报告编号：44090243008-00008-23-0234-01

网络安全等级保护
OA 系统等级测评报告

被测单位：茂名职业技术学院

测评单位：广东中科实数科技有限公司

报告时间：2023 年 08 月 15 日

说明：

一、每个备案系统单独出具测评报告。

二、测评报告编号为四组数据。各组含义和编码规则如下：

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

第二组为年份，由 2 位数字组成。例如 09 代表 2009 年。

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

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

网络安全等级测评基本信息表

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

声明

本报告是 OA 系统的等级测评报告。

本报告测评结论的有效性建立在被测评单位提供相关证据的真实性基础之上。

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

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

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

广东中科实数科技有限公司

2023 年 08 月 15 日

等级测评结论

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

总体评价

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

1.安全物理环境

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

2.安全通信网络

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

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

3.安全区域边界

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

力。

4.安全计算环境

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

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

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

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

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

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

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

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

5.安全管理中心

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

6.安全管理制度

该单位《信息安全制度管理规范》已规定总体安全管理制度和规定以及安全

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

7.安全管理机构

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

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

8.安全管理人员

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

9.安全建设管理

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

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

10.安全运维管理

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

未定期进行漏洞扫描，缺少漏洞扫描报告和修复记录。未提供变更方案和评审记录。

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

主要安全问题及整改建议

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

一、安全物理环境方面

（1）低风险，未提供机房验收文档，机房防震等级不明确。

涉及测评对象：信息机房。

整改建议：建议提供机房防震证明文档，确定机房防震等级，以备日后查看。

（2）低风险，未提供火灾自动消防系统的定期巡检和维护的记录。

涉及测评对象：信息机房。

整改建议：建议对消防设备进行定期巡检维护，并保存巡检记录。

（3）中风险，未提供机房验收文档，无法明确建筑材料的耐火等级。

涉及测评对象：信息机房。

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

（4）中风险，未部署湿度控制设备，不能防止水蒸气结露。

涉及测评对象：信息机房。

整改建议：建议部署湿度控制设备（如精密空调），能防止水蒸气结露。

（5）中风险，机房未铺设防静电地板。

涉及测评对象：信息机房。

整改建议：建议机房统一使用防静电地板，以防止静电对电子设备和人员造成伤害。

（6）低风险，未部署机房专用精密空调，不能设置湿度自动调节。

涉及测评对象：信息机房。

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

二、安全通信网络方面

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

涉及测评对象：安全通信网络。

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

三、安全区域边界方面

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

涉及测评对象：办公区边界、安全管理区边界。

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

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

涉及测评对象：安全管理区边界、办公区边界。

整改建议：建议部署网络入侵检测设备，在关键网络节点处对可能潜在的

攻击行为进行监视。

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

涉及测评对象：办公区边界、安全管理区边界。

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

（4）中风险，无法对边界的流量和边界的安全事件进行审计。

涉及测评对象：安全管理区边界、办公区边界。

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

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

涉及测评对象：办公区边界、安全管理区边界。

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

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

涉及测评对象：安全管理区边界、办公区边界。

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

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

涉及测评对象：办公区边界、外网区边界、服务器区边界、安全管理区边界。

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

四、安全计算环境方面

（1）中风险，未配置口令有效期策略。

涉及测评对象：备份服务器、UIS 超融合管理平台。

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

（2）中风险，未配置屏幕保护程序。

涉及测评对象：运维终端。

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

（3）中风险，未配置登录失败处理策略及登录连接超时策略。

涉及测评对象：备份服务器。

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

（4）中风险，进行远程管理时，鉴别信息通过不安全的协议进行传输。

涉及测评对象：运维终端。

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

（5）中风险，未禁止 root 账户远程登录。

涉及测评对象：数据库服务器、应用服务器、备份服务器。

整改建议：建议严格限制 root 账户的远程访问权限，禁止其进行远程登录。

（6）中风险，未设置审计管理、安全管理员账户，未实现管理用户的权限分离。

涉及测评对象：数据库。

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

（7）中风险，审计记录保存时间不足六个月。

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

整改建议：建议对日志进行集中存放，并确保保存时间能够达到半年以上。

（8）中风险，审计记录仅保存在本机，未进行定期备份。

涉及测评对象：运维终端。

整改建议：建议对日志进行集中存放，定期备份日志，并确保保存时间能

够达到半年以上。

（9）中风险，未严格限制终端登录地址范围。

涉及测评对象：运维终端。

整改建议：建议对接入终端的网络地址范围进行限制。

（10）中风险，未定期进行漏洞扫描。

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

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

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

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

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

（12）中风险，未配置“远程（RDP）连接要求使用指定的安全层”为

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

涉及测评对象：运维终端。

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

（13）中风险，未有备份恢复测试记录。

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

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

（14）中风险，未利用通信网络将关键数据定时批量传送至备用场地。

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

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

五、安全管理制度方面

（1）中风险，未具有管理制度评审记录和修订记录。

涉及测评对象：制度或记录类文档。

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

六、安全建设管理方面

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

涉及测评对象：制度或记录类文档。

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

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

涉及测评对象：制度或记录类文档。

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

（3）中风险，单位缺乏相关测试验收报告。

涉及测评对象：制度或记录类文档。

整改建议：建议对测试结果进行详细的记录，形成测试验收报告。

（4）中风险，该单位未在上线前进行安全性测试，未有相关安全测试报告。

涉及测评对象：制度或记录类文档。

整改建议：建议系统在上线前进行安全性测试，并具有相关安全测试报告。

（5）中风险，单位未对外包开发人员进行资格审查，未有相应的考核记录。

涉及测评对象：移动互联安全扩展要求。

整改建议：建议在移动业务应用软件开发前就对开发者进行资格审查。

七、安全运维管理方面

（1）中风险，未定期进行漏洞扫描，缺少漏洞扫描报告和修复记录。

涉及测评对象：制度或记录类文档。

整改建议：建议指定专人定期对网络和主机、应用进行漏洞扫描并保存检测记录。

（2）中风险，未提供变更方案和评审记录。

涉及测评对象：制度或记录类文档。

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

目录

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

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

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

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

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

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

1 测评项目概述

1.1 测评目的

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

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

1.2 测评依据

测评过程中主要依据的标准:

（1） 《中华人民共和国网络安全法》

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

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

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

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

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

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

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

1.3 测评过程

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

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

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

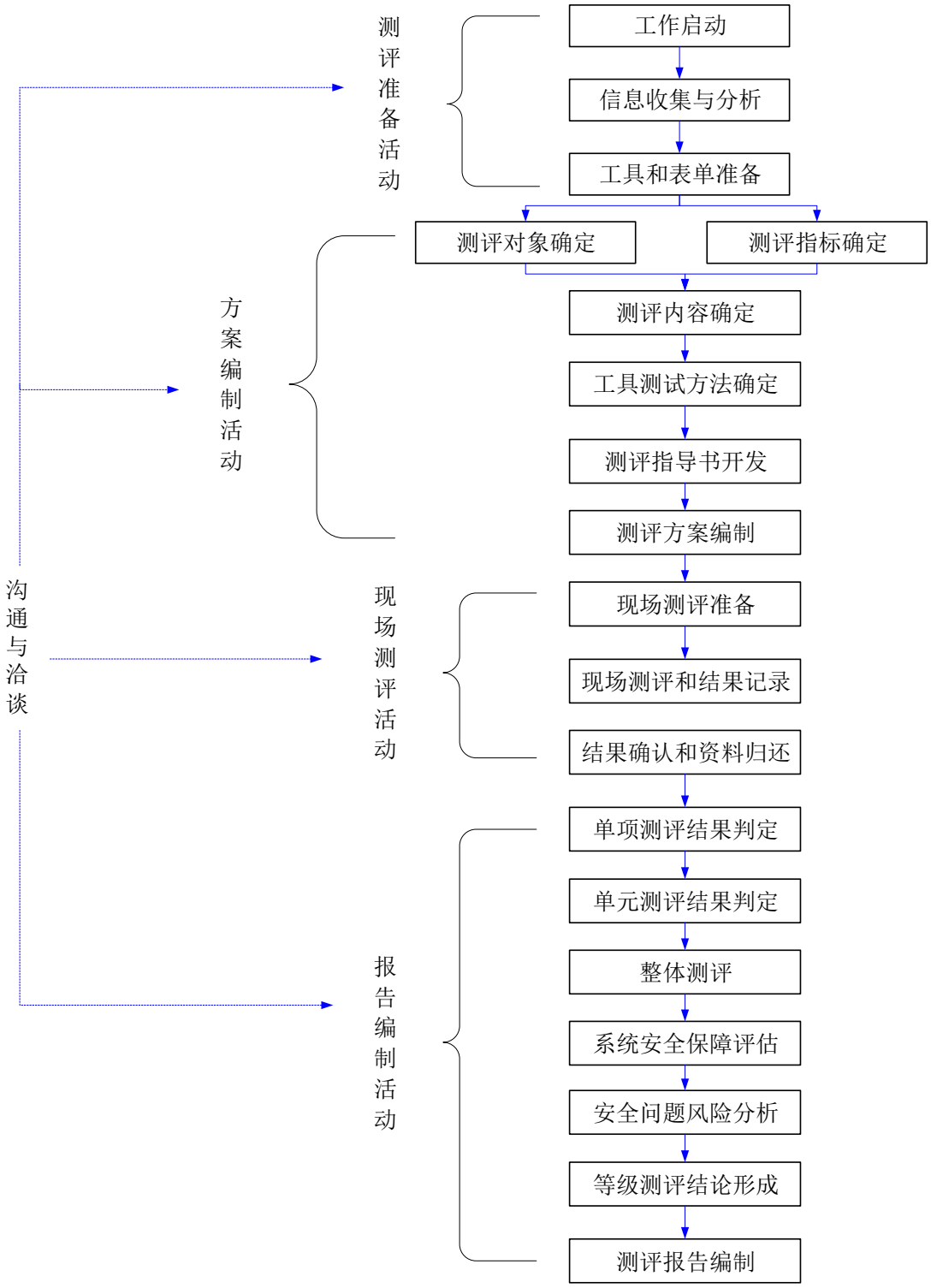
2023 年 07 月 24 日至 2023 年 07 月 27 日期间为现场测评阶段，网络安全等级测评小组按照测评现场工作计划，在茂名职业技术学院开展了网络安全等级保护测评工作。测评组投入相关测试人员，完成了安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面的网络安全等级保护测评。

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

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

编制工作。

具体流程如下图所示：



1.4 报告分发范围

本报告一式 4 份，其中，2 份提交茂名职业技术学院，1 份提交当地等级保

护工作监管部门，1 份由广东中科实数科技有限公司留存。

2 被测对象描述

2.1 被测对象概述

2.1.1 定级结果

表 2-1 定级结果

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

2.1.2 业务和采用的技术

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

2.1.3 网络结构

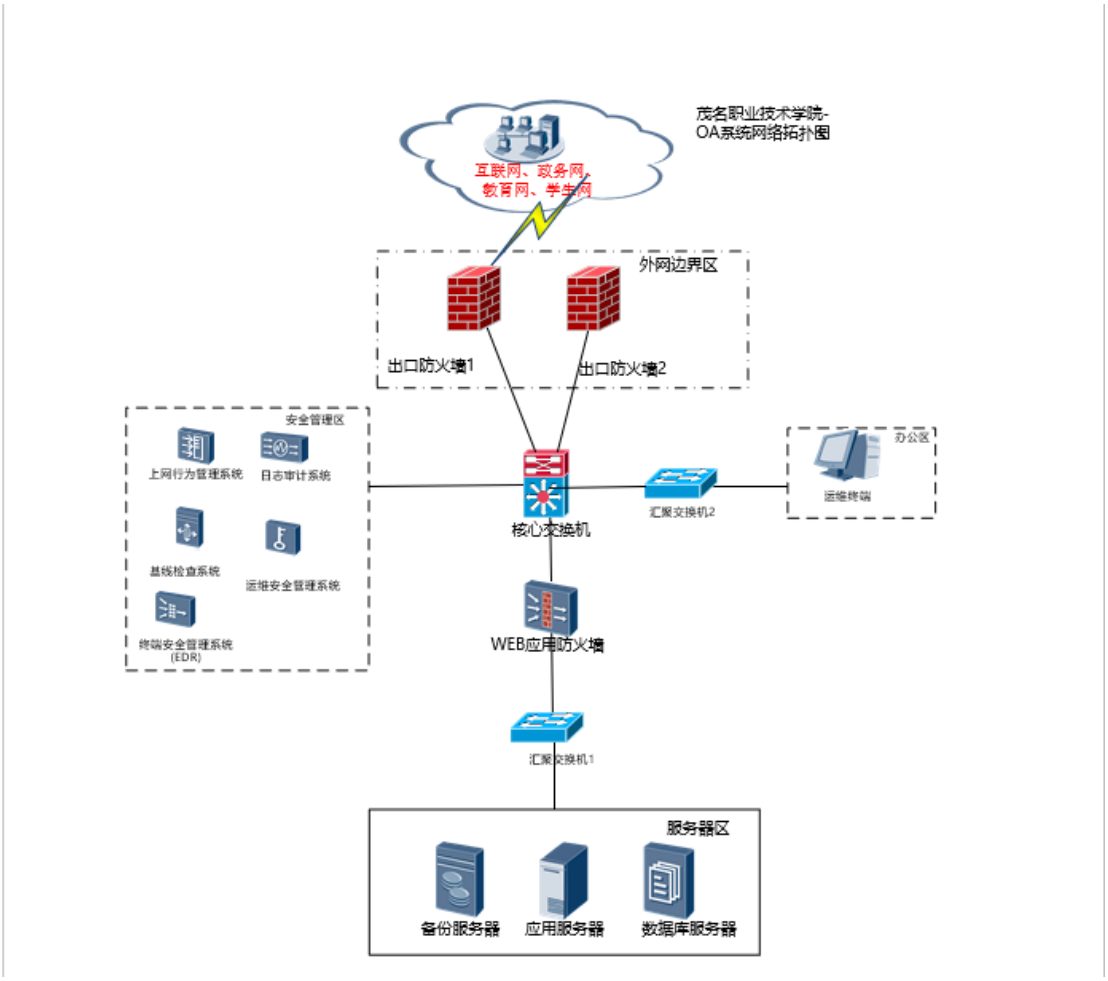


图 2-1 茂名职业技术学院 OA 系统网络拓扑图

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

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

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

2.2 测评指标

2.2.1 安全通用要求指标

表 2-2 安全通用要求指标

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

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

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

安全类	控制点	测评项数
安全通用要求指标数量统计		135

2.2.2 安全扩展要求指标

表 2-3 安全扩展要求指标

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

2.2.3 其他安全要求指标

本次测评不包含其他安全要求指标。

2.2.4 不适用安全要求指标

表 2-4 不适用安全要求指标

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

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

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

2.3 测评对象

2.3.1 测评对象选择方法

本次等级测评中采用抽查的方法兼顾类别与数量，测评原则包括：

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

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

的测评对象种类主要考虑以下几个方面：

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

——存储被测定级对象重要数据的介质的存放环境；

——整个系统的网络拓扑结构；

——安全设备，包括防火墙、入侵检测设备、防病毒网关等；

——边界网络设备(可能会包含安全设备)，包括路由器、防火墙和认证网关等；

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

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

——重要管理终端；

——能够代表被测定级对象主要使命的业务应用系统；

——信息安全主管人员、各方面的负责人员；

——涉及到定级对象安全的所有管理制度和记录。

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

2.3.2 测评对象选择结果

2.3.2.1 物理机房

表 2-5 物理机房

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

2.3.2.2 网络设备

表 2-6 网络设备

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

2.3.2.3 安全设备

表 2-7 安全设备

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

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

2.3.2.4 服务器

表 2-8 服务器

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

2.3.2.5 终端设备

表 2-9 终端设备

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

2.3.2.6 其他系统或设备

本次测评不涉及其他系统或设备。

2.3.2.7 系统管理软件/平台

表 2-10 系统管理软件/平台

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

2.3.2.8 业务应用系统/平台

表 2-11 业务应用系统/平台

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

2.3.2.9 数据资源

表 2-12 数据资源

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

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

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

2.3.2.10 安全相关人员

表 2-13 安全相关人员

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

2.3.2.11 安全管理文档

表 2-14 安全管理文档

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

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

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

3 单项测评结果分析

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

3.1 安全物理环境

3.1.1 已有安全控制措施汇总分析

（1）物理位置选择

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

（2）物理访问控制

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

（3）防盗窃和防破坏

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

2）信息机房采用桥架方式，将通信线缆铺设于机柜上方的线架中。

（4）防雷击

1）信息机房内所有机设施进行了安全接地。

（5）防水和防潮

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

（6）电力供应

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

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

（7）电磁防护

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

3.1.2 主要安全问题汇总分析

安全物理环境存在的安全问题有：

（1）未提供机房验收文档，机房防震等级不明确。

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

（2）未提供火灾自动消防系统的定期巡检和维护的记录。

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

（3）未提供机房验收文档，无法明确建筑材料的耐火等级。

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

（4）未部署湿度控制设备，不能防止水蒸气结露。

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

（5）机房未铺设防静电地板。

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

（6）未部署机房专用精密空调，不能设置湿度自动调节。

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

3.2 安全通信网络

3.2.1 已有安全控制措施汇总分析

（1）网络架构

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

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

（2）通信传输

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

3.2.2 主要安全问题汇总分析

安全通信网络存在的安全问题有：

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

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

3.3 安全区域边界

3.3.1 已有安全控制措施汇总分析

（1）边界防护

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

（2）访问控制

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

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

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

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

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

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

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

（3）入侵防范

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

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

（4）恶意代码防范

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

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

（5）安全审计

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

进行审计。

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

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

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

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

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

3.3.2 主要安全问题汇总分析

安全区域边界存在的安全问题有：

（1）未根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。

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

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

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

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

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

（4）无法对边界的流量和边界的安全事件进行审计。

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

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

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

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

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

（7）未基于可信根对边界设备的系统引导程序、系统程序、重要配置参数

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

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

3.4 安全计算环境

3.4.1 网络设备

3.4.1.1 已有安全控制措施汇总分析

（1）身份鉴别

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

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

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

（2）访问控制

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

2）核心交换机已对登录的用户分配权限，存在网络管理员 super、操作管理

员 long、 操作管理员 nwctrl。

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

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

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

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

（3）安全审计

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

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

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

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

（4）入侵防范

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

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

（5）数据完整性

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

3.4.1.2 主要安全问题汇总分析

安全计算环境网络设备存在的安全问题有：

（1）未定期进行漏洞扫描。

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

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

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

（3）未有备份恢复测试记录。

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

（4）未利用通信网络将关键数据定时批量传送至备用场地。

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

3.4.2 安全设备

3.4.2.1 已有安全控制措施汇总分析

（1）身份鉴别

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

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

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

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

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

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

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

（2）访问控制

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

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

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

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

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

（3）安全审计

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

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

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

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

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

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

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

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

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

（4）入侵防范

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

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

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

（5）数据完整性

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

3.4.2.2 主要安全问题汇总分析

安全计算环境安全设备存在的安全问题有：

（1）审计记录保存时间不足六个月。

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

（2）未定期进行漏洞扫描。

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

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

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

（4）未有备份恢复测试记录。

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

（5）未利用通信网络将关键数据定时批量传送至备用场地。

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

3.4.3 服务器和终端

3.4.3.1 已有安全控制措施汇总分析

（1）身份鉴别

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

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

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

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

（2）访问控制

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

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

登录口令已修改为复杂口令。

3）运维终端不存在默认账户。

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

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

（3）安全审计

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

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

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

4）运维终端审计记录包含：级别、日期和时间、来源、事件 id、任务类别、

关键字等审计相关信息。

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

（4）入侵防范

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

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

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

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

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

（5）恶意代码防范

1）运维终端已安装 360 杀毒，能及时识别和防范病毒行为，已通过互联网

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

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

（6）数据完整性

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

（7）剩余信息保护

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

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

3.4.3.2 主要安全问题汇总分析

安全计算环境服务器和终端存在的安全问题有：

（1）未配置口令有效期策略。

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

（2）未配置登录失败处理策略及登录连接超时策略。

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

（3）未配置屏幕保护程序。

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

（4）进行远程管理时，鉴别信息通过不安全的协议进行传输。

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

（5）未禁止 root 账户远程登录。

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

（6）审计记录保存时间不足六个月。

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

（7）审计记录仅保存在本机，未进行定期备份。

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

（8）未严格限制终端登录地址范围。

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

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

无可信链和可信验证，不能通过主动免疫可信验证技术提高系统自身安全防

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

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

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

（11）未有备份恢复测试记录。

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

（12）未利用通信网络将关键数据定时批量传送至备用场地。

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

3.4.4 系统管理软件/平台

3.4.4.1 已有安全控制措施汇总分析

（1）身份鉴别

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

2）数据库登录失败 5 次锁定一天，超时退出时间为 10 分钟。

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

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

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

（2）访问控制

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

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

3）系统不存在默认账户，不存在默认口令。

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

5）数据库已禁用多余账户，不存在过期账户 ，不存在共享账户的情况。

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

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

（3）安全审计

1）数据库已对普通用户开启审计功能，已启用对所有用户的重要行为进行

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

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

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

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

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

6）数据库告警日志记录了 id、日期、时间、用户、操作、事件、结果等信息。

（4）入侵防范

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

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

描中未发现已知的风险漏洞。

（5）数据完整性

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

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

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

（6）剩余信息保护

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

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

（7）个人信息保护

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

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

3.4.4.2 主要安全问题汇总分析

安全计算环境系统管理软件平台存在的安全问题有：

（1）未配置口令有效期策略。

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

（2）未设置审计管理、安全管理员账户，未实现管理用户的权限分离。

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

（3）审计记录保存时间不足六个月。

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

（4）未定期进行漏洞扫描。

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

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

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

（6）未有备份恢复测试记录。

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

（7）未利用通信网络将关键数据定时批量传送至备用场地。

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

3.4.5 业务应用系统/平台

3.4.5.1 已有安全控制措施汇总分析

（1）身份鉴别

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

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

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

（2）访问控制

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

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

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

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

（3）安全审计

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

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

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

（4）入侵防范

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

（5）数据完整性

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

（6）剩余信息保护

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

（7）个人信息保护

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

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

3.4.5.2 主要安全问题汇总分析

安全计算环境业务应用系统平台存在的安全问题有：

（1）未定期进行漏洞扫描。

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

（2）未有备份恢复测试记录。

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

（3）未利用通信网络将关键数据定时批量传送至备用场地。

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

3.4.6 数据资源

3.4.6.1 已有安全控制措施汇总分析

（1）数据完整性

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

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

（2）个人信息保护

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

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

3.4.6.2 主要安全问题汇总分析

安全计算环境数据资源存在的安全问题有：

（1）未有备份恢复测试记录。

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

（2）未利用通信网络将关键数据定时批量传送至备用场地。

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

3.4.7 其他系统或设备

3.4.7.1 已有安全控制措施汇总分析

本次测评不包含安全计算环境其他设备的测评内容。

3.4.7.2 主要安全问题汇总分析

本次测评不包含安全计算环境其他设备的测评内容。

3.4.8 安全扩展要求

3.4.8.1 已有安全控制措施汇总分析

本次测评不包含安全计算环境扩展要求的测评内容。

3.4.8.2 主要安全问题汇总分析

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

3.5 安全管理中心

3.5.1 已有安全控制措施汇总分析

（1）系统管理

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

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

（2）审计管理

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

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

3.5.2 主要安全问题汇总分析

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

3.6 安全管理制度

3.6.1 已有安全控制措施汇总分析

（1）安全策略

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

（2）管理制度

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

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

（3）制定和发布

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

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

3.6.2 主要安全问题汇总分析

安全管理制度存在的安全问题有:

（1）未具有管理制度评审记录和修订记录。

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

3.7 安全管理机构

3.7.1 已有安全控制措施汇总分析

（1）岗位设置

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

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

（2）人员配备

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

（3）授权和审批

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

2）该单位《授权和审批管理规定》明确审批的内容，重大事项应由信息安

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

（4）沟通和合作

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

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

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

（5）审核和检查

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

3.7.2 主要安全问题汇总分析

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

3.8 安全管理人员

3.8.1 已有安全控制措施汇总分析

（1）人员录用

1）该单位已指定由人力资源保障科负责本学院职工聘用与录用。

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

（2）人员离岗

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

（3）安全意识教育和培训

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

（4）外部人员访问管理

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

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

信息的规定，具有相关登记记录。

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

3.8.2 主要安全问题汇总分析

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

3.9 安全建设管理

3.9.1 已有安全控制措施汇总分析

（1）定级和备案

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

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

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

（2）安全方案设计

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

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

（3）产品采购和使用

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

（4）外包软件开发

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

（5）工程实施

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

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

（6）系统交付

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

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

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

（7）等级测评

1）该系统每年进行等级测评，本次等级测评时间与上次等级测评时间间隔

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

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

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

（8）服务供应商选择

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

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

（9）移动应用软件采购

1）APP 可通过微信扫描指定的二维码获取、安装、来自可靠的分发渠道。

2）单位已与外包开发人员签署有相关保密协议，可保证其可靠。

（10）移动应用软件开发

1）移动业务应用软件的签名证书由腾讯应用宝颁发，具备合法性。

3.9.2 主要安全问题汇总分析

安全建设管理存在的安全问题有：

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

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

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

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

（3）单位缺乏相关测试验收报告。

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

（4）该单位未在上线前进行安全性测试，未有相关安全测试报告。

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

（5）单位未对外包开发人员进行资格审查，未有相应的考核记录。

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

3.10 安全运维管理

3.10.1已有安全控制措施汇总分析

（1）环境管理

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

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

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

（2）资产管理

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

（3）介质管理

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

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

具有“存储介质目录清单”。

（4）设备维护管理

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

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

（5）网络和系统安全管理

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

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

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

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

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

（6）恶意代码防范管理

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

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

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

（7）配置管理

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

（8）密码管理

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

（9）备份与恢复管理

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

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

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

（10）安全事件处置

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

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

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

（11）应急预案管理

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

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

3.10.2主要安全问题汇总分析

安全运维管理存在的安全问题有：

（1）未定期进行漏洞扫描，缺少漏洞扫描报告和修复记录。

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

（2）未提供变更方案和评审记录。

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

3.11 其他安全要求指标

本次测评不包含其他安全要求指标。

3.12 验证测试

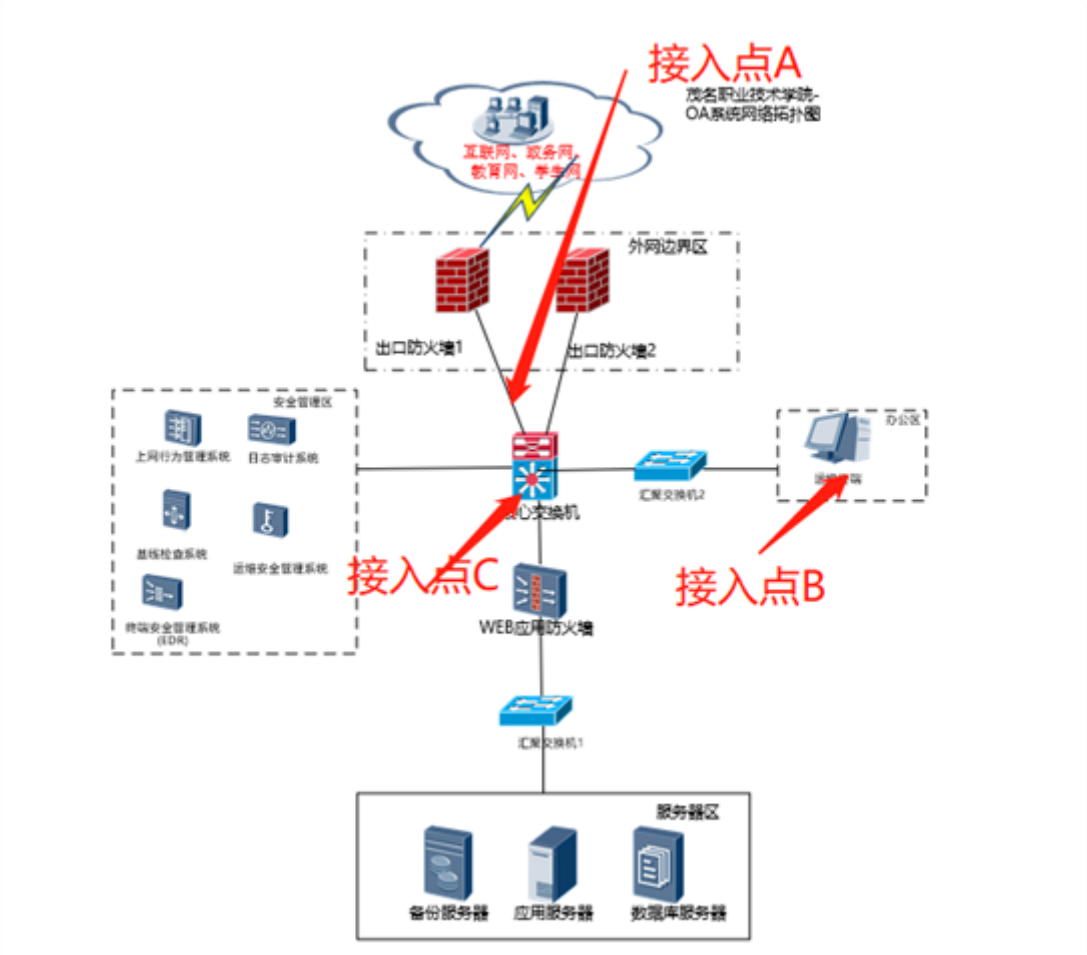


图 3-1 茂名职业技术学院 OA 系统漏洞扫描工具接入测试图

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

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

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

3.12.1漏洞扫描

3.12.1.1 漏洞扫描结果统计

接入点的漏洞扫描结果汇总如下表所示。

表 3-1 接入点 A 漏洞扫描结果汇总表

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

表 3-2 接入点 B 漏洞扫描结果汇总表

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

表 3-3 接入点 C 漏洞扫描结果汇总表

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

3.12.1.2 漏洞扫描问题描述

通过对漏洞扫描结果进行分析，OA 系统存在的主要安全漏洞汇总如下表所示。

表 3-4 主要安全漏洞汇总表

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

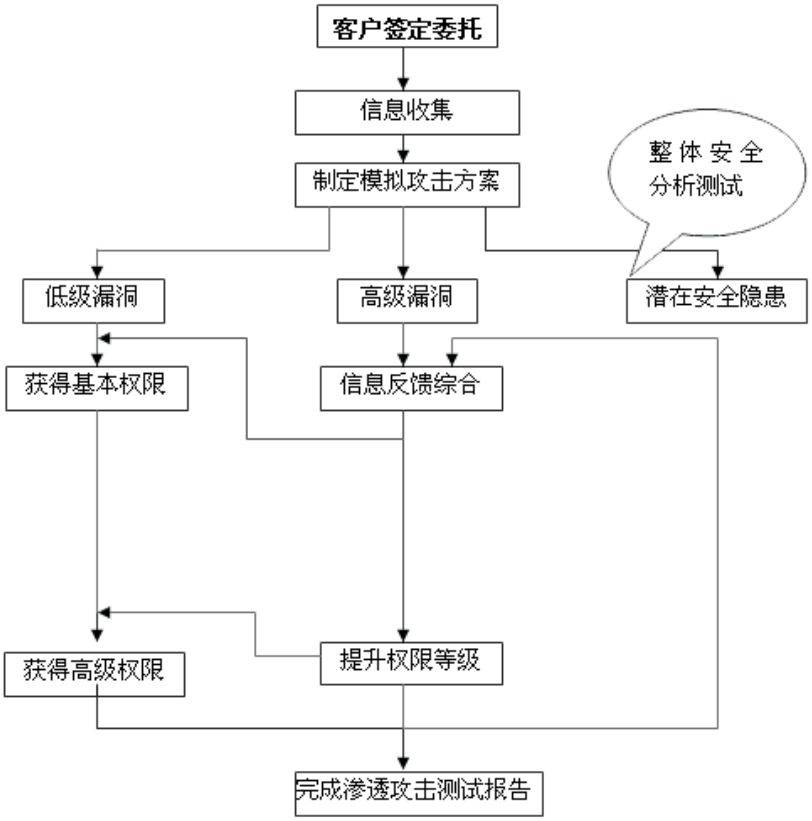
序号	安全漏洞名称	关联资产/域名	严重程度
		172.16.1.18 172.16.1.50 192.168.10.25 172.16.2.1 192.168.10.3 10.1.4.16	
2	SSH 版本信息可被获取	10.1.4.27 10.1.4.28 172.16.1.2 172.16.2.1 172.16.1.50	低
3	探测到 SSH 服务器支持的算法	10.1.4.27 10.1.4.28 172.16.2.1 172.16.1.50 172.16.1.2	低
4	OpenSSH CBC 模式信息泄露漏洞(CVE-2008-5161)【原理扫描】	10.1.4.27 10.1.4.28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

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

3.12.2渗透测试

3.12.2.1 渗透测试过程说明

1. 渗透测试基本流程



1） 实施方案制定、客户书面同意

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

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

2） 内部计划制定、二次确认

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

3） 取得权限、提升权限

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

4） 生成报告

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

2. 渗透测试内容

测试内容包括：业务漏洞测试与技术漏洞测试。

1) 业务漏洞测试

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

量发送短信、进行刷单薅羊毛等行为。

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

2) 技术漏洞测试

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

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

3. 渗透测试工具

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

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

3.12.2.2 渗透测试问题描述

通过渗透测试发现，OA 系统存在的安全问题汇总如下表所示。

表 3-5 渗透测试结果汇总表

序号	安全问题	关联资产/域名	严重程度
1	无		

3.13 单项测评小结

3.13.1控制点符合情况汇总

根据单项测评结果汇总控制点符合情况如下表所示。

表 3-6 控制点符合情况汇总表

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

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

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

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

3.13.2 安全问题汇总

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

表 3-7 安全问题汇总表

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

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

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

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

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

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

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

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

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

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

4 整体测评

4.1 安全控制点间安全测评

本次测评不包含本类安全检测调整项。

4.2 区域间安全测评

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

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

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

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

安全区域边界层面的安全审计中要求“a)应在网络边界、重要网络节点进行

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

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

4.3 整体测评结果汇总

经整体测评后安全问题严重程度变化情况如下表所示。

表 4-1 整体测评结果汇总表

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

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

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

5 安全问题风险分析

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

表 5-1 安全问题风险分析

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

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

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

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

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

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

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

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

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

6 等级测评结论

等级测评结论由安全问题风险分析结果和综合得分共同确定,判定依据如下表所示。

表 6-1 等级测评结论判定依据

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

综合得分计算方法如下:

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

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

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

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

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

X_k 的得分计算如下：

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

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

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

表 6-2 安全问题统计和综合得分

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

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

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

7 安全问题整改建议

表 7-1 安全问题整改建议

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

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

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

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

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

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

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

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

序号	安全类	安全问题	关联资产	整改建议
				程、变更前评估等内容。

【正文结束】

附录A 被测对象资产

A.1 物理机房

附录 A 表-1 物理机房

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

A.2 网络设备

附录 A 表-2 网络设备

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

A.3 安全设备

附录 A 表-3 安全设备

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

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

A.4 服务器

附录 A 表-4 服务器

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

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

A.5 终端设备

附录 A 表-5 终端设备

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

A.6 其他系统或设备

本次测评不涉及其他系统或设备。

A.7 系统管理软件/平台

附录 A 表-6 系统管理软件/平台

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

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

A.8 业务应用系统/平台

附录 A 表-7 业务应用系统/平台

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

A.9 数据资源

附录 A 表-8 数据资源

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

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

A.10密码产品

附录 A 表-9 密码产品

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

A.11安全相关人员

附录 A 表-10 安全相关人员

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

A.12安全管理文档

附录 A 表-11 安全管理文档

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

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

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

附录B　上次测评问题整改情况说明

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

附录 B 表-1 上次测评问题整改情况

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

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

附录C　单项测评结果汇总

C.1 安全物理环境

附录 C　表-1 安全物理环境单项测评结果汇总表（安全通用要求部分）

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

附录 C　表-2 安全物理环境单项测评结果汇总表（安全扩展要求部分）

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

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

C.2 安全通信网络

附录 C 表-3 安全通信网络单项测评结果汇总表（安全通用要求部分）

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

C.3 安全区域边界

附录 C 表-4 安全区域边界单项测评结果汇总表（安全通用要求部分）

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

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

附录 C 表-5 安全区域边界单项测评结果汇总表（安全扩展要求部分）

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

C.4 安全计算环境

C.4.1 网络设备

附录 C 表-6 安全计算环境单项测评结果汇总表（安全通用要求部分）

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

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

C.4.2 安全设备

附录 C 表-7 安全计算环境单项测评结果汇总表（安全通用要求部分）

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

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

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

C.4.3 服务器和终端

附录 C 表-8 安全计算环境单项测评结果汇总表（安全通用要求部分）

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

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

C.4.4 系统管理软件/平台

附录 C 表-9 安全计算环境单项测评结果汇总表（安全通用要求部分）

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

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

C.4.5 业务应用系统/平台

附录 C 表-10 安全计算环境单项测评结果汇总表（安全通用要求部分）

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

C.4.6 数据资源

附录 C 表-11 安全计算环境单项测评结果汇总表（安全通用要求部分）

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

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

C.4.7 其他系统或设备

本次测评不包含“安全计算环境单项测评结果汇总表（安全通用要求部分）”。

C.4.8 安全扩展要求

附录 C 表-12 安全计算环境单项测评结果汇总表（安全扩展要求部分）

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

C.5 安全管理中心

附录 C 表-13 安全管理中心单项测评结果汇总表

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

C.6 安全管理制度

附录 C 表-14 安全管理制度单项测评结果汇总表

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

C.7 安全管理机构

附录 C 表-15 安全管理机构单项测评结果汇总表

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

C.8 安全管理人员

附录 C 表-16 安全管理人员单项测评结果汇总表

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

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

C.9 安全建设管理

附录 C 表-17 安全建设管理单项测评结果汇总表（安全通用要求部分）

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

附录 C 表-18 安全建设管理单项测评结果汇总表（安全扩展要求部分）

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

C.10安全运维管理

附录 C 表-19 安全运维管理单项测评结果汇总表（安全通用要求部分）

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

本次测评不包含“安全运维管理单项测评结果汇总表（安全扩展要求部分）”。

C.11其他安全要求指标

本次测评不包含其他安全要求指标。

附录D 单项测评结果记录

D.1 安全物理环境

D.1.1 安全通用要求部分

D.1.1.1 信息机房

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

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

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

D.1.2 安全扩展要求部分

D.1.2.1 移动互联安全扩展要求

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

D.2 安全通信网络

D.2.1 安全通用要求部分

D.2.1.1 安全通信网络

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

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

D.3 安全区域边界

D.3.1 安全通用要求部分

D.3.1.1 办公区边界

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

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

D.3.1.2 外网区边界

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

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

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

D.3.1.3 服务器区边界

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

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

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

D.3.1.4 安全管理区边界

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

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

控制点	测评项	结果记录	符合情况
	安全管理中心。		

D.3.2 安全扩展要求部分

D.3.2.1 移动互联安全扩展要求

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

D.4 安全计算环境

D.4.1 安全通用要求部分

D.4.1.1 网络设备

D.4.1.1.1 核心交换机

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

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

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

控制点	测评项	结果记录	符合情况
		设备。	

D.4.1.1.2 汇聚交换机 1

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

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

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

D.4.1.1.3 汇聚交换机 2

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

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

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

D.4.1.2 安全设备

D.4.1.2.1 运维安全管理系统

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

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

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

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

控制点	测评项	结果记录	符合情况
		设备。	

D.4.1.2.2 基线核查系统

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

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

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

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

D.4.1.2.3 出口防火墙 1

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

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

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

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

D.4.1.2.4 出口防火墙 2

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

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

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

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

D.4.1.2.5 日志审计系统

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

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

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

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

D.4.1.2.6 WEB 应用防火墙

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

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

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

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

D.4.1.2.7 上网行为管理系统

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

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

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

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

D.4.1.2.8 终端安全管理系统（EDR）

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

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

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

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

D.4.1.3 服务器和终端

D.4.1.3.1 数据库服务器

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

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

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

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

D.4.1.3.2 应用服务器

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

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

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

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

D.4.1.3.3 备份服务器

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

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

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

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

D.4.1.3.4 运维终端

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

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

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

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

D.4.1.4 其他系统或设备

本次测评不包含本安全层面检测项。

D.4.1.5 系统管理软件/平台

D.4.1.5.1 中间件 1

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

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

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

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

D.4.1.5.2 中间件 2

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

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

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

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

D.4.1.5.3 数据库

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

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

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

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

D.4.1.5.4 UIS 超融合管理平台

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

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

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

D.4.1.6 业务应用系统/平台

D.4.1.6.1 OA 系统

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

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

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

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

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

D.4.1.7 数据资源

D.4.1.7.1 重要业务数据

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

D.4.1.7.2 重要个人信息

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

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

D.4.2 安全扩展要求部分

D.4.2.1 移动互联安全扩展要求

附录 D 表-20 安全计算环境结果记录表（移动互联安全扩展要求）

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

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

D.5 安全管理中心

D.5.1 安全通用要求部分

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

D.6 安全管理制度

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

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

D.7 安全管理机构

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

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

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

D.8 安全管理人员

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

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

D.9 安全建设管理

D.9.1 安全通用要求部分

D.9.1.1 制度或记录类文档

附录 D 表-21 安全建设管理结果记录表（制度或记录类文档）

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

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

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

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

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

D.9.2 安全扩展要求部分

D.9.2.1 移动互联安全扩展要求

附录 D 表-22 安全建设管理结果记录表（移动互联安全扩展要求）

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

D.10安全运维管理

D.10.1 安全通用要求部分

D.10.1.1 制度或记录类文档

附录 D 表-23 安全运维管理结果记录表（制度或记录类文档）

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

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

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

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

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

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

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

D.10.2 安全扩展要求部分

D.11其他安全要求

本次测评不包含其他安全要求。

附录E 漏洞扫描结果记录

附录 E 表-1 漏洞扫描主要安全漏洞

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

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

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

附录F 渗透测试结果记录

F.1 项目实施摘要

F.1.1 测试时间

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

表 4.3–II

F.1.2 测试方式

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

F.1.3 测试对象

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

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

表 4.3–III

F.1.4 测试工具

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

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

表 4.3–IV

F.2 渗透测试概述

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

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

主机层面、数据层面以及应用服务层面的安全性测试。

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

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

F.2.1 渗透测试目的

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

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

- 帮助客户理解应用系统当前的安全状况，发现在系统复杂结构中的最脆

弱链路；

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

F.2.2 渗透测试风险管理

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

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

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

F.2.3 渗透测试收益

从攻击者的角度进行测试将有助于发现并识别出一些隐性存在的安全漏洞和风险点。

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

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

F.2.4 渗透测试流程

本次渗透测试基本流程如下:

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

F.2.5 渗透测试技术方法

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

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

F.3 测试结果综述

F.3.1 漏洞等级分布

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

图表 4.3–I

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

F.3.2 漏洞信息摘要

本次渗透测试发现应用系统风险漏洞，具体漏洞信息情况如下：

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

表 4.3–V

F.4 漏洞详情

F.4.1 茂名职业技术学院 OA 系统漏洞详情

F.4.1.1【中】反射型 xss

漏洞名称：反射型 xss

修复结果：已修复

漏洞等级：中

漏洞位置：

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

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

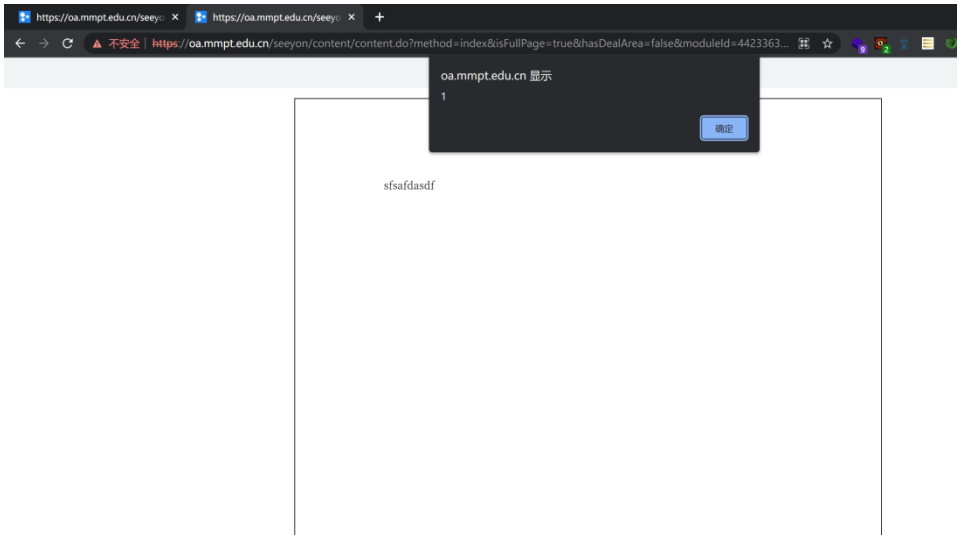
漏洞描述：

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

漏洞说明：。

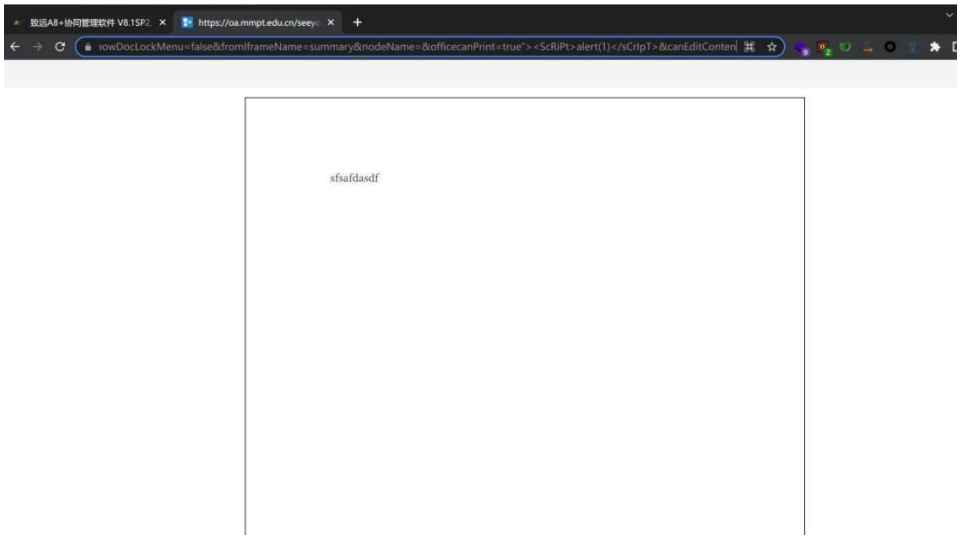
将 payload 放入 officecanPrint 参数当中即可触发 xss 。

Payload:”><ScRiPt>alert(1)</sCrIpT>



漏洞修复证明：

该漏洞经过验证已修复，修复结果：


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

F.5 整体建议

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

附录G 威胁列表

附录 G 表-1 威胁列表

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

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