质使用记录	关于备份介质使用登记工作记录
75	记录类文档-信息管理系统漏洞检查表	关于单位安全漏洞工作检测记录表
76	记录类文档-设备操作维护记录	关于单位设备维护工作记录
77	记录类文档-离职员工物品交回登记表	关于人员离岗工物交接工作记录
78	记录类文档-机房出入登记表	关于人员进出机房登记工作记录
79	记录类文档-安全管理制度评审记录	关于单位制度审计记录
80	记录类文档-专家论证记录表	关于单位网络方案论证记录
81	记录类文档-备份工作汇总表	关于单位数据备份工作总结表
82	记录类文档-安全建设方案评审纪录	关于单位网络与信息化安全设计方案评审工作记录
83	记录类文档-机房设备	关于单位机房设备维修工作记录

序号	文档名称	主要内容
	维修记录表	
84	记录类文档-机房设备维护记录表	关于设备维护登记工作记录
85	记录类文档-收发文登记记录	关于单位文档签发记录
86	记录类文档-网络信息安全事件记录表	关于单位网络安全事件工作记录
87	记录类文档-网络配置信息	关于单位配置信息登记工作记录
88	记录类文档-信息系统存储介质销毁申请表	关于备份介质销毁申请工作记录
89	记录类文档-机房维护日志	关于机房维护工作记录
90	记录类文档-设备出入登记记录表	关于设备进出机房登记工作记录
91	记录类文档-评审和修订记录	关于单位变更评审、修订工作记录
92	记录类文档-机房巡检记录表	关于单位机房环境巡检记录
93	记录类文档-信息系统存储介质使用清单	关于备份介质存储使用清单
94	记录类文档-外部人员访问记录表	关于外来人员访问登记工作记录
95	记录类文档-技能培训记录	关于单位系统培训工作、考核工作记录
96	记录类文档-人员离岗申请表	关于人员离岗申请记录
97	证据类文档-深信服安全采购合同	关于单位与安全厂家服务采购、产品选择合同文件
98	证据类文档-网络安全等级保护工作小组名单	关于单位网络安全等级保护工作小组人员名单文件
99	证据类文档-网络安全系统设计方案	关于单位网络与信息化安全设计方案文档
100	证据类文档-定级备案	关于单位系统定级报告、备案证文件
101	证据类文档-信息安全事件分析报告表	关于单位安全事件分析报告
102	证据类文档-安全职位人员	关于单位人员岗位安排名单
103	证据类文档-网络安全等级保护测评服务合同	关于单位与安全服务商签定的安全服务合同文件
104	证据类文档-资产清单	关于单位信息系统资产清单统计表

序号	文档名称	主要内容
105	证据类文档-外部联系表	关于单位内部联系及外部联系名单
106	证据类文档-工程项目实施方案	关于单位工程实施方案文档

附录B 上次测评问题整改情况说明

此次为智慧校园系统初次等级测评，之前未实施过等级保护测评工作。

附录B 表- 1上次测评问题整改情况

序号	主要安全问题	整改情况	情况说明
/	/	□已整改 □未整改	/

附录C 单项测评结果汇总

C.1 安全物理环境

附录 C 表-1 安全物理环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			物理位置选择	物理访问控制	防盗窃和防破坏	防雷击	防火	防水和防潮	防静电	温湿度控制	电力供应	电磁防护
1	信息化机房	符合	2	0	2	1	1	2	0	1	2	1
		部分符合	0	1	0	0	0	0	0	0	0	0
		不符合	0	0	0	0	1	0	1	0	0	0
		不适用	0	0	0	0	0	0	0	0	0	0

附录 C 表-2 安全物理环境单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.2 安全通信网络

附录 C 表-3 安全通信网络单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求		
			网络架构	通信传输	可信验证
1	安全通信网络	符合	1	1	0
		部分符合	1	0	0
		不符合	0	0	1
		不适用	0	0	0

附录 C 表-4 安全通信网络单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.3 安全区域边界

附录 C 表-5 安全区域边界单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求					
			边界防护	访问控制	入侵防范	恶意代码和垃圾邮件防范	安全审计	可信验证
1	外网边界区域	符合	1	4	1	1	3	0
		部分符合	0	0	0	0	0	0
		不符合	0	0	0	0	0	1
		不适用	0	0	0	0	0	0
2	安全管理区域	符合	1	4	0	0	3	0
		部分符合	0	0	0	1	0	0
		不符合	0	0	1	0	0	1
		不适用	0	0	0	0	0	0
3	服务器存储区域	符合	1	4	1	1	3	0
		部分符合	0	0	0	0	0	0
		不符合	0	0	0	0	0	1
		不适用	0	0	0	0	0	0
4	办公网区域	符合	1	4	0	0	3	0
		部分符合	0	0	0	1	0	0
		不符合	0	0	1	0	0	1
		不适用	0	0	0	0	0	0

附录 C 表-6 安全区域边界单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.4 安全计算环境

C.4.1 网络设备

附录 C 表-7 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	汇聚交换机	符合	3	4	3	4	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	1	0	0	1	1	--
2	核心交换机	符合	3	4	3	4	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	1	0	0	1	1	--

C.4.2 安全设备

附录 C 表-8 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	基线核查系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
2	上网行为管理系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
3	WEB应用防火墙	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
4	防火墙-1	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
5	防火墙-2	符合	3	4	3	5	1	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	0	0	0	1	1	--
6	日志	符合	3	4	3	5	0	0	1	1	0	--

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
	审计系统	部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--
7	运维安全管理系统	符合	3	4	3	5	0	0	1	1	0	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	0	1	0	0	1	1	--

C.4.3 服务器和终端

附录 C 表-9 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	应用服务器	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
2	数据库服务器	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
3	业务终端-2	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
4	业务终端-1	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--
5	运维及管理终端-2	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
		不适用	0	0	0	1	0	0	0	1	0	--
6	运维及管理终端-1	符合	3	4	3	4	1	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	1	0	0	0	--
		不适用	0	0	0	1	0	0	0	1	0	--

C.4.4 系统管理软件/平台

附录 C 表-10 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	应用服务器-Weblogic	符合	3	4	3	2	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	0	0	0	3	1	1	0	0	0	--
2	数据库服务器-Oracle	符合	3	4	3	2	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	0	0	0	3	1	1	0	0	0	--

C.4.5 业务应用系统/平台

附录 C 表-11 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	智慧校园系统	符合	3	4	3	3	0	0	1	1	1	--
		部分符合	0	0	0	0	0	0	0	0	0	--
		不符合	0	0	0	0	0	0	0	1	0	--
		不适用	0	0	0	2	1	1	0	0	0	--

C.4.6 数据资源

附录 C 表-12 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	重要个人信息	符合	--	--	--	--	--	--	1	1	0	2
		部分符合	--	--	--	--	--	--	0	0	0	0
		不符合	--	--	--	--	--	--	0	1	0	0
		不适用	--	--	--	--	--	--	0	0	1	0
2	重要业务数据	符合	--	--	--	--	--	--	1	1	0	0
		部分符合	--	--	--	--	--	--	0	0	0	0
		不符合	--	--	--	--	--	--	0	1	0	0
		不适用	--	--	--	--	--	--	0	0	1	2

C.4.7 其他系统或设备

附录 C 表-13 安全计算环境单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	可信验证	数据完整性	数据备份恢复	剩余信息保护	个人信息保护
1	--	符合	--	--	--	--	--	--	--	--	--	--
		部分符合	--	--	--	--	--	--	--	--	--	--
		不符合	--	--	--	--	--	--	--	--	--	--
		不适用	--	--	--	--	--	--	--	--	--	--

C.5 安全管理中心

附录 C 表-14 安全管理中心单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求	
			系统管理	审计管理
1	管理中心	符合	1	2
		部分符合	0	0
		不符合	1	0
		不适用	0	0

附录 C 表-15 安全管理中心单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.6 安全管理制度

附录 C 表-16 安全管理制度单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求			
			安全策略	管理制度	制定和发布	评审和修订
1	制度文件、执行/记录文件	符合	1	2	2	1
		部分符合	0	0	0	0
		不符合	0	0	0	0
		不适用	0	0	0	0

C.7 安全管理机构

附录 C 表-17 安全管理机构单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求				
			岗位设置	人员配备	授权和审批	沟通和合作	审核和检查
1	制度文件、执行/记录文件	符合	2	1	2	3	0
		部分符合	0	0	0	0	1
		不符合	0	0	0	0	0
		不适用	0	0	0	0	0

C.8 安全管理人员

附录 C 表-18 安全管理人员单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求			
			人员录用	人员离岗	安全意识教育和培训	外部人员访问管理
1	制度文件、执行/记录文件	符合	2	1	1	2
		部分符合	0	0	0	0
		不符合	0	0	0	1
		不适用	0	0	0	0

C.9 安全建设管理

附录 C 表-19 安全建设管理单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求									
			定级和备案	安全方案设计	产品采购和使用	自行软件开发	外包软件开发	工程实施	测试验收	系统交付	等级测评	服务供应商选择
1	制度文件、执行/记录文件	符合	4	0	2	0	1	2	0	3	3	2
		部分符合	0	0	0	0	0	0	1	0	0	0
		不符合	0	3	0	0	1	0	1	0	0	0
		不适用	0	0	0	2	0	0	0	0	0	0

附录 C 表-20 安全建设管理单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.10 安全运维管理

附录 C 表-21 安全运维管理单项测评结果汇总表（安全通用要求部分）

序号	测评对象	符合情况	安全通用要求													
			环境管理	资产管理	介质管理	设备维护管理	漏洞和风险管理	网络和系统安全管理	恶意代码防范管理	配置管理	密码管理	变更管理	备份与恢复管理	安全事件处置	应急预案管理	外包运维管理
1	制度文件、执行/记录文件	符合	3	1	2	2	0	5	2	1	0	1	3	3	2	0
		部分符合	0	0	0	0	0	0	1	0	0	0	0	0	0	0
		不符合	0	0	0	0	1	0	0	0	1	0	0	0	0	0
		不适用	0	0	0	0	0	0	0	0	1	0	0	0	0	2

附录 C 表-22 安全运维管理单项测评结果汇总表（安全扩展要求部分）

序号	测评对象	符合情况
本报告不涉及		

C.11 其他安全要求指标

附录 C 表-23 其他指标单项测评结果汇总表

序号	测评对象	符合情况
本报告不涉及		

附录D 单项测评结果记录

D.1 安全物理环境

D.1.1 安全通用要求

D.1.1.1 信息化机房

安全控制点	测评指标	结果结论	符合程度
物理位置选择	a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；	（1）机房和办公场地场所在建筑物具有建筑验收文档，包含对防震、防风和防雨能力的说明； ■机房建设地址为：茂名市茂南区文明北路232号大院大楼 （2）机房和办公场地未出严重的问题。 ■无雨水渗透痕迹 ■无因风导致的较严重尘土 ■无屋顶、墙体、地面等破损开裂	符合
	b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	（1）机房未部署在易发生问题的位置； （2）机房对于空调设备的排水管等部位采取密封防漏处理； （3）机房对于楼板进行了防护措施。	符合
物理访问控制	机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。	（1）制定了《机房安全管理制度》，内容包含机房出入方面的管理规定； （2）对未配置电子门禁系统的出入口指定专人7*24小时负责机房出入，对出入的人员进行身份鉴别和登记，可查出入记录，且出入有专人陪同； （3）机房存在未配置门禁系统的开放出入口。	部分符合
防盗窃和防破坏	a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识；	（1）机房设备或主要部件都固定在机架上； （2）机房内对主要部件已绑定相应不易除去的标签； ■包括网络设备 ■包括安全设备 ■包括服务器 ■包括网络线缆 （3）重要机柜已进行上锁处理。	符合
	b) 应将通信线缆铺设在隐蔽安全处。	（1）通信线缆铺设在下走线槽隐蔽处中； （2）通信线缆设有明显的源目的标识； （3）通信线缆均铺设整齐、规范。	符合
防雷击	应将各类机柜、设施和设备等通过接地系统安全接地。	（1）机房设置专用地线； （2）机房内机柜、设施和设备等进行接地处理； （3）交流电源接地验收检测结果符合要求。	符合
防火	a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭	（1）机房采用经消防检测部门检测合格并在有效期内的（如 七氟丙烷）气体自动灭火设备，火灾自动报警类型为烟感+红外；	符合

安全控制点	测评指标	结果结论	符合程度
	火；	（2）自动消防系统工作状态正常，有定期巡检和维护记录《机房巡检记录表》； （3）建立机房消防的管理制度相关文档《机房安全管理制度》，按管理要求机房无人情况下气体灭火配置为自动模式，进入机房调整为手动模式，机房报警有7*24小时值班人员进行监控。	
	b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。	（1）机房及相关的工作房间和辅助房没有采用具有耐火等级的建筑材料； （2）缺乏机房防火设计文档； （3）缺乏机房防火验收文档。	不符合
防水和防潮	a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	（1）机房不存在雨水渗透、破损等不合规情况； （2）机房不位于建筑的顶层、边缘区域。	符合
	b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。	（1）机房区域范围已部署1台科华品牌（精密）空调，机房内分别配置1组温湿度传感器监控； （2）机房内空调下方已铺设安装好挡水和排水设施； （3）机房墙壁或楼板的管道采取必要的防渗防漏等防水保护措施； （4）机房安装检测设备（如：漏水检测绳）检测地下积水，及时处理机房水蒸气结露和地下积水的转移与渗透； （5）目前防水\防潮检测未发现异常情况，并且有防水防潮的运维记录《机房维护日志》。	符合
防静电	应采用防静电地板或地面并采用必要的接地防静电措施。	（1）对机房内设备（可导电金属线槽）采用了接地静电泄放措施； （2）机房未采用防静电地板或铺设防静电地毯。	不符合
温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。	（1）机房范围已部署1组科华品牌精密空调进行温湿度调节； （2）机房范围已部署空调及加湿机进行温湿度调节； （3）温湿度自动调节设施运作正常，有运行和维护记录《机房维护日志》； （4）机房温度能保持在24摄氏度到28摄氏度之间； （5）机房湿度能保持在40%到65%之间。	符合
电力供应	a）应在机房供电线路上配置稳压器和过电压防护设备；	（1）机房配备了稳压器和过电压防护设备； （2）稳压器和过电压防护设备正常工作； （3）机房具备电力供应安全设计，并在其中标明配备稳压器、过电压防护设备等要求。	符合
	b）应提供短期的备用电力	（1）机房配备了1组科华品牌UPS；	符合

安全控制点	测评指标	结果结论	符合程度
	供应，至少满足设备在断电情况下的正常运行要求。	（2）UPS正常工作，可满足主要设备断电情况下的至少1小时正常运行要求； （3）UPS有定期（至少每年）检查和维护，有运行和维护记录《机房巡检记录表》。	
电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。	（1）通信线缆铺设采用独立的具有电磁屏蔽作用线槽； （2）电源线缆铺设采用独立的具有电磁屏蔽作用线槽； （3）弱电线缆隔离铺设，没有干扰。	符合

D.2 安全通信网络

D.2.1 安全通用要求

D.2.1.1 安全通信网络

安全控制点	测评指标	结果结论	符合程度
网络架构	a）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；	（1）已对网络地址划分，且便于管理和控制； （2）网络地址划分采用核心交换机实现外网边界区域、服务器存储区域等的划分； （3）重要核心网络区域与非重要网络在同一网段； （4）关键的应用服务和数据库服务网段未独立进行子网划分的情况。	部分符合
	b）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	（1）网络内重要网段未部署在网络边界处，且未直接连接外部信息系统； （2）系统通过防火墙对重要网段采取访问控制策略； （3）各安全域（子网）的出口唯一。	符合
通信传输	应采用校验技术保证通信过程中数据的完整性。	（1）网络系统中未涉及完整性保障设备，但在安全计算环境方面网络设备采用SSH协议、安全设备采用HTTPS协议、操作系统采用SSH协议、应用系统采用HTTPS协议来保证通信过程中数据的完整性。	符合
可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对通信设备可信验证方面的安全设计要求； （2）现有的通信设备存在未能实现操作系统到上层应用的信任链的情况，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■通信应用连接过程	不符合

D.3 安全区域边界

D.3.1 安全通用要求

D.3.1.1 办公网区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■办公网区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	符合
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问	符合

安全控制点	测评指标	结果结论	符合程度
		的能力。	
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略,无法检测、防止或限制从内部发起的网络攻击行为。	不符合
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试； （4）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	部分符合
安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备	（1）缺乏对边界设备可信验证方面的安全设	不符合

安全控制点	测评指标	结果结论	符合程度
	的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	

D.3.1.2 外网边界区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■外网边界区域 （2）网络边界处部署了可提供访问控制功能的设备； ■防火墙 ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	符合
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■防火墙 ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址	符合

安全控制点	测评指标	结果结论	符合程度
		■源端口 ■目的端口 ■协议	
	d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制,能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署支持对内部发起的攻击行为进行防范的设备； ■防火墙(带入侵防御模块) ■WEB应用防火墙 （2）现有的防范措施满足相应防护要求； ■所有关键网络边界均有检测措施 ■设备的规则库及时更新 ■检测(模块)符合国家相关产品检测要求 ■其安全策略有效 (3)内部安全防范措施能检测相应攻击行为。 ■端口扫描 ■强力攻击 ■木马后门攻击 ■拒绝服务攻击 ■缓冲区溢出攻击 ■碎片攻击 ■网络蠕虫攻击 ■应用漏洞攻击	符合
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试。	符合
安全审计	a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块)	符合

安全控制点	测评指标	结果结论	符合程度
		■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.3.1.3 安全管理区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	（1）网络存在受保护的边界； ■安全管理区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设	符合

安全控制点	测评指标	结果结论	符合程度
		备通过非法无线热点接入内部网络。	
访问控制	a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视网络攻击行为。	（1）网络层部署防火墙，防火墙未配置对内部发起的攻击行为实现防范功能策略，无法检测、防止或限制从内部发起的网络攻击行为。	不符合
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容	部分符合

安全控制点	测评指标	结果结论	符合程度
		性进行测试； （4）现有部署的恶意代码防范措施存在不合规的问题，网络边界覆盖不全面。	
安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）网络层部署日志审计系统，统一接收及保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	符合
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.3.1.4 服务器存储区域

安全控制点	测评指标	结果结论	符合程度
边界防护	应保证跨越边界的访问和	（1）网络存在受保护的边界；	符合

安全控制点	测评指标	结果结论	符合程度
	数据流通过边界设备提供的受控接口进行通信。	■服务器存储区域 （2）网络边界处部署了可提供访问控制功能的设备； ■核心交换机 （3）对跨越边界的网络通信均指定了端口，该端口配置并启用了安全策略； （4）通过技术手段如：上网行为管理系统检测网络中无线热点情况，网络内能及时发现网络中存在的非法无线热点，防止非授权设备通过非法无线热点接入内部网络。	
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	（1）网络区域及边界合理划分及保护； （2）网络边界及区域间部署有效的访问控制设备； ■核心交换机 （3）访问控制设备启用访问控制策略及功能； （4）访问控制设备中安全访问策略最后一条显示禁止所有通信网络。	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	（1）网络边界间的设备不存在多余或无效的访问控制策略； （2）设备的访问控制策略之间逻辑关系及前后排列顺序合理，不存在矛盾； （3）设备的访问控制策略实现最小化。	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	（1）管理员已制定明确的访问控制策略要求，明确哪些数据包可以收、哪些数据包需要拒绝； （2）访问控制设备中根据策略要求配置了正确的访问控制列表，并对数据包是被接收还是拒绝通过特定指示条件来决定。 ■源地址 ■目的地址 ■源端口 ■目的端口 ■协议	符合
	d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。	（1）网络内支持状态检测和会话机制检测的区域及边界； （2）网络边界及区域间部署支持状态检测和会话机制检测的访问控制设备； ■WEB应用防火墙（状态检测防火墙） （3）访问控制设备支持并启用基于连接状态的检测机制，能对通信双方之间交互的属于同一连接的所有报文提供明确的允许/拒绝访问的能力。	符合
入侵防范	应在关键网络节点处监视	（1）网络层部署支持对内部发起的攻击行为	符合

安全控制点	测评指标	结果结论	符合程度
	网络攻击行为。	进行防范的设备； ■WEB应用防火墙 （2）现有的防范措施满足相应防护要求； ■所有关键网络边界均有检测措施 ■设备的规则库及时更新 ■检测(模块)符合国家相关产品检测要求 ■其安全策略有效 （3）内部安全防范措施能检测相应攻击行为。 ■端口扫描 ■强力攻击 ■木马后门攻击 ■拒绝服务攻击 ■缓冲区溢出攻击 ■碎片攻击 ■网络蠕虫攻击 ■应用漏洞攻击	
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	（1）在关键网络节点处部署合规的防恶意代码措施； ■WEB应用防火墙(具备防恶意代码功能) （2）恶意代码防护机制的代码库运作正常，定期更新恶意代码库； （3）有对恶意代码库更新前的安全性及兼容性进行测试。	符合
安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）网络层相关设备均开启本地审计功能； （2）网络内部署审计措施对网络边界、重要网络节点进行安全审计； ■WEB应用防火墙（流量检测、行为检测） ■上网行为管理系统（流量检测、行为检测） ■行为审计系统(具备安全审计模块) ■运维安全管理系统（具备安全审计模块） （3）现有的审计措施满足相应的审计要求。 ■审计的范围覆盖关键边界、重要节点 ■审计覆盖到每个用户 ■审计覆盖到重要的用户行为 ■审计覆盖到重要安全事件	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备均开启日志记录功能； （2）现有环境内日志信息较全面； ■包括事件的日期和时间 ■包括用户 ■包括事件类型 ■包括事件是否成功 （3）设备本地时间正常。	符合
	c）应对审计记录进行保	（1）网络层部署日志审计系统，统一接收及	符合

安全控制点	测评指标	结果结论	符合程度
	护，定期备份，避免受到未预期的删除、修改或覆盖等。	保存相关设备的审计记录； （2）相关网络及安全设备的本地日志文件不可删除修改； （3）审计记录的备份机制符合信息安全管理要求； （4）日志及审计记录的保存能力可超过6个月； （5）定期收集日志记录并定期备份。	
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对边界设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，系统运行过程中的可信检验不全面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■边界防护应用程序	不符合

D.4 安全计算环境

D.4.1 安全通用要求

D.4.1.1 网络设备

D.4.1.1.1 核心交换机

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括VTY认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的全局密码策略； ■Password control:Enabled ■Password aging:Enabled (180 days) ■Password length:Enabled (8 characters) ■Password composition:Enabled (4 types, 1 characters per type) （6）设备配置加密的super认证。	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备配置合规的全局登录失败处理策略； ■Password control: Enabled ■Maximum login attempts: 5 ■Action for exceeding login attempts: Lock user for 5 minutes	符合

安全控制点	测评指标	结果结论	符合程度
		（2）设备配置合规的操作超时退出措施。 ■VTY配置idle-timeout 15 0	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式。 ■未启用TELNET ■启用SSH	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； ■Information Center: Enabled ■Console: Enabled ■Monitor: Enabled ■Log host: Enabled 10.2.1.2 ■Security log file: Enabled （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间	符合

安全控制点	测评指标	结果结论	符合程度
		■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制； ■对ssh 登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）网络层相关设备不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的交换功能，不具备恶意代码防范模块，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配	（1）网络层设备不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	前得到完全清除。		
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.1.2 汇聚交换机

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括VTY认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的全局密码策略； ■Password control:Enabled ■Password aging:Enabled (180 days) ■Password length:Enabled (8 characters) ■Password composition:Enabled (4 types, 1 characters per type) （6）设备配置加密的super认证。	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备配置合规的全局登录失败处理策略； ■Password control: Enabled ■Maximum login attempts: 5 ■Action for exceeding login attempts: Lock user for 5 minutes （2）设备配置合规的操作超时退出措施。 ■VTY配置idle-timeout 15 0	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式。 ■未启用TELNET ■启用SSH	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令	符合

安全控制点	测评指标	结果结论	符合程度
		■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个network-admin的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； ■Information Center: Enabled ■Console: Enabled ■Monitor: Enabled ■Log host: Enabled 10.2.1.2 ■Security log file: Enabled （2）采用日志审计平台实现审计要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可使用 reset info-center statistics/reset logbuffer/reset trapbuffer 命令删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）对审计记录进行定期存档备份，其备份策略有效；	符合

安全控制点	测评指标	结果结论	符合程度
		（5）日志及审计记录保存大于6个月。	
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备自身设定有效的终端接入策略，通过ACL策略进行管理终端的地址限制； ■对ssh 登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）网络层相关设备不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的交换功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要	符合

安全控制点	测评指标	结果结论	符合程度
		的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2 安全设备

D.4.1.2.1 WEB应用防火墙

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有	符合

安全控制点	测评指标	结果结论	符合程度
		唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，	（1）设备开启审计功能，审计进程正常；	符合

安全控制点	测评指标	结果结论	符合程度
	审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请	符合

安全控制点	测评指标	结果结论	符合程度
		表》。	
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.2 上网行为管理系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合

安全控制点	测评指标	结果结论	符合程度
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要	符合

安全控制点	测评指标	结果结论	符合程度
		的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.3 基线核查系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性；	符合

安全控制点	测评指标	结果结论	符合程度
		（4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆	符合

安全控制点	测评指标	结果结论	符合程度
	重要的用户行为和重要安全事件进行审计；	盖所有用户操作审计和记录。	
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成	符合

安全控制点	测评指标	结果结论	符合程度
		高风险的漏洞。	
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的基线核查功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要	不适用

安全控制点	测评指标	结果结论	符合程度
	数据定时批量传送至备用场地。	求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.4 日志审计系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合

安全控制点	测评指标	结果结论	符合程度
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2)设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合

安全控制点	测评指标	结果结论	符合程度
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； (2)设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施；	符合

安全控制点	测评指标	结果结论	符合程度
		■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.5 运维安全管理系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合

安全控制点	测评指标	结果结论	符合程度
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； (2)登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 (2)设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期	符合

安全控制点	测评指标	结果结论	符合程度
	他与审计相关的信息；	■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制。 ■对Web登录配置管理地址，限制登录范围	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备为纯粹的行为审计功能，不具备恶意代码防范模块，不适用。	不适用
可信验证	可基于可信根对计算设备	（1）设备不具备相关可信验证的技术措施；	不符合

安全控制点	测评指标	结果结论	符合程度
	的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.6 防火墙-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）设备启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合

安全控制点	测评指标	结果结论	符合程度
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方	（1）设备通过核心交换机的访问控制策略，	符合

安全控制点	测评指标	结果结论	符合程度
	式或网络地址范围对通过网络进行管理的管理终端进行限制；	通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要	符合

安全控制点	测评指标	结果结论	符合程度
		的完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）网络层设备不适用。	不适用
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.2.7 防火墙-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）设备对各登录模式均启用身份鉴别； ■包括Web认证 （2）设备对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）设备名及登录用户设置的身份标识具有唯一性； （4）设备不存在明文或空口令用户； （5）设备配置合规的密码策略。 ■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	符合
	b) 应具有登录失败处理功能，应配置并启用结束会	（1）设备启用合规登录失败处理策略； ■启用登录失败策略	符合

安全控制点	测评指标	结果结论	符合程度
	话、限制非法登录次数和当登录连接超时自动退出等相关措施；	■配置失败5次 ■配置锁定15分钟 （2）设备配置合规的操作超时退出措施。 ■WEB配置超时20分钟	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）设备配置合规的远程管理模式； ■未启用HTTP ■未启用SSH ■启用HTTPS （2）使用运维安全管理系统统一管理设备远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供设备管理权限分配表； （2）登录设备的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，设备现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）设备不存在默认账户名； （2）设备账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）设备不存在多余或过期账户； （2）设备管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）设备根据安全策略要求对特权用户进行分离； ■系统管理员 ■安全审计员 ■系统操作员 （2）设备不存在多个管理级别高的特权用户； （3）设备按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）设备开启审计功能，审计进程正常； （2）设备的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）设备日期、时间正常； （2）设备审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型	符合

安全控制点	测评指标	结果结论	符合程度
		■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）设备限制审计文件的访问控制权限，普通用户不可删除及修改； （2）设备针对日志、审计记录具备充足的存储容量； （3）对审计记录进行定期存档备份，其备份策略有效； （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）设备在全局模式下禁用部分不必要的服务； （2）设备在部分接口模式下禁用部分不必要的服务； （3）漏洞扫描未发现高风险设备固件漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）设备采用安全策略限制部分高危端口； （2）设备采用安全策略限制部分不必要服务； （3）漏洞扫描未发现设备启用高危端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； ■对Web登录配置管理地址，限制登录范围 （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）设备管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）设备管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）设备已根据需要不定期地对已发布的新固件版本进行更新； （2）固件安装前进行安全性和兼容性测试； （3）设备进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）设备使用深信服防恶意代码库； （2）设备具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码库及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合

安全控制点	测评指标	结果结论	符合程度
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）设备不具备相关可信验证的技术措施； ■无可信根芯片 ■无其他可信验证硬件措施 （2）设备启动过程中无法基于可信根覆盖所有系统相关运行的预装软件/程序进行可信验证度量。 ■缺乏引导程序 ■缺乏系统程序 ■缺乏重要设备配置参数 ■缺乏关键应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）设备定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配	（1）网络层设备不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	前得到完全清除。		
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）网络层设备不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）网络层设备不适用。	不适用

D.4.1.3 服务器和终端

D.4.1.3.1 应用服务器

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）操作系统不存在空口令用户； ■etc/passwd文件中各用户的第二字段处不为空 ■/etc/shadow文件中各用户密码字段处不为空 （3）操作系统不存在默认信任的登录模式； （4）操作系统为登录用户设置的身份标识具有唯一性； ■UID具有唯一性 ■UID=0只能root用户 （5）操作系统配置的一定的密码长度且定期更换； ■PASS_MAX_DAYS 180 ■PASS_MIN_DAYS 1 ■PASS_MIN_LEN 8 ■PASS_WARN_AGE 28 （6）操作系统配置一定的密码复杂度策略。 ■minlen=8 ■ucredit=-2 ■lcredit=-1 ■dcredit=-4 ■ocredit=-1	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用pam_tally2模块的合规登录失败处理策略； auth required /lib/security/pam_tally.so onerr=fail no_magic_root和 account required /lib/security/pam_tally.so deny=10 no_magic_root reset （2）操作系统配置合规的操作超时锁定； ■配置具备以下措施：	符合

安全控制点	测评指标	结果结论	符合程度
		/etc/profile设置TMOUT=300 （3）操作系统启用SSH的合规登录超时策略。 ■配置具备以下措施： /sshd_config设置 ClientAliveInterval 60 ClientAliveCountMax 3	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）操作系统配置合规的远程管理模式； ■启用SSH （2）操作系统远程端口使用情况合规； ■21（FTP）未启用 ■23（Telnet）未启用 （3）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在所有用户均属于root组的情况。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统对多余帐户进行删除、锁定或禁止其登录； （2）操作系统账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； （2）操作系统不存在除root外的特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计功能，审计进程正常； ■rsyslog：loaded ■auditctl：enabled=1 （2）操作系统开启审计范围及策略满足要求，审计覆盖所有用户操作审计和记录。 ■rsyslog： *.info;mail.none;news.none;authpriv.none;cron.none /var/log/messages	符合

安全控制点	测评指标	结果结论	符合程度
		■auditctl： 关键目录、文件的审计行为采用 perm=rwxa	
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）操作系统针对日志、审计记录具备充足的存储容量； （3）操作系统采取合规的日志文件权限策略； ■/var/log/messages：640 ■/var/log/secure：640 ■/var/log/audit/audit.log：640 对审计记录进行定期存档备份，其备份策略有效 （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统关闭不必要端口； （2）操作系统禁用不必要服务； （3）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口； （4）漏洞扫描未发现高风险主机端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服edr防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证； ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序 （3）现有的可信验证缺乏以下措施。 ■对可信性破坏报警 ■将可信性验证结果形成审计记录 ■对可信性审计的动态关联感知	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对鉴别数据采取完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）系统在通信传输过程中对重要配置数据采取完整性保护措施。 ■使用SSH加密协议进行传输	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确	符合

安全控制点	测评指标	结果结论	符合程度
		的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为服务器设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统不保存过多终端历史记录。 ■通过echo $HISTSIZE查看history保留数目为30	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）本设备不存在此部分的控制需求，故此项不适用	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）本设备不存在此部分的控制需求，故此项不适用	不适用

D.4.1.3.2 数据库服务器

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）操作系统不存在空口令用户； ■etc/passwd文件中各用户的第二字段处不为空 ■/etc/shadow文件中各用户密码字段处不为空 （3）操作系统不存在默认信任的登录模式； （4）操作系统为登录用户设置的身份标识具有唯一性； ■UID具有唯一性 ■UID=0只能root用户 （5）操作系统配置的一定的密码长度且定期更换； ■PASS_MAX_DAYS 180 ■PASS_MIN_DAYS 1 ■PASS_MIN_LEN 8 ■PASS_WARN_AGE 28	符合

安全控制点	测评指标	结果结论	符合程度
		（6）操作系统配置一定的密码复杂度策略。 ■minlen=8 ■ucredit=-2 ■lcredit=-1 ■dcredit=-4 ■ocredit=-1	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用pam_tally2模块的合规登录失败处理策略； auth required /lib/security/pam_tally.so onerr=fail no_magic_root和 account required /lib/security/pam_tally.so deny=10 no_magic_root reset （2）操作系统配置合规的操作超时锁定； ■配置具备以下措施： /etc/profile设置TMOUT=300 （3）操作系统启用SSH的合规登录超时策略。 ■配置具备以下措施： /sshd_config设置 ClientAliveInterval 60 ClientAliveCountMax 3	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）操作系统配置合规的远程管理模式； ■启用SSH （2）操作系统远程端口使用情况合规； ■21（FTP）未启用 ■23（Telnet）未启用 （3）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在所有用户均属于root组的情况。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统对多余帐户进行删除、锁定或禁止其登录； （2）操作系统账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合

安全控制点	测评指标	结果结论	符合程度
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； （2）操作系统不存在除root外的特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计功能，审计进程正常； ■rsyslog：loaded ■auditctl：enabled=1 （2）操作系统开启审计范围及策略满足要求，审计覆盖所有用户操作审计和记录。 ■rsyslog：*.info;mail.none;news.none;authpriv.none;cron.none /var/log/messages ■auditctl： 关键目录、文件的审计行为采用 perm=rwxa	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）操作系统针对日志、审计记录具备充足的存储容量； （3）操作系统采取合规的日志文件权限策略； ■/var/log/messages：640 ■/var/log/secure：640 ■/var/log/audit/audit.log：640 对审计记录进行定期存档备份,其备份策略有效 （4）部署日志审计系统实时对日志进行统一收集存储； （5）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合

安全控制点	测评指标	结果结论	符合程度
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统关闭不必要端口； （2）操作系统禁用不必要服务； （3）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口； （4）漏洞扫描未发现高风险主机端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）设备通过核心交换机的访问控制策略，通过ACL策略进行管理终端的地址限制； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服edr防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证； ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序 （3）现有的可信验证缺乏以下措施。 ■对可信性破坏报警 ■将可信性验证结果形成审计记录 ■对可信性审计的动态关联感知	不符合
数据完整性	应采用校验技术保证重要	鉴别数据:	符合

安全控制点	测评指标	结果结论	符合程度
	数据在传输过程中的完整性。	（1）系统在通信传输过程中对鉴别数据采取完整性保护措施。 ■使用SSH加密协议进行传输 重要配置数据: （1）系统在通信传输过程中对重要配置数据采取完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为服务器设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统不保存过多终端历史记录。 ■通过echo $HISTSIZE查看history保留数目为30	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）本设备不存在此部分的控制需求，故此项不适用	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）本设备不存在此部分的控制需求，故此项不适用	不适用

D.4.1.3.3 业务终端-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的	（1）操作系统根据安全策略要求对特权用户	符合

安全控制点	测评指标	结果结论	符合程度
	最小权限，实现管理用户的权限分离。	进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下：运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序；	符合

安全控制点	测评指标	结果结论	符合程度
	应用程序；	（3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要	鉴别数据:	符合

安全控制点	测评指标	结果结论	符合程度
	数据在传输过程中的完整性。	（1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施： 安全选项“不显示上次的用户名”->启用	符合

安全控制点	测评指标	结果结论	符合程度
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.4 业务终端-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 (5)用户属性策略未勾选“密码永不过期”。	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保	（1）操作系统采取对审计记录存储容量如下：	符合

安全控制点	测评指标	结果结论	符合程度
	护，定期备份，避免受到未预期的删除、修改或覆盖等。	运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G; （2）限制审计文件的访问控制权限，用户不可删除及修改; （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限; （4）对审计记录进行定期存档备份，其备份策略有效; （5）部署日志审计系统实时对日志进行统一收集存储; （6）日志及审计记录保存6个月。	
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序;	（1）操作系统仅安装必需的组件; （2）操作系统仅安装必需的应用程序; （3）操作系统遵循最小安装的原则，仅启用必需的功能软件; （4）漏洞扫描未发现高风险主机漏洞。	符合
	b) 应关闭不需要的系统服务、默认共享和高危端口;	（1）操作系统不存在多余的默认共享及其它文件共享; ■如：C$、D$、E$ （2）操作系统关闭不必要端口; ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务; （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制;	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式; （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求;	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁; （2）补丁安装前进行安全性和兼容性测试; （3）操作系统不存在启用未加控制的高危端口; （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更	（1）操作系统安装深信服EDR防恶意代码软件; （2）系统具备且启用在发现入侵和病毒行为	符合

安全控制点	测评指标	结果结论	符合程度
	新防恶意代码库。	时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每	符合

安全控制点	测评指标	结果结论	符合程度
		月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.5 运维及管理终端-1

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施； ■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员 （2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败	符合

安全控制点	测评指标	结果结论	符合程度
		■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下：运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	（1）操作系统不存在多余的默认共享及其它文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d）应提供数据有效性检验功能，保证通过人机接口	（1）操作系统不存在此部分的控制需求，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	输入或通过通信接口输入的内容符合系统设定要求；		
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输	符合

安全控制点	测评指标	结果结论	符合程度
		（3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.3.6 运维及管理终端-2

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）操作系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）系统勾选“要使用本机，用户必需输入用户名和密码”； （3）操作系统身份标识具有唯一性，不同用户采用不同账号登录系统，不存在同名用户； （4）操作系统口令策略配置具备相应安全措施；	符合

安全控制点	测评指标	结果结论	符合程度
		■密码必需符合复杂性要求->启用 ■密码长度最小值->8 ■密码最长使用期限->180天 ■密码最短使用期限->1天 ■强制密码历史->5次 （5）用户属性策略未勾选“密码永不过期”。	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）操作系统启用登录失败处理策略，且配置具备以下措施： ■复位帐户锁定计数器->5分钟 ■帐户锁定时间->15分钟 ■帐户锁定阀值->15次无效登录 （2）操作系统本地登录启用开启带密码的屏幕保护功能，超时锁定≤10分钟； （3）操作系统远程终端登录启用登录连接超时及自动退出策略，且配置具备以下措施： ■“为断开的会话设置时间限制”->启用 ■“空闲会话限制”->≤10分钟	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）禁用telnet服务，已变更采用3389端口号的远程桌面方式； （2）“终端服务配置”启用”RDP安全层”参数； （3）使用运维安全管理系统统一管理操作系统远程登录，采用了HTTPS 的管理。	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）可提供操作系统权限表； （2）登录操作系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）操作系统针对默认账户采用相应的安全策略配置； ■重命名Administrator帐户 ■修改Administrator帐户的默认口令 ■禁用Guest帐户 （2）操作系统账户不存在弱口令或空口令。	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）操作系统不存在多余或过期账户； （2）操作系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）操作系统根据安全策略要求对特权用户进行分离； ■安全管理员 ■安全审计员 ■系统操作员	符合

安全控制点	测评指标	结果结论	符合程度
		（2）操作系统不存在特权用户； （3）操作系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）操作系统开启审计策略，操作系统审计策略基本完整； ■审计帐户登录事件： 成功，失败 ■审计帐户管理： 成功，失败 ■审计目录服务访问： 成功，失败 ■审计登录事件： 成功，失败 ■审计对象访问： 成功，失败 ■审计策略更改： 成功，失败 ■审计特权使用： 成功，失败 ■审计系统事件： 成功，失败 ■审计过程追踪： 成功，失败 （2）审计覆盖所有用户操作审计和记录。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）操作系统日期、时间正常； （2）操作系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识 ■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）操作系统采取对审计记录存储容量如下:运维审计和日志记录 应用日志 1G、安全日志 1G、系统日志 1G； （2）限制审计文件的访问控制权限，用户不可删除及修改； （3）“管理审核和安全日志”，除审计员、administrators外其他用户无权限； （4）对审计记录进行定期存档备份，其备份策略有效； （5）部署日志审计系统实时对日志进行统一收集存储； （6）日志及审计记录保存6个月。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）操作系统仅安装必需的组件； （2）操作系统仅安装必需的应用程序； （3）操作系统遵循最小安装的原则，仅启用必需的功能软件； （4）漏洞扫描未发现高风险主机漏洞。	符合
	b）应关闭不需要的系统服	（1）操作系统不存在多余的默认共享及其它	符合

安全控制点	测评指标	结果结论	符合程度
	务、默认共享和高危端口；	文件共享； ■如：C$、D$、E$ （2）操作系统关闭不必要端口； ■如：137，138、139、445、123、1900 （3）操作系统禁用不必要服务； （4）操作系统删除多余组件和应用程序，并停止或禁用与承载业务无关的服务或端口。	
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）安全设备ACL策略有效限制访问本机的IP地址及管理模式； （2）通过运维安全管理系统，在有效的策略要求下，统一集中管理远程登录地址。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）操作系统已安装最新的SP及后续的hotfix补丁； （2）补丁安装前进行安全性和兼容性测试； （3）操作系统不存在启用未加控制的高危端口； （4）操作系统进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）操作系统安装深信服EDR防恶意代码软件； （2）系统具备且启用在发现入侵和病毒行为时能及时阻断的功能； （3）防恶意代码软件及病毒库更新及时，可防止来自外部的恶意攻击或系统漏洞带来的危害。	符合
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）缺乏对计算设备可信验证方面的安全设计要求； （2）系统未实现对所有可执行环节进行可信验证，缺乏以下方面。 ■系统引导 ■重要系统程序或文件 ■重要配置参数 ■业务应用程序	不符合
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必	符合

安全控制点	测评指标	结果结论	符合程度
		要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）操作系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据件 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施：安全选项“不显示上次的用户名”->启用	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）操作系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）操作系统不存在此部分的控制需求，不适用。	不适用

D.4.1.4 系统管理软件/平台

D.4.1.4.1 应用服务器-Weblogic

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）WebLogic中间件对各登录模式均启用身份鉴别； ■包括web管理控制后台认证 （2）对登录管理的中间件用户进行身份鉴别； ■采用用户名 ■采用口令 （3）WebLogic中间件登录用户设置的身份标识具有唯一性； （4）WebLogic中间件不存在弱口令用户； （5）WebLogic中间件配置合规的密码长度策略。 ■配置用户口令 ■现有口令配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■按安全管理要求定期更新密码(更新周期90天)	符合
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）WebLogic中间件web管理控制台仅内部授权网段可访问； （2）WebLogic中间件合规登录失败处理策略； ■已启用封锁 ■封锁阀值 15次 ■封锁持续时间 30分钟 ■封锁重置持续时间 30分钟 （3）WebLogic中间件配置空闲连接超时。 ■超时时间为15分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）WebLogic中间件管理控制台开启了SSL监听端口。	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）WebLogic中间件可提供管理控制台权限功能； （2）对应不同的账户均按需分配不同的用户权限，不存在中间件用户均属于管理级别、高权限的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）中间件不存在除如默认账户名； （2）中间件账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令	符合

安全控制点	测评指标	结果结论	符合程度
		■未设置弱口令 ■未设置空口令	
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）中间件不存在多余或过期账户； (2)中间件管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）中间件根据安全策略要求对特权用户及宿主管理用户进行分离； （2）中间件管理不存在多个管理级别高的特权用户； （3）中间件管理按不同用户分配了不同的角色并且授予的角色是管理用户所需的最小权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）中间件开启审计功能，审计进程正常； （2）系统的日志审计级别满足要求； （3）审计记录覆盖所有用户。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）中间件日期、时间正常； （2）宿主系统启用NTP服务，服务端的地址配置正确； （3）中间件审计记录开启审核策略且日志级别正常。	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）中间件限制审计文件的访问控制权限，普通用户不可删除及修改； （2）宿主系统针对中间件日志、审计记录具备充足的存储容量； （3）对中间件审计记录进行定期存档备份，其备份策略有效； （4）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）中间件系统不存在此部分的安装控制需求，不适用。	不适用
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）中间件的管理地址限制功能由宿主操作系统实现，故该项不适用。	不适用
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）中间件管理具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）中间件管理的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合

安全控制点	测评指标	结果结论	符合程度
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）中间件已根据需要不定期地对已发布的版本进行更新； （2）中间件更新安装前进行安全性和兼容性测试； （3）在系统上线或发生重大变更时测试并安装最新的中间件版本或更新补丁； （4）在不影响业务系统正常运行情况下，对发现的中间件漏洞在确保安全的情况下进行修补； （5）中间件进行渗透及扫描未发现存在可造成高风险的漏洞。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议传输信息 重要配置数据: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议传输信息	符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份的中间件重要数据； ■包括鉴别数据 ■包括重要配置数据 ■包括重要审计数据 （2）单位具备合理的重要数据的备份策略规	符合

安全控制点	测评指标	结果结论	符合程度
		范； （3）宿主系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）中间件相关数据的备份周期合理； ■每天增量一次 ■每月全备一次 （5）中间件开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）宿主系统具有清除用户鉴别信息的功能； （2）经测试，宿主系统退出后无法访问先前中间件登录过的页面； （3）经测试，宿主系统关闭后无残留的中间件用户鉴别信息。 ■包括临时目录 ■包括文件 ■包括注册表	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）中间件系统不存在此部分的控制需求，不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）中间件系统不存在此部分的控制需求，不适用。	不适用

D.4.1.4.2 数据库服务器-Oracle

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）数据库系统对登录系统的用户进行身份鉴别； ■采用用户名 ■采用密码 （2）数据库系统不存在弱口令用户； ■ORACLE数据库已修改默认口令 ■ORACLE数据库不存在空口令用户 （3）数据库系统为登录用户设置的身份标识具有唯一性； （4）数据库系统配置合规的密码长度及复杂度策略； ■PASSWORD_VERIFY_FUNCTION ，LIMIT=VERIFY_FUNCTION ■IF LENGTH(password) 值为8 ■PASSWORD_REUSE_MAX值为5	符合

安全控制点	测评指标	结果结论	符合程度
		（5）数据库系统配置合规的密码有效周期策略。 ■PASSWORD_LIFE_TIME值为 180	
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）数据库系统启用合规登录失败处理策略； ■ORACLE 数据库系统FAILED_LOGIN_ATTEMPTS= 10 （2）数据库系统执行合规的锁定策略。 ■PASSWORD_LOCK_TIME=1	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）数据库系统配置合规的远程管理模式。 ■ORACLE 数据库系统sqlnet.encryption为true ■ORACLE 数据库系统采用sqlplus连接数据库，客户端与服务器端之间通信是加密的	符合
访问控制	a）应对登录的用户分配账户和权限；	（1）登录数据库系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （2）对应不同的账户均按需求分配不同的用户组及对应的权限，不存在多用户均与sys、DBA用户权限一致的情况； （3）安全管理规范制定了对应的用户与账户权限分配表，系统现状与权限分配表情况一致。	符合
	b）应重命名或删除默认账户，修改默认账户的默认口令；	（1）数据库系统对多余帐户进行删除、锁定或禁止其登录； ■数据库系统账户禁用不常用的默认用户 （2）数据库系统账户口令设置合规。 ■数据库系统各用户未使用空口令 ■数据库系统未使用弱口令或默认与用户名相同的口令	符合
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）数据库系统不存在多余或过期账户； （2）数据库系统管理员用户与账户之间一一对应。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）数据库系统根据安全策略要求对特权用户进行分离； ■配置系统管理员 ■配置安全审计员 ■配置系统操作员 （2）数据库系统用户权限合理，非管理员未设置过大权限； ■具备DBA角色的用户仅为 SYS、SYSTEM （3）数据库系统按最小授权原则分配，不赋予一般用户管理员权限,不赋予用户不必要的操作权限。	符合
安全审计	a）应启用安全审计功能，	（1）数据库系统开启审计功能，审计进程正	符合

安全控制点	测评指标	结果结论	符合程度
	审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	常； ■ORACLE 数据库系统audit_sys_operations=TRUE ■ORACLE 数据库系统audit_trail=DB （2）ORACLE数据库系统启动数据库日志模式和自动归档； ■Automatic archival=Enabled （3）审计覆盖所有用户操作审计和记录。	
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）数据库宿主系统日期、时间正常； （2）数据库系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括重要用户行为 ■包括系统资源的异常使用情况 ■包括重要系统命令的使用 ■包括重要的安全相关事件	符合
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）数据库系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）数据库系统针对日志、审计记录具备充足的存储容量； （3）部署日志审计系统实时对日志进行统一收集存储； （4）日志及审计记录保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
	b) 应关闭不需要的系统服务、默认共享和高危端口；	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）网络设备ACL策略有效限制访问本机的IP地址及管理模式。	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）数据库系统已根据需要不定期地对已发布的安全性补丁进行更新； （2）数据库宿主系统不存在启用未加控制的高危端口； （3）MY_SQL分离默认安装的示例数据库；	符合

安全控制点	测评指标	结果结论	符合程度
		（4）数据库系统进行渗透及扫描未发现存在可造成高风险的漏洞。	
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	（1）数据库系统不存在此部分的控制需求，不适用。	不适用
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	鉴别数据: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■SQLNET.ENCRYPTION_SERVER = REQUIRED ■SQLNET.ENCRYPTION_TYPES_SERVER = RC4_256 ■SQLNET.CRYPTO_CHECKSUM_SERVER = REQUIRED 重要配置数据: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■SQLNET.ENCRYPTION_SERVER = REQUIRED ■SQLNET.ENCRYPTION_TYPES_SERVER = RC4_256 ■SQLNET.CRYPTO_CHECKSUM_SERVER = REQUIRED	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）数据库系统定义了相关重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规	符合

安全控制点	测评指标	结果结论	符合程度
		范； （3）数据库系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）数据库系统未能提供异地数据备份功能。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）身份鉴别信息释放或清除机制正常且满足要求； （2）数据库系统不保存终端历史记录。	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）数据库存储的用户个人信息均为业务应用必需的环节。	符合
	b）应禁止未授权访问和非法使用用户个人信息。	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； ■包括信息采集 ■包括信息保存 ■包括信息访问 ■包括信息使用 （2）数据库具备控制措施禁止未授权访问用户个人信息表单； （3）数据库具备控制措施禁止非法使用用户个人信息表单。	符合

D.4.1.5 业务应用系统/平台

D.4.1.5.1 智慧校园系统

安全控制点	测评指标	结果结论	符合程度
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	（1）系统对各登录模式均启用身份鉴别； ■包括管理后台认证 （2）系统对登录管理的用户进行身份鉴别； ■采用用户名 ■采用密码 （3）系统登录用户设置的身份标识具有唯一性； （4）系统不存在空口令用户； （5）设备配置合规的密码策略。	符合

安全控制点	测评指标	结果结论	符合程度
		■配置复杂度要求（长度>8、包括大小写字母、数字、特殊符号） ■配置密码有效期要求（有效期180天）	
	b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	（1）系统启用合规登录失败处理策略； ■启用登录失败策略 ■配置失败5次 ■配置锁定15分钟 （2）系统配置合规的操作超时退出措施。 ■管理后台配置超时15分钟	符合
	c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	（1）应用系统的用户鉴别数据采用SHA-512算法在可控网络环境中传输； （2）系统配置合规的远程管理模式。 ■启用HTTPS	符合
访问控制	a) 应对登录的用户分配账户和权限；	（1）可提供系统权限分配表； （2）登录系统的用户均相应分配不同的账户，不存在使用共用账户的情况； （3）对应不同的账户均按需分配不同的用户权限，不存在所有用户均属于管理级别、高权限的情况。	符合
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	（1）系统禁用默认账户名； （2）系统账户口令设置合规。 ■未设置默认口令 ■未设置与用户名相同的口令 ■未设置弱口令 ■未设置空口令	符合
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；	（1）系统不存在多余或过期账户； （2）系统管理员用户与账户之间一一对应。	符合
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。	（1）系统不存在多个管理级别高的特权用户； （2）系统按最小授权原则分配，不赋予一般用户管理员权限，不赋予用户不必要的操作权限。	符合
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	（1）系统开启审计功能，审计进程正常； （2）系统的日志审计级别满足要求，审计覆盖所有用户操作审计和记录。	符合
	b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	（1）系统日期、时间正常； （2）系统审计记录内容基本完整。 ■包括事件的日期 ■包括时间 ■包括类型 ■包括主体标识 ■包括客体标识	符合

安全控制点	测评指标	结果结论	符合程度
		■包括结果（事件的失败或成功） ■包括身份鉴别事件中请求的来源	
	c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	（1）系统限制审计文件的访问控制权限，普通用户不可删除及修改； （2）系统针对日志、审计记录具备充足的存储容量； （3）审计记录及日志保存大于6个月。	符合
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；	（1）应用软件系统不存在此部分的安装控制需求，不适用。	不适用
	b) 应关闭不需要的系统服务、默认共享和高危端口；	(1)应用软件系统不存在此部分的控制需求，不适用。	不适用
	c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	（1）系统自身设定有效的终端访问策略，通过访问措施进行管理地址的限制。 ■系统管理页面仅能内网登录	符合
	d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	（1）系统具备数据有效性检验功能； ■可校验录入数据 ■可校验文档内容 （2）系统的校验接口范围较全面。 ■包括人机接口校验 ■包括通信接口校验	符合
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	（1）系统已根据需要不定期地对已发布的版本进行更新； （2）在系统上线或发生重大变更时测试并安装最新的版本或更新补丁； （3）在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补。	符合
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	(1)应用软件系统不存在此部分的控制需求，不适用。	不适用
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	(1)应用软件系统不存在此部分的控制需求，不适用。	不适用
数据完整性	应采用校验技术保证重要数据在传输过程中的完整	鉴别数据: （1）系统在通信传输过程中对相关数据采取	符合

安全控制点	测评指标	结果结论	符合程度
	性。	完整性保护措施； ■包括鉴别数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输 重要配置数据: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份重要数据； ■包括重要配置数据 ■包括重要审计数据 ■包括鉴别数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）系统具有清除用户鉴别信息的功能； （2）经测试，系统退出后无法访问先前登录过的页面； （3）经测试，系统关闭后无残留的用户鉴别信息。	符合
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息； （3）系统采集的用户个人信息均为业务应用必需的环节。	符合
	b）应禁止未授权访问和非法使用用户个人信息。	（1）系统不采集和保存任何形式的用户个人信息；	符合

安全控制点	测评指标	结果结论	符合程度
		（2）系统对所有涉及个人信息的环节均有明确的授权同意过程； ■包括信息采集 ■包括信息保存 ■包括信息访问 ■包括信息使用 （3）系统具备控制措施禁止未授权访问用户个人信息； （4）系统具备控制措施禁止非法使用用户个人信息。	

D.4.1.6 数据资源

D.4.1.6.1 重要业务数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	（1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要业务数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份重要数据； ■包括重要业务数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）该测评项测评对象鉴别数据，已在安全计算环境层面其他对象判定，此项不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）该测评项测评对象为重要个人信息的内容，已在安全计算环境层面其他对象判定，该项不适用。	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	（1）该测评项测评对象为重要个人信息的内容，已在安全计算环境层面其他对象判定，该	不适用

安全控制点	测评指标	结果结论	符合程度
		项不适用。	

D.4.1.6.2 重要个人信息

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	（1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要个人信息 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输	符合
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	（1）系统定义了相关需要备份重要数据； ■包括重要个人信息 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	（1）单位未能提供异地数据备份措施。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	（1）该测评项测评对象鉴别数据，已在安全计算环境层面其他对象判定，此项不适用。	不适用
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	（1）单位针对系统需采集和保存用户个人信息的需求建立了有关用户个人信息保护的管理制度和流程； （2）系统按管理规范，仅最小化采集必需的用户个人信息； （3）系统采集的用户个人信息均为业务应用必需的环节。	符合
	b）应禁止未授权访问和非法使用用户个人信息。	（1）系统对所有涉及个人信息的环节均有明确的授权同意过程； ■包括信息采集 ■包括信息保存 ■包括信息访问 ■包括信息使用 （2）系统具备控制措施禁止未授权访问用户个人信息；	符合

安全控制点	测评指标	结果结论	符合程度
		（3）系统具备控制措施禁止非法使用用户个人信息。	

D.4.1.6.3 鉴别数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	数据库服务器-Oracle: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■SQLNET.ENCRYPTION_SERVER = REQUIRED ■SQLNET.ENCRYPTION_TYPES_SERVER = RC4_256 ■SQLNET.CRYPTO_CHECKSUM_SERVER = REQUIRED 应用服务器-Weblogic: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议传输信息 业务终端-1、业务终端-2、运维及管理终端-1、运维及管理终端-2: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据	符合

安全控制点	测评指标	结果结论	符合程度
		（2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 智慧校园系统: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括鉴别数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输 应用服务器、数据库服务器: （1）系统在通信传输过程中对鉴别数据采取完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	该测评项在各系统及设备已做判定,数据资源针对鉴别数据不做判定	不适用
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	该测评项在各系统及设备已做判定,数据资源针对鉴别数据不做判定，不适用。	不适用
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）网络层设备不适用。 业务终端-1、业务终端-2、运维及管理终端-1、运维及管理终端-2: （1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统用户的鉴别信息释放措施:安全选项“不显示上次的用户名”->启用 应用服务器、数据库服务器: （1）身份鉴别信息释放或清除机制正常且满足要求； （2）操作系统不保存过多终端历史记录。 ■通过echo $HISTSIZE查看history保留数目为30 智慧校园系统: （1）系统具有清除用户鉴别信息的功能； （2）经测试，系统退出后无法访问先前登录过的页面； （3）经测试，系统关闭后无残留的用户鉴别信息。	符合

安全控制点	测评指标	结果结论	符合程度
		应用服务器-Weblogic: （1）宿主系统具有清除用户鉴别信息的功能； （2）经测试，宿主系统退出后无法访问先前中间件登录过的页面； （3）经测试，宿主系统关闭后无残留的中间件用户鉴别信息。 ■包括临时目录 ■包括文件 ■包括注册表 数据库服务器-Oracle: （1）身份鉴别信息释放或清除机制正常且满足要求； （2）数据库系统不保存终端历史记录。	
个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	鉴别数据不存在此部分的控制需求,故此项不适用	不适用
	b）应禁止未授权访问和非法使用用户个人信息。	鉴别数据不存在此部分的控制需求,故此项不适用	不适用

D.4.1.6.4 重要配置数据

安全控制点	测评指标	结果结论	符合程度
数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	数据库服务器-Oracle: （1）数据库系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）数据库系统重要数据在传输过程中采取必要的完整性保护措施。 ■SQLNET.ENCRYPTION_SERVER = REQUIRED ■SQLNET.ENCRYPTION_TYPES_SERVER = RC4_256 ■SQLNET.CRYPTO_CHECKSUM_SERVER = REQUIRED 智慧校园系统: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）系统对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议进行传输 WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2:	符合

安全控制点	测评指标	结果结论	符合程度
		（1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■使用SSH加密协议进行传输 业务终端-1、业务终端-2、运维及管理终端-1、运维及管理终端-2: （1）系统在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）操作系统重要数据在传输过程中采取必要的完整性保护措施； ■使用RDP高密级协议进行传输 （3）系统提供的数据完整性恢复措施包括能发现完整性被破坏时进行处理。 ■能实现丢弃或要求重传相应的数据 ■能实现保护措施和恢复措施有效 应用服务器-Weblogic: （1）中间件管理在通信传输过程中对相关数据采取完整性保护措施； ■包括重要配置数据 （2）中间件对重要数据在传输过程中采取必要的完整性保护措施。 ■使用HTTPS加密协议传输信息 应用服务器、数据库服务器: （1）系统在通信传输过程中对重要配置数据采取完整性保护措施。 ■使用SSH加密协议进行传输	
数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、核心交换机、汇聚交换机、运维安全管理系统、防火墙-1、防火墙-2: （1）设备定义了相关重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）设备定期完全依照备份策略，采用正确的配置进行本地备份； （4）设备的备份周期为：每月一次； （5）设备开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	符合

安全控制点	测评指标	结果结论	符合程度
		应用服务器-Weblogic: （1）系统定义了相关需要备份的中间件重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）宿主系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）中间件相关数据的备份周期合理； ■每天增量一次 ■每月全备一次 （5）中间件开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 业务终端-1、业务终端-2、应用服务器、数据库服务器、运维及管理终端-1、运维及管理终端-2: （1）操作系统定义了相关重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 智慧校园系统: （1）系统定义了相关需要备份重要数据； ■包括重要配置数据 （2）单位具备合理的重要数据的备份策略规范； （3）系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期合理：每天增量一次、每月全备一次； （5）系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。 数据库服务器-Oracle: （1）数据库系统定义了相关重要数据； ■包括重要配置数据	

安全控制点	测评指标	结果结论	符合程度
		（2）单位具备合理的重要数据的备份策略规范； （3）数据库系统定期完全依照备份策略，采用正确的配置进行本地备份； （4）系统的备份周期为：每天一次增量、每月一次全备； （5）数据库系统开展过恢复演练，具备近期能够进行正常的数据恢复的测试记录《数据恢复申请表》。	
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	WEB应用防火墙、上网行为管理系统、基线核查系统、日志审计系统、运维安全管理系统、防火墙-1、防火墙-2: （1）设备为安全设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 数据库服务器-Oracle: （1）数据库系统未能提供异地数据备份功能。 应用服务器-Weblogic、智慧校园系统: （1）单位未能提供异地数据备份措施。 业务终端-1、业务终端-2、运维及管理终端-1、运维及管理终端-2: （1）设备为终端服务器，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 应用服务器、数据库服务器: （1）设备为服务器设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。 核心交换机、汇聚交换机: （1）设备为网络设备，其鉴别数据、重要配置数据、重要审计数据在机构安全运维管理要求《备份与恢复管理制度》内数据分类的备份要求中，未定义为容灾要求高的对象，不属于需要异地备份的对象。不适用。	不符合
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	重要配置数据不存在此部分的控制需求,故此项不适用	不适用

安全控制点	测评指标	结果结论	符合程度
个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；	重要配置数据不存在此部分的控制需求,故此项不适用	不适用
	b) 应禁止未授权访问和非法使用用户个人信息。	重要配置数据不存在此部分的控制需求,故此项不适用	不适用

D.4.1.7 其他系统或设备

无

D.5 安全管理中心

D.5.1 安全通用要求

D.5.1.1 管理中心

安全控制点	测评指标	结果结论	符合程度
系统管理	a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；	（1）网络中部署运维安全管理系统实现集中的系统管理； （2）系统对登录用户进行身份鉴别； ■包括合规的用户名 ■包括合规的口令策略 （3）系统用户标识具有唯一性； ■不存在多人共享 ■增加、删除用户或权限变更需经过审批 （4）系统可实现对账户的身份鉴别数据进行保密性和完整性保护； （5）系统管理操作模式具备控制措施； ■只允许系统管理员登录 ■具备特定的登录命令 ■具备特定的登录操作界面 （6）系统具备相应的管理操作审计措施。 ■可实现对系统管理操作进行审计 ■审计范围覆盖所有用户 ■操作审计不可被删除	符合
	b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。	（1）系统管理员对系统的资源和运行进行配置、控制和管理； ■包括用户身份管理 ■包括资源配置管理 ■包括系统加载和启动管理 ■包括系统运行的异常处理管理 ■包括数据和设备的备份与恢复管理 （2）系统的资源、运行及配置管理不够全面。 ■缺乏可信证书管理 ■缺乏可信基准库管理	不符合
审计管理	a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行	（1）网络中部署运维安全管理系统实现集中安全审计功能； （2）审计系统对审计管理员进行身份鉴别；	符合

安全控制点	测评指标	结果结论	符合程度
	安全审计操作，并对这些操作进行审计；	■包括合规的用户名 ■包括合规的口令策略 （3）审计系统用户标识具有唯一性； ■不存在多人共享 ■增加、删除用户或权限变更需经过审批 （4）审计系统管理操作模式具备控制措施； ■只允许审计管理员登录 ■具备特定的登录命令 ■具备特定的登录操作界面 （5）审计系统具备相应的管理操作审计措施。 ■可实现对安全审计操作进行审计 ■审计范围覆盖所有审计管理用户 ■操作审计不可被删除	
	b）应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	智慧校园系统: （1）审计管理员定期对审计记录进行分析，对发现的安全可疑事件及时处理； （2）单位具有安全审计策略文件，规范审计记录的存储、管理和查询要求； （3）审计管理员按规范要求对审计记录进行管理。 ■审计记录不可随意删除/修改 ■定期备份、存储审计记录 ■审计记录存储周期满足6个月要求 重要审计数据: 日志审计系统、运维安全管理系统: （1）设备在通信传输过程中对相关数据采取完整性保护措施； ■包括重要审计数据 （2）设备对重要数据在传输过程中采取必要的完整性保护措施。 ■网络设备、安全设备使用rsyslog协议进行传输 ■Linux操作系统使用rsyslog协议进行传输 ■Windows操作系统使用插件+SSL协议进行传输	符合

D.6 安全管理制度

D.6.1 安全通用要求

D.6.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
安全策略	应制定网络安全工作的总体方针和安全策略，阐明	（1）单位具有网络安全工作的总体方针和安全策略文件；	符合

安全控制点	测评指标	结果结论	符合程度
	机构安全工作的总体目标、范围、原则和安全框架等。	■具备独立的网络安全总体方针文件 ■具备涵盖网络安全总体方针策略要求的相关管理文件 ■具备安全策略文件 （2）制度内容包括明确的单位安全工作要求; ■安全目标 ■安全范围 ■安全原则 ■安全框架 ■各类安全策略 （3）管理文件详见《信息安全总体策略》。	
管理制度	a）应对安全管理活动中的主要管理内容建立安全管理制度;	（1）单位有针对安全管理活动中的各类管理内容建立安全管理制度; （2）现有制度已覆盖管理活动的主要的方面; ■具备文件控制管理 ■具备安全检查管理 ■具备人力资源及培训 ■具备设备管理 ■具备软件开发/外包开发项目管理 ■具备机房安全管理 ■具备信息分类及管理 ■具备网络安全管理 ■具备系统安全管理 ■具备恶意代码管理 ■具备变更控制 ■具备备份及介质管理 ■具备事件管理 ■具备应急预案 （3）制度详见：《信息安全总体策略》、《网络安全管理规范》、《组织安全结构和人员职责制度》、《人员管理制度》、《员工考核管理制度》。	符合
	b）应对管理人员或操作人员执行的日常管理操作建立操作规程。	（1）单位针对相关业务日常管理的操作建立规程类管理制度; （2）现有制度已覆盖重要管理方面的系统维护手册和用户操作规程等; ■具备网络/安全管理 ■具备服务器管理 ■具备数据库管理 ■具备机房硬件设施管理 ■具备业务应用管理 （3）管理文件详见《设备及系统软件配置和操作手册》。	符合

安全控制点	测评指标	结果结论	符合程度
制定和发布	a) 应指定或授权专门的部门或人员负责安全管理制度的制定；	（1）单位针对安全管理制度的制定，指定教育信息与网络中心部主要负责； （2）在已制定的相关制度中可查阅到被授权制定管理制度的部门/人员信息； （3）管理文件详见《安全管理组织规范》。	符合
	b) 安全管理制度应通过正式、有效的方式发布，并进行版本控制。	（1）单位针对制度的制定和发布要求，制定管理规范文件； （2）管理规范文件对文件制定及发布定义了规范要求； ■包括安全管理制度的制定和发布程序 ■包括格式要求 ■包括版本编号要求 （3）安全管理制度的收发登记记录有效； ■具备通过正式、有效的方式收发 ■具备正式发文 ■具备领导签署、单位盖章等 （4）管理文件详见《制度制定、发布、评审和修订管理制度》、《收发文登记记录》。	符合
评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	（1）单位针对制度的合理性和适用性需进行论证和审定及修订的要求，制定管理规范文件； （2）管理规范文件对制度的评审及修订定义了规范要求； （3）单位具有安全管理制度的审定或论证的过程记录； （4）单位对做过修订的制度，具备有修订版本的安全管理过程记录； （5）管理文件详见《制度制定、发布、评审和修订管理制度》及 《安全管理制度评审记录》。	符合

D.7 安全管理机构

D.7.1 安全通用要求

D.7.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
岗位设置	a) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；	（1）单位已明确网络安全管理工作的职能部门，并明确了各岗位职责； ■已设置机房管理员 ■已设置网络管理员 ■已设置安全管理员 （2）单位各部门职责文档已明确网络安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备网络安全岗	符合

安全控制点	测评指标	结果结论	符合程度
		位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	
	b）应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。	（1）单位已明确系统安全管理工作的职能部门，并明确了各岗位职责； ■已设置系统管理员 ■已设置数据管理员 ■已设置审计管理员 ■已设置应用管理员 （2）单位各部门职责文档已明确系统安全管理工作的职能部门和各负责人职责； （3）单位各岗位职责文档已具备系统安全岗位划分情况和岗位职责的详细说明； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	符合
人员配备	应配备一定数量的系统管理员、审计管理员和安全管理员等。	（1）单位针对人员配备要求，制定了管理制度； （2）单位按要求配备一定数量的重要岗位管理人员； （3）单位针对各岗位人员，制定并维护人员档案； （4）管理文件详见《 岗位安排及岗位职责》、《组织安全结构和人员职责制度》。	符合
授权和审批	a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；	（1）单位在制度中用文字描述或在流程图中明确，对关键活动进行审批； ■具备部门职责文档明确各部门审批事项 ■具备岗位职责文档明确各岗位审批事项 （2）单位对审批过程明确审批权限，对各项信息系统的重要操作与变更明确审批部门和批准人； （3）管理文件详见《授权和审批管理规定》。	符合
	b）应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。	（1）单位针对各项业务操作及变更等建立了审批程序规定； ■包括系统变更 ■包括重要操作 ■包括物理访问 ■包括系统接入 （2）单位针对系统变更、系统接入、物理范围等事项已明确按审批程序执行,记录有批准人签字； （3）管理文件详见《授权和审批管理规定》。	符合
沟通和合作	a）应加强各类管理人员、组织内部机构和网络安全	（1）单位针对机构内部管理人员之间、部门之间的沟通与合作，制定了管理制度；	符合

安全控制点	测评指标	结果结论	符合程度
	管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；	（2）单位的管理制度规范了合作和沟通的方式和周期； （3）单位有组织机构内部人员联系表； （4）单位有定期召开信息安全会议，保存有会议纪要； （5）管理文件详见《安全教育和培训制度》、《技能培训记录》《外部联系表》。	
	b）应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；	（1）单位针对加强与外部单位的合作与沟通，制定了管理制度规定； ■包括公安机关 ■包括网络安全职能部门 ■包括职能监管机构 ■包括各类供应商 ■包括业界专家 ■包括安全组织 （2）单位能按要求与相关单位保持沟通合作，并提供相关单位联系方式和交流会议纪要； （3）管理文件详见《安全教育和培训制度》、《技能培训记录》、《外部联系表》。	符合
	c）应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	（1）单位建立了完善的对外联单位的联系列表； ■记录单位名称 ■记录合作内容 ■记录联系人 ■记录联系方式 （2）管理文件详见《外部联系表》。	符合
审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。	（1）单位针对定期开展常规安全检查，制定了管理制度； （2）单位对检查工作的范围、过程、要求等管理的比较完善； ■系统日常运行 ■系统漏洞 ■数据备份 ■包括敏感系统检查人员 （3）单位已按要求由安全管理员定期检查，检查内容需覆盖系统运行相关的管理活动，并能提供安全检查报告； （4）管理文件详见《安全审查和检查管理规范》； （5）单位开展的检查工作不够完善。 ■未定期检查	部分符合

D.8 安全管理人员

D.8.1 安全通用要求

D.8.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
人员录用	a) 应指定或授权专门的部门或人员负责人员录用；	（1）单位授权专门的部门负责人员录用工作，制定了管理制度规范； （2）由人力资源保障科负责人员录用工作； （3）管理文件详见《人员管理制度》。	符合
	b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查。	（1）单位针对人员录用过程，制定了明确要求，并形成人员安全管理制度； （2）单位现有管理制度明确说明录用人员应具备的条件； ■包括学历/学位要求 ■包括技术人员的专业技术要求 ■包括管理人员的安全管理要求 （3）单位按规定执行人员录用的相关审查过程； ■包括录用人身份 ■包括安全背景 ■包括专业资格 ■包括资质 （4）管理文件详见《人员管理制度》、《人员入职考核记录》。	符合
人员离岗	应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。	（1）单位针对离岗人员权限终止及取回机构提供的各种设施的要求，制定了管理制度； （2）单位按规范开展对离岗人员的相关管理工作； ■明确负责部门 ■及时终止其访问权限 ■交还身份证件 ■交还软硬件设备 （3）管理文件详见《人员管理度》、《人员离岗申请表》、《离场信息资料交接表》。	符合
安全意识教育和培训	应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。	（1）单位针对人员安全培训及责任和惩戒措施，制定了管理制度； （2）单位已开展安全意识教育及岗位技能培训 ■具备明确培训周期 ■具备有效的培训方式 ■具备清晰的培训内容 ■具备考核要求 （3）管理文件详见《安全教育和培训制度》。	符合
外部人员访问管理	a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；	（1）单位针对外部人员物理访问，制定了外部人员访问管理文档； ■明确允许外部人员访问的范围 ■明确外部人员进入的条件	符合

安全控制点	测评指标	结果结论	符合程度
		■明确外部人员进入的访问控制措施 （2）单位具备有效的外部人员访问重要区域的书面申请文档； ■具有申请人 ■具有申请原因 ■具有范围 ■具有日期 ■具有批准人签字 （3）单位具备外部人员访问重要区域的登记记录； ■记录进入时间、 ■记录离开时间 ■记录访问区域 ■记录陪同人信息 （4)管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。	
	b）应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；	（1）单位针对外部接入受控网络访问系统，制定了管理制度； （2）单位具备外部人员接入受控网络前的申请审批流程； （3）单位具备外部人员接入及访问系统的书面申请文档； ■具有申请人 ■具有申请原因 ■具有访问权限 ■具有日期 ■具有批准人签字 （4）单位具备外部人员接入及访问系统的登记记录； ■记录访问权限 ■记录访问时限 ■记录账户 （5)管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申请表》、《外部人员访问记录表》。	符合
	c）外部人员离场后应及时清除其所有的访问权限。	（1）单位针对人员离场后的清理工作，制定了管理制度； （2)管理文件详见《外部人员访问管理制度》、《外部服务人员管理规范》、《外部接入受控网络访问系统管理规范》、《外部人员访问申	不符合

安全控制点	测评指标	结果结论	符合程度
		请表》、《外部人员访问记录表》； （3）单位未完全按管理规范开展人员离场后的清理工作。 ■缺乏清理记录 ■未及时清除离场后的所有访问权限 ■未记录访问权限清除时间	

D.9 安全建设管理

D.9.1 安全通用要求

D.9.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
定级和备案	a）应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；	（1）单位的被测系统于2022年4月已完成备案； （2）系统备案相关文档（定级报告）中明确等级划分方法和理由，SAG三个方面的级别描述清晰； （3）管理文件详见《定级备案》。	符合
	b）应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；	（1）单位针对系统定级结果的审批及评审工作等要求，制定了管理制度； （2）现有系统的定级已具备合理性和正确性审定； ■具备单位部门审定 （3）管理文件详见《定级备案》。	符合
	c）应保证定级结果经过相关部门的批准；	（1）单位针对系统定级结果的上级批准要求，制定了管理制度； （2）现有系统的定级获得了相关部门的批准； （3）管理文件详见《定级备案》。	符合
	d）应将备案材料报主管部门和相应公安机关备案。	（1）单位对被测系统的等级备案表、定级报告等备案材料已经报相应公安机关备案； （2）单位具备公安机关出具的备案号； （3）管理文件详见《定级备案》。	符合
安全方案设计	a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；	（1）单位未具备适用于被测系统的安全规划设计方案； （2）现有方案文档未能完全按照规范要求选择安全措施。 ■缺乏安全保护等级的要求 ■缺乏风险分析结果的要求 ■缺乏实际安全需求	不符合
	b）应根据保护对象的安全保护等级进行安全方案设计；	（1）单位未具备完整的安全设计方案相关的文档。 ■缺乏总体规划 ■缺乏安全设计方案	不符合

安全控制点	测评指标	结果结论	符合程度
		■缺乏相关配套文件 ■缺乏保护对象的安全保护等级要求	
	c) 应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。	(1)单位未组织相关部门/人员对所有安全规划类文件进行论证和审定； ■缺乏安全整体规划 ■缺乏安全设计方案 ■缺乏安全配套文件 (2) 单位未对相关论证过程及内容进行完整的记录。	不符合
产品采购和使用	a) 应确保网络安全产品采购和使用符合国家的有关规定；	(1) 单位已建立安全产品管理的相关管理规定； ■包括采购要求 ■包括使用要求 (2) 单位具备安全产品采购流程及相关实施文档； (3) 被测系统使用的安全产品具备销售许可资质； (4) 安全产品具均为国内产品； (5) 管理文件详见《设备安全管理制度》。	符合
	b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。	(1) 单位已建立密码产品与服务管理的相关管理制度； ■包括采购要求 ■包括使用要求 (2) 系统未使用密码产品； (3) 管理文件详见《设备安全管理制度》。	符合
自行软件开发	a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；	(1)单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员,本测评项目不适用。	不适用
	b) 应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。	(1)单位未开展任何内部自行软件开发工作，不具备软件开发部门及人员,本测评项目不适用。	不适用
外包软件开发	a) 应在软件交付前检测其中可能存在的恶意代码；	(1) 单位针对软件交付前测试恶意代码的要求，制定了管理制度； (2)管理文件详见《外包开发软件管理规定》； (3) 单位未在软件交付之前按要求对所有软件开展恶意代码检测。 ■缺乏恶意代码检测报告	不符合
	b) 应保证开发单位提供软件设计文档和使用指南。	(1) 单位制定软件开发项目验收要求，明确开发单位的提交材料； (2) 开发单位提供软件日常维护和使用所需的文档； ■包括需求分析说明书	符合

安全控制点	测评指标	结果结论	符合程度
		■包括软件设计说明书 ■包括软件操作手册 （3）管理文件详见《外包开发软件管理规定》、《设备及系统软件配置和操作手册》。	
工程实施	a）应指定或授权专门的部门或人员负责工程实施过程的管理；	（1）单位针对专门的部门负责工程实施过程的管理要求，制定管理度； （2）单位由专岗负责系统建设的工程实施，且按照实施方案的要求对进度和质量进行控制； （3）管理文件详见《工程实施管理制度》。	符合
	b）应制定安全工程实施方案控制工程实施过程。	（1）单位制定了详细的工程实施方案； ■包括工程时间限制 ■包括进度控制 ■包括质量控制 （2）工程实施单位严格按照方案执行，并有过程记录； （3）管理文件详见《测试及验收方案》、《工程项目实施方案》。	符合
测试验收	a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；	（1）单位可提供被测系统的合规测试验收方案； ■包括测试人员 ■包括测试验收内容 ■包括现场操作过程 （2）管理文件详见《测试及验收方案》、《工程项目实施方案》； （3）单位未完全根据测试验收方案组织相关部门和人员开展验收工作。 ■缺乏验收报告 ■缺乏报告审定意见	部分符合
	b）应进行上线前的安全性测试，并出具安全测试报告。	（1）单位对系统上线前需开展安全性测试的要求，制定管理制度； （2）管理文件详见《外包开发软件管理规定》、《系统交付管理》； （3）针对系统上线前的安全性测试工作存在问题。 ■缺乏测试报告	不符合
系统交付	a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；	（1）单位具备系统交付清单； （2）系统交付清单内容较详细； ■包括设备 ■包括软件 ■包括文档 （3）单位的清点工作较合规； ■已依据交付清单开展清点工作	符合

安全控制点	测评指标	结果结论	符合程度
		（4）管理文件详见《系统交付管理》、《资产清单》。	
	b）应对负责运行维护的技术人员进行相应的技能培训；	（1）单位已对负责系统运行维护的技术人员进行了技能培训； （2）具备运维人员的培训记录； ■包括培训时间 ■包括培训地点 ■包括培训对象 ■包括培训内容 ■包括培训参与人员签字 （3）管理文件详见《系统交付管理》、《资产清单》、《系统交付清单》、《技能培训记录》。	符合
	c）应提供建设过程文档和运行维护文档。	（1）单位提供了系统建设过程中的文档； （2）单位提供了指导用户进行系统运维的文档和系统培训手册； （3）管理文件详见《系统交付管理》、《系统交付清单》、《设备及系统软件配置和操作手册》。	符合
等级测评	a）应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；	（1）单位针对系统等级测评要求，制定管理制度； （2）系统按要求开展首次测评工作； （3）管理文件详见《系统安全管理制度》。	符合
	b）应在发生重大变更或级别发生变化时进行等级测评；	（1）管理制度中已规定在系统发生变更时及时对系统进行等级测评； （2）系统未发生过重大变更，系统等级未发生变化； （3）管理文件详见《系统安全管理制度》。	符合
	c）应确保测评机构的选择符合国家有关规定。	（1）已选择在“全国等级保护测评机构推荐目录”中的测评单位进行等级测评； （2）管理文件详见《系统安全管理制度》、《网络安全等级保护测评服务合同》。	符合
服务供应商选择	a）应确保服务供应商的选择符合国家的有关规定；	（1）单位在管理制度内明确提出安全服务供应商选择的要求； （2）单位选择的安全服务商符合国家的有关规定，具备相应的安全服务资质； （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。	符合
	b）应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。	（1）单位的管理制度中已规定，需与安全服务商签订安全相关的协议并明确整个服务供应链各方需履行的网络安全相关义务； （2）单位已按规定与选定的安全服务商签订合规的协议；	符合

安全控制点	测评指标	结果结论	符合程度
		■明确整个服务供应链各方需履行的网络安全相关义务 ■包括保密范围 ■包括安全责任 ■包括违约责任 ■包括协议的有效期限 ■包括责任人签字 （3）管理文件详见《服务供应商选择安全管理制度》、《深信服安全采购合同》。	

D.10 安全运维管理

D.10.1 安全通用要求

D.10.1.1 制度文件、执行/记录文件

安全控制点	测评指标	结果结论	符合程度
环境管理	a）应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；	（1）单位建立机房安全方面的管理制度，对有关运维方面的管理作出规定； ■指定教育信息与网络中心部门负责管理 ■包括出入管理要求 ■包括定期维护要求 ■包括空调要求 ■包括供配电设备要求 ■包括消防设施要求 ■包括温湿度控制要求 （2）单位具备完整的机房出入登记记录； ■记录来访人员 ■记录来访时间 ■记录离开时间 ■记录携带物品 （3）单位具备完整的机房基础设施的维护记录； ■记录维护日期 ■记录维护人 ■记录维护设备 ■记录故障原因 ■记录维护结果 （4）管理文件详见《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。	符合
	b）应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；	（1）单位建立机房安全方面的管理制度； ■包括物理访问管理 ■包括物品进出管理 ■包括环境安全管理	符合

安全控制点	测评指标	结果结论	符合程度
		（2）单位现有机房管理记录与制度相符； ■具备物理访问记录 ■具备物品进出记录 ■具备环境安全相关记录 （3）制度详见：《机房安全管理制度》、《物理安全管理规范》、《机房出入登记表》、《机房设备维护记录表》、《机房维护日志》、《机房巡检记录表》。	
	c）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	（1）单位机房安全管理制度已明确来访人员的接待区域的要求； （2）单位按规范要求开展人员来访接待； ■划分来访人员的接待区域 ■记录来访人员的情况 （3）单位办公环境未发现有随意放置含有敏感信息介质的情况； ■无纸档文件 ■无移动介质 （4）制度详见：《机房安全管理制度》、《物理安全管理规范》、《办公环境保密管理》。	符合
资产管理	应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。	（1）单位已建立有效的资产清单； （2）单位现有资产清单内容较全面； ■包括设备设施类别 ■包括软件类别 ■包括文档类别 ■包括资产责任人 ■包括所属级别 ■包括所处位置 ■包括所处部门 （3）制度详见：《设备安全管理制度》、《资产清单》。	符合
介质管理	a）应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；	（1）介质按管理要求放置于受控的环境中（如：机房）； （2）介质管理具备较全面的记录； ■包括介质归档 ■包括使用情况 ■包括定期盘点记录 （3）制度详见：《设备安全管理制度》、《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。	符合
	b）应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并	（1）介质管理制度中对介质安全传输有明确规定； ■包括人员选择	符合

安全控制点	测评指标	结果结论	符合程度
	对介质的归档和查询等进行登记记录。	■包括打包要求 ■包括交付要求 （2）存储重要信息的介质在物理传输过程，具备严格的环节控制，无重大环节疏漏； （3）对介质的归档和查询均具备记录； （4）制度详见：《介质管理制度》、《备份介质使用记录》、《存储介质目录清单》、《信息系统存储介质使用清单》、《信息系统存储介质销毁申请表》。	
设备维护管理	a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	（1）单位人员岗位职责相关文档已明确设备维护管理的责任部门； （2）单位对各类设施、设备进行定期维护； （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。	符合
	b）应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。	（1）单位建立了配套设施、软硬件维护管理方面的管理制度； ■包括维护人员的责任 ■包括维修和服务的审批 ■包括维修过程的监督控制 （2）单位开展相关工作与制度相符，且保留记录； ■包括维修和服务审批 ■包括维修过程记录 （3）制度详见：《设备安全管理制度》、《设备维修申请表》、《机房设备维修记录表》、《设备操作维护记录》。	符合
漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。	（1）单位制定管理制度，规范对安全漏洞和隐患的检测、识别及评估修补要求； （2）制度详见：《恶意代码防范管理制度》； （3）单位未严格按规范开展漏洞及安全隐患检测工作。 ■未定期开展漏洞扫描	不符合
网络和系统安全管理	a）应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；	（1）单位建立系统安全管理文档，对系统管理员的管理制定了要求； ■包括角色划分 ■包括角色的责任 ■包括角色权限 （2）单位对各类关键角色建立了相应的工作职责文档； ■包括安全管理员 ■包括网络管理员 ■包括系统管理员	符合

安全控制点	测评指标	结果结论	符合程度
		■包括数据管理员 ■包括审计管理员 （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	
	b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	（1）单位制定管理制度，对系统账号进行管理； ■指定专人 ■包括申请账户管理 ■包括建立账户管理 ■包括删除账户管理 （2）单位按管理规范开展账号管理工作； ■具备相关审批流程 ■具备相关审批记录 ■具备管理登记记录 （3）账户管理记录内容较完整； ■包括变更日期 ■包括变更时间 ■包括变更人 ■包括变更设备/系统 ■包括变更结果 （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	符合
	c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	（1）单位建立了网络和系统安全管理制度； （2）网络和系统安全管理制度内容较全面； ■包括安全策略要求 ■包括账户管理 ■包括配置文件的生成及备份 ■包括变更审批管理 ■包括授权访问 ■包括最小服务控制 ■包括升级与打补丁管理 ■包括审计日志管理 ■包括口令管理 （3）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》。	符合
	d）应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；	（1）单位对重要设备、系统的配置和操作建立配置手册； ■包括操作系统 ■包括数据库 ■包括网络设备 ■包括安全设备 ■包括应用和组件 （2）现有操作配置手册已明确操作步骤、参	符合

安全控制点	测评指标	结果结论	符合程度
		数配置； （3）制度详见：《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。	
	e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。	（1）单位制定日常运维管理的相关制度规范； （2）单位按制度规范开展日常运维管理工作； （3）单位具备合规的运维记录； ■包括日常巡检记录 ■包括运行维护记录 ■包括参数的设置记录 ■包括参数的修改记录 （4）制度详见：《系统安全管理制度》、《网络安全管理规范》、《网络安全管理制度》、《设备及系统软件配置和操作手册》、《软硬件日常维护管理规程》。	符合
恶意代码防范管理	a）应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	（1）单位制定恶意代码防范管理制度，明确对外来计算机或存储设备接入系统前进行恶意代码检查； （2）单位按外来计算机接入恶意代码检查规范开展工作； ■对外来计算机接入进行恶意代码检查 ■具备合规的检测记录 （3）单位制定培训管理制度，明确需通过培训提升员工的防恶意代码意识； （4）单位按培训管理要求开展工作； ■定期对员工开展防恶意代码意识培训 ■具备合规的培训记录 （5）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申请表》、《信息管理系统漏洞检查表》。	符合
	b）应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；	（1）建立恶意代码防范管理文档； （2）管理制度中覆盖防恶意代码软件的授权使用、恶意代码库升级、定期查杀等内容； （3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》。	符合
	c）应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。	（1）单位指定专门的部门负责定期验证防范恶意代码攻击的技术措施的有效性； （2）单位近期未发生过严重的恶意代码攻击事件； （3）制度详见：《恶意代码防范管理制度》、《安全教育和培训制度》、《接入受控网络申请表》、《信息管理系统漏洞检查表》； （4）单位未严格按规范要求，针对防范恶意代码攻击的技术措施的有效性验证，开展工	部分符合

安全控制点	测评指标	结果结论	符合程度
		作。 ■未定期对相关产品的恶意代码库进行升级 ■未对所有防病毒产品上截获的恶意代码进行分析并汇总上报	
配置管理	应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。	（1）单位制定了基本配置信息管理的制度要求； ■包括网络拓扑结构 ■包括设备安装的软件组件 ■包括软件组件的版本 （2）管理文件详见：《主机安全管理规范》、《网络安全管理规范》、《应用安全管理规范》、《网络配置信息》。	符合
密码管理	a）应遵循密码相关国家标准和行业标准；	（1）单位不了解现有密码相关的国家标准和行业标准； （2）单位缺乏密码管理要求的制度文档。	不符合
	b）应使用国家密码管理主管部门认证核准的密码技术和产品。	（1）单位未采购涉及密码技术的产品，不适用。	不适用
变更管理	应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。	（1）单位建立了关于系统变更管理的制度文件； （2）现有变更管理制度覆盖了变更管理的各方面要求； ■包括变更管理要求 ■包括整体变更管理流程 ■包括变更内容分析与论证 ■包括变更方案审批流程 ■包括变更后通报 （3）制度详见：《变更控制管理制度》、《通用变更记录表》。	符合
备份与恢复管理	a）应识别需要定期备份的重要业务信息、系统数据及软件系统等；	（1）单位根据业务重要程度，制定了需要定期备份的重要业务信息列表或清单。清单内需要定期备份的重要数据已经过用户方确认； （2）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。	符合
	b）应规定备份信息的备份方式、备份频度、存储介质、保存期等；	（1）单位建立了备份与恢复管理相关的安全管理制度； （2）备份与恢复管理的相关要求比较明确； ■规定备份方式 ■规定备份频度 ■规定存储介质 ■规定保存期	符合

安全控制点	测评指标	结果结论	符合程度
		（3）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。	
	c）应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	（1）单位现有管理制度，明确了数据备份策略和数据恢复策略，以及备份程序和恢复程序； （2）单位可按策略要求实现重要数据的定期备份与恢复性测试； （3）单位现有的备份的数据均经过恢复性测试，可确保备份的数据可用； （4）制度详见：《数据备份策略》、《备份工作汇总表》、《数据备份记录表》、《备份与恢复管理制度》、《系统及应用数据备份管理规范》。	符合
安全事件处置	a）应及时向安全管理部门报告所发现的安全弱点和可疑事件；	（1）单位已在安全培训及宣传过程中告知用户在发现安全弱点和可疑事件时及时向安全管理部门报告； （2）单位在系统运维过程中对发现的安全弱点和可疑事件均编制了对应的报告或相关文档； （3）单位现有安全弱点和可疑事件报告文档内容较详实； （4）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	符合
	b）应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；	（1）单位制定了安全事件报告和处置管理制度； （2）现有安全事件管理制度内容较完整； ■包括安全事件类型分类 ■包括安全事件有关的工作职责 ■包括安全事件的报告 ■包括安全事件的处置 ■包括安全事件的响应流程 （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	符合
	c）应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。	（1）单位具备对安全事件的分析、处理、总结、防范等的报告／过程文档； （2）单位提供的安全事件报告和响应处置记录内容较完整； ■记录引发安全事件的原因 ■记录事件的证据 ■记录处置过程 ■包括经验教训	符合

安全控制点	测评指标	结果结论	符合程度
		■提出补救措施 （3）制度详见：《网络安全事件报告制度》、《安全事件报告和处置》。	
应急预案管理	a）应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；	（1）单位制定重要事件的应急预案； （2）单位现有应急预案涉及的类型范围较全面； ■包括针对机房的预案 ■包括针对网络传输的预案 ■包括针对网络设备的预案 ■包括针对操作系统的预案 ■包括针对数据库的预案 ■包括针对安全漏洞攻击的预案 ■包括针对恶意代码的预案 ■包括针对数据泄露的预案 （3）单位现有应急预案的内容较完整； ■明确重要事件的应急处理流程 ■明确系统恢复流程等内容 （4）制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。	符合
	b）应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。	（1）单位定期对相关人员进行应急预案培训； （2）单位根据不同的应急预案，按要求进行应急演练； （3）单位具备近期应急预案工作开展的相关记录； ■具备培训记录 ■具备演练记录 （4）单位提供的应急预案培训记录比较完整； ■明确培训对象 ■明确培训内容 ■明确培训结果 （5）单位提供的应急预案演练记录比较完整； ■记录演练时间 ■记录主要操作内容 ■记录演练结果 （6）经检查单位目前一旦出现应急事件，可参照预案合理有序的进行应急事件处置过程； （7）制度详见：《网络安全事件应急预案》、《应急预案培训记录表》。	符合
外包运维管理	a）应确保外包运维服务商的选择符合国家的有关规定；	（1）单位目前未涉及任何外包运维服务情况，不适用。	不适用
	b）应与选定的外包运维服务商签订相关的协议，明	（1）单位目前未涉及任何外包运维服务情况，不适用。	不适用

安全控制点	测评指标	结果结论	符合程度
	确约定外包运维的范围、工作内容。		

D.11 其他安全要求

本次测评不涉及其他安全要求指标。

附录E 漏洞扫描结果记录

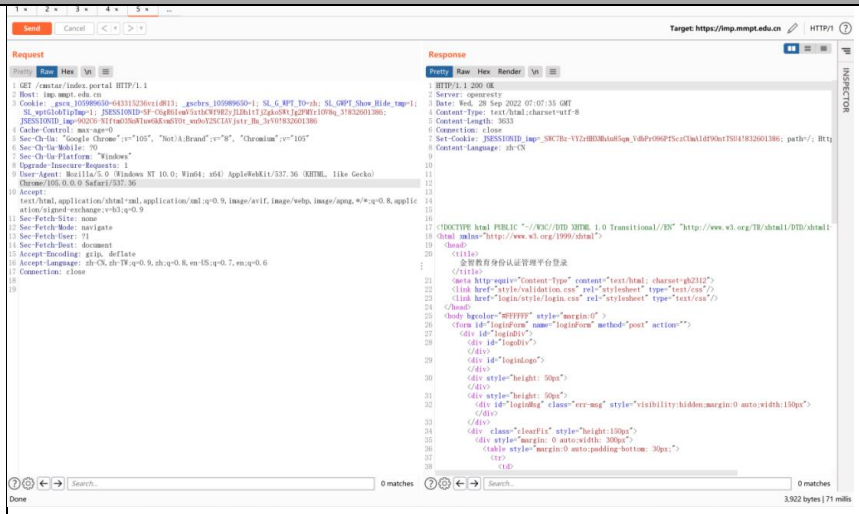
附录E表-1漏洞扫描主要安全漏洞

序号	危险程度	漏洞名称	影响IP
1	低	SSH版本信息可被获取 此类漏洞涉及服务器存储设备。	10.1.8.10/数据库服务器 10.1.8.17/应用服务器
2	低	允许Traceroute探测 此类漏洞涉及网络设备、安全设备、服务器存储设备。	10.1.8.17/应用服务器 10.1.8.10/数据库服务器 10.2.1.4/运维安全管理系统 10.2.1.2/日志审计系统 10.2.1.3/基线核查系统 172.16.1.14/上网行为管理系统 172.16.1.18/WEB应用防火墙 172.16.1.1/防火墙-2,防火墙-1 172.16.1.19/汇聚交换机 172.16.1.2/核心交换机
3	低	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161) 此类漏洞涉及网络设备。	172.16.1.2/核心交换机

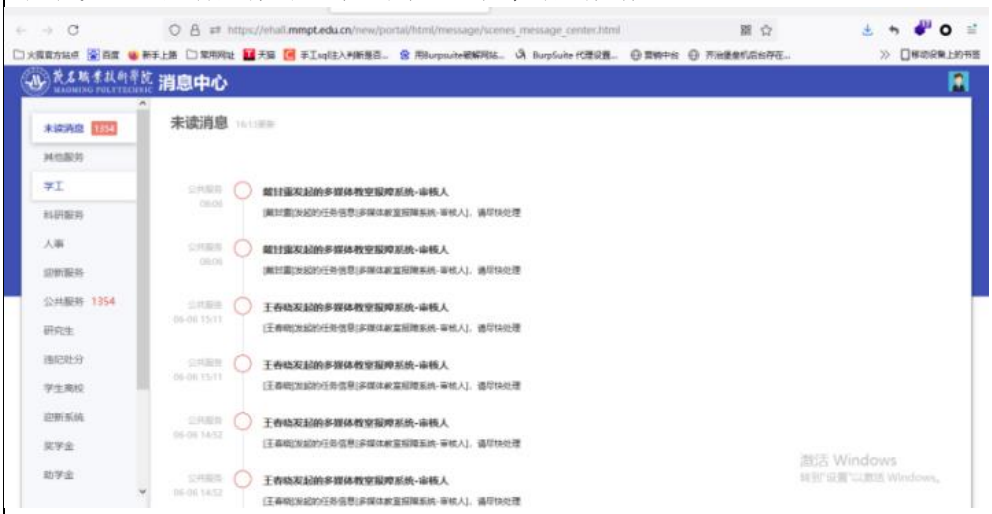
附录F 渗透测试结果记录

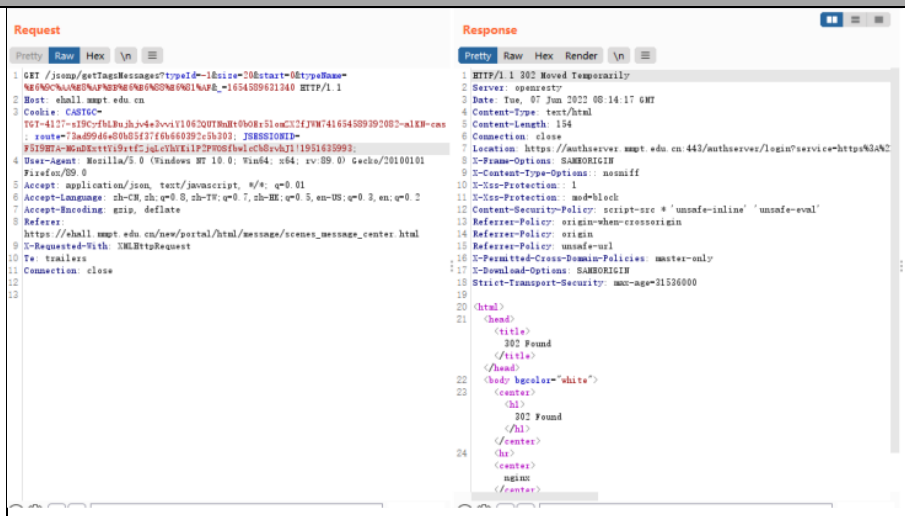
F.1 业务应用软件平台 缺少“Content-Security-Policy”响应头

缺少“Content-Security-Policy”响应头	
危险程度	低
渗透位置	JA,JB,JC
影响URL实体	https://ehall.mmpt.edu.cn/jsonp/ywtb/home/getPortalInfoNew?pageCode=Lite_home&_=1664345401039
渗透详情	渗透方法：使用BurpSuite抓包查看响应头未包含Content-Security-Policy字段： 采用的工具：BurpSuite 测试过程：使用BurpSuite抓包查看响应头未包含Content-Security-Policy字段：

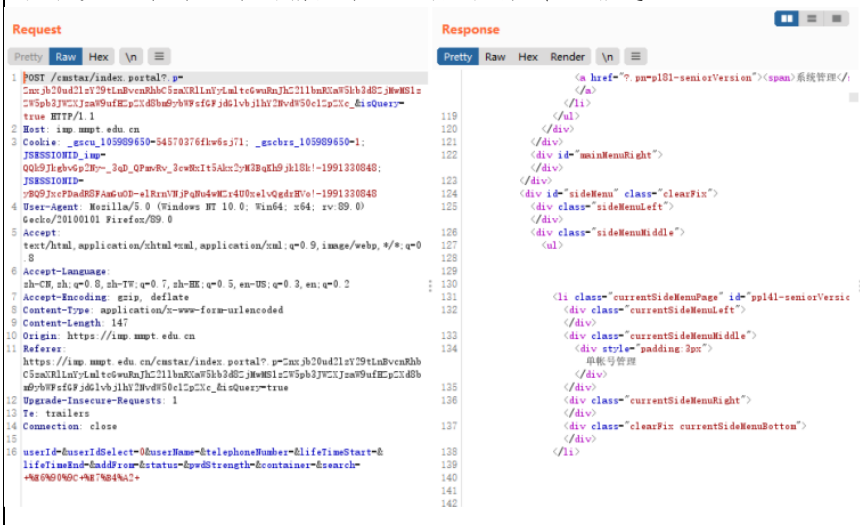
缺少“Content-Security-Policy”响应头


F.2 业务应用软件平台 越权访问

越权访问	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：测试能否对非当前用户权限的界面及功能进行访问操作。 采用的工具：BurpSuite 测试过程：尝试访问其他用户的个人通知，访问失败。 

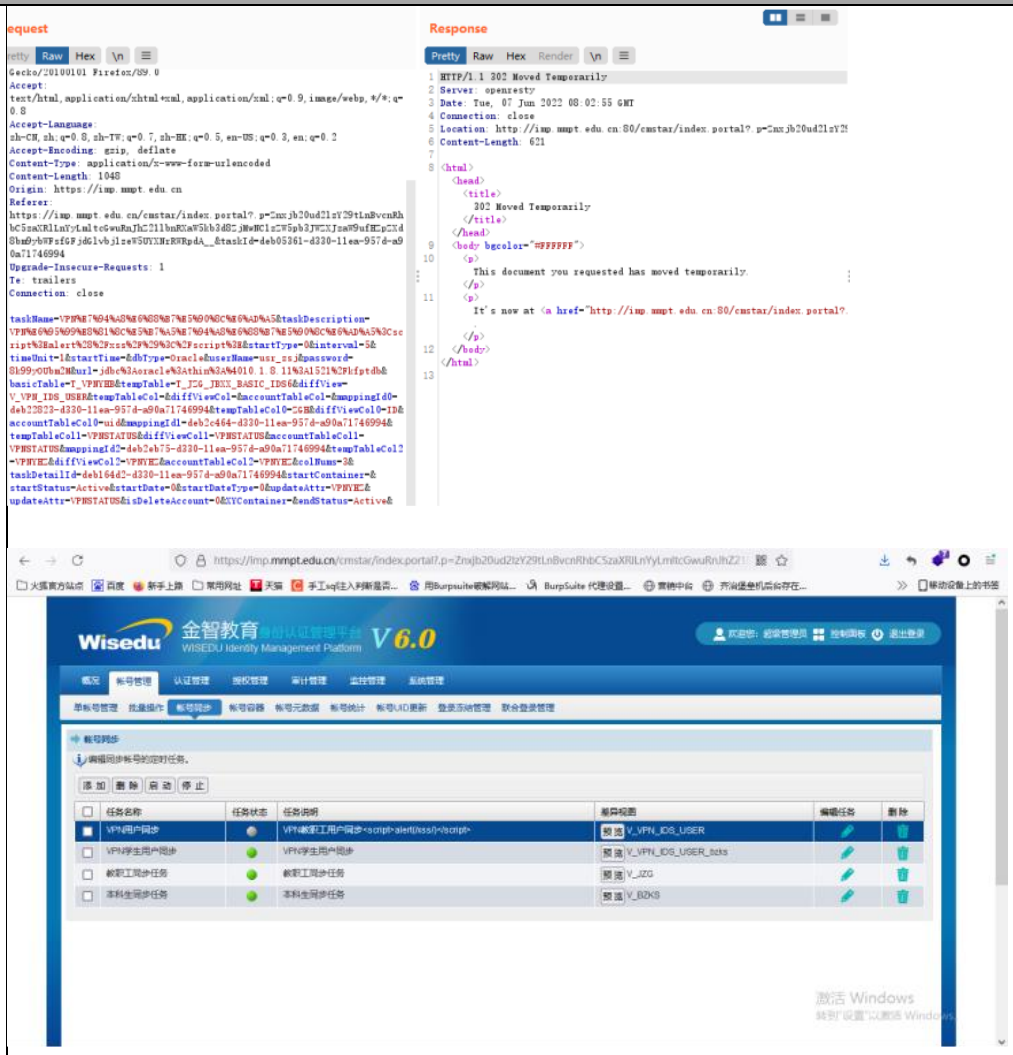
越权访问	
	

F.3 业务应用软件平台 未授权访问

未授权访问	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：测试能否在系统未登录的状态下进行登录后功能访问或操作。 采用的工具：BurpSuite 测试过程：在未登录的情况下无法访问用户管理信息。 

F.4 业务应用软件平台 XSS跨站脚本攻击

XSS跨站脚本攻击	
渗透位置	暂未发现此漏洞
测试详情	渗透方法：测试是否对客户端输入的HTML代码、客户端脚本进行过滤或限制。 采用的工具：Burpsuite 测试过程：在浏览器的url，系统的查询框或者新增数据处插入payload检测是否修改js，检测是否可以篡改js进行弹窗。

XSS跨站脚本攻击


附录G 威胁列表

附录G 表- 1威胁列表

序号	威胁列表	描述
1	恶意攻击	利用工具和技术对信息系统进行攻击和入侵。威胁行为包括：恶意代码、邮件勒索、网络攻击等。
2	软硬件故障	对业务实施或系统运行产生影响的设备硬件故障、通讯链路中断、系统本身或软件缺陷造等问题。威胁行为包括：设备故障、软件故障等。
3	管理不到位	由于制度缺失、不完善等原因导致安全管理无法落实或者不到位。威胁行为包括：管理不到位、媒体负面报道等。
4	无作为或操作失误	应该执行而没有执行相应的操作，或者无意执行了错误的操作。威胁行为包括：操作失误、维护错误等。
5	敏感信息泄漏	敏感信息泄露给不应了解的他人。威胁行为包括：内部信息泄露、外部信息泄露等。
6	物理环境影响	对信息系统正常运行造成影响的物理环境问题和自然

序号	威胁列表	描述
		灾害。威胁行为包括：物理损害等。
7	越权或滥用	越权访问本来无权访问的资源，或者滥用自己的权限破坏信息系统。威胁行为包括：未授权的设备使用、权限滥用、权限伪造等。
8	物理攻击	通过物理的接触造成对软件、硬件和数据的破坏。威胁行为包括：设备失效等。
9	篡改	非法修改信息，破坏信息的完整性使系统的安全性降低或信息不可用。威胁行为包括：硬件篡改、数据篡改等。
10	抵赖	否认所做的操作。威胁行为包括：行为否认（抵赖）、媒体负面报道等。

信息系统安全等级保护

备案证明

依据《信息安全等级保护管理办法》的有关规定，茂名职业技术学院单位的：

第二级OA系统

予以备案。

证书编号：44090243008-00008

中华人民共和国公安部监制

备案公安机关公章

2021年4月27日

茂名市公安局 信息安全等级保护专用章

信息系统安全等级保护
备案证明

依据《信息安全等级保护管理办法》的有关规定，茂名职业技术学院单位的：

第二级财务管理系统

予以备案。

证书编号：44090243008-00003

中华人民共和国公安部监制

备案公安机关公章

2024年1月27日

信息系统安全等级保护
备案证明

依据《信息安全等级保护管理办法》的有关规定，茂名职业技术学院单位的：

第二级档案管理系统

予以备案。

证书编号：44090243008-00007

中华人民共和国公安部监制

备案公安机关公章

2022年1月7日

信息系统安全等级保护
备案证明

依据《信息安全等级保护管理办法》的有关规定，茂名职业技术学院单位的：

第二级教学管理信息服务平台系统

予以备案。

证书编号：44090243008-00006

中华人民共和国公安部监制

备案公安机关公章

2021年4月27日

信息系统安全等级保护备案证明

依据《信息安全等级保护管理办法》的有关规定，茂名职业技术学院单位的：

第二级科研创新信息化管理系统予以备案。

证书编号：44090243008-00005

中华人民共和国公安部监制

备案公安机关公章

2024年1月27日

信息系统安全等级保护
备案证明

依据《信息安全等级保护管理办法》的有关规定，茂名职业技术学院单位的：

第二级门户网站系统

予以备案。

证书编号：44090243008-00001

备案公安机关公章

2021年3月1日

中华人民共和国公安部监制

信息系统安全等级保护
备案证明

依据《信息安全等级保护管理办法》的有关规定，茂名职业技术学院单位的：

第二级招生信息网系统

予以备案。

证书编号：44090243008-00004

中华人民共和国公安部监制

备案公安机关公章

2021年4月27日

信息系统安全等级保护

备案证明

依据《信息安全等级保护管理办法》的有关规定，茂名职业技术学院单位的：

第二级智慧校园系统予以备案。

证书编号：44090243008-00002

中华人民共和国公安部监制

备案公安机关公章

2020年7月27日

茂名职业技术学院纪要

（24）

茂名职业技术学院　　2021年12月2日

茂名职业技术学院
2021年第24次院长办公会议纪要

2021年11月26日上午，学院在北校区综合楼三楼第一会议室召开了今年第24次院长办公会议。会议审议《茂名职业技术学院干部人事档案专项审核工作实施方案》；审议向茂名市茂南区学信教育培训中心支付联合办学经费的申请（成人专科）；审议向江门市新会机电职业技术学校支付联合办学经费的申请（高技能人才学历提升计划）；审议关于聘请学校常年法律顾问事项；审议南

校区 4 号宿舍楼消防泵房维修改造项目；审议南校区 7 号教学楼电房增设开关柜项目；审议废止《茂名职业技术学院教研科研成果奖励试行办法》（茂职院〔2012〕39 号）；审议关于发放 2020 年 9 月、2021 年 3 月及 2021 年 9 月全国计算机等级考试考务费的申请；审议服兵役学生学费补偿、减免资助发放事项；审议 2021-2022 学年新生资助评审结果及资金发放事项；审议 2020-2021 学年先进班集体、三好学生、优秀学生干部、优秀学生奖学金名单及资金发放事项；审议 2021-2022 学年国家助学金候选学生名单及资金发放事项；审议支付教科网租赁服务费事项；审议网络安全等级保护测评采购项目；审议 2021 年多媒体教室大屏显示项目；审议向茂名市茂南区学信教育培训中心支付联合办学经费的申请（高技能人才学历提升计划）；审议向广州远智教育科技有限公司支付联合办学经费的申请（高技能人才学历提升计划）；审议向茂名市高级技工学校支付联合办学经费的申请（社会人员学历提升计划）；审议向东莞市莞城区华泰教育培训中心有限公司支付联合办学经费的申请（社会人员学历提升计划）；审议向深圳市嘉文教育培训中心支付联合办学经费的申请（社会人员学历提升计划）；审议向茂名市茂南区城南成人教育培训中心支付联合办学经费的申请（成人专科）；审议联合开展专业技能证书培训合同（凤鸣九天（肇庆）教育科技有限公司）；审议《茂名职业技术学院内部审计管理规定》。会议纪要如下：

一、审议通过《茂名职业技术学院干部人事档案专项审核工作实施方案》，由人事处提交党委会研究。

二、会议审议了向茂名市茂南区学信教育培训中心支付联合办学经费的申请(成人专科)。根据双方联合办学协议及补充协议，会议同意向茂名市茂南区学信教育培训中心支付联合办学经费8.004万元（支付的联合办学经费为所收学费总额的80%)。

三、会议审议了向江门市新会机电职业技术学校支付联合办学经费的申请（高技能人才学历提升计划)。根据双方联合办学协议，会议同意向江门市新会机电职业技术学校支付联合办学经费7.2万元（支付的联合办学经费为所收续费总额的80%)。

四、会议审议了聘请学校常年法律顾问事项。会议经研究，同意聘请广东海日律师事务所为学校提供法律顾问服务，聘请该律师事务所阮传欣、卢艺、邓耀洲3位律师组成的法律顾问团担任学校常年法律顾问，法律顾问服务费预算为5万元/年，服务期1年，相关服务采购事项按学校中介服务机构采购相关规定执行。

五、审议同意南校区4号宿舍楼消防泵房维修改造项目，经费预算5.24255万元，从基建经费——其他项目支出。

六、审议同意南校区7号教学楼电房增设开关柜项目，经费预算6.567万元，从基建经费——其他项目支出。

七、审议同意废止《茂名职业技术学院教研科研成果奖励试行办法》(茂职院〔2012〕39号)。会议要求，在制定新的管理办法时要综合考虑在教学、科研、社会服务等方面的激励作用；在新的管理办法出台前，教务处要统筹做好各方面的衔接，避免出现激励的空档期对学校教研科研等方面造成影响。

八、会议审议了关于发放2020年9月、2021年3月及2021年9月全国计算机等级考试考务费的申请议题。会议经审议，因发放考务费的校外人员有公务员身份人员，为进一步核准发放人员范围及资格，会议决定，暂缓通过本次发放2020年9月、2021年3月及2021年9月全国计算机等级考试考务费的申请。由教务处根据相关规定，进一步核准相关情况后，再提交院长办公会研究。

九、审议通过服兵役学生学费补偿、减免资助发放事项。经审核，符合服兵役学生学费补偿及减免资助条件学生共计186人（其中毕业生应征入伍服兵役学生47人，在校生应征入伍学生46人，退役复学学生93人），合计发放学费补偿、学费减免费用189.764万元，从应征入伍服义务兵学费补偿资助款支出。

十、审议通过2021-2022学年新生资助评审结果及资助资金发放事项。经审核，符合2021-2022学年新生资助条件学生177人，合计发放新生资助资金17.7万元，从学院助学金支出。

十一、审议通过2020-2021学年先进班集体、三好学生、优秀学生干部、优秀学生奖学金名单及资金发放事项。经评审，2020-2021学年先进班集体7个、三好学生67名，优秀学生干部269名，优秀学生一等奖学金78名、二等奖学金281名、三等奖学金689名，合计发放奖金46.662万元，从学院奖学金支出。

十二、审议通过2021-2022学年国家助学金候选学生名单及资金发放事项。经评审，2021-2022学年国家助学金学生人数2206人，合计发放国家助学金371.41万元，从国家助学金项目支出。

十三、会议审议了支付教科网租赁服务费事项。鉴于教信中心2021年申报的“智能网络设备管理平台”项目无法推进，会议同意终止“智能网络设备管理平台”项目建设，同意从该项目原预算（22万元）调整10.8万元用于支付教科网租赁服务费。

十四、会议审议了网络安全等级保护测评采购项目。同意立项建设网络安全等级保护测评项目，经费预算38万元，从原“智能网络设备管理平台”项目预算调整4.8万元用于网络安全等级保护测评项目前期“定级备案服务”，剩余建设经费从2022年经费预算支出。

十五、审议同意2021年多媒体教室大屏显示项目，经费预算14.2万元，从2021年教室大屏显示项目资金支出。

十六、会议审议了向茂名市茂南区学信教育培训中心支付联合办学经费的申请（高技能人才学历提升计划）。根据双方联合办学协议，会议同意向茂名市茂南区学信教育培训中心支付联合办学经费34.8万元（支付的联合办学经费为所收学费总额的80%）。

十七、会议审议了向广州远智教育科技有限公司支付联合办学经费的申请（高技能人才学历提升计划）。根据双方联合办学协议，会议同意向广州远智教育科技有限公司支付联合办学经费20.32万元（支付的联合办学经费为所收学费总额的80%）。

十八、会议审议了向茂名市高级技工学校支付联合办学经费的申请（社会人员学历提升计划），根据双方联合办学协议，会议同意向茂名市高级技工学校支付联合办学经费18.4万元（支付的联合办学经费为所收学费总额的80%）。

十九、会议审议了向东莞市莞城区华泰教育培训中心有限公司支付联合办学经费的申请（社会人员学历提升计划），根据双方联合办学协议，会议同意向东莞市莞城区华泰教育培训中心有限公司支付联合办学经费32.48万元（支付的联合办学经费为所收学费总额的80%）。

二十、会议审议了向深圳市嘉文教育培训中心支付联合办学经费的申请（社会人员学历提升计划），根据双方联合办学协议，会议同意向深圳市嘉文教育培训中心支付联合办学经费19.84万元（支付的联合办学经费为所收学费总额的80%）。

二十一、会议审议了向茂名市茂南区城南成人教育培训中心支付联合办学经费的申请（成人专科），根据双方联合办学协议及补充协议，会议同意向茂名市茂南区城南成人教育培训中心支付联合办学经费11.975813万元（支付的联合办学经费为所收学费总额的75%）。

二十二、审议通过联合开展专业技能证书培训合同（凤鸣九天（肇庆）教育科技有限公司）。

二十三、原则通过《茂名职业技术学院内部审计管理规定》。由纪监审室根据会议意见修改完善后于2022年1月1日起实施。会议要求，纪监审室要梳理学校与审计相关的各项规章制度，按照省关于审计最新要求进行修订后，报学校研究。

以上议题经院长办公会审议通过后，按规定需提交党委会讨论决定的，由议题提请部门提交党委会讨论决定。

参加：扶国、张庆、罗卫东、谈毅、杨云、钟茹、曾萍。

列席：全程列席会议：谭清、梁晓、陈景宜、梁亚成。具体议题列席人员如下：审议《茂名职业技术学院干部人事档案专项审核工作实施方案》：周智；审议向茂名市茂南区学信教育培训中心支付联合办学经费的申请（成人专科）：杨海、朱颖颖；审议向江门市新会机电职业技术学校支付联合办学经费的申请（高技能人才学历提升计划）：杨海、朱颖颖；审议关于聘请学校常年法律顾问事项：梁亚成、朱颖颖；审议南校区 4 号宿舍楼消防泵房维修改造项目：钟球、朱颖颖、陈耀；审议南校区 7 号教学楼电房增设开关柜项目：钟球、朱颖颖、陈耀；审议废止《茂名职业技术学院教研科研成果奖励试行办法》（茂职院〔2012〕39 号）：孙国勇；审议关于发放 2020 年 9 月、2021 年 3 月及 2021 年 9 月全国计算机等级考试考务费的申请：彭勇、朱颖颖；审议服兵役学生学费补偿、减免资助发放事项：谢深根、朱颖颖；审议 2021-2022 学年新生资助评审结果及资助资金发放事项：谢深根、朱颖颖；审议 2020-2021 学年先进班集体、三好学生、优秀学生干部、优秀学生奖学金名单及资金发放事项：谢深根、朱颖颖；审议 2021-2022 学年国家助学金候选学生名单及资金发放事项：谢深根、朱颖颖；审议支付教科网租赁服务费事项：叶永利、朱颖颖、陈耀；审议网络安全等级保护测评采购项目：叶永利、朱颖颖、陈耀；审议 2021 年多媒体教室大屏显示项目：叶永利、朱颖颖、陈耀；审议向茂名市茂南区学信教育培训中心支付联合办学经费的申请（高技能人才学历提升计划）：杨海、朱颖颖；审议向广州远智教育科技有限公司支付联合办学经费的申请（高技能人才学

历提升计划）：杨海、朱颖颖；审议向茂名市高级技工学校支付联合办学经费的申请（社会人员学历提升计划）：杨海、朱颖颖；审议向东莞市莞城区华泰教育培训中心有限公司支付联合办学经费的申请（社会人员学历提升计划）：杨海、朱颖颖；审议向深圳市嘉文教育培训中心支付联合办学经费的申请（社会人员学历提升计划）：杨海、朱颖颖；审议向茂名市茂南区城南成人教育培训中心支付联合办学经费的申请（成人专科）：杨海、朱颖颖；审议联合开展专业技能证书培训合同（凤鸣九天（肇庆）教育科技有限公司）：梁辉良、朱颖颖；审议《茂名职业技术学院内部审计管理规定》：梁亚成。

公开方式：依申请公开

分送：学院领导，各系（部）、各部门。

茂名职业技术学院办公室　　2021年12月2日印发

茂名职业技术学院招标采购立项申报表

<table>
<tr><td>项目名称</td><td colspan="5">茂名职业技术学院网络安全等级保护测评项目</td></tr>
<tr><td>采购分类</td><td colspan="5">服务</td></tr>
<tr><td>预算金额</td><td colspan="2">学院资金： ￥ 48,000.00 元</td><td colspan="3">财政资金 ￥ 332,000.00 元</td></tr>
<tr><td rowspan="6">资金来源</td><td>资金科目或批文名称</td><td colspan="4">智能网络设备管理平台</td></tr>
<tr><td>上传附件（word、excel或pdf）</td><td colspan="4">茂名职业技术学院网络安全等级保护测评项目方案（20211026）.doc(116KB)

茂名职业技术学院网络安全等级保护测评项目合同书.doc(51KB)

茂名职业技术学院网络安全等级保护测评项目-论证书.pdf(2MB)</td></tr>
<tr><td colspan="5">备注：1.此为必填项，名称须具体。2.属上级财政的须提供原版文件或批文复印件</td></tr>
<tr><td>付款方式是否有特殊要求</td><td colspan="4"></td></tr>
<tr><td>采购需求部门负责人意见</td><td>拟同意，请领导批示。
[叶永利 2021-12-06]</td><td>经费管理部门负责人意见</td><td colspan="2">项目经费有预算安排
[吴栋 2021-12-07]</td></tr>
<tr><td>资产管理部门负责人意见</td><td>拟同意立项采购
[吴栋 2021-12-07]</td><td>财务处负责人意见</td><td colspan="2">拟同意
[朱颖颖 2021-12-07]</td></tr>
<tr><td>招标办公室负责人意见</td><td colspan="2">根据学校招标采购管理办法，并结合本项目实际，拟采用竞争性磋商方式采购。
[陈耀 2021-12-07]</td><td>学院办公室负责人意见</td><td colspan="2">拟同意。
[陈景宜 2021-12-08]</td></tr>
<tr><td>纪检监察审计室负责人意见</td><td colspan="2">已阅
[梁亚成 2021-12-09]</td><td>需求部门分管校领导审签</td><td colspan="2">【同意】
[杨云 2021-12-09]</td></tr>
<tr><td>分管资产校领导审签</td><td colspan="2">【同意】
[谈毅 2021-12-09]</td><td>分管招标校领导审签</td><td colspan="2">【同意】
[罗卫东 2021-12-09]</td></tr>
<tr><td>校长审批</td><td colspan="5">【同意】
[张庆 2021-12-09]</td></tr>
</table>

茂名职业技术学院合同（协议）审批表

经办部门：教育技术与网络中心　经办人：吴国华　送审日期：2022-02-13

合同名称	茂名职业技术学院网络安全等级保护测评项目采购合同书	合同编号	MZY2022-024
甲方全称	茂名职业技术学院	乙方全称	中国移动通信集团广东有限公司茂名分公司
合同文本	茂名职业技术学院网络安全等级保护测评项目（未用印）.pdf(3MB)		
合同类型	货物服务采购及资产处置合同	合同期限	12个月

合同应收款项	应收金额/分成比例	应收日期/期限	应收催款责任人	其他应收说明
	无	无	无	

合同应付款项	应付总额	应付日期/期限	经费来源	专项经费使用期限
	368000	2022年12月31日	学院自筹+专项	2022年12月31日

项目批文/会议纪要	招标采购立项申报表.pdf(269KB) 茂名职业技术学院2021年第24次院长办公会议纪要.PDF(321KB)
中标（成交）通知书/采购记录 （如无，则不需上传）	成交通知书.jpg(251KB)
资格/资质/收费标准等证明文件	备注：除学校集中采购项目合同外，其他委托、合作项目合同应上传合同相对方证明文件（如身份证、营业执照、经营许可、职业资格、收费许可或收费标准等证明文件（盖章）扫描件）
经办单位（部门）审核意见	同意，请领导批示。 [叶永利 2022-02-20]
合同管理部门初审意见	已核。合同编号见审批表。 [曾薇 2022-02-21]
相关职能部门审核意见	已阅。 [陈景宜 2022-02-21] 已阅 [朱颖颖 2022-02-21]
合同管理部门审核意见	拟同意 [梁亚成 2022-02-22]
分管领导审核意见	【同意】 [谈毅 2022-02-22] 【同意】 [杨云 2022-02-22] 【同意】 [罗卫东 2022-02-22]
学校法定代表人审批	【同意】 [张庆 2022-02-22]

茂名职业技术学院

网络安全等级保护测评项目

采 购 合 同 书

采购编号：MZY2021NBZB066

项目名称：茂名职业技术学院网络安全等级保护测评项目

甲方：茂名职业技术学院

乙方：中国移动通信集团广东有限公司茂名分公司

茂名职业技术学院（以下简称甲方）与 中国移动通信集团广东有限公司茂名分公司 （以下简称乙方）本着严谨负责、诚实信用、真诚合作的原则，经友好协商，按照中华人民共和国相关法律法规规定，现就茂名职业技术学院网络安全等级保护测评项目事宜达成如下协议，共同订立合同如下：

一、项目名称

茂名职业技术学院网络安全等级保护测评项目

二、项目内容及服务范围

1、项目内容：按照国家相关信息安全等级保护标准及其它标准，乙方为甲方指定的信息系统进行网络安全等级保护测评服务，提交符合公安部网络安全等级保护测评报告格式要求的《网络安全等级保护测评报告》（报告须加盖具备等级保护测评资质机构印章）具体如下：

（1）风险梳理服务。对甲方指定的信息系统提供资产核查、风险识别服务。若判定系统安全防护能力无法达到相应级别或要求，则提交《整改问题清单》或《风险梳理报告》。

（2）网络等级保护测评服务。对本项目服务范围中的 8 个二级系统开展网络安全等级保护测评服务，提交符合公安部网络安全等级保护测评报告格式要求的《网络安全等级保护测评报告》。

3、服务范围及内容：

序号	系统名称	服务名称	服务内容
1	1、招生信息网 2、智慧校园系统 3、门户网站系统 4、档案管理系统 5、科研创新信息化管理系统	定级备案服务	对拟定的信息系统进行定级备案材料梳理，出具等级保护定级专家评审意见，协助网监备案服务；

2	6、财务管理系统 7、教学管理信息服务平台 8、OA 系统 备注：拟定二级信息系统，硬件设备 80 台以内，需渗透测试服务	等级保护测评	1、安全等级保护差距测评（二级）服务 2、安全等级保护验收测评（二级）服务 3、使用漏洞扫描工具对业务系统、服务器进行漏洞扫描，并对扫描结果进行人工分析，验证漏洞真伪 4、信息系统进行渗透测试服务

三、双方权利和义务

1、甲方的权利和义务

甲方应按约定的时间和要求完成以下工作：

（1） 安排专人协助乙方进行网络安全服务工作；

（2） 向乙方提供网络安全服务所需的真实、准确、完整的文件、资料，参与配合网络安全服务工作，甲方对其提供文件的真实性、合法性负责；

（3） 若系统需要整改，甲方应请具备资质的第三方单位或自行完成系统整改加固；

（4） 确保不干预乙方报告结论。

（5） 按照本合同约定按时支付合同款项。

2、乙方的权利和义务

乙方应按约定时间和要求，完成以下工作：

（1） 负责按合同实施进度完成本服务项目的各项工作；

（2） 负责按网络安全相关标准具体要求，提供风险梳理服务、等级保护测评服务；

（3）提交《网络安全等级保护测评报告》。

四、合同周期及实施计划

1、合同自签字盖章生效之日起 12 个月内有效。

2、实施计划：

（1）自双方签订合同后，15 天内完成服务内容的第一项“定级备案服务”，并出具等级保护定级专家评审意见，达到网监备案服务的要求；

（2）自双方签订合同后，120 天内完成服务内容的第二项“等级保护测评”，并提供符合公安部网络安全等级保护测评报告格式要求的《网络安全等级保护测评报告》。

五、服务费及支付方式

一、服务费总金额为（大写）人民币：叁拾陆万捌仟万元整，（￥368000.00元）。

二、支付方式:

1、本合同签订生效之日起 30 日内，乙方完成服务内容的第一项“定级备案服务”，并出具等级保护定级专家评审意见，达到网监备案服务的要求，经甲方检查合符要求后，甲方向乙方支付“定级备案服务”费，金额（大写）人民币：肆万捌仟元整，（￥48,000.00 元）。

2、乙方完成本合同约定的等级保护测评工作后，提交符合公安部网络安全等级保护测评报告格式要求的《网络安全等级保护测评报告》之日起 30 日内，甲方向乙方支付本合同剩余款，金额(大写)人民币：叁拾贰万元整（￥320000.00元)。

3、甲方全额支付上述款项前，乙方向甲方开具合法有效的等额发票。

4、乙方收款账户信息：

开户名称：中国移动通信集团广东有限公司茂名分公司

开户银行：中国工商银行股份有限公司广州粤秀支行

账号：9558853602004561345

六、违约责任

1、由于乙方单方面的原因造成服务延期完成的，逾期超过 15 日后，乙方每日向甲方支付合同总金额的 3‰的违约金，违约金总额不超过合同总金额的百分之十；逾期一个月以上的，甲方有权终止合同，由此造成的甲方经济损失由乙方承担。但因甲方未配合提供资料等非乙方原因造成的延期完成，乙方不承担违约责任。

2、由于甲方单方面的原因造成服务延期完成的，或者因甲方原因造成逾期

付款的，逾期超过 15 日后，甲方每日向乙方支付合同总金额的 3‰的违约金，违约金总额不超过合同总金额的百分之十；逾期一个月以上的，乙方有权终止合同，由此造成的乙方经济损失由甲方承担。

七、保密条款

1、在本合同订立前、履行中、终止后，未经合同其他方书面同意，任何一方对本合同和各方相互提供的资料、信息（包含但不限于工作秘密、内部管理制度、安全措施、技术资料、图纸、数据以及与业务有关的客户的信息及其他信息等）负保密责任，不得向任何第三方披露上述资料和信息，但正常履行本合同项下义务的除外。

2、乙方在项目执行期间，必须遵守甲方规定的保密规章、制度，履行与其工作岗位相应的保密职责，未经甲方允许，不得利用工作之便了解、获取、泄露甲方的内部情况、信息系统内部数据及信息。

3、甲方的保密规章、制度没有规定或者规定不明确之处，乙方亦应本着谨慎、诚实的态度，采取任何必要、合理的措施，维护其于该期间知悉或者持有的任何属于甲方或者虽属于第三方但甲方承诺有保密义务的资料、数据及信息。

4、任何一方违反上述约定的，责任方应承担由此引起的一切法律责任，并按本合同约定的违约责任条款支付违约金，违约金不足以赔偿合同另一方损失的，责任方应对合同另一方的实际损失进行赔偿。

5、其他相关保密义务约定参见双方签订的协议附件《保密协议》。

八、风险揭示与承诺

1、甲方授权乙方进行现场服务。乙方在甲方的许可和配合下，将利用安全检测工具或相关技术手段，对甲方的网络及信息系统进行安全服务。

2、在测试之前，乙方应及时与甲方技术人员协商沟通，在相关数据已经备份，不影响甲方正常业务开展并得到甲方技术人员认可的前提下开展服务工作。

3、如果在授权测试期间发生上述风险，乙方应配合甲方进行原因分析。如确认是乙方服务导致上述风险的发生，乙方将承担相应的法律责任并赔偿相应损失；如果与服务活动无关，则由甲方承担上述风险导致的法律责任和经济损失。

4、测评报告测评结论的有效性建立在被测评单位提供相关证据的真实性基础之上。报告中给出的测评结论仅对被测信息系统当时的安全状态有效。当测评

工作完成后，由于信息系统发生变更而涉及到的系统构成组件（或子系统）都应重新进行测评，本报告不再适用。

九、争议解决方式

凡与本合同有关的一切争议，甲乙双方首先通过友好协商的方式加以解决；若协商后仍未能达成一致，任何一方均可向乙方所在地人民法院提出诉讼。

十、其他

1、本合同自双方法定代表人（或委托代理人）签字盖章之日起生效，至合同义务履行完毕之日起终止（保密义务除外）。

2、本合同未尽事宜，由双方协商解决。

3、本合同正本一式陆份，甲方肆份，乙方贰份，均具同等法律效力。

甲方：茂名职业技术学院

签约代表：

签约日期：2022年2月23日

乙方：中国移动通信集团广东有限公司茂名分公司

签约代表：

经办人：

签约日期：　　年　　月　　日

广东增值税电子普通发票

发票代码:044001631111
发票号码:42002555
开票日期: 2022 年11 月29日
校 验 码:74965 55730 00308 77449

机器编号: 661616301184

购买方	名　　称: 茂名职业技术学院 纳税人识别号: 12440900456408565M 地 址、电 话: 茂名市文明北路232号 0668-2920026 开户行及账号: 中国建设银行股份有限公司茂名文明北路分理处,44001690311051434400	密码区	73474<-4>9031<34+*/12/+<1*> 4+446833<1+/818<4>9+0627716 989237>/685/0+0<1<332*/524- *14>48646*75>0+/84+>*7**9<7

货物或应税劳务、服务名称	规格型号	单位	数 量	单 价	金 额	税率	税 额
*信息技术服务*ICT集成服务费			1	320000.00	320000.00	*	*
合　　计					¥320000.00		*
价税合计(大写)	⊗叁拾贰万圆整				(小写)¥320000.00		

销售方	名　　称: 中国移动通信集团广东有限公司茂名分公司 纳税人识别号: 914409007081981208 地 址、电 话: 广东省茂名市迎宾四路233号13592998888 开户行及账号: 中国工商银行股份有限公司广州粤秀支行9558853602004561345	备注	集团产品号码:41530000586(备注：茂名职业技术学院网络安全等级保护测评项目)

收款人: 杨静茵　　复核: 朱晓灵　　开票人: 杨静茵　　销售方: (章)

广东增值税电子普通发票

发票代码:044001631111
发票号码:41941031
开票日期: 2022 年07 月14日
校 验 码:84194 68616 28927 20540

机器编号: 661616301184

购买方		密码区
	名　　称: 茂名职业技术学院 纳税人识别号: 12440900456408565M 地 址、电 话: 茂名市文明北路232号 0668-2920026 开户行及账号: 中国建设银行股份有限公司茂名文明北路分理处,44001690311051434400	<<2/<4>39-104--6-//9/27/481 <9+64747<5+0/4061*3547728+3 -622++97*21+681/4--13////-6 >401<-864301>4+0/1279463/42

货物或应税劳务、服务名称	规格型号	单位	数 量	单 价	金 额	税率	税 额
*电信服务*通信业务服务费			1	48000.00	48000.00	*	*
合　　计					¥48000.00		*
价税合计(大写)	⊗肆万捌仟圆整				(小写)¥48000.00		

销售方		备注
	名　　称: 中国移动通信集团广东有限公司茂名分公司 纳税人识别号: 914409007081981208 地 址、电 话: 广东省茂名市迎宾四路233号13592998888 开户行及账号: 中国工商银行股份有限公司广州粤秀支行9558853602004561345	集团产品号码:41530000586 (备注:网络安全等级保护测评项目)

收款人: 李丹红　　复核: 朱晓灵　　开票人: 李丹红　　销售方: (章)

茂名职业技术学院

成交通知书

中国移动通信集团广东有限公司茂名分公司：

茂名职业技术学院网络安全等级保护测评项目（重招），采购编号：MZY2021NBZB066，于2022年1月4日15:00进行磋商评审，根据评审小组评审结果和推荐意见，现确定你公司为本项目成交单位，成交金额：￥368,000.00元。

请你公司收到本成交通知书后及时与我校联系签订有关合同，本项目将严格按照采购文件要求、响应文件承诺进行验收，弄虚作假将不予验收通过，责任由你公司全部承担。

联系部门：教信中心

联系人：麦才赞　　联系电话：0668—2920568

茂名职业技术学院

2022年1月5日

茂名市政府采购项目验收报告单

根据政府采购合同（合同编号：MZY2022-024）的约定，我单位对合同项目名称：茂名职业技术学院网络安全等级保护测评项目（招标编号：MZY2021NBZB066），对中标供应商：中国移动通信集团广东有限公司茂名分公司提供服务进行验收。验收情况如下：

序号	商品名称	数量	单价	合同金额/元
1	定级备案服务	8	6000	48000
2	等级保护测评	8	40000	320000
3				
4				
5				
6				
7				
8				
	合 计			¥368000

验收具体内容	品牌厂商是否正确：☐	规格型号是否正确：☐	材质配置是否正确：☐
	数量是否正确：☑	是否全新原厂正品：☐	包装是否完好：☐
	安装调试是否正常：☑	现场测试是否达标：☑	运行是否存在安全隐患：☐
	操作培训是否完成：☐	是否有随机资料、保修卡：☐	
	其他内容与合同条款是否一致：☐		
	（超出上述选项的，应当另附验收内容。）		

是否有专业机构检测验收报告（选择有的，必须填写）：有☐ 没有☑	与代理机构联合验收意见（选择有的，必须填写）：有☐ 没有☑

采购验收结论及付款建议：

经验收，本项目已按合同要求完成八套二级系统的定级备案、差距测评和验收测评工作，八套系统的定级备案证书及等级保护测评报告均已收到，验收合格。

验收小组成员分别（签字）：龙恒 陈凯 郑纯原

验收小组组长（签字）：郑纯原

采购人（公章）

2022年11月16日

茂名职业技术学院纪要

（13）

茂名职业技术学院　　2022年7月18日

茂名职业技术学院

2022年第13次院长办公会会议纪要

2022年7月9日上午，学院在北校区综合楼三楼第一会议室召开了今年第13次院长办公会议。会议审议采购2022年校园卡事项；审议采购2022届毕业生就业质量年度报告撰编服务事项；审议采购2022级学生手册、学生证事项；审议注销学生林楷佳、吴仁豪2人学籍事项；审议成人教育学生黄和珍转专业事宜；审议成人教育2019级、2020级学生退学处理事项；审议北校区校园网络中心机房加装不间断电源（UPS）项目；审议采购中国教育和科研计算机网网络服务事项；审议《茂名职业技术学院 东莞市莞城华泰培训中心有限公司联合办学协议》；审议《茂名职业技术学院 广

东财经大学自学考试“相沟通”合作办学协议》；审议学院与广东工业大学、广州市升科自学考试辅导中心签订合作举办自学考试相沟通班补充协议事项；审议《茂名职业技术学院 华南农业大学 广州市升科自学考试辅导中心高等教育自学考试助学联合办学协议书》（续签）；审议《茂名职业技术学院 华南理工大学 广州市升科自学考试辅导中心自学考试相沟通合作办学协议书》；审议支付2020—2022年现代学徒制办学经费事项（深圳好顺佳财务顾问有限公司）；审议《茂名职业技术学院 广东华畅文化传媒有限公司共建数字电商产业学院协议》；审议《广东省粤西建工工程有限公司诉我校施工合同纠纷案应诉情况报告》；审议《茂名职业技术学院纵向科研项目和校级科研项目及经费管理办法（试行）》《茂名职业技术学院横向科研项目及经费管理办法（试行）》；审议《茂名职业技术学院2022年“1+X”证书制度试点奖补资金使用方案》；审议《茂名职业技术学院2022年夏季普通专科招生录取工作方案》；审议2021-2022学年度疫情防控先进个人评选结果；审议省教育厅关于学校职称评审制度修改意见事宜；审议聘用冯波为督导室督导员事项；审议学院2022年公开招聘思政课教师公告（第二批）；审议《茂名职业技术学院食堂服务保障与物价平抑资金管理办法（试行）》；审议《茂名职业技术学院精准征兵试点暂行实施方案》；审议南校区饭堂F—2中空防火卷帘工程项目；审议采购南、北校区宿舍公用插座项目；审议南校区10、11号教学楼窗帘安装项目；审议采购南校区白蚁防治服务项目。会议纪要如下：

一、会议同意通过单一来源谈判的方式向新开普公司采购采购6000张校园卡。经费预算为6.6万元，从2022年包干经费—校园维护费支出。

二、暂缓研究采购2022届毕业生就业质量年度报告撰编服务事项。由学生处根据会议意见，组织调研、完善采购方案再提请院长办公会研究。

三、会议同意采购2022级学生手册5500本、学生证6000本。经费预算为4.93万元，从学生处2022年部门包干经费—学生证件制作费支出。

四、会议审议了注销学生林楷佳、吴仁豪2人学籍事项。土木工程系2021级建筑室内设计6班林楷佳未经批准连续两周未参加学校规定的教学活动、2020级建筑工程技术三二分段1班吴仁豪休学期满后两周内未申请复学，根据学校学籍管理有关规定，会议经研究，同意注销林楷佳、吴仁豪2人学籍，由教务处根据有关规定办理相关手续。

五、会议审议了成人教育学生黄和珍转专业事宜。根据学校成人教育学籍管理有关规定，会议经研究，同意该生由电气自动化技术专业转为建筑工程技术专业，由成人教育部根据有关规定办理相关手续。

六、会议审议了成人教育2019级、2020级学生退学处理事项。2019级电子商务卢子洋、马家敏2人因转读高职扩招；2019级电子商务吕景勇、黄淑燕，2019级汽车检测与维修技术朱相光，2020级食品营养与检测刘宝林，2020级电气自动化技术王元胜5人因未请假离校连续两周未参加学校规定的教学活动，根据学校成人教育学籍管理有关规定，

会议经研究，同意对上述 7 人作退学处理，由成人教育部根据有关规定办理退学手续。

七、审议同意北校区校园网络中心机房加装不间断电源（UPS）项目。经费预算为 5.362 万元，从基建预算中其他费用的零星费用支出。

八、会议审议了采购中国教育和科研计算机网网络服务事项。会议经研究，同意以单一来源谈判方式租赁赛尔网络有限公司教科网信息服务,服务期为 3 年。经费预算为 32.4 万元，每年经费为 10.8 万元，从统管经费—网络通信费支出，以逐年下拨方式支付经费。

九、原则通过《茂名职业技术学院 东莞市莞城华泰培训中心有限公司联合办学协议》。由成人教育部、纪检监察审计室根据会议意进一步修改完善后再组织实施。

十、审议通过《茂名职业技术学院 广东财经大学自学考试“相沟通”合作办学协议》。

十一、审议通过《茂名职业技术学院 广东工业大学 广州市升科自学考试辅导中心签订合作举办自学考试相沟通班补充协议》。

十二、审议通过《茂名职业技术学院 华南农业大学 广州市升科自学考试辅导中心高等教育自学考试助学联合办学协议书》。

十三、审议通过《茂名职业技术学院 华南理工大学 广州市升科自学考试辅导中心自学考试相沟通合作办学协议书》。

十四、会议审议了支付 2020—2022 年现代学徒制办学

经费事项（深圳好顺佳财务顾问有限公司）。根据《茂名职业技术学院 深圳好顺佳财务顾问有限公司现代学徒制人才培养补充协议》相关约定，会议经研究，同意向深圳好顺佳财务顾问有限公司支付 2020—2022 年现代学徒制办学经费 75.88125 万元。

十五、原则通过《茂名职业技术学院 广东华畅文化传媒有限公司共建数字电商产业学院协议》。由经济管理系、纪检监察审计室根据会议意见进一步修改完善后再组织实施。

十六、会议审议了《广东省粤西建工工程有限公司诉我校施工合同纠纷案应诉情况报告》。会议经研究，同意接受法庭调解，按照生效的《法庭调解书》支付《茂名职业技术学院新校区首期工程—教学楼（1、2、3、6 号楼）施工合同》项目结算款余额。对于因缺乏概算资料导致茂名市投资审核中心不同意接收结算资料进行复核的其他自筹资金项目，通过签订补充协议，理顺结算程序后，由学校委托第三方结算咨询机构进行结算审核。经学校与合同相对方同意定案后，按定案金额计算支付项目结算款余额，不再以茂名市投资审核中心审定的金额作为有关项目结算依据。

十七、暂缓研究《茂名职业技术学院纵向科研项目和校级科研项目及经费管理办法（试行）》《茂名职业技术学院横向科研项目及经费管理办法（试行）》。由教务处根据会议意见进一步修改完善后再提请院长办公会研究。

十八、审议通过《茂名职业技术学院 2022 年“1+X”证书制度试点奖补资金使用方案》。

十九、审议通过《茂名职业技术学院 2022 年夏季普通专科招生录取工作方案》。

二十、会议审议了 2021-2022 学年度疫情防控先进个人评选结果。经研究，同意评定计算机工程系张劲勇、崔森蕊、麦敏君，机电信息系王开、刘天生、邓向明，人文与传媒系潘坤才、李宇威，化学工程系王丹菊、李世林，经济管理系徐海涛、陈伟霞、钟诗微、容偲铭，土木工程系何光灿、高林海、杨木兰、梁励志；防控办周智、罗良宏、黄海东、杨小燕、陈景奕、井雨宁、赖寿建、车琼娇、邓桃新、李连珠、吴春柳、周武超、樊瑞珍、林海银、朱林、梁志勇、杨坤有、李 莉、陈春玉、冯群娟 38 人为 2021-2022 学年度疫情防控先进个人。

二十一、会议同意根据省教育厅关于学校职称评审制度修改意见，由人事处进一步修改完善后再报省教育厅审核。

二十二、会议同意聘用广东石油化工学院马克思主义学院退休副教授冯波为学校督导室督导员，具体待遇和聘期按学校聘用人员管理办法的有关规定执行。

二十三、审议通过学校 2022 年公开招聘思政课教师公告（第二批）。由人事处根据会议意见进一步修改完善后再组织实施。

二十四、会议暂不通过《茂名职业技术学院食堂服务保障与物价平抑资金管理办法（试行）》。由总务处根据会议意见，在食堂经营协议书中进一步细化食堂服务保障相关措施。

二十五、审议通过《茂名职业技术学院精准征兵试点暂

行实施方案》。由总务处根据会议意见进一步修改完善后组织实施。

二十六、审议同意南校区饭堂 F—2 中空防火卷帘工程项目。经费预算为 33.29786 万元，从 2022 年其他费用-零星费用支出。

二十七、暂缓通过采购南、北校区宿舍公用插座项目。由总务处根据会议意见开展相关调研，进一步优化采购方案后再提请院长办公会研究。

二十八、审议同意南校区 10、11 号教学楼窗帘安装项目。经费预算为 20.56491 元，从 2022 年基建的其他费用支出。

二十九、审议同意采购南校区白蚁防治服务项目。服务期限为 5 年，经费总预算为 25.08994 万元，从 2022 年基建项目的南校区白蚁防治工程经费支出。

以上议题经院长办公会审议通过后，按规定需提交党委会讨论决定，由提请部门提交党委会讨论决定。

参加：扶国、张庆、罗卫东、谈毅、杨云、钟茹、曾萍。

列席：全程列席会议：谭清、梁晓、陈景宜、梁亚成。具体议题列席人员如下：审议采购 2022 年校园卡事项：谢深根、朱颖颖、陈耀；审议采购 2022 届毕业生就业质量年度报告撰编服务事项：谢深根、朱颖颖、陈耀；审议采购 2022 级学生手册、学生证事项：谢深根、朱颖颖、陈耀；审议注销学生林楷佳、吴仁豪 2 人学籍事项：陈平请、冯川萍；审议成人教育学生黄和珍转专业事宜：杨海、陈平请；审议成

人教育2019级、2020级学生退学处理事项：杨海、陈平请；审议北校区校园网络中心机房加装不间断电源（UPS）项目：叶永利、吴栋、朱颖颖、陈耀；审议采购中国教育和科研计算机网网络服务事项：叶永利、吴栋、朱颖颖、陈耀；审议《茂名职业技术学院 东莞市莞城华泰培训中心有限公司联合办学协议》：杨海、陈平请、朱颖颖；审议《茂名职业技术学院 广东财经大学 自学考试“相沟通”合作办学协议》：杨海、陈平请、朱颖颖；审议学院与广东工业大学、广州市升科自学考试辅导中心签订合作举办自学考试相沟通班补充协议事项：杨海、陈平请、朱颖颖；审议《茂名职业技术学院 华南农业大学 广州市升科自学考试辅导中心高等教育自学考试助学联合办学协议书》（续签）：杨海、陈平请、朱颖颖；审议《茂名职业技术学院 华南理工大学 广州市升科自学考试辅导中心自学考试相沟通合作办学协议书》：杨海、陈平请、朱颖颖；审议支付2020—2022年现代学徒制办学经费事项（深圳好顺佳财务顾问有限公司）：赵丽金、陈平请、朱颖颖；审议《茂名职业技术学院 广东华畅文化传媒有限公司 共建数字电商产业学院协议》：张耿峰、吴栋、陈平请、朱颖颖；审议《广东省粤西建工工程有限公司诉我校施工合同纠纷案应诉情况报告》：吴栋、朱颖颖；审议《茂名职业技术学院纵向科研项目和校级科研项目及经费管理办法（试行）》《茂名职业技术学院横向科研项目及经费管理办法（试行）》：陈平请、朱颖颖；审议《茂名职业技术学院2022年“1+X”证书制度试点奖补资金使用方案》：陈平请、朱颖颖；审议《茂名职业技术学院 2022 年夏季普

通专科招生录取工作方案》：陈平清；审议 2021-2022 学年度疫情防控先进个人评选结果：周智、陈平请、谢深根；审议省教育厅关于学校职称评审制度修改意见事宜：周智、陈平请、谢深根；审议聘用冯波为督导室督导员事项：周智、陈平请；审议学院 2022 年公开招聘思政课教师公告（第二批）：周智、梁辉良；审议《茂名职业技术学院食堂服务保障与物价平抑资金管理办法（试行）》：吴栋、朱颖颖；审议《茂名职业技术学院精准征兵试点暂行实施方案》：吴栋、陈平请、谢深根、李锋成；审议南校区饭堂 F—2 中空防火卷帘工程项目：吴栋、朱颖颖、陈耀；审议采购南、北校区宿舍公用插座项目：吴栋、朱颖颖、陈耀；审议南校区 10、11 号教学楼窗帘安装项目：吴栋、朱颖颖、陈耀；审议采购南校区白蚁防治服务项目：吴栋、朱颖颖、陈耀。

公开方式：依申请公开

分送：学院领导，各系（部）、各部门。

茂名职业技术学院办公室　　2022 年 7 月 18 日印发

茂名职业技术学院招标采购立项申报表

<table>
<tr><td>项目名称</td><td colspan="4">北校区校园网络中心机房加装不间断电源（UPS）项目</td></tr>
<tr><td>采购分类</td><td colspan="4">货物</td></tr>
<tr><td>预算金额</td><td colspan="2">学院资金： ￥ 53,620.00 元</td><td colspan="2">财政资金 ￥ 0.00 元</td></tr>
<tr><td rowspan="7">资金来源</td><td>资金科目或批文名称</td><td colspan="3">基建预算-其他费用-零星费用</td></tr>
<tr><td>上传附件（word、excel或pdf）</td><td colspan="3">在北校区校园网络中心机房加装不间断电源（UPS）的申请.pdf(692KB)

北校区校园网络中心机房加装不间断电源（UPS）项目-清单.docx(17KB)</td></tr>
<tr><td colspan="4">备注：1.此为必填项，名称须具体。2.属上级财政的须提供原版文件或批文复印件</td></tr>
<tr><td>付款方式是否有特殊要求</td><td colspan="3"></td></tr>
<tr><td>采购需求部门负责人意见</td><td>同意。
[叶永利 2022-07-11]</td><td>经费管理部门负责人意见</td><td>项目从2022年基建预算--其他费用--零星费用支出
[吴栋 2022-07-11]</td></tr>
<tr><td>资产管理部门负责人意见</td><td>拟同意立项采购
[吴栋 2022-07-11]</td><td>财务处负责人意见</td><td>拟同意
[朱颖颖 2022-07-12]</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>招标办公室负责人意见</td><td>根据学校招标采购管理办法，并结合本项目实际，拟采用询价方式采购。
[陈耀 2022-07-12]</td><td>学院办公室负责人意见</td><td>拟同意。
[陈景宜 2022-07-12]</td></tr>
<tr><td>纪检监察审计室负责人意见</td><td>已阅
[梁亚成 2022-07-13]</td><td>需求部门分管校领导审签</td><td>【同意】
[杨云 2022-07-13]</td></tr>
<tr><td>分管资产校领导审签</td><td>【同意】
[谈毅 2022-07-13]</td><td>分管招标校领导审签</td><td>【同意】
[罗卫东 2022-07-14]</td></tr>
<tr><td>校长审批</td><td colspan="3">【同意】
[张庆 2022-07-14]</td></tr>
</table>

茂名职业技术学院合同（协议）审批表

经办部门：教育信息与网络中心　经办人：吴国华　送审日期：2022-08-03

合同名称	茂名职业技术学院北校区校园网络中心机房加装不间断电源(UPS)项目采购合同书	合同编号	MZY2022-167
甲方全称	茂名职业技术学院	乙方全称	广州逸翔信息科技有限公司
合同文本	茂名职业技术学院北校区校园网络中心机房加装不间断电源(UPS)项目（未用印）.doc(57KB)		
合同类型	货物服务采购及资产处置合同	合同期限	2022年12月31日前

合同应收款项	应收金额/分成比例	应收日期/期限	应收催款责任人	其他应收说明
	无	无	无	

合同应付款项	应付总额	应付日期/期限	经费来源	专项经费使用期限
	45300	2022年12月31日前	基建预算--其他费用--零星费用	无

项目批文/会议纪要	茂名职业技术学院2022年第13次院长办公会会议纪要.PDF(489KB)
中标（成交）通知书/采购记录 (如无，则不需上传)	成交通知书.jpg(238KB)
资格/资质/收费标准等证明文件	备注：除学校集中采购项目合同外，其他委托、合作项目合同应上传合同相对方证明文件（如身份证、营业执照、经营许可、职业资格、收费许可或收费标准等证明文件（盖章）扫描件）
经办单位（部门）审核意见	同意 [叶永利 2022-08-11]
合同管理部门初审意见	已核。 [曾薇 2022-08-14]
相关职能部门审核意见	已阅。 [陈景宜 2022-08-14] 已阅 [陈耀 2022-08-14] 已阅 [朱颖颖 2022-08-14]
合同管理部门审核意见	拟同意 [梁亚成 2022-08-15]
分管领导审核意见	

	【同意】 [杨云 2022-08-15] 【同意】 [谈毅 2022-08-15] 【同意】 [罗卫东 2022-08-15]
学校法定代表人审批	【同意】 [张庆 2022-08-15]

采 购 合 同 书

合同编号：MZY2022-167

采购编号：MZY2022NBZB041

项目名称：茂名职业技术学院北校区校园网络中心机房加装不间断电源(UPS)项目

合同主要条款

根据茂名职业技术学院北校区校园网络中心机房加装不间断电源(UPS)项目的采购结果，按照《中华人民共和国民法典》的规定，经双方协商，本着平等互利和诚实信用的原则，一致同意签订本合同如下。

一、货物内容

序列	设备名称	型号	数量	单位	单价（元）	小计（元）
1	科华 UPS	YTR3330-J	1	个	25000	25000
2	华申蓄电池	HSG12-65	32	个	400	12800
3	电池柜	C-16	1	个	600	600
4	电池柜承重架	定制	1	个	600	600
5	配电箱	定制	1	个	200	200
6	安装调试费	含安装搬运，5 米距离内 UPS 主机到电池连接线，含电池开关，电池连接电缆等（不含输入输出连接线及走线）	1	项	800	800
7	视频监控系统安装	海康威视视频 7808N-K1/C 监控主机 1 台（含硬盘），3 支 200 万视频监控枪，包布线安装	1	套	1500	1500
8	机房不锈钢门安装	304 不锈钢机房门一套（根据机房门尺寸定制），包安装	1	套	3800	3800

二、合同金额

合计总金额：￥45300 元（大写：肆万伍仟叁佰元整）

三、项目完成时间：

合同签订之日起 30 日内全部完成供货、安装调试并交付正常使用。

四、交货和安装地点：

乙方负责把货物运输至甲方指定地点，货物的包装、运输、装卸必须符合货物保护特性要求。

五、安装与调试：

供应商负责货物安装并调试至正常使用状态。

六、质量和权利要求：

1、货物为原制造商制造的全新产品，未曾使用过，无污染，无侵权行为，其质量、规格及技术特征符合国家行业标准、规范以及磋商文件要求或响应文件承诺，在中国境内可依常规安全合法使用。

2、权利保证：乙方应保证出售给甲方的产品（含配件）或产品任何部分非他人所有或与他人共有，未设有抵押权、租赁权，未侵犯他人的专利权、版权、商标权等知识产权。一旦出现侵权，乙方应承担全部责任。

七、验收：

验收标准依次序对照适用标准为：①符合中华人民共和国国家安全质量标准、环保标准或行业标准；②符合磋商文件要求或响应文件承诺；③货物来源国官方标准。

八、质量保证期（简称“质保期”）及售后服务要求：

1、质保期：自项目验收合格并交付使用之日起乙方对本项目货物提供不少于__1__年质保期（设备参数中对质保期有更高要求的则从其要求）和终生技术支持保障服务（若国家和/或生产厂家对本项目货物质保期的规定高于本项目要求的，应按国家和/或生产厂家的规定执行）。

2、质保期内发生的质量问题及安装问题，由乙方负责免费解决（因甲方使用不当或其他人为因素造成的故障除外），并承担由此产生的一切责任和费用。质保期内乙方对所供货物实行无偿包修、包换、包维护和技术支持。

3、质保期内对甲方的报障通知，乙方必须在接报后 24 小时内到达现场，在 48 小时内处理完毕，若在 48 小时内仍未能有效解决，乙方须免费提供同档次的设备给甲方临时使用，且须按逾期天数按 2000 元/天向甲方支付违约金。

4、质保期内服务方式均为乙方上门服务，即由乙方派员到货物使用现场维修、更换坏损设备等，由此产生的一切责任和费用均由乙方承担。

5、任何时候，乙方均不能免除因货物本身的缺陷所应承担的责任。

九、付款方式：

本项目无预付款，乙方完成供货、安装调试，经甲方验收合格，交付使用后 30 日内甲方支付 100%合同款。乙方负责开具合法的全额完税销售发票。

十、其他要求：

乙方应承担商标、版权和专利等侵权引起的法律裁决、诉讼和费用。

十一、违约责任

1、由于乙方原因造成交货延期，乙方应按日支付违约金，每逾期一日违约金为应当交货的货值 1%，由甲方直接从乙方的合同款中扣抵。乙方交换日期为货物安装调试完

成可正常使用，且以书面形式通知甲方的日期。

2、甲方无正当理由逾期付款，则每日按本合同总价的 1%向乙方偿付违约金。

十二、材料、设备等要求

本项目所采用的材料必须是环保材料并符合消防要求。

十三、争议的解决

1、合同执行过程中发生的任何争议，如双方不能通过友好协商解决，由甲方所在地仲裁机构或法院按相关法律法规处理。

2、因任何一方违约致使对方采取诉讼方式实现债权的，违约方应承担对方为此支付的合理费用，包括但不限于诉讼费、律师费、差旅费。

十四、不可抗力

任何一方由于不可抗力原因不能履行合同时，应在不可抗力事件结束后 1 日内向对方通报，以减轻可能给对方造成的损失，在取得有关机构的不可抗力证明或双方谅解确认后，允许延期履行或修订合同，并根据情况可部分或全部免于承担违约责任。

十五、税费

在中国境内、外发生的与本合同执行有关的一切税费均由乙方负担。

十六、其它

1. 本合同所有附件、磋商文件、响应文件、成交通知书均为合同的有效组成部分，与本合同具有同等法律效力。

2. 在执行本合同的过程中，所有经双方签署确认的文件（包括会议纪要、补充协议、往来信函）即成为本合同的有效组成部分。

3. 如一方地址、电话、传真号码有变更，应在变更当日内书面通知对方，否则，应承担相应责任。

十七、合同生效：

1. 本合同在甲乙双方法人代表或其授权代表签字盖章后生效。

2. 本合同一式拾份，均为正本，具有同等法律效力，甲方执捌份，乙方执贰份。

甲方(公章)：

法定代表人(签字或盖私章)：

2022 年 8 月 18 日

乙方(公章)：广州逸翔信息科技有限公司

法定代表人（签字或盖私章）：

开户行：广州银行天河南支行

账　号：800263273708012

2022 年 8 月 17 日

茂名职业技术学院

成交通知书

广州逸翔信息科技有限公司：

茂名职业技术学院北校区校园网络中心机房加装不间断电源(UPS)项目，采购编号：MZY2022NBZB041，于2022年7月27日上午进行询价，根据询价小组询价结果和推荐意见，现确定你公司为本项目成交单位，成交金额：￥45,300.00元。

请你公司收到本成交通知书后及时与我校联系签订有关合同。

联系部门：教信中心

联系人：吴国华　　联系电话：0668—2920568

茂名职业技术学院

2022年8月1日

茂名市政府采购项目验收报告单

根据政府采购合同（合同编号：MZY2022-167）的约定，我单位对合同项目名称：茂名职业技术学院北校区校园网络中心机房加装不间断电源(UPS)项目（招标编号：MZY2022NBZB041），对中标供应商：广州逸翔信息科技有限公司提供货物进行验收。验收情况如下：

序号	商品名称	数量	单价	合同金额/元
1	科华 UPS	1	25000	25000
2	华申蓄电池	32	400	12800
3	电池柜	1	600	600
4	电池柜承重架	1	600	600
5	配电箱	1	200	200
6	安装调试费	1	800	800
7	视频监控系统安装	1	1500	1500
8	机房不锈钢门安装	1	3800	3800
	合　计			¥45300

验收具体内容	品牌厂商是否正确：☑	规格型号是否正确：☑	材质配置是否正确：☑
	数量是否正确：☑	是否全新原厂正品：☑	包装是否完好：☑
	安装调试是否正常：☑	现场测试是否达标：☑	运行是否存在安全隐患：☐
	操作培训是否完成：☐	是否有随机资料、保修卡：☐	
	其他内容与合同条款是否一致：☐		
	（超出上述选项的，应当另附验收内容。）		

是否有专业机构检测验收报告（选择有的，必须填写）：有☐　没有☑	与代理机构联合验收意见（选择有的，必须填写）：有☐　没有☑

采购验收结论及付款建议：

项目货物经验收，与合同等采购文件约定要求、内容相符，验收合格。

验收小组成员分别（签字）：吴同冬　陈郑　郑纯厚

验收小组组长（签字）：郑纯厚

采购人（公章）：茂名职业技术学院 总务处

2022年9月12日

税总函〔2019〕299号 广州市人民印刷厂股份有限公司

广东增值税普通发票

044001900204

№ 89221107

044001900204
89221107

开票日期：2022年09月27日

校验码 57274 40107 03549 35041

购买方	名称：茂名职业技术学院 纳税人识别号：1244090045640856 5M 地址、电话：广东省茂名市文明北路232号 开户行及账号：建行茂名市分行文明北路支行44001690311051434400	密码区	>6**<*/>54/6128*00918-88<<7 2--6*0-50619/<88>038+1>7914 00/9/27-<+3<+7/-161+52+1/+1 0/7-1996*4>31719/-+9786+35+

货物或应税劳务、服务名称	规格型号	单位	数量	单价	金额	税率	税额
*变压器整流器*不间断电源UPS	YTR3330-J	台	1	22123.893805	22123.89	13%	2876.11
*蓄电池*蓄电池	12V65AH	只	32	353.98230088	11327.43	13%	1472.57
*金属制品*电池柜	C-16	个	1	1238.9380531	1238.94	13%	161.06
*电子计算机*硬盘录像机	DS-7808N-K1/C	台	1	309.73451327	309.73	13%	40.27
*公共安全设备*网络摄像机	DS-LPC-B12HV3-1A/ PDE	台	1	371.68141593	371.68	13%	48.32
*计算机外部设备*3.5寸监控级硬盘	WD10PURX	个	1	646.01769912	646.02	13%	83.98
*金属制品*不锈钢门	1m×2.15m	㎡	2.15	1564.1078411	3362.83	13%	437.17
*建筑服务*安装服务		项	1	733.94495413	733.94	9%	66.06
合计					¥40114.46		¥5185.54

价税合计（大写） ⊗ 肆万伍仟叁佰圆整 （小写）¥45300.00

销售方	名称：广州逸翔信息科技有限公司 纳税人识别号：91440101MA5CHXPE33 地址、电话：广州市天河区五山金顺路1号金顺大厦504房（仅限办公） 020-38550250 开户行及账号：广州银行天河南支行800263273708012	备注	

收款人：尉云飞　　复核：吴楚玲　　开票人：周霖　　销售方：（章）

广州逸翔信息科技有限公司 91440101MA5CHXPE33 发票专用章

第二联：发票联 购买方记账凭证

资产卡片列表

单位：茂名职业技术学院　　制表日期：2022年9月29日

资产编号	名称	型号	分类号	单位	数量	单价	总值	存放地点	管理人员	资产类别
2022005201	机房不锈钢门	304不锈钢机房门（定制）	2010399	张	1	3,800.00	3,800.00	[01Z501-1]北校区中心机房	[2018020009]吴国华	通用设备
2022031502	科华UPS（电源）	YTR3330-J	2400299	台	1	25,000.00	25,000.00	[01Z501-1]北校区中心机房	[2018020009]吴国华	通用设备
2022031602	华申蓄电池	HSG12-65	2400204	批	1	12,800.00	12,800.00	[01Z501-1]北校区中心机房	[2018020009]吴国华	通用设备
2022034902	海康威视视频监控器	7808N-K1/C	2321099	套	1	1,500.00	1,500.00	[01Z501-1]北校区中心机房	[2018020009]吴国华	通用设备
合计							43,100.00			

注：1、登记依据：《茂名职业技术学院北校区校园网络中心机房加装不间断电源(UPS)项目》的采购立项、合同、发票、验收等资料；

2、资产总体情况：　通用设备　43,100.00 元。

经办人员：黄健　　制卡人员：

管理人员：吴国华　　复核人员：

经办部门负责人：叶永利　　资产管理部门负责人：吴栋