报告编号：11011499364-24001-24-0050-01

网络安全等级保护
光华荣昌智能数字化平台系统
等级测评报告

被测单位：北京光华荣昌汽车部件有限公司

测评单位：国源天顺科技产业集团有限公司

报告时间：2024 年 11 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	光华荣昌智能数字化平台系统		安全保护等级	第二级（S2A2）
备案证明编号	11011499364-24001			
被测单位				
单位名称	北京光华荣昌汽车部件有限公司			
单位地址	北京市昌平区流村镇工业园区		邮政编码	102204
联系人	姓名	郑晓旭	职务/职称	IT 经理
	所属部门	信息管理部	办公电话	18610116864
	移动电话	18610116864	电子邮件	zhengxiaoxu@bjgrc.com
测评单位				
单位名称	国源天顺科技产业集团有限公司		机构代码	SC202127130010050
单位地址	北京市东城区东花市街道启达大厦 501		邮政编码	100061
联系人	姓名	张东	职务/职称	副总经理
	所属部门	技术部	办公电话	010-68276413
	移动电话	18634202340	电子邮件	gytsdjcp@guoyuants.com
审核批准	编制人	常磊	编制日期	2024.11.13
	审核人	张宇	审核日期	2024.11.14
	批准人		批准日期	2024.11.15

声明

本报告是光华荣昌智能数字化平台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。

国源天顺科技产业集团有限公司

2024 年 11 月 15 日

等级测评结论

测评结论和综合得分			
被测对象名称	光华荣昌智能数字化平台系统	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	主要为北京光华荣昌汽车部件有限公司提供单位内部办公功能，包含财务和员工日常流程审批等方面，助力企业高效快速低运营成本的开展业务。 在安全技术方面：系统部署在北京市昌平区流村镇工业园区北京光华荣昌公司院内一层，已按照重要性原则划分了边界防护区、运维管理区、服务器区等区域，并为各区域分配了地址；网络拓扑图区域划分情况与实际运行环境一致；网络边界处部署有网络入侵防御系统，可以用于检测和限制从外部发起的网络攻击行为，网络入侵防御系统的安全防护策略覆盖了网络中的所有关键节点，网络入侵防御系统的热门威胁库规则库已更新到最新版本（2024-10-16）。 在安全管理方面：该单位已制定《信息安全策略总纲 V1.1》明确了该单位的信息安全建设原则、总体方针和各类安全策略，如物理安全策略、网络安全策略、系统安全策略等，明确了安全工作的目标、范围和原则等。		
安全状况描述	系统部署在北京市昌平区流村镇工业园区北京光华荣昌公司院内一层，已按照重要性原则划分了边界防护区、运维管理区、服务器区等区域，并为各区域分配了地址；网络拓扑图区域划分情况与实际运行环境一致；网络边界处部署有网络入侵防御系统，可以用于检测和限制从外部发起的网络攻击行为，网络入侵防御系统的安全防护策略覆盖了网络中的所有关键节点，网络入侵防御系统的热门威胁库规则库已更新到最新版本（2024-10-16）；该单位已经建立了完善的安全管理制度，有《信息安全策略总纲 V1.1》、《信息安全岗位职责要求 V1.1》、《机房管理制度》等，其内容涵盖了全体单位人员、物理环境、安全建设、安全运维等方面。 主要安全问题有：未采取措施防止地下积水的转移和渗透；未采用校验技术保证通信过程中数据的完整性；安全通信网络、安全区域边界、安全计算环境无可信验证环境；应用系统未采取措施防止鉴别信息在网络传输过程中被窃听；未定期对备份文件进行恢复测试；未提供信息安全管理制度评审与修订记录；未提供恶意代码检测报告。 根据本次测评结果分析，光华荣昌智能数字化平台系统中存在 0 个高风险安全问题，26 个中风险安全问题，10 个低风险安全问题，综合得分为 71.31，等级测评结论为中。		
等级测评结论	中	综合得分	71.31 分

总体评价

为贯彻落实《中华人民共和国网络安全法》等相关法律、法规和标准对网络安全等级测评工作的要求，北京光华荣昌汽车部件有限公司特委托国源天顺科技产业集团有限公司对其光华荣昌智能数字化平台系统实施网络安全等级测评。通过对安全物理环境、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、安全运维管理十个方面的安全措施测试评估，数据分析。光华荣昌智能数字化平台系统安全保护状况描述如下：

在安全物理环境方面，经访谈并核查，机房具有建筑物抗震设防审批验收文件，机房不存在天花板、窗台下的水渗漏现象，机房内安装的窗户具有防护措施，机房不存在屋顶、墙体、门窗和地面等开裂的情况。机房位于北京市昌平区流村镇工业园区北京光华荣昌公司院内一层，未在建筑物的顶层或地下室，周边无用水设施。机房已安排专人值守，电子门禁系统可以正常工作，能对进出人员进行鉴别，专人值守能对进出人员进行鉴别。机房采用耐火的建筑材料，并设置了防火墙体。机房具有防雨水渗透措施，设置了墙壁防水层、双层玻璃，并对窗口进行了防护措施。机房具有稳压器和过电压防护设备，现场观测时稳压器和过电压防护设备处于正常工作状态。具有 UPS 后备电源系统，UPS 满足短期断电时的供电要求（2 小时）。

在安全通信网络方面，经访谈并核查得知，已按照重要性原则划分了边界防护区、运维管理区、服务器区等区域，并为各区域分配了地址；网络拓扑图区域划分情况与实际运行环境一致。被测系统具有与实际网络运行情况相符的网络拓扑图；重要网络区域未部署在网络边界处；区域之间采用 VLAN 隔离技术进行

区域间的逻辑隔离。

在安全区域边界方面，系统在网络边界处部署了边界防火墙，配置了双向的访问控制策略，策略指定通过特定端口进行通信，保证了网络边界访问的安全性，并且每条访问控制规则均有明确的源 IP 地址、目的 IP 地址以及协议端口等。网络边界处部署有网络入侵防御系统，可以用于检测和限制从外部发起的网络攻击行为，网络入侵防御系统的安全防护策略覆盖了网络中的所有关键节点，网络入侵防御系统的热门威胁库规则库已更新到最新版本（2024-10-16）。网络边界处部署有网络入侵防御系统，可以对网络环境中的恶意代码进行检测和清除，漏洞攻击特征识别库已更新到最新版本（2024-8-14）。经测试，网络入侵防御系统的安全防护策略处于有效运行状态。网络设备、安全设备、服务器、数据库和应用系统均启用了安全审计功能，可以对登录事件、操作事件和相关安全事件进行审计，审计覆盖到每个用户。网络入侵防御系统的审计记录包括事件的序号、攻击者 IP、归属地、严重等级、影响业务/服务器、事件描述、攻击事件、操作等审计相关信息。、网络入侵防御系统、WEB 应用防火墙、上网行为管理等关键计算节点设备产生的日志定时推送到日志分析管理系统（192.168.5.253）中，审计日志留存时间满足 6 个月。

在安全计算环境网络设备方面，网络设备使用“用户名+静态口令”方式对用户进行身份标识和鉴别，身份标识具有唯一性，不存在空口令用户，密码由数字、字母等组合而成。网络设备关闭了 Telnet 远程方式，采用 HTTPS 协议进行远程管理，可以防止鉴别信息在网络传输过程中被窃听。网络设备已启用安全审计功能，可以对系统事件、运行状态等进行审计，审计覆盖所有用户。网络设备的审计日志可以保存 6 个月以上，能够避免受到未预期的删除、修改或覆盖等。

在安全计算环境安全设备方面，安全设备均使用“用户名+静态口令”方式对用户进行身份标识和鉴别，身份标识具有唯一性，不存在空口令用户，密码由数字、字母等组合而成。安全设备均采用 HTTPS 协议进行远程管理，可以防止鉴别信息在网络传输过程中被窃听。安全设备均已启用安全审计功能，审计覆盖所有用户，可以对系统事件、设备操作事件等进行审计。审计日志可以保存 6 个月以上，能够避免受到未预期的删除、修改或覆盖等。

在安全计算环境服务器和终端方面，服务器和终端均采用“用户名+静态口令”的方式进行身份标识和鉴别，身份标识唯一，无空口令账户，密码由数字、字母等组合而成。服务器采用安全协议进行远程管理，可以防止鉴别信息在网络传输过程中被窃听。服务器和终端的登录账户均在使用，未有多余和过期的账户，且账户与管理员一一对应，不存在多人使用同一账户的情况。审计日志可以保存 6 个月以上，能够避免受到未预期的删除、修改或覆盖等。服务器和终端安装的组件和应用软件均为业务所需，已遵循最小安装原则。

在安全计算环境应用和数据方面，应用系统和数据库采用“用户名+静态口令”的方式对用户进行身份标识和鉴别，身份标识唯一，无空口令账户，密码由数字、字母等组合而成。应用系统和数据库启用了安全审计功能，审计范围覆盖到每个用户，可以对登录事件、操作事件等进行审计。审计日志可以保存 6 个月以上。应用系统和数据库业务数据每天进行全量备份，备份策略合理，备份结果与备份策略一致。

在安全管理中心方面，网络设备、安全设备、服务器通过运维安全管理系统进行登录，堡垒机和各设备已划分系统管理员账号，已对系统管理员进行了身份鉴别；设备均开启了日志审计功能，可以对系统管理员的操作行为进行审计。网

络设备、安全设备、服务器已划分系统管理员，系统管理员的管理和操作权限有别于审计管理员和安全管理员，指定由系统管理员对设备的资源和运行进行配置、控制和管理，其中包括账户创建、系统资源配置和重要数据的备份与恢复等。

在安全管理制度方面，该单位已制定《信息安全策略总纲 V1.1》明确了该单位的信息安全建设原则、总体方针和各类安全策略，如物理安全策略、网络安全策略、系统安全策略等，明确了安全工作的目标、范围和原则等。该单位已经建立了完善的安全管理制度，有《信息安全策略总纲 V1.1》、《信息安全岗位职责要求 V1.1》、《机房管理制度》等，其内容涵盖了全体单位人员、物理环境、安全建设、安全运维等方面。该单位已提供《运行维护和监控管理规定 V1.1》、《防火墙策略配置规范 v1.0》。

在安全管理机构方面，该单位设立了信息安全领导小组，已制定《信息安全策略总纲 V1.1》明确了信息安全领导小组的构成情况和工作职责，其最高领导由单位主管领导委任。该单位设立了信息安全部负责网络安全管理工作，已制定《信息安全岗位职责要求 V1.1》明确安全主管、安全管理各个方面的负责人的岗位和职责，明确设立安全管理员、系统管理员、审计管理员等，提供了信息安全人员名单，配备了安全管理员、系统管理员、审计管理员各一名。该单位已制定《信息安全策略总纲 V1.1》明确了与单位外部沟通的机制和流程，包括与各类设备供应商、业界专家等的沟通，并且提供了腾讯会议记录，会议主题明确了会议内容。该单位提供了《外联单位联系列表》，列表包含了外联单位名称、合作内容、联系人和联系方式等内容。

在安全管理人员方面，该单位已制定《人员安全管理制度 V1.1》明确了由人力资源部负责人员招聘、录用和离职等工作，明确要求负责人员从候选简历中挑

选出初步符合所招岗位的人员进行面试、笔试和复试，并对其身份、背景、专业资格和资质进行审查。提供了《录用人员审查表》明确了录用人员的学习简历、工作经历、单位意见、考核结果等内容。该单位已制定《人员安全管理制度 V1.1》明确了当人员离职时，按照单位离职流程，归还所持有的信息资产，归还所有的物理安全设备，包括笔记本、门禁卡、钥匙和证件等，终止该员工的所有访问权限，撤销该员工的账号，收回该员工曾掌握过的密码或密钥，并确认密码或密钥的正确性。该单位已制定《外部人员访问管理规定》规范了外部人员的来访流程，明确了外包人员的访问范围、进入条件等。制定了《外来人员进出机房申请表》，由单位接待人员填写后，经单位领导审批通过后，还必须由接待人员陪同，陪同人员填写《机房人员进出登记表》后才能进入机房进行访问。提供了《外来人员进出机房申请表》明确了审批人签字等内容；提供了《机房人员进出登记表》明确了人员的进出时间、陪同人员等内容。该单位已制定《外部人员访问管理制度 V1.1》明确了外部人员离场后应及时清除其所有的访问权限。运维安全管理系统可以查看到访问权限被清除的时间以及相关账号等。

在安全建设管理方面，《光华荣昌智能数字化平台系统网络安全等级保护定级报告》文档内容已经明确该系统的安全保护等级以及定级的方法和理由。该单位已组织相关部门和技术专家对定级结果的合理性和正确性进行论证和审定，并提供了《光华荣昌智能数字化平台系统网络安全等级保护定级评审意见》。该系统的定级结果已获得相关部门批准，并取得备案证明。该单位已将系统备案材料上传至北京市公安局昌平分局进行备案，并取得备案证明，备案证编号：11011499364-24001。《光华荣昌智能数字化平台系统网络安全等级保护定级报告》已明确系统安全保护等级为第二级；被测单位已按照第二级保护需求进行了安全

加固和调整。该单位由信息安全部负责对工程实施过程进行监督和管理。该单位选择的服务供应商(国源天顺科技产业集团有限公司、深信服科技股份有限公司)具备相应的安全服务资质，符合国家有关规定。该单位已与选定的服务供应商签订了合同协议，明确约定了相关责任、技术培训、服务承诺、服务期限等内容。

在安全运维管理方面，该单位已制定《机房管理制度》明确了由机房管理员对机房的环境安全和网络通信等进行管理；提供了《机房设备运行及维护记录》明确了设备参数、用途和设备运行是否正常等。该单位已制定《机房管理制度》覆盖了机房的物理环境、物理访问、物品进出、人员出入等内容的管理，提供了《机房人员出入登记表》明确了来访人员、来访时间、携带物品等内容。该单位已制定《北京光华荣昌汽车部件有限公司办公环境安全管理制度》明确了办公区应设置专门的接待区域，由接待人员统一处理外来人员的出入申请，在受访者陪同下进入办公区域；办公区内不得随意存放涉及单位管理、技术、财务、人力资源等部门机密信息；明确了资产管理员应制定和维护所管辖的资产清单，提供了《信息设备资产清单》明确了资产类别、责任部门、所处地点、存放形式等内容。具有备份恢复策略和程序，文件名为《北京光华荣昌汽车部件有限公司数据备份与恢复管理办法》，内容包括：明确数据备份策略和恢复策略、备份程序和恢复程序等，内容根据数据的重要程度制定。具有明确告知用户在发现安全弱点和可疑事件时应及时向安全管理部门报告的文件，文件名为《北京光华荣昌汽车部件有限公司信息安全事件报告和处置管理制度》；具有安全弱点和可疑事件对应的报告或记录，报告或记录为《安全检查报告及安全检查表》。具有安全事件管理制度，文件名为《北京光华荣昌汽车部件有限公司信息安全事件报告和处置管理制度》，内容包括：明确安全事件的报告、处置和响应流程，并且规定安全事件

的现场处理、事件报告，内容覆盖全面；具有安全事件报告的模板文件，模板文件名为《安全检查报告及安全检查表》。该单位已制定《安全事件报告和处置管理制度 V1.1》规范安全事件报告和响应处理流程，要求事件调查组利用合法手段在安全事件现场收取证据；向信息系统使用或维护单位了解事件发生经过，收集相关资料，查明事件发生的原因、危害程度及造成的损失等情况，检查预防和控制事件发生的措施以及事件发生后应急预案是否得当并得到落实，确定事件的级别和性质，查明相关责任并提出处理建议，提出防止类似事件再次发生的措施和建议。具有重要事件的专项应急预案，针对机房(供电、火灾、漏水等)、系统(病毒爆发、数据泄露等)、网络(断网、拥塞等)等各个层面；具有专项事件应急预案，内容包含：应急处理流程、恢复流程。1)定期对系统相关的人员进行应急预案培训和演练：每年组织次应急预案培训和演练，演练内容：通过演练发现应急工作体系和工作机制存在的问题，不断完善应急预案，提高应急处置能力；具有应急预案的培训记录、演练记录；应急预案的培训记录：《应急预案培训记录》，内容包括：培训人员、培训时间、培训内容、培训地点；应急预案演练记录：《应急预案演练记录》，内容包括：演练方式、演练目的、演练内容、整改措施。

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》的第二级要求，经对光华荣昌智能数字化平台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：

光华荣昌智能数字化平台系统本次等级测评的综合得分为 71.31，且不存在高等级安全风险，等级测评结论为中。

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，光华荣昌智能数字化平台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）中风险 消防装置为手动灭火，未开启自动灭火功能。

整改建议：建议在机房内安装可靠的自动灭火系统，如气体灭火系统（七氟丙烷），以及与火灾检测设备配合使用，并定期对自动灭火系统进行检查和维护，确保其可靠性和有效性。

（2）中风险 未采取措施防止地下积水的转移和渗透。

整改建议：建设在空调下方设立拦水坝，防止积水转移，并安装地下水位监测设备，实时监测地下水位变化，及时发现异常情况。

二、安全通信网络方面

（1）中风险 未采用校验技术保证通信过程中数据的完整性。

整改建议：建议采用校验技术可以确保数据在传输过程中不被窃听或篡改，以保护数据的完整性，确保只有授权用户能够访问和修改数据。

（2）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，也未将验证结果形成审计记录送至安全管理中心。

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、重要配置参数和应用程序等进行可信验证，在检测到其可信性受到破坏后进行报警。

三、安全区域边界方面

（1）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，也未将验证结果形成审计记录送至安全管理中心。

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、重要配置参数和应用程序等进行可信验证，在检测到其可信性受到破坏后进行报警。

四、安全计算环境方面

（1）中风险 核心交换机、ERP 服务器、BPM 系统、ERP 系统、ERP 系统数据库未配置口令复杂度校验和口令有效期策略。

整改建议：建议启用并配置口令复杂度校验，如口令最小长度 8 位以上，口令组成元素至少三种（数字、小写字母、大写字母、特殊字符），增加破解难度；配置口令有效期策略，定期（如 90 天）更换口令，减少长期口令暴露的风险。

（2）中风险 BPM 服务器、ERP 服务器、BPM 系统、ERP 系统数据库未配置登录失败处理和登录连接超时自动退出功能。

整改建议：建议配置登录失败处理策略（如登录失败 5-10 次，锁定账户 5-10 分钟），以防止暴力攻击和密码猜测；并配置登录连接超时自动退出策略（空闲无操作 5-10 分钟，账户自动退出），减少未经授权的访问和信息泄露的风险。

（3）中风险 BPM 系统、ERP 系统未采取措施防止鉴别信息在网络传输过程中被窃听。

整改建议：建议采用安全的通信协议，如 HTTPS、SSH、SSL/TLS 等，确保传输过程中的数据安全性，防止窃听者获取敏感信息。

（4）中风险 核心交换机、网络入侵防御系统、上网行为管理、VPN、WEB 应用防火墙、日志分析管理系统、边界防火墙、ERP 服务器、BPM 系统、ERP 系统数据库、BMP 系统数据库未限制默认账户的访问权限。

整改建议：建议禁用或删除系统中的默认账户，特别是那些不必要的或具有高权限的默认账户，以减少攻击面和提高系统安全性；对于必须保留的默认账户，应该限制其访问权限，确保其仅具有必要的权限，避免滥用和未授权访问。

（5）中风险 BPM 系统存在多余测试账户。

整改建议：建议定期进行账户审核，清理不再需要的账户，如测试账户、离岗人员账户或其他未被使用的账户等。

（6）中风险 核心交换机、网络入侵防御系统、上网行为管理、VPN、WEB 应用防火墙、日志分析管理系统、边界防火墙、BPM 服务器、ERP 服务器、BPM 数据库服务器、BPM 系统、ERP 系统数据库、BMP 系统数据库未划分审计管理员、安全管理员账号，且存在超级管理员账户，不能实现管理用户的权限分离。

整改建议：建议依据三权分立原则划分系统管理员、安全管理员、审计管理员，禁用或限制超级管理员账户，并授予管理用户所需的最小权限，实现管理用户的权限分离。

（7）中风险 BPM 服务器、BPM 数据库服务器审计记录内容不全面。

整改建议：建议开启各项审计日志，确保所有相关活动都有相应的记录。

（8）中风险 核心交换机、网络入侵防御系统、上网行为管理、VPN、WEB 应用防火墙、日志分析管理系统、运维安全管理系统、边界防火墙、BPM 服务器、ERP 服务器、运维终端、BPM 数据库服务器、办公终端、BPM 系统、ERP 系统、ERP 系统数据库、BMP 系统数据库、中间件未定期对设备/系统进行漏洞扫

描。

整改建议：建议定期（如每季度）进行漏洞扫描，并制定漏洞修复计划，经过充分测试评估后，及时修复风险漏洞，以防止攻击者利用漏洞对系统造成损害，并根据漏洞的严重性和潜在影响，优先修复高级别漏洞，最大程度降低安全风险。

（9）中风险 ERP 服务器、运维终端、办公终端未安装防恶意代码软件。

整改建议：建议在服务器上安装专业的、可信赖的防病毒软件，并保持其及时更新，以及时识别和清除潜在的恶意软件。

（10）中风险 BPM 系统、ERP 系统、鉴别数据、审计数据、业务数据、个人信息、配置数据未采用校验技术保证重要数据在传输过程中的完整性。

整改建议：建议采用校验技术或经国家密码主管部门认可的密码技术来保护传输中的重要数据，如使用循环冗余校验（CRC）、消息认证码（MAC）、HTTPS、SSL/TLS 等技术，确保重要数据在传输过程中不被篡改或窃取。

（11）中风险 核心交换机、网络入侵防御系统、上网行为管理、VPN、WEB 应用防火墙、日志分析管理系统、运维安全管理系统、边界防火墙、BPM 服务器、ERP 服务器、BPM 数据库服务器、ERP 系统、ERP 系统数据库、中间件、业务数据、配置数据未定期对备份文件进行恢复测试。

整改建议：建议制定定期的备份文件恢复测试计划，以确保备份文件的完整性和可用性，并在测试过程中模拟真实的灾难或数据丢失情景，以确保备份文件能够成功恢复。

（12）中风险 核心交换机、网络入侵防御系统、上网行为管理、VPN、WEB 应用防火墙、日志分析管理系统、运维安全管理系统、边界防火墙、BPM 服务器、ERP 服务器、BPM 数据库服务器、BPM 系统、ERP 系统、ERP 系统数据库、

BMP 系统数据库、中间件、业务数据、配置数据未将重要数据定时备份至异地。

整改建议：建议将系统的重要数据备份到地理位置不同的远程数据中心或云存储服务中，以确保即使发生本地灾难，数据仍然安全可恢复。

（13）低风险 核心交换机、网络入侵防御系统、上网行为管理、VPN、WEB 应用防火墙、日志分析管理系统、运维安全管理系统、边界防火墙、BPM 服务器、ERP 服务器、运维终端、BPM 数据库服务器、办公终端、BPM 系统、ERP 系统、ERP 系统数据库、BMP 系统数据库、中间件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，也未将验证结果形成审计记录送至安全管理中心。

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，在检测到其可信性受到破坏后进行报警。

五、安全管理中心方面

（1）中风险 网络设备、部分安全设备、部分服务器未划分审计管理员账户，无法对审计管理员进行身份鉴别、授权、操作审计等。

整改建议：建议划分审计管理员账户，为其分配审计策略配置、审计记录查询配置、日志备份等权限，并对审计管理员进行身份标识和鉴别，对其操作行为进行审计。

（2）低风险 网络设备、部分安全设备、部分服务器未划分审计管理员账户，不能通过审计管理员对审计记录进行分析。

整改建议：建议划分审计管理员账户，为其分配审计策略配置、审计记录查询配置、日志备份等权限，并审计管理员对审计记录进行分析。

六、安全管理制度方面

（1）低风险 未提供信息安全管理制度评审与修订记录。

整改建议：建议组织建立并执行定期评审安全管理制度的流程，确保对安全策略、控制措施和流程进行全面审查；借助评审过程发现的问题和机会，不断改进安全策略、流程和控制措施，以应对不断变化的安全威胁和风险，并在每次安全管理制度评审后，记录评审结果和必要的改进计划。

七、安全管理机构方面

（1）中风险 未提供常规性安全检查记录。

整改建议：建议每次安全检查后都应详细记录检查结果，并形成报告，以便追踪问题整改情况。

（2）低风险 未提供单位内部关于信息安全的沟通交流记录。

整改建议：建议所有关于信息安全的重要沟通交流都被记录下来，包括会议记录、电子邮件、即时消息等。这可以帮助团队成员在需要时回顾相关信息，确保他们理解并遵循信息安全政策。

八、安全管理人员方面

（1）中风险 未提供外部人员访问申请记录

整改建议：建议所有外部人员在访问前提交书面申请，并经过相关部门的审批，并在每次访问后，记录访问者的姓名、单位、访问日期、时间、访问目的和陪同人员等信息。

九、安全建设管理方面

（1）中风险 无相关的安全规划设计类文档和被测系统安全方案设计文档。

整改建议:建议制定详细的安全规划设计文档(需包含密码技术相关内容)，确定系统的安全目标、需求和风险评估，有计划地开展安全建设工作。

（2）中风险 未提供整体安全规划和安全方案设计的专家论证文档和批准意见。

整改建议:建议组织相关部门和有关安全专家对安全设计方案的合理性和正确性进行论证和审定，并留存安全设计方案审定记录。

（3）中风险 未提供恶意代码检测报告。

整改建议：建议在软件交付之前，进行全面的恶意代码安全审查，包括静态代码分析、动态代码分析和安全架构审查等，并留存相关检测报告。

（4）中风险 未制定安全工程实施方案控制工程实施过程。

整改建议：建议制定工程实施方案控制工程实施过程，方案需包括工程时间限制、进度控制和质量控制等方面内容，并按照工程实施方面的管理制度进行各类控制。

（5）中风险 未提供测试验收方案和测试验收报告。

整改建议:建议核查工程测试验收方案是否明确说明参与测试的部门、人员、测试验收内容、现场操作过程等内容；并形成测试验收报告，测试验收报告应有相关部门和人员对测试验收报告进行审定的意见。

（6）中风险 未在系统上线前进行安全性测试。

整改建议:建议在系统上线前委托专业的安全团队或第三方安全公司进行全面的安全性测试，包括漏洞扫描、渗透测试、安全配置审查、软件测试、密码应用安全性测试等，确保系统的安全性达到预期标准。

（7）低风险 未提供对运行维护技术人员的相关的技术培训记录。

整改建议：建议建立定期的技能培训计划，主要从系统的整体架构、主要的安全实现手段和系统实现的主要业务功能等方面进行培训，并留存相关的培训记录，培训记录包括培训内容、培训时间、参与人员等方面的信息。

（8）低风险 未提供《项目测试验收报告》、《运维培训记录表》等记录表单，系统交付文档不完善。

整改建议：建议在信息系统交付后，提供完整的测试验收报告，包括项目各阶段的测试结果，包括功能测试、性能测试、安全测试等；并实施运维技术培训，并留存相关的培训记录，培训记录包括培训内容、培训时间、参与人员、培训方式等方面的信息。

十、安全运维管理方面

（1）中风险 单位未采取必要的措施识别安全漏洞和隐患，未提供漏洞扫描报告。

整改建议：建议提供漏洞扫描报告，报告应描述存在的漏洞、严重级别、原因分析和改进意见等方面，报告的时间应与定期扫描的要求相符。

（2）中风险 未提供变更方案评审记录。

整改建议：建议制定并实施规范的变更方案评审和变更过程记录流程，明确评审的标准、参与人员和记录方式，并对变更方案评审和实施过程进行详细记录，包括变更方案的提出、评审意见、变更过程的执行情况、实施结果等信息。

（3）低风险 未提供维修审批、维修过程等方面的记录。

整改建议：建议实施完善的维修审批流程，包括维修申请、审批人员、审批步骤和审批标准等内容，确保每次维修都经过审批，记录下审批人员和审批结果；并对每次维修进行详细记录，包括维修人员、维修时间、维修内容、使用的工具

和材料等信息。

（4）低风险 未提供账户管理相关审批记录或流程文件。

整改建议：建议制定明确的账户管理审批流程，包括账户创建、权限变更、账户删除等操作，确保每个账户管理活动都经过适当的审批和授权。

目录

1 测评项目概述

1.1 测评目的

网络安全等级保护测评是依据国家网络安全等级保护制度,按照有关管理规范和技术标准，对已定级备案的非涉及国家秘密的网络（含信息系统、数据资源等）的安全保护状况进行检验评估的活动。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。

为进一步提高信息系统的保障能力,贯彻落实《中华人民共和国网络安全法》、《信息安全等级保护管理办法》（公通字 2007【43】号）等法律和文件的要求，北京光华荣昌汽车部件有限公司委托国源天顺科技产业集团有限公司（SC202127130010050）通过对光华荣昌智能数字化平台系统在安全技术及管理方面的测评，对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。

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/T 36627-2018《信息安全技术 网络安全等级保护测试评估技术指南》

（7） GB/T 25058-2019《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》

（9） 《信息安全等级保护管理办法》

（10） 《团体标准-网络安全等级保护测评高风险判定指引》 (T/ISEAA 001-2020)

其他：

（1） 《光华荣昌智能数字化平台系统网络安全等级保护定级报告》

1.3 测评过程

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

1、2024 年 09 月 23 日~2024 年 09 月 24 日，测评准备阶段。

2、2024 年 09 月 25 日~2024 年 09 月 27 日，方案编制过程。

3、2024 年 10 月 08 日~2024 年 10 月 15 日，现场实施过程。

4、2024 年 10 月 16 日~2024 年 11 月 15 日，分析与报告编制过程。

其中，2024 年 10 月 08 日召开了测评现场首次会议，确定了现场测评工作计划安排；2024 年 10 月 15 日召开了测评现场末次会议，确认测评发现的问题，并

对系统的整改情况进行了复核确认。

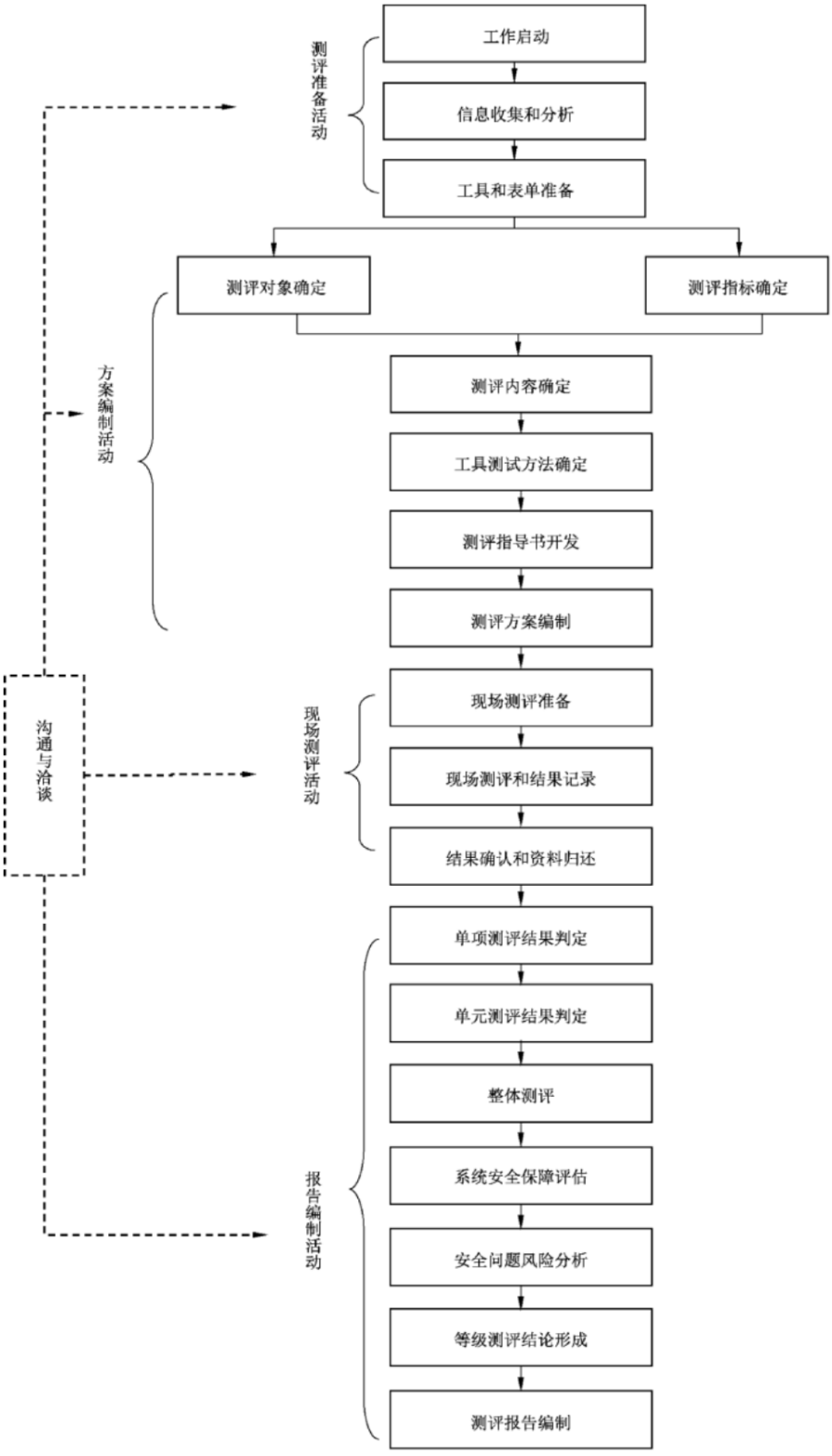

图 1-1 等级保护测评工作流程图

1.4 报告分发范围

等级测评报告正本一式 3 份，其中北京市公安局昌平分局警务支援大队 1 份，北京光华荣昌汽车部件有限公司 1 份，国源天顺科技产业集团有限公司 1 份。

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
光华荣昌智能数字化平台系统	第二级	第二级	第二级

2.1.2 业务和采用的技术

主要为北京光华荣昌汽车部件有限公司提供单位内部办公功能，包含财务和员工日常流程审批等方面，助力企业高效快速低运营成本的开展业务。

系统部署有边界防火墙、网络入侵防御系统、WEB 应用防火墙，能够对边界访问流量进行访问控制、网络层入侵检测以及应用层 WEB 防护等，业务数据每天进行全量备份，备份策略合理，备份结果与备份策略一致。

2.1.3 网络结构

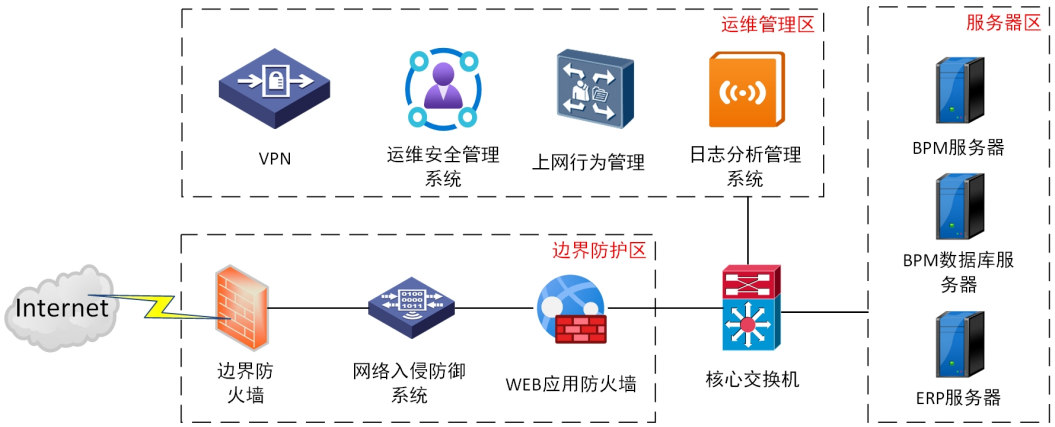

图 2-1 光华荣昌智能数字化平台系统网络拓扑图

如图 2-1 光华荣昌智能数字化平台系统网络拓扑图所示，系统部署在北京市昌平区流村镇工业园区北京光华荣昌公司院内一层，民防图像信息管理平台总体网络区域划分为：边界防护区、运维管理区、服务器区。核心交换机承载了网络核心节点的数据传输，转发来自于不同区域的流量。

边界防护区

边界防护区实现对外部网络的访问及安全防护功能，部署有边界防火墙、网络入侵防御系统、WEB 应用防火墙，能够对边界访问流量进行访问控制、网络层入侵检测以及应用层 WEB 防护等。

运维管理区

运维管理区主要实现系统运行环境的综合安全管理，通过 VPN 实现外部网络安全接入内部网络；运维安全管理系统用于对设备的安全运维和操作审计；日志分析管理系统用于收集分散在网络中各设备日志，并进行集中分析；上网行为管理用于规范员工上网行为，控制和管理访问互联网的行为。

服务器区

服务器区主要承载业务系统的运行，共有 3 台服务器，主要为应用系统各类组件、服务提供了运行环境，业务数据每天进行全量备份，备份策略合理，备份结果与备份策略一致。

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[1]	控制点[2]	测评项数
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	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

[1] 安全类对应《基本要求》中的安全物理环境、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、安全建设管理和安全运维管理。

[2] 控制点是对安全类的进一步细化，对应《基本要求》目录级别中安全类的下一级目录。

安全类[1]	控制点[2]	测评项数
	可信验证	1
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

安全类[1]	控制点[2]	测评项数
	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

安全类[1]	控制点[2]	测评项数
	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
本次测评不涉及安全扩展要求指标			

2.2.3 其他安全要求指标

表 2-4 其他安全要求指标

安全类	控制点	测评项数
本次测评不涉及其他安全要求指标		

2.2.4 不适用安全要求指标

表 2-5 不适用安全要求指标

安全类	控制点	不适用项	不适用原因
安全通用要求			
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，该单位未有密码产品，此项不适用。
	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，该系统为外包开发，此项不适用。
		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，该系统为外包开发，此项不适用。
	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，该系统为首次等级测评，不适用。
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，该单位未使用相关的密码产品，不涉及此项内容，不适用。
	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，该单位未有外包运维服务情况，不涉及此项内容，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，该单位未有外包运维服务情况，不涉及此项内容，不适用。
表中不适用指标数量			7

2.3 测评对象

2.3.1 测评对象选择方法

结合光华荣昌智能数字化平台系统的网络拓扑结构和业务情况，本次测评的对象包括物理机房、网络设备、安全设备、服务器设备、终端设备、业务应用系统、数据对象、管理体系和人员等。通过综合考虑安全保护等级、业务应用特点和具体设备的重要情况等要素选择测评对象。

1) 存储被测系统重要数据的介质的存放环境；

2) 办公场地；

3) 整个系统的网络拓扑结构；

4) 安全设备，包括边界防火墙、网络入侵防御系统等；

5) 承载业务处理系统主要业务或数据的服务器（包括其操作系统和数据库系统）；

6) 运维终端和主要应用系统；

7) 能够完成光华荣昌智能数字化平台系统不同业务使命的业务应用系统；

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

9) 涉及到信息系统安全的所有管理制度和记录。

抽样原则：在等级测评时，业务处理系统中配置相同的网络设备、安全设备、服务器、数据库、终端等，每类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 2-6 物理机房

序号	机房名称	物理位置	重要程度
1	信息机房	北京市昌平区流村镇工业园区北京光华荣昌公司院内一层	关键

2.3.2.2 网络设备

表 2-7 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	×	V200R019C00SPC500B327	HUAWEI S5731S-S24T4X-A	核心数据交换、转发	关键

2.3.2.3 安全设备

表 2-8 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	VPN	×	7.1	深信服 VPN-2150	建立一个安全的加密连接，以保护用户的数据隐私和网络安全，确保信息传输的安全性	重要
2	边界防火墙	×	V600R007C	HUAWEI	互联网	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
			20SPC600 (VRP (R) software，Version 5.170)	USG6315E	边界访问控制	
3	网络入侵防御系统	×	NIPS 8.0.7	深信服 NIPS-1000-B1400	互联网边界入侵检测及限制	关键
4	WEB 应用防火墙	×	WAF 8.0.42	深信服 WAF-1000-B1200	互联网边界应用层防护	关键
5	上网行为管理	×	AC11.0R2	深信服 AC1200	控制、管理、规范员工访问互联网的行为	重要
6	运维安全管理系统	×	V3.0.1020220210	深信服 SM-1000-B1150	设备的安全运维、运维审计	重要
7	日志分析管理系统	×	SIP-Logger3.0.22 Build20240103	深信服 SIP-Logger-A600	收集分散在网络中各设备的日志	重要

2.3.2.4 服务器

表 2-9 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	BPM 服务器	BPM 系统	×	Microsoft Windows Server 2012	-	Internet Inform	关键

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
				R2 Standard		ation Services (Version 8.5.9600.16384)	
2	BPM 数据库服务器	BPM 系统	×	Microsoft Windows Server 2012 R2 Datacenter	MSSQL 2012 (11.0.3128.0)	-	关键
3	ERP 服务器	ERP 系统	×	Red Hat Enterprise Linux Server release 7.2 (Maipo)	Progress Version 11.7.09.0002026	-	关键

2.3.2.5 终端设备

表 2-10 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	×	Windows 10 专业版	运维管理	重要
2	办公终端	×	Windows 10 专业版	日常办公	重要

2.3.2.6 其他系统或设备

表 2-11 其他系统或设备

序号	设备名称	是否虚拟设备	系统及版本	设备类别/用途	重要程度
该系统不涉及其他系统或设备					

2.3.2.7 系统管理软件/平台

表 2-12 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	URL 请求、转发、响应	Internet Information Services (Version 8.5.9600.16384)	BPM 服务器	重要
2	BMP 系统数据库	数据存储、管理	MSSQL 2012（11.0.3128.0）	BPM 数据库服务器	关键
3	ERP 系统数据库	数据存储、管理	Progress Version 11.7.09.000 2026	ERP 服务器	关键

2.3.2.8 业务应用系统/平台

表 2-13 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	BPM 系统	主要为员工提供各种工作流程申请和公司相关制度文档的管理功能，包括员工考勤，费用报销、印章使用、合同申请、车辆使用等审批功能	V1.0	安码商务软件系统（上海）	关键
2	ERP 系统	主要为公司提供物料采购订单、采购入库、生产排产生产备料、领料、产成品入库、耗料、销售	V3.5.0.38	上海快意信息科技有限公司	关键

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
		订单、销售发运、开票等各环节管理，所有业务数据自动进入并形成财务会计核算数据。财务管理包括应收账款、应付账款、总账、固定资产、成本管理、现金管理等模块，实现财务智能管理核算			

2.3.2.9 数据资源

表 2-14 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	鉴别数据	BPM 系统	完整性、保密性	重要
2	业务数据	BPM 系统	完整性、保密性	关键
3	审计数据	BPM 系统	完整性	重要
4	配置数据	BPM 系统	完整性	重要
5	个人信息	BPM 系统	完整性、保密性	关键

2.3.2.10 安全相关人员

表 2-15 安全相关人员

序号	姓名	岗位/角色	联系方式	所属单位
1	魏弈壮	系统管理员	18830035572	北京光华荣昌汽车部件有限公司
2	曹艳芳	审计管理员	18610117403	北京光华荣昌汽车部件有限公司
3	郑晓旭	安全管理员	18610116864	北京光华荣昌汽车部件有限公司

2.3.2.11 安全管理文档

表 2-16 安全管理文档

序号	文档名称	主要内容
1	《个人信息管理制度》	明确个人信息的收集范围和目的，确保在合法、合理、必要的情况下收集和使用个人信息，并遵守相关的法律法规。
2	《信息安全策略总纲 V1.1》	主要包含了方针、目标、原则、总体安全策略、制度的制定与发布、制度的评审和修订等内容。
3	《信息安全岗位职责要求 V1.1》	主要包含了技能安全培训要求、信息安全主管岗位职责、安全管理员岗位职责、系统管理员岗位职责、审计管理员岗位职责等内容。
4	《机房管理制度》	主要包含了机房管理制度、机房的常规检查和维护、机房消防系统等内容。
5	《运行维护和监控管理规定 V1.1》	主要包含了组织及岗位职责、系统运行维护和监控管理等内容。
6	《防火墙策略配置规范 v1.0》	主要包含了防火墙的策略配置要求等内容。
7	《外联单位联系列表》	列出了与外部单位建立联系和沟通所需的单位名称、联系人以及联系方式等。
8	《信息系统安全审核和安全检查管理制度》	主要包含了安全审核和安全检查等内容。
9	《人员安全管理制度 V1.1》	主要包含了人员录用、人员转岗和离岗、人员考核、人员惩戒、人员教育和培训等内容。
10	《外部人员访问管理制度 V1.1》	主要包含了外部人员访问安全管理等内容。
11	《光华荣昌智能数字化平台系统网络安全等级保护定级报告》	主要包含光华荣昌智能数字化平台系统的定级系统描述、网络结构、业务描述、系统安全等级确认等。
12	《光华荣昌智能数字化平台系统网络安全等级保护定级评审意见》	主要包含民防图像信息管理平台业务信息安全保护等级和系统服务安全保护等级的描述和专家评审意见。
13	《软件设计说明书》	详细描述软件设计的技术规范、功能需求和设计思路。
14	《系统操作手册》	指导用户如何操作和使用办公信息系统或软件的手册。

序号	文档名称	主要内容
15	《北京光华荣昌汽车部件有限公司办公环境安全管理制度》	主要包含了办公场所安全管理规定、办公场所消防安全要求等内容。
16	《资产安全管理制度》	主要包含了资产责任制度、资产标识管理、资产使用管理、资产传输管理、资产维护管理、资产报废与处置管理等内容。
17	《运行维护和监控管理制度》	主要包含了组织及岗位职责、系统运行维护和监控管理等内容。
18	《北京光华荣昌汽车部件有限公司恶意代码防范管理制度》	主要包含了恶意代码（病毒）防范具体要求。
19	《北京光华荣昌汽车部件有限公司变更管理办法》	主要包含了变更的分类和界定、变更管理等内容。

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

光华荣昌智能数字化平台系统在安全物理环境方面采取了以下安全措施：

在物理位置选择方面，经访谈并核查得知，机房具有建筑物抗震设防审批验收文件；机房不存在天花板、窗台下的水渗漏现象；机房有窗户；机房内安装的窗户具有防护措施；机房不存在屋顶、墙体、门窗和地面等开裂的情况。机房位于北京市昌平区流村镇工业园区北京光华荣昌公司院内一层，未在建筑物的顶层或地下室，周边无用水设施。

在物理访问控制方面，经访谈并核查得知，机房具有电子门禁；机房已安排专人值守；电子门禁系统可以正常工作，能对进出人员进行鉴别；专人值守能对进出人员进行鉴别。

在防盗窃和防破坏方面，经访谈并核查得知，机房内设备放置在机柜或机架上，并已采取固定措施；设备或主要部件具有不易除去的标识、标志。机房内通信线缆铺设在线槽中，线缆不易损坏。

在防雷击方面，经访谈并核查得知，机房内所有机柜、设施和设备等已采取

接地控制措施。

在防火方面，经访谈并核查得知，机房采用耐火的建筑材料，并设置了防火墙体。

在防水和防潮方面，经访谈并核查得知，机房具有防雨水渗透措施，设置了墙壁防水层、双层玻璃，并对窗口进行了防护措施。

在防静电方面，经访谈并核查得知，机房内具有防静电地板；机房内采取了接地措施。

在温湿度控制方面，经访谈并核查得知，机房内配有专用的精密空调；机房内温度:22℃至 23℃，湿度:45%至 55%。

在电力供应方面，经访谈并核查得知，机房具有稳压器和过电压防护设备；现场观测时稳压器和过电压防护设备处于正常工作状态。具有 UPS 后备电源系统；UPS 满足短期断电时的供电要求（2 小时）。

在电磁防护方面，经访谈并核查得知，电源线缆和通信线缆隔离铺设在线槽里。

3.1.2 主要安全问题汇总分析

1）消防装置为手动灭火，未开启自动灭火功能。

机房内的设备可能因电气故障、过载或其他原因而引发火灾，而缺乏自动灭火系统可能导致火势迅速蔓延，增加人员安全和设备损坏的风险，涉及测评对象**信息机房。**

2）未采取措施防止地下积水的转移和渗透。

地下积水可能侵蚀电缆、管道等基础设施，导致电力供应中断、供水系统故

障等问题，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

光华荣昌智能数字化平台系统在安全通信网络方面采取了以下安全措施：

在网络架构方面，经访谈并核查得知，已按照重要性原则划分了边界防护区、运维管理区、服务器区等区域，并为各区域分配了地址；网络拓扑图区域划分情况与实际运行环境一致。经访谈并核查得知，被测系统具有与实际网络运行情况相符的网络拓扑图；重要网络区域未部署在网络边界处；区域之间采用 VLAN 隔离技术进行区域间的逻辑隔离。

3.2.2 主要安全问题汇总分析

1）未采用校验技术保证通信过程中数据的完整性。

未采用校验技术保证通信过程中数据的完整性，如果没有数据完整性检查机制，接收方可能无法意识到数据已经损坏，从而导致错误的解释或决策，涉及测评对象**安全通信网络**。

2）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，也未将验证结果形成审计记录送至安全管理中心。

未基于可信根对通信设备进行可信验证，无法保证通信设备底层、应用程序的可信验证，存在未授权或滥用的风险，可信性遭到破坏时无法进行告警、记录，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

光华荣昌智能数字化平台系统在安全区域边界方面采取了以下安全措施：

在边界防护方面，经核查，系统在网络边界处部署了边界防火墙，配置了双向的访问控制策略，策略指定通过特定端口进行通信，保证了网络边界访问的安全性，并且每条访问控制规则均有明确的源 IP 地址、目的 IP 地址以及协议端口等。

在访问控制方面，经核查，网络边界处部署了边界防火墙进行访问控制，配置了合理的访问控制规则，防火墙为隐式拒绝防火墙，默认最后一条为拒绝所有通信。边界防火墙中的访问控制规则已进行相关的优化，不存在多余的、无效的访问控制规则，访问控制规则之间的逻辑关系和前后排序合理，不存在矛盾的地方，并且访问控制规则的数量达到了最小化。防火墙通过配置访问控制策略，对源地址、目的地址、源端口、目的端口和服务协议等进行检查，允许或拒绝数据包进出。经测试，未经授权的 IP 或端口无法访问系统设备，访问控制策略的配置参数有效。边界防火墙能够根据会话状态检测表追踪连接会话状态，并结合前后会话关系综合判断，能够为进出的数据流提供明确的允许/拒绝的能力。

在入侵防范方面，经核查，网络边界处部署有网络入侵防御系统，可以用于检测和限制从外部发起的网络攻击行为，网络入侵防御系统的安全防护策略覆盖了网络中的所有关键节点，网络入侵防御系统的热门威胁库规则库已更新到最新版本（2024-10-16）。

在恶意代码防范方面，经核查，网络边界处部署有网络入侵防御系统，可以对网络环境中的恶意代码进行检测和清除，漏洞攻击特征识别库已更新到最新版本（2024-8-14）。经测试，网络入侵防御系统的安全防护策略处于有效运行状态。

在安全审计方面，经核查，网络设备、安全设备、服务器、数据库和应用系统均启用了安全审计功能，可以对登录事件、操作事件和相关安全事件进行审计，审计覆盖到每个用户。网络入侵防御系统的审计记录包括事件的序号、攻击者 IP、归属地、严重等级、影响业务/服务器、事件描述、攻击事件、操作等审计相关信息。经核查、网络入侵防御系统、WEB 应用防火墙、上网行为管理等关键计算节点设备产生的日志定时推送到日志分析管理系统（192.168.5.253）中，审计日志留存时间满足 6 个月。

3.3.2 主要安全问题汇总分析

1）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，也未将验证结果形成审计记录送至安全管理中心。

未基于可信根对边界设备进行可信验证，无法保证边界设备底层、应用程序的可信验证，存在未授权或滥用的风险，可信性遭到破坏时无法进行告警、记录，涉及测评对象**互联网接入区。**

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

光华荣昌智能数字化平台系统在安全计算环境网络设备方面采取了以下安全措施：

在身份鉴别方面，经核查，网络设备启用了登录失败处理功能和登录连接超时自动退出功能，连续登录失败 3 次锁定账号 5 分钟，登录后无操作 20 分钟，设备自动退出登录状态。网络设备采用 HTTPS 协议进行远程管理，可以防止鉴别信息在网络传输中被窃听。

在访问控制方面，经核查，网络设备已修改默认账户的默认口令。网络设备不存在多余或过期账户，且管理员用户与账户之间一一对应，不存在多人使用同一账户的情况。

在安全审计方面，经核查，网络设备已开启安全审计功能，可以对登录事件、操作事件等重要用户行为和重要安全事件进行审计，审计覆盖到每个账户。网络设备的审计记录包括事件的日志时间、日志模块、日志级别、日志助记符、日志内容等审计相关信息。网络设备产生的日志每月进行本地备份，审计日志留存时间满足 6 个月。

在入侵防范方面，经核查，网络设备安装的组件均为业务所需，已遵循最小安装原则。网络设备关闭了非必要的系统服务和高危端口。已对终端接入方式进行限制，交换机通过运维安全管理系统进行登录管理。

在数据完整性方面，经核查，网络设备采用 HTTPS 协议进行通信传输，可

以保证鉴别数据、重要配置数据、重要审计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

1）核心交换机未配置口令复杂度校验和口令有效期策略。

缺乏口令复杂度校验和口令有效期策略可能减弱系统的整体安全性，用户可能会选择简单、易于猜测或容易破解的密码，增加了系统遭受口令猜测、字典攻击和暴力攻击的风险；如果用户的密码被泄露，攻击者可以长时间使用这些凭据进行未经授权的访问，导致数据泄露和安全漏洞，涉及测评对象**核心交换机。**

2）核心交换机未限制默认账户的访问权限。

未限制默认账户的访问权限，可能会被攻击者利用来获取未经授权的访问权限，从而对系统进行潜在的恶意操作或数据泄露，涉及测评对象**核心交换机。**

3）核心交换机未划分审计管理员、安全管理员账号，且存在超级管理员账户，不能实现管理用户的权限分离。

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；管理用户拥有的权限越高，意味着他们能够访问的数据范围越广泛。如果这些用户的账户被攻击者入侵，可能会导致敏感数据的泄露或篡改，涉及测评对象**核心交换机。**

4）核心交换机未定期对设备/系统进行漏洞扫描。

未定期对设备/系统进行漏洞扫描，可能会增加黑客攻击的风险，导致数据泄露、系统瘫痪或其他安全事故，涉及测评对象**核心交换机。**

5）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，也未将验证结果形成审计记录送至安全管理中心。

未基于可信根对计算设备进行可信验证，无法保证计算设备底层、应用程序的可信验证,存在未授权或滥用的风险,可信性遭到破坏时无法进行告警、记录，涉及测评对象**核心交换机。**

6）核心交换机未定期对备份文件进行恢复测试。

未定期对备份文件进行恢复测试，可能会在实际需要恢复数据时发现备份文件无法正常恢复，导致面临长时间的业务中断、数据丢失或不完整的恢复，涉及测评对象**核心交换机。**

7）核心交换机未将重要数据定时备份至异地。

未将重要数据定时备份至异地，如果发生灾难性事件，如硬件故障、自然灾害或恶意攻击，未进行异地定时备份的数据可能会永久丢失，导致无法恢复重要数据，进而影响业务系统可用性，涉及测评对象**核心交换机。**

3.4.2 安全设备

3.4.2.1 已有安全控制措施汇总分析

光华荣昌智能数字化平台系统在安全计算环境安全设备方面采取了以下安全措施:

在身份鉴别方面，经核查，安全设备采用“用户名+静态口令”方式对用户进行身份标识和鉴别；查看用户列表得知，身份标识具有唯一性，不存在空口令用户；已启用口令复杂度策略,要求口令最小长度 8 位,口令由数字、大写字母、小写字母、特殊字符中的两种组成，并配置了口令每隔 90 天更换一次。安全设备启用了登录失败处理功能和登录连接超时自动退出功能,连续登录失败 5 次锁

定账号 30 分钟，登录后无操作 10 分钟，设备自动退出登录状态。安全设备采用 HTTPS 协议进行远程管理，可以防止鉴别信息在网络传输中被窃听。

在访问控制方面，经核查，安全设备已修改默认账户的默认口令。安全设备不存在多余或过期账户，且管理员用户与账户之间一一对应，不存在多人使用同一账户的情况。已对登录的用户分配了账号和权限，已限制默认账户 admin 的访问权限。安全设备已按照三权分立原则，划分了系统管理员 sysadmin、安全管理员 secadmin、审计管理员 audadmin，并为其分配了不同权限或角色，已限制默认账户 admin 的访问控制权限。

在安全审计方面，经核查，安全设备已开启安全审计功能，可以对登录事件、操作事件等重要用户行为和重要安全事件进行审计，审计覆盖到每个账户。安全设备的审计记录包括事件的用户名、IP 地址、操作权限、操作时间、配置类型、操作过程、操作结果等审计相关信息。安全设备产生的日志定时推送到日志分析管理系统（192.168.5.253）中，审计日志留存时间满足 6 个月。

在入侵防范方面，经核查，安全设备安装的组件均为业务所需，已遵循最小安装原则。安全设备关闭了非必要的系统服务和高危端口。已对终端接入方式进行限制，安全设备通过运维安全管理系统进行登录管理。安全设备安装的组件均为业务所需，已遵循最小安装原则。

在数据完整性方面，经核查，安全设备采用 HTTPS 协议进行通信传输，可以保证鉴别数据、重要配置数据、重要审计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

1）网络入侵防御系统、上网行为管理、VPN、WEB 应用防火墙、日志分析管理

系统、边界防火墙未限制默认账户的访问权限。

未限制默认账户的访问权限，可能会被攻击者利用来获取未经授权的访问权限，从而对系统进行潜在的恶意操作或数据泄露，涉及测评对象**网络入侵防御系统、上网行为管理、VPN、WEB 应用防火墙、日志分析管理系统、边界防火墙。**

2）网络入侵防御系统、上网行为管理、VPN、WEB 应用防火墙、日志分析管理系统、边界防火墙未划分审计管理员、安全管理员账号，且存在超级管理员账户，不能实现管理用户的权限分离。

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；管理用户拥有的权限越高，意味着他们能够访问的数据范围越广泛。如果这些用户的账户被攻击者入侵，可能会导致敏感数据的泄露或篡改，涉及测评对象**网络入侵防御系统、上网行为管理、VPN、WEB 应用防火墙、日志分析管理系统、边界防火墙。**

3）网络入侵防御系统、上网行为管理、VPN、WEB 应用防火墙、日志分析管理系统、运维安全管理系统、边界防火墙未定期对设备/系统进行漏洞扫描。

未定期对设备/系统进行漏洞扫描，可能会增加黑客攻击的风险，导致数据泄露、系统瘫痪或其他安全事故，涉及测评对象**网络入侵防御系统、上网行为管理、VPN、WEB 应用防火墙、日志分析管理系统、运维安全管理系统、边界防火墙。**

4）网络入侵防御系统、上网行为管理、VPN、WEB 应用防火墙、日志分析管理系统、运维安全管理系统、边界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，也未将验证结果形成审计记录送至安全管理中心。

未基于可信根对计算设备进行可信验证，无法保证计算设备底层、应用程序的可信验证，存在未授权或滥用的风险，可信性遭到破坏时无法进行告警、记录，

涉及测评对象**网络入侵防御系统、上网行为管理、VPN、WEB 应用防火墙、日志分析管理系统、运维安全管理系统、边界防火墙。**

5）网络入侵防御系统、上网行为管理、VPN、WEB 应用防火墙、日志分析管理系统、运维安全管理系统、边界防火墙未定期对备份文件进行恢复测试。

未定期对备份文件进行恢复测试，可能会在实际需要恢复数据时发现备份文件无法正常恢复，导致面临长时间的业务中断、数据丢失或不完整的恢复，涉及测评对象**网络入侵防御系统、上网行为管理、VPN、WEB 应用防火墙、日志分析管理系统、运维安全管理系统、边界防火墙。**

6）网络入侵防御系统、上网行为管理、VPN、WEB 应用防火墙、日志分析管理系统、运维安全管理系统、边界防火墙未将重要数据定时备份至异地。

未将重要数据定时备份至异地，如果发生灾难性事件，如硬件故障、自然灾害或恶意攻击，未进行异地定时备份的数据可能会永久丢失，导致无法恢复重要数据，进而影响业务系统可用性，涉及测评对象**网络入侵防御系统、上网行为管理、VPN、WEB 应用防火墙、日志分析管理系统、运维安全管理系统、边界防火墙。**

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

光华荣昌智能数字化平台系统在安全计算环境服务器和终端方面采取了以下安全措施：

在身份鉴别方面，经核查，服务器已勾选“要使用本计算机，用户必须输入

用户名和密码”；每个账户身份标识具有唯一性；无空口令用户；密码必须符合复杂性要求：已启用（口令需包含数字、小写字母、大写字母、特殊字符中的三类），密码长度最小值：8 个字符；密码最长使用期限：29 天。已启用“远程（RDP）连接要求使用指定的安全层”，安全层为 SSL（TLS1.0），可以保证鉴别信息在网络传输过程中被窃听。服务器采用 SSH 协议进行远程管理，可以防止鉴别信息在网络传输中被窃听。终端已勾选“要使用本计算机，用户必须输入用户名和密码”；每个账户身份标识具有唯一性；无空口令用户；

在访问控制方面，经核查，服务器已对用户或用户组权限进行合理分配；访问 C 盘的 Program Files 文件夹，已限制默认账户 Administrator 的访问控制权限。已禁用默认账户 Guest，已修改默认账户 Administrator 的默认口令。不存在多余或过期账户，且管理员用户与账户之间一一对应，不存在多人使用同一账户的情况。已修改默认账户 root 的默认口令。不存在多余或过期账户，且管理员用户与账户之间一一对应，不存在多人使用同一账户的情况。

在安全审计方面，经核查，服务器审计记录包括日志名称、来源、事件 ID、级别、用户、操作代码、记录时间、任务类别、关键字、计算机等审计相关信息。服务器产生的日志定时推送到日志分析管理系统中，审计日志留存时间满足 6 个月。服务器已开启 audit 和 rsyslog 服务，审计覆盖到每个用户，能够对重要的用户行为和重要安全事件进行审计。服务器审计记录包括日期/时间、对象、路径、相关系统调用、用户 ID、用户组 ID、命令、可执行文件路径等审计相关信息。非授权账户无法访问审计日志，系统产生的日志定时推送到日志分析管理系统（192.168.5.253）中，审计日志留存时间满足 6 个月。

在入侵防范方面，经核查，服务器无多余组件，无多余应用程序，无多余系

统服务，未开启默认共享；服务器开启了 135、139、445 等高危端口，但已在主机防火墙入站规则中制定了高危端口阻断策略，策略名为禁用 135、139、445。已对终端接入方式进行限制，服务器通过运维安全管理系统进行登录管理。

在恶意代码防范方面，经核查，服务器安装了火绒安全软件，可以识别恶意代码和病毒行为并进行阻断，特征库已更新至最新版本（2024-10-16 18:22）。服务器安装了 360 安全卫士，可以识别恶意代码和病毒行为并进行阻断，特征库已更新至最新版本（2024-09-26）。

在数据完整性方面，经核查，服务器已启用“远程（RDP）连接要求使用指定的安全层”，安全层为 SSL（TLS1.0），可以保证鉴别数据、重要配置数据、重要审计数据在传输过程中的完整性。服务器采用 SSH 协议进行远程管理，可以保证鉴别数据、重要配置数据、重要审计数据在传输过程中的完整性。

在剩余信息保护方面，经核查，服务器“交互式登录：不显示最后的用户名”安全设置为已启用状态，能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。服务器自身具有剩余信息处理机制，用户注销后，系统会进行相关的剩余信息处理，可以完全清除鉴别信息所处的存储空间。

3.4.3.2 主要安全问题汇总分析

1）ERP 服务器未配置口令复杂度校验和口令有效期策略。

缺乏口令复杂度校验和口令有效期策略可能减弱系统的整体安全性，用户可能会选择简单、易于猜测或容易破解的密码，增加了系统遭受口令猜测、字典攻击和暴力攻击的风险；如果用户的密码被泄露，攻击者可以长时间使用这些凭据进行未经授权的访问，导致数据泄露和安全漏洞，涉及测评对象 **ERP 服务器。**

2）BPM 服务器、ERP 服务器未配置登录失败处理和登录连接超时自动退出功能。

缺乏登录失败处理和登录连接超时自动退出功能可能减弱系统的整体安全性，如果系统不及时锁定或禁止登录失败次数过多的账户，攻击者可能通过暴力攻击或密码猜测获得未经授权的访问权限;如果用户长时间保持登录状态而未采取措施进行自动退出，可能会使系统受到会话劫持、敏感信息泄露和其他安全漏洞的攻击，涉及测评对象 **BPM 服务器、ERP 服务器。**

3）ERP 服务器未限制默认账户的访问权限。

未限制默认账户的访问权限，可能会被攻击者利用来获取未经授权的访问权限，从而对系统进行潜在的恶意操作或数据泄露，涉及测评对象 **ERP 服务器。**

4）BPM 服务器、ERP 服务器、BPM 数据库服务器未划分审计管理员、安全管理员账号，且存在超级管理员账户，不能实现管理用户的权限分离。

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；管理用户拥有的权限越高，意味着他们能够访问的数据范围越广泛。如果这些用户的账户被攻击者入侵，可能会导致敏感数据的泄露或篡改，涉及测评对象 **BPM 服务器、ERP 服务器、BPM 数据库服务器。**

5）BPM 服务器、BPM 数据库服务器审计记录内容不全面。

审计记录内容不全面可能导致重要信息丢失或无法追踪，使得在需要时无法对业务活动进行准确的审计和监控，增加面临的风险，涉及测评对象 **BPM 服务器、BPM 数据库服务器。**

6）BPM 服务器、ERP 服务器、运维终端、BPM 数据库服务器、办公终端未定期对设备/系统进行漏洞扫描。

未定期对设备/系统进行漏洞扫描，可能会增加黑客攻击的风险，导致数据泄露、系统瘫痪或其他安全事故，涉及测评对象**BPM 服务器、ERP 服务器、运维终端、BPM 数据库服务器、办公终端。**

7）ERP 服务器、运维终端、办公终端未安装防恶意代码软件。

服务器未安装防病毒软件，设备容易受到各种恶意软件（如病毒、蠕虫、木马等）的感染，导致系统崩溃、数据损坏或盗取等安全问题，涉及测评对象**ERP 服务器、运维终端、办公终端。**

8）BPM 服务器、ERP 服务器、运维终端、BPM 数据库服务器、办公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，也未将验证结果形成审计记录送至安全管理中心。

未基于可信根对计算设备进行可信验证，无法保证计算设备底层、应用程序的可信验证,存在未授权或滥用的风险,可信性遭到破坏时无法进行告警、记录，涉及测评对象**BPM 服务器、ERP 服务器、运维终端、BPM 数据库服务器、办公终端。**

9）BPM 服务器、ERP 服务器、BPM 数据库服务器未定期对备份文件进行恢复测试。

未定期对备份文件进行恢复测试，可能会在实际需要恢复数据时发现备份文件无法正常恢复，导致面临长时间的业务中断、数据丢失或不完整的恢复，涉及测评对象**BPM 服务器、ERP 服务器、BPM 数据库服务器。**

10）BPM 服务器、ERP 服务器、BPM 数据库服务器未将重要数据定时备份至异地。

未将重要数据定时备份至异地，如果发生灾难性事件，如硬件故障、自然灾

害或恶意攻击，未进行异地定时备份的数据可能会永久丢失，导致无法恢复重要数据，进而影响业务系统可用性，涉及测评对象 **BPM 服务器、ERP 服务器、BPM 数据库服务器。**

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

光华荣昌智能数字化平台系统在安全计算环境系统管理软件/平台方面采取了以下安全措施：

在安全审计方面，经核查，通过“BPM 应用系统站点属性”得知，中间件已开启安全审计功能，可以对访问事件和重要安全事件进行审计。日志格式为 W3C，审计记录包括发出请求时候的日期、客户端 IP 地址、用户名、服务名、服务器的名称、服务器的 IP 地址、为服务配置的服务器端口号、请求中使用的 HTTP 方法、URI 资源、URI 资源、协议状态等审计相关信息。非授权用户无法访问审计日志，审计日志每天进行本地归档备份，日志留存时间满足 6 个月。数据库启用了安全审计功能，审计覆盖到每个用户，已设置登录审核策略为“失败和成功的登录”，并启用“C2 审核跟踪”，可以对登录事件、操作事件等进行审计。数据库的审计记录包括事件时间、源、信息和事件结果等信息。数据库审计日志存放在数据库中，数据库每天全量备份，数据库的审计日志可以保存 6 个月以上。数据库已开启安全审计功能，可以对登录事件、操作事件等重要用户行为和重要安全事件进行审计，审计覆盖到每个账户。数据库的审计记录包括事件的日期和时间、用户、事件类型、事件是否成功等审计相关信息。

在数据完整性方面，经核查，IIS 中间件的身份鉴别功能由 Windows 操作系统实现，中间件所在的服务器采用 RDP（安全层为 SSL（TLS1.0））协议进行通信传输，能够保证鉴别数据、重要配置数据和重要审计数据在传输过程中的完整性。数据库只能通过所在的服务器进行管理，服务器已启用“远程（RDP）连接要求使用指定的安全层”，安全层为 RDP，可以保证鉴别数据、重要审计数据、重要配置数据、重要业务数据和个人信息在传输过程中的完整性。数据库只能通过所在的服务器进行管理，服务器采用 SSH 协议进行远程管理，可以保证鉴别数据、重要审计数据、重要配置数据、重要业务数据和个人信息在传输过程中的完整性。

在身份鉴别方面，经核查，数据库采用 SQL Server 和 Windows 身份验证模式进行身份标识和鉴别，用户名具有唯一性，勾选了“强制实施密码策略”已引用所在服务器身份鉴别策略（密码必须符合复杂性要求：已启用，密码长度最小值：8 个字符），密码最长使用期限：90 天。数据库采用 SQL Server 和 Windows 身份验证模式进行身份鉴别，数据库所在服务器已启用登录失败处理功能，账户锁定时间：30 分钟，账户锁定阈值：5 次无效登录，重置账户锁定计数器：30 分钟；通过查看“远程服务器连接→远程查询超时值”得知，空闲查询超时退出时间为 600 秒。数据库只能通过所在的服务器进行管理，服务器已启用“远程(RDP)连接要求使用指定的安全层”，安全层为 RDP，可以防止鉴别信息在网络传输过程中被窃听。数据库只能通过所在的服务器进行管理，服务器采用 SSH 协议进行远程管理，可以防止鉴别信息在网络传输过程中被窃听。

在访问控制方面，经核查，已修改默认账户 sa 的默认口令。数据库不存在多余的、过期的账户，不存在多人使用同一账户的情况。数据库已修改默认账户

的默认口令。数据库不存在多余或过期账户，且管理员用户与账户之间一一对应，不存在多人使用同一账户的情况。

在入侵防范方面，经核查，数据库对管理员的登录地址进行了限制，只允许通过所在服务器本地登录数据库。

在数据备份恢复方面，经核查，数据库在重大变更前/后进行本地配置备份，业务数据每天进行全量备份，备份策略合理，备份结果与备份策略一致，每 1-2 个月对备份文件进行恢复测试。

在剩余信息保护方面，经核查，数据库退出登录后，不存在残留用户鉴别信息，可以完全清除鉴别信息所处的存储空间。

在个人信息保护方面，经核查，数据库仅采集和保存业务必需的用户个人信息，如用户姓名、单位等，未收集其他多余信息，并且单位制定了《个人信息管理制度》对个人信息采集、保存等内容进行规定。数据库禁止未授权访问和非法使用用户个人信息，并且单位制定了《个人信息管理制度》对个人信息的访问授权、使用等内容进行了规定。

3.4.4.2 主要安全问题汇总分析

1）ERP 系统数据库未配置口令复杂度校验和口令有效期策略。

缺乏口令复杂度校验和口令有效期策略可能减弱系统的整体安全性，用户可能会选择简单、易于猜测或容易破解的密码，增加了系统遭受口令猜测、字典攻击和暴力攻击的风险；如果用户的密码被泄露，攻击者可以长时间使用这些凭据进行未经授权的访问，导致数据泄露和安全漏洞，涉及测评对象 **ERP 系统数据库。**

2）ERP 系统数据库未配置登录失败处理和登录连接超时自动退出功能。

缺乏登录失败处理和登录连接超时自动退出功能可能减弱系统的整体安全性，如果系统不及时锁定或禁止登录失败次数过多的账户，攻击者可能通过暴力攻击或密码猜测获得未经授权的访问权限;如果用户长时间保持登录状态而未采取措施进行自动退出，可能会使系统受到会话劫持、敏感信息泄露和其他安全漏洞的攻击，涉及测评对象 **ERP 系统数据库。**

3）ERP 系统数据库、BMP 系统数据库未限制默认账户的访问权限。

未限制默认账户的访问权限，可能会被攻击者利用来获取未经授权的访问权限，从而对系统进行潜在的恶意操作或数据泄露，涉及测评对象 **ERP 系统数据库、BMP 系统数据库。**

4）ERP 系统数据库、BMP 系统数据库未划分审计管理员、安全管理员账号，且存在超级管理员账户，不能实现管理用户的权限分离。

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；管理用户拥有的权限越高，意味着他们能够访问的数据范围越广泛。如果这些用户的账户被攻击者入侵，可能会导致敏感数据的泄露或篡改，涉及测评对象 **ERP 系统数据库、BMP 系统数据库。**

5）ERP 系统数据库、BMP 系统数据库、中间件未定期对设备/系统进行漏洞扫描。

未定期对设备/系统进行漏洞扫描，可能会增加黑客攻击的风险，导致数据泄露、系统瘫痪或其他安全事故，涉及测评对象 **ERP 系统数据库、BMP 系统数据库、中间件。**

6）ERP 系统数据库、BMP 系统数据库、中间件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，也未将验证结果形成审计记录送至安全管理中心。

未基于可信根对计算设备进行可信验证，无法保证计算设备底层、应用程序的可信验证,存在未授权或滥用的风险,可信性遭到破坏时无法进行告警、记录，涉及测评对象 **ERP 系统数据库、BMP 系统数据库、中间件。**

7）ERP 系统数据库、中间件未定期对备份文件进行恢复测试。

未定期对备份文件进行恢复测试，可能会在实际需要恢复数据时发现备份文件无法正常恢复，导致面临长时间的业务中断、数据丢失或不完整的恢复，涉及测评对象 **ERP 系统数据库、中间件。**

8) ERP 系统数据库、BMP 系统数据库、中间件未将重要数据定时备份至异地。

未将重要数据定时备份至异地，如果发生灾难性事件，如硬件故障、自然灾害或恶意攻击，未进行异地定时备份的数据可能会永久丢失，导致无法恢复重要数据，进而影响业务系统可用性，涉及测评对象 **ERP 系统数据库、BMP 系统数据库、中间件。**

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

光华荣昌智能数字化平台系统在安全计算环境业务应用系统/平台方面采取了以下安全措施：

在访问控制方面，经核查，应用系统已修改默认账户的默认口令。应用系统由系统管理员进行角色划分与权限分配,基于权限列表对登录的账户进行模块化

授权，并删除了默认账户。应用系统不存在多余或过期账户，且管理员用户与账户之间一一对应，不存在多人使用同一账户的情况。应用系统已按照三权分立原则，划分了系统管理员、安全管理员、审计管理员，并为其分配了不同权限或角色，实现了管理用户的权限分离。

在安全审计方面,经核查,应用系统已开启安全审计功能,可以对登录事件、操作事件等重要用户行为和重要安全事件进行审计，审计覆盖到每个账户。应用系统的审计记录包括事件的 ID、UserID、User、IP、place、时间日期等审计相关信息。应用系统审计日志存放在数据库中,数据库每天对审计日志进行全量备份，审计日志留存时间满足 6 个月。应用系统的审计记录包括事件的日期和时间、用户、事件类型、事件是否成功等审计相关信息。

在入侵防范方面，经核查，应用系统提供了数据有效性检验功能，对文本输入框进行了格式和长度限制，如输入包含特殊字符的语句时，系统进行了字符转义，可以正常处理请求。

在数据备份恢复方面，经核查，应用系统在重大变更前/后进行本地配置备份，业务数据每天进行全量备份，备份策略合理，备份结果与备份策略一致，每 1-2 个月对备份文件进行恢复测试。

在剩余信息保护方面，经核查，应用系统退出登录后无法通过复制链接直接访问应用系统，需要重新进行登录验证，应用系统的临时文件未有残留的用户鉴别信息，可以保证鉴别信息所处的存储空间被释放或重新分配前得到完全清除。

在个人信息保护方面，经核查，应用系统仅采集和保存业务必需的用户个人信息，如用户姓名、单位等，未收集其他多余信息，并且单位制定了《个人信息管理制度》对个人信息采集、保存等内容进行规定。应用系统禁止未授权访问和

非法使用用户个人信息，并且单位制定了《个人信息管理制度》对个人信息的访问授权、使用等内容进行了规定。

在身份鉴别方面，经核查，应用系统启用了登录失败处理功能和登录连接超时自动退出功能，连续登录失败 3 次锁定账号，由管理员解锁，登录后无操作 60 分钟，设备自动退出登录状态。

3.4.5.2 主要安全问题汇总分析

1）BPM 系统、ERP 系统未配置口令复杂度校验和口令有效期策略。

缺乏口令复杂度校验和口令有效期策略可能减弱系统的整体安全性，用户可能会选择简单、易于猜测或容易破解的密码，增加了系统遭受口令猜测、字典攻击和暴力攻击的风险；如果用户的密码被泄露，攻击者可以长时间使用这些凭据进行未经授权的访问，导致数据泄露和安全漏洞，涉及测评对象 **BPM 系统、ERP 系统。**

2）BPM 系统未配置登录失败处理和登录连接超时自动退出功能。

缺乏登录失败处理和登录连接超时自动退出功能可能减弱系统的整体安全性，如果系统不及时锁定或禁止登录失败次数过多的账户，攻击者可能通过暴力攻击或密码猜测获得未经授权的访问权限；如果用户长时间保持登录状态而未采取措施进行自动退出，可能会使系统受到会话劫持、敏感信息泄露和其他安全漏洞的攻击，涉及测评对象 **BPM 系统。**

3）BPM 系统、ERP 系统未采取措施防止鉴别信息在网络传输过程中被窃听。

未经加密的鉴别信息在传输过程中可能被恶意用户或黑客窃听并获取，导致个人隐私泄露或敏感信息暴露，涉及测评对象 **BPM 系统、ERP 系统。**

4）BPM 系统未限制默认账户的访问权限。

未限制默认账户的访问权限，可能会被攻击者利用来获取未经授权的访问权限，从而对系统进行潜在的恶意操作或数据泄露，涉及测评对象 **BPM 系统。**

5）BPM 系统存在多余测试账户。

多余账户的口令可能被恶意用户猜测获得，或账号被滥用，导致被非授权访问，涉及测评对象 **BPM 系统。**

6）BPM 系统未划分审计管理员、安全管理员账号，且存在超级管理员账户，不能实现管理用户的权限分离。

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；管理用户拥有的权限越高，意味着他们能够访问的数据范围越广泛。如果这些用户的账户被攻击者入侵，可能会导致敏感数据的泄露或篡改，涉及测评对象 **BPM 系统。**

7）BPM 系统、ERP 系统未定期对设备/系统进行漏洞扫描。

未定期对设备/系统进行漏洞扫描，可能会增加黑客攻击的风险，导致数据泄露、系统瘫痪或其他安全事故，涉及测评对象 **BPM 系统、ERP 系统。**

8）BPM 系统、ERP 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，也未将验证结果形成审计记录送至安全管理中心。

未基于可信根对计算设备进行可信验证，无法保证计算设备底层、应用程序的可信验证，存在未授权或滥用的风险，可信性遭到破坏时无法进行告警、记录，涉及测评对象 **BPM 系统、ERP 系统。**

9）BPM 系统、ERP 系统未采用校验技术保证重要数据在传输过程中的完整性。

未采用校验技术保证重要数据在传输过程中的完整性，可能导致数据的内容

被修改、损坏或替换，发生信息泄露、错误的数据解释或错误的决策等事件，影响业务的正常运作和数据的完整性，涉及测评对象 **BPM 系统、ERP 系统。**

10）ERP 系统未定期对备份文件进行恢复测试。

未定期对备份文件进行恢复测试，可能会在实际需要恢复数据时发现备份文件无法正常恢复，导致面临长时间的业务中断、数据丢失或不完整的恢复，涉及测评对象 **ERP 系统。**

11）BPM 系统、ERP 系统未将重要数据定时备份至异地。

未将重要数据定时备份至异地，如果发生灾难性事件，如硬件故障、自然灾害或恶意攻击，未进行异地定时备份的数据可能会永久丢失，导致无法恢复重要数据，进而影响业务系统可用性，涉及测评对象 **BPM 系统、ERP 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

光华荣昌智能数字化平台系统在安全计算环境数据资源方面采取了以下安全措施：

在剩余信息保护方面，经核查，Windows 服务器已开启“交互式登录：不显示最后的用户名”能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；Linux 服务器自身具有剩余信息处理机制，用户注销后，系统会进行相关的剩余信息处理，可以完全清除鉴别信息所处的存储空间；数据库用户在退出或注销时会自动清除鉴别信息所在的存储空间，不会残留用户鉴别信息；应用系统退出登录后无法通过复制链接直接访问应用系统，需要重新进行登录验证，应用

系统的临时文件未有残留的用户鉴别信息。

在个人信息保护方面，经核查，应用系统仅采集和保存业务必需的用户个人信息，如用户姓名、单位等，未收集其他多余信息，并且单位制定了《个人信息管理制度》对个人信息采集、保存等内容进行规定。应用系统禁止未授权访问和非法使用用户个人信息，并且单位制定了《个人信息管理制度》对个人信息的访问授权、使用等内容进行了规定。

3.4.6.2 主要安全问题汇总分析

1）鉴别数据、审计数据、业务数据、个人信息、配置数据未采用校验技术保证重要数据在传输过程中的完整性。

未采用校验技术保证重要数据在传输过程中的完整性，可能导致数据的内容被修改、损坏或替换，发生信息泄露、错误的数据解释或错误的决策等事件，影响业务的正常运作和数据的完整性，涉及测评对象**鉴别数据、审计数据、业务数据、个人信息、配置数据。**

2）业务数据、配置数据未定期对备份文件进行恢复测试。

未定期对备份文件进行恢复测试，可能会在实际需要恢复数据时发现备份文件无法正常恢复，导致面临长时间的业务中断、数据丢失或不完整的恢复，涉及测评对象**业务数据、配置数据。**

3）业务数据、配置数据未将重要数据定时备份至异地。

未将重要数据定时备份至异地，如果发生灾难性事件，如硬件故障、自然灾害或恶意攻击，未进行异地定时备份的数据可能会永久丢失，导致无法恢复重要数据，进而影响业务系统可用性，涉及测评对象**业务数据、配置数据。**

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

该系统不涉及其他系统或设备。

3.4.7.2 主要安全问题汇总分析

该系统不涉及其他系统或设备。

3.5 安全管理中心

3.5.1 已有安全控制措施汇总分析

光华荣昌智能数字化平台系统在安全管理中心方面采取了以下安全措施：

在系统管理方面，经核查，网络设备、安全设备、服务器通过运维安全管理系统进行登录，堡垒机和各设备已划分系统管理员账号，已对系统管理员进行了身份鉴别;设备均开启了日志审计功能,可以对系统管理员的操作行为进行审计。网络设备、安全设备、服务器已划分系统管理员，系统管理员的管理和操作权限有别于审计管理员和安全管理员,指定由系统管理员对设备的资源和运行进行配置、控制和管理,其中包括账户创建、系统资源配置和重要数据的备份与恢复等。

3.5.2 主要安全问题汇总分析

1）网络设备、部分安全设备、部分服务器未划分审计管理员账户，无法对审

计管理员进行身份鉴别、授权、操作审计等。

网络设备和部分安全设备没有单独的审计管理员账户意味着部分管理员具有审计日志的访问权限，可能导致审计操作无法被追踪到具体的个人账户，不能确保审计日志的完整性和可信度，涉及测评对象**安全管理中心。**

2）网络设备、部分安全设备、部分服务器未划分审计管理员账户，不能通过审计管理员对审计记录进行分析。

网络设备和部分安全设备没有单独的审计管理员账户意味着部分管理员具有审计日志的访问权限，可能导致审计操作无法被追踪到具体的个人账户，不能确保审计日志的完整性和可信度，涉及测评对象**安全管理中心。**

3.6 安全管理制度

3.6.1 已有安全控制措施汇总分析

光华荣昌智能数字化平台系统在安全管理制度方面采取了以下安全措施：

在安全策略方面，经核查，该单位已制定《信息安全策略总纲 V1.1》明确了该单位的信息安全建设原则、总体方针和各类安全策略，如物理安全策略、网络安全策略、系统安全策略等，明确了安全工作的目标、范围和原则等。

在管理制度方面，经核查，该单位已经建立了完善的安全管理制度，有《信息安全策略总纲 V1.1》、《信息安全岗位职责要求 V1.1》、《机房管理制度》等，其内容涵盖了全体单位人员、物理环境、安全建设、安全运维等方面。该单位已提供《运行维护和监控管理规定 V1.1》、《防火墙策略配置规范 v1.0》。

在制定和发布方面，经核查，该单位已制定《信息安全策略总纲 V1.1》明确

了由第信息管理部负责实施和制定具体的安全要求和流程，并形成相应的管理制度。该单位在《信息安全策略总纲 V1.1》→制度的制定与发布中，明确了安全管理制度的制定应具有统一的格式，对制度进行了编号和版本控制；安全管理制度经信息安全领导小组讨论通过，由信息安全领导小组负责人审批发布，并且在其中注明了相应的发布范围。

3.6.2 主要安全问题汇总分析

1）未提供信息安全管理制度评审与修订记录。

缺乏安全管理制度论证审定记录意味着无法保证安全管理制度在实际环境下实施的合理性和适用性，尤其是在出现重大变更(如组织变更、环境变更、管理要求变更)等情况下的合理性和适用性，涉及测评对象**安全管理制度。**

3.7 安全管理机构

3.7.1 已有安全控制措施汇总分析

光华荣昌智能数字化平台系统在安全管理机构方面采取了以下安全措施：

在岗位设置方面，经核查，该单位设立了信息安全领导小组，已制定《信息安全策略总纲 V1.1》明确了信息安全领导小组的构成情况和工作职责，其最高领导由单位主管领导委任。该单位设立了信息安全部负责网络安全管理工作，已制定《信息安全岗位职责要求 V1.1》明确安全主管、安全管理各个方面的负责人的岗位和职责。

在人员配备方面，经核查，该单位已制定《信息安全岗位职责要求 V1.1》明

确设立安全管理员、系统管理员、审计管理员等，提供了信息安全人员名单，配备了安全管理员、系统管理员、审计管理员各一名。

在授权和审批方面，经核查，该单位已制定《信息安全策略总纲 V1.1》明确了信息安全领导小组负责信息系统的所有安全管理活动相关事宜，第一审批人为单位主管领导，关键安全管理活动一律由第一审批人或授权责任人审批，并且已经提供了《变更申请表》等审批记录表单。明确了对于信息系统中发生的重大及关键安全管理活动的授权和审批过程，已建立了完善的逐级审批程序，要求必须通过部门负责人和单位主管领导的双重审批，并且《变更申请表》等记录表单的审批结果和管理制度要求一致。

在沟通和合作方面，经核查，该单位已制定《信息安全策略总纲 V1.1》明确了与单位外部沟通的机制和流程，包括与各类设备供应商、业界专家等的沟通，并且提供了腾讯会议记录，会议主题明确了会议内容。该单位提供了《外联单位联系列表》，列表包含了外联单位名称、合作内容、联系人和联系方式等内容。

3.7.2 主要安全问题汇总分析

1）未提供单位内部关于信息安全的沟通交流记录。

缺乏沟通交流记录会使得在发生安全事件或威胁时的应对变得困难，可能会导致对策的不一致性，从而降低了应对安全事件的效率和效果，涉及测评对象**安全管理机构。**

2）未提供常规性安全检查记录。

未提供常规性安全检查记录，缺乏定期的安全检查可能导致安全漏洞未被及时发现和修复，从而增加被攻击的风险，涉及测评对象**安全管理机构。**

3.8 安全管理人员

3.8.1 已有安全控制措施汇总分析

光华荣昌智能数字化平台系统在安全管理人员方面采取了以下安全措施：

在人员录用方面，经核查及访谈，该单位已制定《人员安全管理制度 V1.1》明确了由人力资源部负责人员招聘、录用和离职等工作。《人员安全管理制度 V1.1》明确要求负责人员从候选简历中挑选出初步符合所招岗位的人员进行面试、笔试和复试，并对其身份、背景、专业资格和资质进行审查。提供了《录用人员审查表》明确了录用人员的学习简历、工作经历、单位意见、考核结果等内容。

在人员离岗方面，经核查，该单位已制定《人员安全管理制度 V1.1》明确了当人员离职时，按照单位离职流程，归还所持有的信息资产，归还所有的物理安全设备，包括笔记本、门禁卡、钥匙和证件等，终止该员工的所有访问权限，撤销该员工的账号，收回该员工曾掌握过的密码或密钥，并确认密码或密钥的正确性。

在安全意识教育和培训方面，经核查，该单位已制定《人员安全管理制度 V1.1》明确了安全培训的各项内容以及安全职责、惩戒措施等相关内容；每年至少进行一次安全意识和岗位技能培训，已提供《培训签到表》明确了培训内容和参与人员。

在外部人员访问管理方面，经核查，该单位已制定《外部人员访问管理规定》规范了外部人员的来访流程，明确了外包人员的访问范围、进入条件等。制定了《外来人员进出机房申请表》，由单位接待人员填写后，经单位领导审批通过后，

还必须由接待人员陪同，陪同人员填写《机房人员进出登记表》后才能进入机房进行访问。提供了《外来人员进出机房申请表》明确了审批人签字等内容；提供了《机房人员进出登记表》明确了人员的进出时间、陪同人员等内容。该单位已制定《外部人员访问管理制度 V1.1》明确了外部人员离场后应及时清除其所有的访问权限。运维安全管理系统可以查看到访问权限被清除的时间以及相关账号等。

3.8.2 主要安全问题汇总分析

1 未提供外部人员访问申请记录

缺乏外部人员访问申请记录，可能导致难以追踪和管理谁进入了敏感区域或访问了重要系统，增加了信息泄露和物理安全风险，涉及测评对象**安全管理人员。**

3.9 安全建设管理

3.9.1 已有安全控制措施汇总分析

光华荣昌智能数字化平台系统在安全建设管理方面采取了以下安全措施：

在定级和备案方面，经核查，《光华荣昌智能数字化平台系统网络安全等级保护定级报告》文档内容已经明确该系统的安全保护等级以及定级的方法和理由。该单位已组织相关部门和技术专家对定级结果的合理性和正确性进行论证和审定，并提供了《光华荣昌智能数字化平台系统网络安全等级保护定级评审意见》。该系统的定级结果已获得相关部门批准，并取得备案证明。该单位已将系统备案材料上传至北京市公安局昌平分局进行备案，并取得备案证明，备案证编号：

11011499364-24001。

在安全方案设计方面，经核查，《光华荣昌智能数字化平台系统网络安全等级保护定级报告》已明确系统安全保护等级为第二级；被测单位已按照第二级保护需求进行了安全加固和调整。

在产品采购和使用方面，经核查，该单位的相关网络安全产品采购和使用已符合国家的有关规定，具有销售许可证明。

在外包软件开发方面，经核查，该单位已提供《软件设计说明书》、《系统操作手册》等。

在工程实施方面，经核查，该单位由信息安全部负责对工程实施过程进行监督和管理。

在系统交付方面，经核查，该单位提供了《系统交付清单》明确了系统资产、项目阶段文档等内容。该单位已提供《软件设计说明书》、《系统操作手册》，但未提供《项目测试验收报告》、《运维培训记录表》等记录表单。

在等级测评方面，经核查，该系统暂无发生过重大变更或级别发生变化，在《信息安全策略总纲 V1.1》中，规定系统发生重大变更或者系统等级发生变化后，将相关修订实施细则报信息安全办公室进行备案，并开展等级测评。该单位已选取符合国家有关规定的测评机构开展等级测评工作。本次等级测评选取的测评机构为国源天顺科技产业集团有限公司，该测评机构已获得公安部第三研究所（国家认证认可委员会批准的认证机构）认证发放的《网络安全等级测评与检测评估机构服务认证证书》，认证证书编号为 SC202127130010050。

在服务供应商选择方面，经核查及访谈，该单位选择的服务供应商（国源天顺科技产业集团有限公司、深信服科技股份有限公司）具备相应的安全服务资质，

符合国家有关规定。该单位已与选定的服务供应商签订了合同协议，明确约定了相关责任、技术培训、服务承诺、服务期限等内容。

3.9.2 主要安全问题汇总分析

1）无相关的安全规划设计类文档和被测系统安全方案设计文档。

缺乏安全规划设计文档意味着可能没有全面评估和识别系统中的安全漏洞和潜在风险。这会使得系统更容易受到未知威胁和攻击，涉及测评对象**安全建设管理。**

2）未提供整体安全规划和安全方案设计的专家论证文档和批准意见。

在缺乏专家论证、审定的情况下，安全设计方案可能不符合合理性和正确性的要求，导致组织面临合规性问题和法律责任，涉及测评对象**安全建设管理。**

3）未提供恶意代码检测报告。

未在软件交付前检测其中可能存在的恶意代码，可能会导致系统遭受安全攻击，并使单位承担一定的法律责任等，涉及测评对象**安全建设管理。**

4）未制定安全工程实施方案控制工程实施过程。

没有明确的安全工程实施方案，可能导致在项目或系统开发过程中缺乏必要的安全控制措施，使得工程实施过程缺乏计划性或不可控，涉及测评对象**安全建设管理。**

5）未提供测试验收方案和测试验收报告。

缺乏测试验收方案和报告可能意味着无法保证工程交付的质量和完整性是否符合要求，增加了质量风险，可能会导致系统不稳定或功能不完善，涉及测评对象**安全建设管理。**

6）未在系统上线前进行安全性测试。

缺乏安全性测试报告意味着未能充分评估系统的安全性，可能存在未发现的安全漏洞和弱点,使系统容易受到攻击或数据泄露,涉及测评对象**安全建设管理。**

7）未提供对运行维护技术人员的相关的技术培训记录。

缺乏技术培训，技术人员可能会在运维过程中遇到困难和挑战，导致执行效率低下、操作不规范等，对系统安全稳定运行带来的风险，涉及测评对象**安全建设管理。**

8）未提供《项目测试验收报告》、《运维培训记录表》等记录表单，系统交付文档不完善。

信息系统交付后缺少项目测试验收报告意味着无法准确评估项目交付的质量,可能会导致未能及时发现项目中存在的风险和问题;缺少《运维培训记录表》,可能导致在员工离职或转岗时知识流失,新员工无法获得必要的培训信息和指导,从而影响到系统的稳定性和运行效率，涉及测评对象**安全建设管理。**

3.10 安全运维管理

3.10.1已有安全控制措施汇总分析

光华荣昌智能数字化平台系统在安全运维管理方面采取了以下安全措施:

在环境管理方面，经核查及访谈，该单位已制定《机房管理制度》明确了由机房管理员对机房的环境安全和网络通信等进行管理；提供了《机房设备运行及维护记录》明确了设备参数、用途和设备运行是否正常等；覆盖了机房的物理环境、物理访问、物品进出、人员出入等内容的管理，提供了《机房人员出入登记

表》明确了来访人员、来访时间、携带物品等内容。该单位已制定《北京光华荣昌汽车部件有限公司办公环境安全管理制度》明确了办公区应设置专门的接待区域，由接待人员统一处理外来人员的出入申请，在受访者陪同下进入办公区域；办公区内不得随意存放涉及单位管理、技术、财务、人力资源等部门机密信息。

在资产管理方面，经核查，该单位已制定《北京光华荣昌汽车部件有限公司办公环境安全管理制度》明确了资产管理员应制定和维护所管辖的资产清单，提供了《信息设备资产清单》明确了资产类别、责任部门、所处地点、存放形式等内容。

在介质管理方面，经访谈并核查得知，当前使用的存储介质形态是：硬盘；存放环境是：系统管理员保存，负责的部门或人员是：系统管理员；盘点记录：《存储介质管理登记表》，内容包括：介质名称、介质数量、盘点人、盘点时间。经核查及访谈，该单位已制定《存储介质管理规定》明确了对介质的传输过程进行控制，资产管理员对存储介质的转移和支配必须进行登记，填写《信息系统存储介质使用清单》,对存储介质传递过程需要有记录并定期对登记记录进行复核；提供了《信息系统存储介质使用清单》明确了介质的使用情况、归还情况等内容。

在设备维护管理方面，经访谈并核查得知，系统管理员负责对各类设备进行定期维护；具有明确设备维护管理责任部门的文件；文件名：《资产安全管理制度》，制度要求和访谈结果一致。

在网络和系统安全管理方面，经访谈并核查得知，具有管理员职责文档；职责文件名：《信息安全管理组织职责》，文件明确各个角色的责任和权限，包括网络管理员、系统管理员、安全管理员、审计管理员等角色；与技术测评人员核实，网络和系统的运维管理人员和职责文件定义一致。具有网络和系统安全管理

制度；文件名：《信息系统安全审核和安全检查管理制度》；3)制度内容包括：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，内容覆盖全面。1)具有重要设备的配置和操作手册；2)文件名：《防火墙策略配置规范》、《安全域划分规范》、《入侵检测系统策略配置规范》、《终端安全管理制度》，手册内容包括操作步骤、维护记录、参数配置等；具有对系统进行日常操作、运维管理等工作记录；记录名：《操作日志》内容包括日常巡检工作、运行维护记录、参数的设置和修改等。

在恶意代码防范管理方面，经访谈并核查得知，采取定期培训方式提升员工的防恶意代码意识；具有提升员工防恶意代码意识的培训记录或宣贯记录；记录名：《安全培训记录表》；制定了《北京光华荣昌汽车部件有限公司恶意代码防范管理制度》，对恶意代码检查作出了规定，对外来计算机或存储设备接入系统前进行恶意代码检查。具有恶意代码防范措施，已制定《北京光华荣昌汽车部件有限公司恶意代码防范管理制度》；具有恶意代码防范措施特征库的更新记录，内容包括主程序版本、病毒库日期。经核查及访谈，该单位已定期对安全设备的恶意代码库进行升级，并且对截获的恶意代码进行分析和汇总上报，已经提供了《恶意代码库升级记录》和《恶意代码分析报告》。

在配置管理方面，经访谈并核查得知，具有对配置信息进行保存的记录；记录名：《北京光华荣昌汽车部件有限公司信息网络安全检查实施细则》，内容包括应记录和保存基本配置信息，包括网络拓扑结构、IP 地址、软件组件的版本和补丁信息等，已提供相关的配置信息记录，覆盖全面。

在密码管理方面，经核查，《信息安全策略总纲 V1.1》中明确要求安全管理员在密码管理过程中必须遵循密码相关标准和规定，要求重要数据的传输和存储

必须使用安全的加密算法。

在备份与恢复管理方面，经访谈并核查得知，具有定期备份的重要业务信息、系统数据及软件系统的备份记录；备份重要业务信息的周期是每天增量备份、每周全量备份，备份记录清单名称是《存储介质管理登记表》；备份系统数据的周期是每天增量备份、每周全量备份，备份记录清单名称是《存储介质管理登记表》；备份软件系统的周期是每天增量备份、每周全量备份，备份记录清单名称是《存储介质管理登记表》；具有备份与恢复管理制度；文件名：《北京光华荣昌汽车部件有限公司数据备份与恢复管理办法》，内容包括：对应用系统、操作系统、数据库系统、网络系统等的业务数据和系统数据进行定期备份，每天增量备份，每周全量备份，备份数据保留在硬盘中，备份保留 1 年，内容覆盖全面。具有备份恢复策略和程序；文件名：《北京光华荣昌汽车部件有限公司数据备份与恢复管理办法》，内容包括：明确数据备份策略和恢复策略、备份程序和恢复程序等，内容根据数据的重要程度制定。

在安全事件处置方面，经访谈并核查得知，具有明确告知用户在发现安全弱点和可疑事件时应及时向安全管理部门报告的文件；文件名：《北京光华荣昌汽车部件有限公司信息安全事件报告和处置管理制度》；具有安全弱点和可疑事件对应的报告或记录；报告或记录：《安全检查报告及安全检查表》。具有安全事件管理制度；文件名：《北京光华荣昌汽车部件有限公司信息安全事件报告和处置管理制度》，内容包括：明确安全事件的报告、处置和响应流程，并且规定安全事件的现场处理、事件报告，内容覆盖全面；具有安全事件报告的模板文件；模板文件名：《安全检查报告及安全检查表》经核查，该单位已制定《安全事件报告和处置管理制度 V1.1》规范安全事件报告和响应处理流程，要求事件调查

组利用合法手段在安全事件现场收取证据;向信息系统使用或维护单位了解事件发生经过,收集相关资料,查明事件发生的原因、危害程度及造成的损失等情况,检查预防和控制事件发生的措施以及事件发生后应急预案是否得当并得到落实,确定事件的级别和性质,查明相关责任并提出处理建议,提出防止类似事件再次发生的措施和建议。

在应急预案管理方面，经访谈并核查得知，具有重要事件的专项应急预案，针对机房(供电、火灾、漏水等)、系统(病毒爆发、数据泄露等)、网络(断网、拥塞等)等各个层面；具有专项事件应急预案，内容包含：应急处理流程、恢复流程。定期对系统相关的人员进行应急预案培训和演练：每年组织次应急预案培训和演练，演练内容：通过演练发现应急工作体系和工作机制存在的问题，不断完善应急预案，提高应急处置能力；具有应急预案的培训记录、演练记录；应急预案的培训记录：《应急预案培训记录》，内容包括：培训人员、培训时间、培训内容、培训地点爱 5)应急预案演练记录：《应急预案演练记录》，内容包括：演练方式、演练目的、演练内容、整改措施。

3.10.2主要安全问题汇总分析

1）未提供维修审批、维修过程等方面的记录。

缺乏维修审批和过程记录可能导致无法跟踪和验证维修工作的执行情况，可能导致维修操作不规范和报废设备泄密，增加安全事故发生的风险；当出现维修问题或者设备损坏时，无法确定责任人员和维修历史，影响责任追究和问题的解决，涉及测评对象**安全运维管理。**

2）单位未采取必要的措施识别安全漏洞和隐患，未提供漏洞扫描报告。

未定期进行漏洞扫描，系统存在的安全漏洞可能会长时间存在而不被发现，增加未授权人员利用漏洞攻击信息系统的风险，涉及测评对象**安全运维管理。**

3）未提供账户管理相关审批记录或流程文件。

缺乏审批记录和流程文件意味着缺乏对账户管理过程的透明度和监督，可能导致安全漏洞的存在，例如未经授权的账户访问或权限提升，涉及测评对象**安全运维管理。**

4）未提供变更方案评审记录。

缺乏变更方案评审记录意味着没有对变更提出合理的建议或反对意见进行评审和记录；没有变更过程记录会使得变更实施的过程不透明，可能导致变更方案的实施过程中出现混乱、误解或错误，从而增加变更带来的风险，涉及测评对象**安全运维管理。**

3.11 其他安全要求指标

3.11.1 已有安全控制措施汇总分析

本次测评不涉及其他安全要求指标。

3.11.2 主要安全问题汇总分析

本次测评不涉及其他安全要求指标。

3.12 验证测试

对光华荣昌智能数字化平台系统进行测评，涉及到漏洞扫描工具、渗透性测

试工具集等多种测试工具。为了发挥测评工具的作用，达到测评的目的，各种测评工具需要接入到被测系统网络中，并配置合法的网络 IP 地址。

3.12.1漏洞扫描

3.12.1.1 漏洞扫描结果统计

通过使用绿盟远程安全评估系统 V6.0R04F 对网络设备、安全设备、服务器、终端设备进行了漏洞扫描。

针对被测系统的网络边界和抽查设备、主机和业务应用系统的情况，需要在被测系统及其互联网络中设置各测试工具接入点，如图 3-1 所示。

接入点 JA：在 Internet 接入，主要目的是：模拟外部恶意用户发现操作系统、数据库、应用系统等安全漏洞的过程，并尝试利用以上漏洞实施诸如获取系统控制权（GetShell）、获得大量敏感信息（DragLibrary）等模拟攻击行为。

接入点 JB：在服务器区接入，主要目的是：模拟内部恶意用户发现操作系统、数据库、应用系统等安全漏洞的过程，并尝试利用以上漏洞实施诸如获取系统控制权（GetShell）、获得大量敏感信息（DragLibrary）等模拟攻击行为。

使用设备名称:

1.绿盟远程安全评估系统 V6.0

系统版本 : V6.0R04F04

系统插件版本 : V6.0R02F01.3507

Web 插件版本 : V6.0R02F00.3406

资产指纹版本 : V6.0R04F02.0108

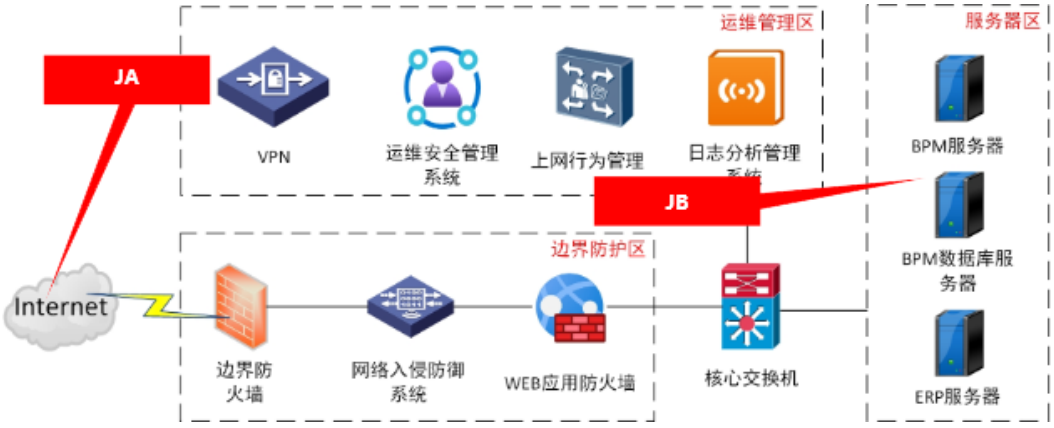

图 3-1 漏洞扫描工具接入测试示意图

（1）接入点 JA 漏洞扫描结果统计

接入点 JA 的漏洞扫描结果汇总如下表所示。

表 3-1 接入点 JA 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	BPM 系统（http://neiwang.bjghrc.com/#/_TAB）	V1.0	0	0	0	0
安全漏洞数量合计			0	0	0	0

（2）接入点 JB 漏洞扫描结果统计

接入点 JB 的漏洞扫描结果汇总如下表所示。

表 3-2 接入点 JB 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	核心交换机 (192.168.0.1)	V200R019C00SPC500B327	0	0	6	6
2	BPM 数据库服务器 (192.168.0.5)	Microsoft Windows Server 2012 R2 Datacenter	0	2	16	18
3	ERP 服务器 (192.168.0.204)	Red Hat Enterprise Linux Server release 7.2 (Maipo)	0	0	1	1

序号	设备名称	系统及版本	安全漏洞数量			
			高	中	低	小计
4	BPM 服务器 (192.168.0.16)	Microsoft Windows Server 2012 R2 Standard	0	0	4	4
5	上网行为管理 (192.168.10.218)	AC11.0R2	0	2	5	7
6	日志分析管理系统 (192.168.5.253)	SIP-Logger3.0.22 Build20240103	0	0	1	1
7	VPN(192.168.12.254)	7.1	0	0	1	1
8	运维终端 (192.168.5.93)	Windows 10 专业版	0	0	1	1
安全漏洞数量合计			0	4	35	39

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，光华荣昌智能数字化平台系统存在的主要安全漏洞汇总如下表所示。

表 3-3 接入点 JA 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
接入点 JA 未测试出安全漏洞			

表 3-4 接入点 JB 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	获取 SSL 证书中的 hostname【原理扫描】	192.168.0.1 192.168.0.5 192.168.10.218	低
2	获取目标 SSL 证书过期时间【原理扫描】	192.168.0.1 192.168.10.218	低
3	检测到目标主机加密通信	192.168.0.1	低

序号	安全漏洞名称	关联资产/域名	严重程度
	支持的 SSL 加密算法【原理扫描】	192.168.10.218	
4	SMTP 服务器版本信息可被获取	192.168.0.1 192.168.0.5 192.168.0.204 192.168.0.16 192.168.12.254 192.168.5.93	低
5	探测到服务器支持的 SSL 加密协议【原理扫描】	192.168.0.1 192.168.0.5	低
6	可通过 HTTP 获取远端 WWW 服务信息	192.168.0.1 192.168.0.5 192.168.0.16	低
7	检测到目标 SSL 证书已过期【原理扫描】	192.168.0.5	中
8	服务器支持 TLS Client-initiated 重协商攻击(CVE-2011-1473)【原理扫描】	192.168.0.5	中
9	使用了自签名证书【原理扫描】	192.168.0.5	低
10	SSL 证书链不完整【原理扫描】	192.168.0.5	低
11	SSL 证书无法受到信任【原理扫描】	192.168.0.5	低
12	Oracle Database Server 安全漏洞(CVE-2014-2478)	192.168.0.5	低
13	Oracle Enterprise Manager Grid Control Enterprise	192.168.0.5	低

序号	安全漏洞名称	关联资产/域名	严重程度
	Manager for Oracle Database 组件安全漏洞 (CVE-2014-6488)		
14	Oracle Database Server Core RDBMS 组件安全漏洞(CVE-2013-3790)	192.168.0.5	低
15	远端 VMWARE SERVER 服务正在运行	192.168.0.5	低
16	Oracle tnslsnr 的版本可以查询	192.168.0.5	低
17	服务器允许 SSL 会话恢复【原理扫描】	192.168.0.5 192.168.5.253 192.168.10.218	低
18	工作站服务正在运行	192.168.0.5	低
19	远程主机计算机名检测	192.168.0.5 192.168.0.16	低
20	远程桌面服务(RDS)协议探测	192.168.0.5 192.168.0.16	低
21	伪来源 IP 地址的 DNS 远程攻击漏洞(CVE-2006-0987)【原理扫描】	192.168.10.218	中
22	远端 DNS 服务允许递归查询	192.168.10.218	中
23	检测到远端 DNS 服务正在运行中	192.168.10.218	低

3.12.2渗透测试

被测系统安全保护等级为第二级（S2A2），不涉及渗透测试。

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 3-5 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
安全通用要求						
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			√
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	系统管理	√		

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
31		心	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			自行软件开发			
49			外包软件开发		√	
50			工程实施		√	
51			测试验收			√
52			系统交付		√	
53			等级测评	√		
54			服务供应商选择	√		
55		安全运维管理	环境管理	√		
56			资产管理	√		
57			介质管理	√		
58			设备维护管理		√	
59			漏洞和风险管理			√
60			网络和系统安全管理		√	
61			恶意代码防范管理	√		
62			配置管理	√		
63			密码管理	√		
64			变更管理		√	
65			备份与恢复管理	√		
66			安全事件处置	√		
67			应急预案管理	√		
68			外包运维管理			

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
控制点符合情况数量统计				39	22	5

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 3-6 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
安全通用要求						
T1	消防装置为手动灭火，未开启自动灭火功能。	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；
T2	未采取措施防止地下积水的转移和渗透。	信息机房			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。
T3	未采用校验技术保证通信过程中数据的完整性。	安全通信网络		安全通信网络	通信传输	a) 应采用校验技术保证通信过程中数据的完整性。
T4	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，也未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			可信验证	a) 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。
T5	未基于可信根对边界设备的系统引导程	互联网接入区		安全区域边界		a) 可基于可信根对边界设备的系统引导程序、系统程序、重要

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
	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，也未将验证结果形成审计记录送至安全管理中心。					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。
T6	BPM 系统、ERP 服务器、ERP 系统、ERP 系统数据库、核心交换机未配置口令复杂度校验和口令有效期策略。	BPM 系统、ERP 服务器、ERP 系统、ERP 系统数据库、核心交换机		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；
T7	BPM 服务器、BPM 系统、ERP 服务器、ERP 系统数据库未配置登录失败处理和登录连接超时自动退出功能。	BPM 服务器、BPM 系统、ERP 服务器、ERP 系统数据库				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；
T8	BPM 系统、ERP 系统未采取措施防止鉴别信息在网络传输过程中被窃听。	BPM 系统、ERP 系统				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。
T9	BMP 系统数据库、BPM 系统、ERP 服务器、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、日志分析管理系统、核	BMP 系统数据库、BPM 系统、ERP 服务器、ERP 系统数据库、VPN、WEB 应用防火			访问控制	a) 应对登录的用户分配账户和权限；

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
	心交换机、网络入侵防御系统、边界防火墙未限制默认账户的访问权限。	墙、上网行为管理、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙				
T10	BPM 系统存在多余测试账户。	BPM 系统				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；
T11	BMP 系统数据库、BPM 数据库服务器、BPM 服务器、BPM 系统、ERP 服务器、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙未划分审计管理员、安全管理员账号，且存在超级管理员账户，不能实现管理用户的权限分离。	BMP 系统数据库、BPM 数据库服务器、BPM 服务器、BPM 系统、ERP 服务器、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙				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。
T12	BPM 数据库服务器、BPM 服务器审计记录内容不全面。	BPM 数据库服务器、BPM 服务器			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

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
						进行审计；
T13	BMP 系统数据库、BPM 数据库服务器、BPM 服务器、BPM 系统、ERP 服务器、ERP 系统、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、中间件、办公终端、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙、运维安全管理系统、运维终端未定期对设备/系统进行漏洞扫描。	BMP 系统数据库、BPM 数据库服务器、BPM 服务器、BPM 系统、ERP 服务器、ERP 系统、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、中间件、办公终端、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙、运维安全管理系统、运维终端			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；
T14	ERP 服务器、办公终端、运维终端未安装防恶意代码软件。	ERP 服务器、办公终端、运维终端			恶意代码防范	a) 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。
T15	BMP 系统数据库、BPM 数据库服务器、BPM 服务器、	BMP 系统数据库、BPM 数据库服务			可信验证	a) 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

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
	BPM 系统、ERP 服务器、ERP 系统、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、中间件、办公终端、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙、运维安全管理系统、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，也未将验证结果形成审计记录送至安全管理中心。	器、BPM 服务器、BPM 系统、ERP 服务器、ERP 系统、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、中间件、办公终端、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙、运维安全管理系统、运维终端				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。
T16	BPM 系统、ERP 系统、业务数据、个人信息、审计数据、配置数据、鉴别数据未采用校验技术保证重要数据在传输过程中的完整性。	BPM 系统、ERP 系统、业务数据、个人信息、审计数据、配置数据、鉴别数据			数据完整性	a) 应采用校验技术保证重要数据在传输过程中的完整性。
T17	BPM 数据库服务器、BPM 服务器、ERP 服务器、ERP 系	BPM 数据库服务器、BPM 服务器、			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、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、业务数据、中间件、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙、运维安全管理系统、配置数据未定期对备份文件进行恢复测试。	ERP 服务器、ERP 系统、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、业务数据、中间件、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙、运维安全管理系统、配置数据				
T18	BMP 系统数据库、BPM 数据库服务器、BPM 服务器、BPM 系统、ERP 服务器、ERP 系统、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、业务数据、中间件、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火	BMP 系统数据库、BPM 数据库服务器、BPM 服务器、BPM 系统、ERP 服务器、ERP 系统、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管				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
	墙、运维安全管理系统、配置数据未将重要数据定时备份至异地。	理、业务数据、中间件、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙、运维安全管理系统、配置数据				
T19	网络设备、部分安全设备、部分服务器未划分审计管理员账户，无法对审计管理员进行身份鉴别、授权、操作审计等。	安全管理中心		安全管理中心	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；
T20	网络设备、部分安全设备、部分服务器未划分审计管理员账户，不能通过审计管理员对审计记录进行分析。	安全管理中心				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。
T21	未提供信息安全管理制度评审与修订记录。	安全管理制度		安全管理制度	评审和修订	a) 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。
T22	未提供单位内部关于信息安全的沟通交流记录。	安全管理机构		安全管理机构	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

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
						同协作处理网络安全问题；
T23	未提供常规性安全检查记录。	安全管理机构			审核和检查	a) 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。
T24	未提供外部人员访问申请记录	安全管理人员		安全管理人员	外部人员访问管理	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；
T25	无相关的安全规划设计类文档和被测系统安全方案设计文档。	安全建设管理		安全建设管理	安全方案设计	b) 应根据保护对象的安全保护等级进行安全方案设计；
T26	未提供整体安全规划和安全方案设计的专家论证文档和批准意见。	安全建设管理				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。
T27	未提供恶意代码检测报告。	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；
T28	未制定安全工程实施方案控制工程实施过程。	安全建设管理			工程实施	b) 应制定安全工程实施方案控制工程实施过程。
T29	未提供测试验收方案和测试验收报告。	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；
T30	未在系统上线前进行安全性测试。	安全建设管理				b) 应进行上线前的安全性测试，并出具安全测试报告。
T31	未提供对运行维护技术人员的相关的技术	安全建设管理			系统交付	b) 应对负责运行维护的技术人员进行相应的技能培训；

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
	培训记录。					
T32	未提供《项目测试验收报告》、《运维培训记录表》等记录表单，系统交付文档不完善。	安全建设管理				c) 应提供建设过程文档和运行维护文档。
T33	未提供维修审批、维修过程等方面的记录。	安全运维管理		安全运维管理	设备维护管理	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。
T34	单位未采取必要的措施识别安全漏洞和隐患，未提供漏洞扫描报告。	安全运维管理			漏洞和风险管理	a) 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。
T35	未提供账户管理相关审批记录或流程文件。	安全运维管理			网络和系统安全管理	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；
T36	未提供变更方案评审记录。	安全运维管理			变更管理	a) 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

安全控制点间的安全测评主要考虑同一区域内、同一层面上的不同安全控制点间存在的功能增强、补充或削弱等关联作用。安全功能上的增强和补充可以使两个不同强度、不同等级的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。

在安全计算环境层面“身份鉴别”要求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。在本次测评过程中，BPM 系统、ERP 系统未配置口令复杂度校验和口令有效期策略，但设备/系统当前口令满足口令复杂度要求，并且管理制度要求，口令长度 8 位以上，由三类字符组成；设备/系统通过运维安全管理系统进行管理；以上安全措施能在一定程度上降低此问题带来的风险。

4.2 区域间安全测评

区域间的安全测评主要考虑互连互通（包括物理上和逻辑上的互连互通等）的不同区域之间存在的安全功能增强、补充和削弱等关联作用，特别是有数据交换的两个不同区域。

在安全计算环境层面“身份鉴别”要求当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。在本次测评过程中，BPM 系统、ERP 系统未采取措施防止鉴别信息在网络传输过程中被窃听，但系统关闭了互联网访问方式，外部网络访问系统需通过 VPN 接入内部网络，VPN 采用 SSL 技术，能够

建立一条安全、加密的通信链路；系统具有登录失败处理措施，能够在错误一定次数，锁定登录账号，避免恶意的口令爆破；以上安全措施能在一定程度上降低此问题带来的风险。

在安全计算环境层面“入侵防范”要求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。在本次测评过程中，未定期对设备/系统进行漏洞扫描，但网络设备、安全设备、服务器等通过运维安全管理系统进行管理，并在网络层部署了边界防火墙、网络入侵防御系统、WEB 应用防火墙，能够对边界访问流量进行访问控制、网络层入侵检测以及应用层 WEB 防护等；经漏扫扫描测试，当前系统不存在已知的高危漏洞；以上安全措施能在一定程度上降低此问题带来的风险。

在安全计算环境层面“恶意代码防范”要求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。在本次测评过程中，服务器、终端未安装防恶意代码软件，但服务器通过运维安全管理系统进行管理，并在网络层部署有网络入侵防御系统，可以对网络环境中的恶意代码进行检测和清除，漏洞攻击特征识别库已更新到最新版本（2024-8-14）；以上安全措施能在一定程度上降低此问题带来的风险。

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
安全通用要求				
T5	未配置口令复杂度校验和口令有效期	BPM 系统、ERP	设备/系统当前口令满足口令复杂度要求，并且管理制度要求，口令	☐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
	策略。	服务器、ERP 系统、ERP 系统数据库、核心交换机	长度 8 位以上，由三类字符组成；设备/系统通过运维安全管理系统进行管理；以上安全措施能在一定程度上降低此问题带来的风险。	
T7	未采取措施防止鉴别信息在网络传输过程中被窃听。	BPM 系统、ERP 系统	系统关闭了互联网访问方式，外部网络访问系统需通过 VPN 接入内部网络，VPN 采用 SSL 技术，能够建立一条安全、加密的通信链路；系统具有登录失败处理措施，能够在错误一定次数，锁定登录账号，避免恶意的口令爆破；以上安全措施能在一定程度上降低此问题带来的风险。	□升高 ☑降低
T12	未定期对设备/系统进行漏洞扫描。	BMP 系统数据库、BPM 数据库服务器、BPM 服务器、BPM 系统、ERP 服务器、ERP 系统、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、中间件、办公终端、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙、运维安全管理系统、运维终端	网络设备、安全设备、服务器等通过运维安全管理系统进行管理，并在网络层部署了边界防火墙、网络入侵防御系统、WEB 应用防火墙，能够对边界访问流量进行访问控制、网络层入侵检测以及应用层 WEB 防护等；经漏扫扫描测试，当前系统不存在已知的高危漏洞；以上安全措施能在一定程度上降低此问题带来的风险。	□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
T13	未安装防恶意代码软件。	ERP 服务器、办公终端、运维终端	服务器通过运维安全管理系统进行管理，并在网络层部署有网络入侵防御系统，可以对网络环境中的恶意代码进行检测和清除，漏洞攻击特征识别库已更新到最新版本（2024-8-14）；以上安全措施能在一定程度上降低此问题带来的风险。	☐升高 ☑降低

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[3]	关联威胁	危害分析结果	风险等级
安全通用要求						
1	安全物理环境	消防装置为手动灭火，未开启自动灭火功能。	信息机房	物理环境影响	机房内的设备可能因电气故障、过载或其他原因而引发火灾，而缺乏自动灭火系统可能导致火势迅速蔓延，增加人员安全和设备损坏的风险。	中
2		未采取措施防止地下积水的转移和渗透。	信息机房	物理环境影响	地下积水可能侵蚀电缆、管道等基础设施，导致电力	中

[3] 如风险值和评价相同，可填写多个关联资产。

序号	安全类	安全问题	关联资产[3]	关联威胁	危害分析结果	风险等级
					供应中断、供水系统故障等问题。	
3	安全通信网络	未采用校验技术保证通信过程中数据的完整性。	安全通信网络	篡改	未经校验的通信可能会被攻击者篡改，攻击者可能在传输过程中修改数据包，从而改变数据的内容，这可能导致信息泄露、损坏或误导	中
4		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，也未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	抵赖	无法保证通信设备底层、应用程序的可信验证，存在未授权或滥用的风险，可信性遭到破坏时无法进行告警、记录。	低
5	安全区	未基于可信	互联网接	抵赖	无法保证边界	低

序号	安全类	安全问题	关联资产[3]	关联威胁	危害分析结果	风险等级
	域边界	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，也未将验证结果形成审计记录送至安全管理中心。	入区		设备底层、应用程序的可信验证，存在未授权或滥用的风险，可信性遭到破坏时无法进行告警、记录。	
6	安全计算环境	BPM 系统、ERP 服务器、ERP 系统、ERP 系统数据库、核心交换机未配置口令复杂度校验和口令有效期策略。	BPM 系统、ERP 服务器、ERP 系统、ERP 系统数据库、核心交换机	恶意攻击	缺乏口令复杂度校验和口令有效期策略可能减弱系统的整体安全性，用户可能会选择简单、易于猜测或容易破解的密码，增加了系统遭受口令猜测、字典攻击和暴力攻击的风险；如果用户的密码被泄露，攻	中

序号	安全类	安全问题	关联资产[3]	关联威胁	危害分析结果	风险等级
					击者可以长时间使用这些凭据进行未经授权的访问，导致数据泄露和安全漏洞。	
7		BPM 服务器、BPM 系统、ERP 服务器、ERP 系统数据库未配置登录失败处理和登录连接超时自动退出功能。	BPM 服务器、BPM 系统、ERP 服务器、ERP 系统数据库	恶意攻击，抵赖	如果系统不及时锁定或禁止登录失败次数过多的账户，攻击者可能通过暴力攻击或密码猜测获得未经授权的访问权限；如果用户长时间保持登录状态而未采取措施进行自动退出，可能会使系统受到会话劫持、敏感信息泄露和其他安全漏洞的攻击。	中
8		BPM 系统、ERP 系统未采取措	BPM 系统、ERP 系统	越权或滥用,恶意攻击,敏感信	窃听者可以截取鉴别信息，例如用户名和	中

序号	安全类	安全问题	关联资产[3]	关联威胁	危害分析结果	风险等级
		施防止鉴别信息在网络传输过程中被窃听。		息泄露	口令，从而冒充合法用户登录系统，进行未授权的操作或盗取个人资产；除了窃听外，鉴别信息也可能被篡改，导致身份验证失败或者信息被冒用。	
9		BMP 系统数据库、BPM 系统、ERP 服务器、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙未限制	BMP 系统数据库、BPM 系统、ERP 服务器、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、日志分析管理系统、核心交换机、网络入侵防御	越权或滥用	默认账户通常具有较高的权限，如果未对其进行限制，可能会被攻击者利用来获取未经授权的访问权限，从而对系统进行潜在的恶意操作或数据泄露。	中

序号	安全类	安全问题	关联资产[3]	关联威胁	危害分析结果	风险等级
		默认账户的访问权限。	系统、边界防火墙			
10		BPM 系统存在多余测试账户。	BPM 系统	越权或滥用,恶意攻击	多余账户的口令可能被恶意用户猜测获得，或账号被滥用，导致被非授权访问。	中
11		BMP 系统数据库、BPM 数据库服务器、BPM 服务器、BPM 系统、ERP 服务器、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙未划	BMP 系统数据库、BPM 数据库服务器、BPM 服务器、BPM 系统、ERP 服务器、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、日志分析管理系统、核心交换机、网络	越权或滥用	如果管理用户拥有超出其工作职责所需的权限，可能会导致滥用权限的情况发生；拥有过多权限的管理用户可能会成为攻击者的目标，因为攻击者可以利用这些权限来获取对系统的更广泛访问权限，从而增加系统受攻击的风险。	中

序号	安全类	安全问题	关联资产[3]	关联威胁	危害分析结果	风险等级
		分审计管理员、安全管理员账号，且存在超级管理员账户，不能实现管理用户的权限分离。	入侵防御系统、边界防火墙			
12		BPM 数据库服务器、BPM 服务器审计记录内容不全面。	BPM 数据库服务器、BPM 服务器	抵赖	不完善的审计记录可能导致重要信息丢失或无法追踪，使得在需要时无法对业务活动进行准确的审计和监控，增加面临的风险。	中
13		BMP 系统数据库、BPM 数据库服务器、BPM 服务器、BPM 系统、ERP 服务器、ERP 系统、	BMP 系统数据库、BPM 数据库服务器、BPM 服务器、BPM 系统、ERP 服务器、	恶意攻击，篡改	漏洞可能被恶意攻击者利用来获取系统中的敏感数据或网络入侵，导致数据泄露、业务中断等，面临勒索威胁。	中

序号	安全类	安全问题	关联资产[3]	关联威胁	危害分析结果	风险等级
		ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、中间件、办公终端、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙、运维安全管理系统、运维终端未定期对设备/系统进行漏洞扫描。	ERP 系统、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、中间件、办公终端、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙、运维安全管理系统、运维终端			
14		ERP 服务器、办公终端、运维终端未安装防恶意代码软	ERP 服务器、办公终端、运维终端	恶意攻击	服务器未安装防病毒软件，设备容易受到各种恶意软件（如病毒、蠕	中

序号	安全类	安全问题	关联资产[3]	关联威胁	危害分析结果	风险等级
		件。			虫、木马等）的感染，导致系统崩溃、数据损坏或盗取等安全问题。	
15		BMP 系统数据库、BPM 数据库服务器、BPM 服务器、BPM 系统、ERP 服务器、ERP 系统、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、中间件、办公终端、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙、运维	BMP 系统数据库、BPM 数据库服务器、BPM 服务器、BPM 系统、ERP 服务器、ERP 系统、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、中间件、办公终端、日志分析管理系统、核心	抵赖	无法保证计算设备底层、应用程序的可信验证，存在未授权或滥用的风险，可信性遭到破坏时无法进行告警、记录。	低

序号	安全类	安全问题	关联资产[3]	关联威胁	危害分析结果	风险等级
		安全管理系统、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，也未将验证结果形成审计记录送至安全管理中心。	交换机、网络入侵防御系统、边界防火墙、运维安全管理系统、运维终端			
16		BPM 系统、ERP 系统、业务数据、个人信息、审计数据、配置数据、鉴别数据未采用校验技术保证重要数据在传输过程中的完整性。	BPM 系统、ERP 系统、业务数据、个人信息、审计数据、配置数据、鉴别数据	篡改	在数据传输过程中，未经完整性保护的数据可能会被篡改，导致数据的内容被修改、损坏或替换，发生信息泄露、错误的数据解释或错误的决策等事件，影响业务	中

序号	安全类	安全问题	关联资产[3]	关联威胁	危害分析结果	风险等级
					的正常运作和数据的完整性。	
17		BPM 数据库服务器、BPM 服务器、ERP 服务器、ERP 系统、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、业务数据、中间件、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙、运维安全管理系统、配置数据未定期对备份文件进行恢复测	BPM 数据库服务器、BPM 服务器、ERP 服务器、ERP 系统、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、业务数据、中间件、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙、运维安全	无作为或操作失误	如果备份文件受损或不完整，在实际需要恢复数据时，备份文件可能无法成功恢复数据，导致数据丢失或不完整的恢复。	中

序号	安全类	安全问题	关联资产[3]	关联威胁	危害分析结果	风险等级
		试。	管理系统、配置数据			
18		BMP 系统数据库、BPM 数据库服务器、BPM 服务器、BPM 系统、ERP 服务器、ERP 系统、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、业务数据、中间件、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙、运维安全管理系统、配置数	BMP 系统数据库、BPM 数据库服务器、BPM 服务器、BPM 系统、ERP 服务器、ERP 系统、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、业务数据、中间件、日志分析管理系统、核心交换机、网络入侵	软硬件故障	如果发生灾难性事件，如硬件故障、自然灾害或恶意攻击，未进行异地定时备份的数据可能会永久丢失，导致无法恢复重要数据，进而影响业务系统可用性。	中

序号	安全类	安全问题	关联资产[3]	关联威胁	危害分析结果	风险等级
		据未将重要数据定时备份至异地。	防御系统、边界防火墙、运维安全管理系统、配置数据			
19	安全管理中心	网络设备、部分安全设备、部分服务器未划分审计管理员账户，无法对审计管理员进行身份鉴别、授权、操作审计等。	安全管理中心	越权或滥用	没有单独的审计管理员账户意味着部分管理员具有审计日志的访问权限，可能导致审计操作无法被追踪到具体的个人账户，不能确保审计日志的完整性和可信度。	中
20		网络设备、部分安全设备、部分服务器未划分审计管理员账户，不能通过审计管理员对审计记录进行分	安全管理中心	越权或滥用	没有单独的审计管理员账户意味着部分管理员具有审计日志的访问权限，可能导致审计操作无法被追踪到具体的个人账户，	低

序号	安全类	安全问题	关联资产[3]	关联威胁	危害分析结果	风险等级
		析。			不能确保审计日志的完整性和可信度。	
21	安全管理制度	未提供信息安全管理制度评审与修订记录。	安全管理制度	管理不到位	缺乏安全管理制度论证审定记录，可能导致对安全事件的响应不及时或不充分，从而增加了安全事件的严重性。	低
22	安全管理机构	未提供单位内部关于信息安全的沟通交流记录。	安全管理机构	管理不到位	缺乏沟通交流记录会使得在发生安全事件或威胁时的应对变得困难，可能会导致对策的不一致性，从而降低了应对安全事件的效率和效果。	低
23		未提供常规性安全检查记录。	安全管理机构	管理不到位	缺乏定期的安全检查可能导致安全漏洞未被及时发现和修复，从而增	中

序号	安全类	安全问题	关联资产 [3]	关联威胁	危害分析结果	风险等级
					加被攻击的风险。	
24	安全管理人员	未提供外部人员访问申请记录	安全管理人员	管理不到位	缺乏外部人员访问申请记录，可能导致难以追踪和管理谁进入了敏感区域或访问了重要系统，增加了信息泄露和物理安全风险。	中
25	安全建设管理	无相关的安全规划设计类文档和被测系统安全方案设计文档。	安全建设管理	管理不到位	缺乏安全规划设计文档意味着可能没有全面评估和识别系统中的安全漏洞和潜在风险。这会使得系统更容易受到未知威胁和攻击。	中
26		未提供整体安全规划和安全方案设计的专家论证文档和批准意见。	安全建设管理	管理不到位	未经过专家论证和审定的安全设计方案可能存在合理性与正确性的不足，导致系统	中

序号	安全类	安全问题	关联资产 [3]	关联威胁	危害分析结果	风险等级
					易受到攻击或滥用。可能包括未考虑到的安全漏洞、弱密码策略、访问控制不严格等问题，增加了系统被威胁的风险。	
27		未提供恶意代码检测报告。	安全建设管理	管理不到位	恶意代码可能会导致系统遭受安全攻击，例如数据泄露、系统瘫痪或篡改等，可能会损害用户的隐私，造成数据丢失或泄露，以及对业务流程造成严重影响。	中
28		未制定安全工程实施方案控制工程实施过程。	安全建设管理	无作为或操作失误,管理不到位	没有明确的安全工程实施方案，可能导致在项目或系统开发过程中缺乏必要的安全控制措施，使	中

序号	安全类	安全问题	关联资产 [3]	关联威胁	危害分析结果	风险等级
					得工程实施过程缺乏计划性或不可控。	
29		未提供测试验收方案和测试验收报告。	安全建设管理	无作为或操作失误,管理不到位	缺乏测试验收方案和报告可能意味着无法保证工程交付的质量和完整性是否符合要求，增加了质量风险，可能会导致系统不稳定或功能不完善。	中
30		未在系统上线前进行安全性测试。	安全建设管理	无作为或操作失误,管理不到位	缺乏安全性测试报告意味着未能充分评估系统的安全性，可能存在未发现的安全漏洞和弱点，使系统容易受到攻击或数据泄露。	中
31		未提供对运行维护技术人员的相关的技术培训	安全建设管理	无作为或操作失误,管理不到位	缺乏技术培训，技术人员可能会在运维过程中遇到困	低

序号	安全类	安全问题	关联资产[3]	关联威胁	危害分析结果	风险等级
		记录。			难和挑战，导致执行效率低下、误删除重要文件、配置错误导致系统故障等，可能造成数据丢失、服务中断或系统不稳定，给单位带来不必要的损失和风险。	
32		未提供《项目测试验收报告》、《运维培训记录表》等记录表单，系统交付文档不完善。	安全建设管理	无作为或操作失误,管理不到位	缺少项目测试验收报告意味着无法准确评估项目交付的质量，可能会导致未能及时发现项目中存在的风险和问题；缺少运维培训记录表，可能导致在员工离职或转岗时知识流失，新员工无法获得必要的培训信息和指导，	低

序号	安全类	安全问题	关联资产[3]	关联威胁	危害分析结果	风险等级
					从而影响到系统的稳定性和运行效率。	
33	安全运维管理	未提供维修审批、维修过程等方面的记录。	安全运维管理	管理不到位	缺乏维修审批和过程记录可能导致无法跟踪和验证维修工作的执行情况，可能导致维修操作不规范和报废设备泄密，增加安全事故发生的风险；当出现维修问题或者设备损坏时，无法确定责任人员和维修历史，影响责任追究和问题的解决。	低
34		单位未采取必要的措施识别安全漏洞和隐患，未提供漏洞扫描报告。	安全运维管理	管理不到位,恶意攻击	未定期进行漏洞扫描，系统存在的安全漏洞可能会长时间存在而不被发现，增加未授权人员利用	中

序号	安全类	安全问题	关联资产[3]	关联威胁	危害分析结果	风险等级
					漏洞攻击信息系统的风险。	
35		未提供账户管理相关审批记录或流程文件。	安全运维管理	管理不到位	缺乏审批记录和流程文件意味着缺乏对账户管理过程的透明度和监督，可能导致安全漏洞的存在，例如未经授权的账户访问或权限提升。	低
36		未提供变更方案评审记录。	安全运维管理	管理不到位	缺乏变更方案评审记录意味着没有对变更提出合理的建议或反对意见进行评审和记录；没有变更过程记录会使得变更实施的过程不透明，可能导致变更方案的实施过程中出现混乱、误解或错误，从而增加	中

序号	安全类	安全问题	关联资产[3]	关联威胁	危害分析结果	风险等级
					变更带来的风险。	

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。

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

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

$$x_k=(0,0.5,1),\quad S=100\cdot\frac{1}{n},\quad f(\omega_k)=\begin{cases}1, & \omega_k=\text{一般}\\ 2, & \omega_k=\text{重要}\\ 3, & \omega_k=\text{关键}\end{cases}$$

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	
光华荣昌智能数字化平台系统	0	26	10	71.31

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》的第二级要求，经对光华荣昌智能数字化平台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：

光华荣昌智能数字化平台系统本次等级测评的综合得分为 71.31，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
安全通用要求				
1	安全物理环境	消防装置为手动灭火，未开启自动灭火功能。	信息机房	建议在机房内安装可靠的自动灭火系统，如气体灭火系统（七氟丙烷），以及与火灾检测设备配合使用，并定期对自动灭火系统进行检查和维护，确保其可靠性和有效性。
2		未采取措施防止地下积水的转移和渗透。	信息机房	建设在空调下方设立拦水坝，防止积水转移，并安装地下水位监测设备，实时监测地下水位变化，及时发现异常情况。
3	安全通信网络	未采用校验技术保证通信过程中数据的完整性。	安全通信网络	建议采用校验技术可以确保数据在传输过程中不被窃听或篡改，以保护数据的完整性，确保只有授权用户能够访问和修改数据。
4		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，也未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	建议基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，在检测到其可信性受到破坏后进行报警。
5	安全区域边界	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	互联网接入区	建议基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，在检测到其可信性受到破坏后进行报警。

序号	安全类	安全问题	关联资产	整改建议
		进行可信验证，也未将验证结果形成审计记录送至安全管理中心。		
6	安全计算环境	BPM 系统、ERP 服务器、ERP 系统、ERP 系统数据库、核心交换机未配置口令复杂度校验和口令有效期策略。	BPM 系统、ERP 服务器、ERP 系统、ERP 系统数据库、核心交换机	建议启用并配置口令复杂度校验，如口令最小长度 8 位以上，口令组成元素至少三种（数字、小写字母、大写字母、特殊字符），增加破解难度；配置口令有效期策略，定期（如 90 天）更换口令，减少长期口令暴露的风险。
7		BPM 服务器、BPM 系统、ERP 服务器、ERP 系统数据库未配置登录失败处理和登录连接超时自动退出功能。	BPM 服务器、BPM 系统、ERP 服务器、ERP 系统数据库	建议配置登录失败处理策略（如登录失败 5-10 次，锁定账户 5-10 分钟），以防止暴力攻击和密码猜测；并配置登录连接超时自动退出策略（空闲无操作 5-10 分钟，账户自动退出），减少未经授权的访问和信息泄露的风险。
8		BPM 系统、ERP 系统未采取措施防止鉴别信息在网络传输过程中被窃听。	BPM 系统、ERP 系统	建议采用安全的通信协议，如 HTTPS、SSH、SSL/TLS 等，确保传输过程中的数据安全性，防止窃听者获取敏感信息。
9		BMP 系统数据库、BPM 系统、ERP 服务器、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火	BMP 系统数据库、BPM 系统、ERP 服务器、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙	建议禁用或删除系统中的默认账户，特别是那些不必要的或具有高权限的默认账户，以减少攻击面和提高系统安全性；对于必须保留的默认账户，应该限制其访问权限，确保其仅具有必要的权限，避免滥用和未授权访问。

序号	安全类	安全问题	关联资产	整改建议
		墙未限制默认账户的访问权限。		
10		BPM 系统存在多余测试账户。	BPM 系统	建议定期进行账户审核，清理不再需要的账户，如测试账户、离岗人员账户或其他未被使用的账户等。
11		BMP 系统数据库、BPM 数据库服务器、BPM 服务器、BPM 系统、ERP 服务器、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙未划分审计管理员、安全管理员账号，且存在超级管理员账户，不能实现管理用户的权限分离。	BMP 系统数据库、BPM 数据库服务器、BPM 服务器、BPM 系统、ERP 服务器、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙	建议依据三权分立原则划分系统管理员、安全管理员、审计管理员，禁用或限制超级管理员账户，并授予管理用户所需的最小权限，实现管理用户的权限分离。
12		BPM 数据库服务器、BPM 服务器审计记录内容不全面。	BPM 数据库服务器、BPM 服务器	建议开启各项审计日志，确保所有相关活动都有相应的记录。
13		BMP 系统数据库、BPM 数据库服务器、BPM 服务器、BPM 系统、ERP 服	BMP 系统数据库、BPM 数据库服务器、BPM 服务器、BPM 系统、ERP 服务器、ERP 系统、ERP 系统数据库、VPN、WEB	建议定期（如每季度）进行漏洞扫描，并制定漏洞修复计划，经过充分测试评估后，及时修复风险漏洞，以防止攻击者利用漏洞对系统造成损害，并根

序号	安全类	安全问题	关联资产	整改建议
		务器、ERP 系统、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、中间件、办公终端、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙、运维安全管理系统、运维终端未定期对设备/系统进行漏洞扫描。	应用防火墙、上网行为管理、中间件、办公终端、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙、运维安全管理系统、运维终端	据漏洞的严重性和潜在影响，优先修复高级别漏洞，最大程度降低安全风险。
14		ERP 服务器、办公终端、运维终端未安装防恶意代码软件。	ERP 服务器、办公终端、运维终端	建议在服务器上安装专业的、可信赖的防病毒软件，并保持其及时更新，以及时识别和清除潜在的恶意软件。
15		BMP 系统数据库、BPM 数据库服务器、BPM 服务器、BPM 系统、ERP 服务器、ERP 系统、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、中间件、办公终端、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙、运维安全管理系	BMP 系统数据库、BPM 数据库服务器、BPM 服务器、BPM 系统、ERP 服务器、ERP 系统、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、中间件、办公终端、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙、运维安全管理系统、运维终端	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，在检测到其可信性受到破坏后进行报警。

序号	安全类	安全问题	关联资产	整改建议
		统、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，也未将验证结果形成审计记录送至安全管理中心。		
16		BPM 系统、ERP 系统、业务数据、个人信息、审计数据、配置数据、鉴别数据未采用校验技术保证重要数据在传输过程中的完整性。	BPM 系统、ERP 系统、业务数据、个人信息、审计数据、配置数据、鉴别数据	建议采用校验技术或经国家密码主管部门认可的密码技术来保护传输中的重要数据，如使用循环冗余校验（CRC）、消息认证码（MAC）、HTTPS、SSL/TLS 等技术，确保重要数据在传输过程中不被篡改或窃取。
17		BPM 数据库服务器、BPM 服务器、ERP 服务器、ERP 系统、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、业务数据、中间件、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙、运维安全管理系统、配置数据未定期对备份文件进行恢	BPM 数据库服务器、BPM 服务器、ERP 服务器、ERP 系统、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、业务数据、中间件、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙、运维安全管理系统、配置数据	建议制定定期的备份文件恢复测试计划，以确保备份文件的完整性和可用性，并在测试过程中模拟真实的灾难或数据丢失情景，以确保备份文件能够成功恢复。

序号	安全类	安全问题	关联资产	整改建议
		复测试。		
18		BMP 系统数据库、BPM 数据库服务器、BPM 服务器、BPM 系统、ERP 服务器、ERP 系统、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、业务数据、中间件、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙、运维安全管理系统、配置数据未将重要数据定时备份至异地。	BMP 系统数据库、BPM 数据库服务器、BPM 服务器、BPM 系统、ERP 服务器、ERP 系统、ERP 系统数据库、VPN、WEB 应用防火墙、上网行为管理、业务数据、中间件、日志分析管理系统、核心交换机、网络入侵防御系统、边界防火墙、运维安全管理系统、配置数据	建议将系统的重要数据备份到地理位置不同的远程数据中心或云存储服务中，以确保即使发生本地灾难，数据仍然安全可恢复。
19	安全管理中心	网络设备、部分安全设备、部分服务器未划分审计管理员账户，无法对审计管理员进行身份鉴别、授权、操作审计等。	安全管理中心	建议划分审计管理员账户，为其分配审计策略配置、审计记录查询配置、日志备份等权限，并对审计管理员进行身份标识和鉴别，对其操作行为进行审计。
20		网络设备、部分安全设备、部分服务器未划分审计管理员账户，不能通过审计管理员对审计记录进行分析。	安全管理中心	建议划分审计管理员账户，为其分配审计策略配置、审计记录查询配置、日志备份等权限，并审计管理员对审计记录进行分析。
21	安全管	未提供信息安	安全管理制度	建议组织建立并执行定期

序号	安全类	安全问题	关联资产	整改建议
	理制度	全管理制度评审与修订记录。		评审安全管理制度的流程，确保对安全策略、控制措施和流程进行全面审查；借助评审过程发现的问题和机会，不断改进安全策略、流程和控制措施，以应对不断变化的安全威胁和风险，并在每次安全管理制度评审后，记录评审结果和必要的改进计划。
22	安全管理机构	未提供单位内部关于信息安全的沟通交流记录。	安全管理机构	建议所有关于信息安全的重要沟通交流都被记录下来，包括会议记录、电子邮件、即时消息等。这可以帮助团队成员在需要时回顾相关信息，确保他们理解并遵循信息安全政策。
23		未提供常规性安全检查记录。	安全管理机构	建议每次安全检查后都应详细记录检查结果，并形成报告，以便追踪问题整改情况。
24	安全管理人员	未提供外部人员访问申请记录	安全管理人员	建议所有外部人员在访问前提交书面申请，并经过相关部门的审批，并在每次访问后，记录访问者的姓名、单位、访问日期、时间、访问目的和陪同人员等信息。
25	安全建设管理	无相关的安全规划设计类文档和被测系统安全方案设计文档。	安全建设管理	建议制定详细的安全规划设计文档（需包含密码技术相关内容），确定系统的安全目标、需求和风险评估，有计划地开展安全建设工作。
26		未提供整体安全规划和安全方案设计的专家论证文档和批准意见。	安全建设管理	建议组织相关部门和有关安全专家对安全设计方案的合理性和正确性进行论证和审定，并留存安全设计方案审定记录。
27		未提供恶意代码检测报告。	安全建设管理	建议在软件交付之前，进行全面的恶意代码安全审

序号	安全类	安全问题	关联资产	整改建议
				查，包括静态代码分析、动态代码分析和安全架构审查等，并留存相关检测报告。
28		未制定安全工程实施方案控制工程实施过程。	安全建设管理	建议制定工程实施方案控制工程实施过程，方案需包括工程时间限制、进度控制和质量控制等方面内容，并按照工程实施方面的管理制度进行各类控制。
29		未提供测试验收方案和测试验收报告。	安全建设管理	建议核查工程测试验收方案是否明确说明参与测试的部门、人员、测试验收内容、现场操作过程等内容；并形成测试验收报告，测试验收报告应有相关部门和人员对测试验收报告进行审定的意见。
30		未在系统上线前进行安全性测试。	安全建设管理	建议在系统上线前委托专业的安全团队或第三方安全公司进行全面的安全性测试，包括漏洞扫描、渗透测试、安全配置审查、软件测试、密码应用安全性测试等，确保系统的安全性达到预期标准。
31		未提供对运行维护技术人员的相关的技术培训记录。	安全建设管理	建议建立定期的技能培训计划，主要从系统的整体架构、主要的安全实现手段和系统实现的主要业务功能等方面进行培训，并留存相关的培训记录，培训记录包括培训内容、培训时间、参与人员等方面的信息。
32		未提供《项目测试验收报告》、《运维培训记录表》等记录表单，系统交付文档不完善。	安全建设管理	建议在信息系统交付后，提供完整的测试验收报告，包括项目各阶段的测试结果，包括功能测试、性能测试、安全测试等；并实施运维技术培训，并留存相关的培训记录，培

序号	安全类	安全问题	关联资产	整改建议
				训记录包括培训内容、培训时间、参与人员、培训方式等方面的信息。
33	安全运维管理	未提供维修审批、维修过程等方面的记录。	安全运维管理	建议实施完善的维修审批流程，包括维修申请、审批人员、审批步骤和审批标准等内容，确保每次维修都经过审批，记录下审批人员和审批结果；并对每次维修进行详细记录，包括维修人员、维修时间、维修内容、使用的工具和材料等信息。
34		单位未采取必要的措施识别安全漏洞和隐患，未提供漏洞扫描报告。	安全运维管理	建议提供漏洞扫描报告，报告应描述存在的漏洞、严重级别、原因分析和改进意见等方面，报告的时间应与定期扫描的要求相符。
35		未提供账户管理相关审批记录或流程文件。	安全运维管理	建议制定明确的账户管理审批流程，包括账户创建、权限变更、账户删除等操作，确保每个账户管理活动都经过适当的审批和授权。
36		未提供变更方案评审记录。	安全运维管理	建议制定并实施规范的变更方案评审和变更过程记录流程，明确评审的标准、参与人员和记录方式，并对变更方案评审和实施过程进行详细记录，包括变更方案的提出、评审意见、变更过程的执行情况、实施结果等信息。

【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	北京市昌平区流村镇工业园区北京光华荣昌公司院内一层	关键	1

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	×	V200R019C00SPC500B327	HUAWEI S5731S-S24T4X-A	核心数据交换、转发	关键	1

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	VPN	×	7.1	深信服 VPN-2150	建立一个安全的加密连接，以保护用户的数据隐私和网络安全，确保信息传输的安全性	重要	1
2	边界防火墙	×	V600R007C20SPC600 (VRP (R) software, Version 5.170)	HUAWEI USG6315E	互联网边界访问控制	关键	1

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
3	网络入侵防御系统	×	NIPS 8.0.7	深信服 NIPS-1000-B1400	互联网边界入侵检测及限制	关键	1
4	WEB 应用防火墙	×	WAF 8.0.42	深信服 WAF-1000-B1200	互联网边界应用层防护	关键	1
5	上网行为管理	×	AC11.0R2	深信服 AC1200	控制、管理、规范员工访问互联网的行为	重要	1
6	运维安全管理系统	×	V3.0.1020220210	深信服 SM-1000-B1150	设备的安全运维、运维审计	重要	1
7	日志分析管理系统	×	SIP-Logger3.0.22 Build20240103	深信服 SIP-Logger-A600	收集分散在网络中各设备的日志	重要	1
8	火绒安全软件	√	6.0.2.3	火绒安全软件	服务器入侵防御、防病毒	一般	1
9	360 安全卫士	√	13.0.0.2006	360 安全卫士	服务器入侵防御、防病毒	一般	1

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	BPM 服	BPM 系统	×	Microsoft	-	Inter	关键	1

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
	务器			Windows Server 2012 R2 Standard		net Information Services (Version 8.5.9600.16384)		
2	BPM 数据库服务器	BPM 系统	×	Microsoft Windows Server 2012 R2 Datacenter	MSSQL 2012 (11.0.3128.0)	-	关键	1
3	ERP 服务器	ERP 系统	×	Red Hat Enterprise Linux Server release 7.2 (Maipo)	Progress Version 11.7.09.000 2026	-	关键	1

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/控制软件及版本	用途	重要程度	备注
1	运维终端	×	Windows 10 专业版	运维管理	重要	1
2	办公终端	×	Windows 10 专业版	日常办公	重要	1

A.6 其他系统或设备

附录 A 表-6 其他系统或设备

序号	设备名称	是否虚拟设备	操作系统/控制软件及版本	设备类别/用途	重要程度	备注
该系统不涉及其他系统或设备						

A.7 系统管理软件/平台

附录 A 表-7 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	BPM 服务器	Internet Information Services (Version 8.5.9600.16384)	URL 请求、转发、响应	重要	1
2	BMP 系统数据库	BPM 数据库服务器	MSSQL 2012（11.0.3128.0）	数据存储、管理	关键	1
3	ERP 系统数据库	ERP 服务器	Progress Version 11.7.09.000 2026	数据存储、管理	关键	1

A.8 业务应用系统/平台

附录 A 表-8 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	BPM 系统	主要为员工提供各种工作流程申请和公司相关制度文档的管理功能，包括员工考勤，费用报销、印章使用、合同申请、车辆使用等审批功能	V1.0	安码商务软件系统（上海）	关键	1
2	ERP 系统	主要为公司提供物料采购订单、采	V3.5.0.38	上海快意信息科技有限公司	关键	1

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
		购入库、生产排产生产备料、领料、产成品入库、耗料、销售订单、销售发运、开票等各环节管理，所有业务数据自动进入并形成财务会计核算数据。财务管理包括应收账款、应付账款、总账、固定资产、成本管理、现金管理等模块，实现财务智能管理核算				

A.9 数据资源

附录 A 表-9 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	鉴别数据	BPM 系统	完整性、保密性	重要
2	业务数据	BPM 系统	完整性、保密性	关键
3	审计数据	BPM 系统	完整性	重要
4	配置数据	BPM 系统	完整性	重要
5	个人信息	BPM 系统	完整性、保密性	关键

A.10 密码产品

附录 A 表- 10 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
该系统不涉及密码产品						

A.11 安全相关人员

附录 A 表-11 安全相关人员

序号	姓名	岗位/角色	联系方式	所属单位
1	魏弈壮	系统管理员	18830035572	北京光华荣昌汽车部件有限公司
2	曹艳芳	审计管理员	18610117403	北京光华荣昌汽车部件有限公司
3	郑晓旭	安全管理员	18610116864	北京光华荣昌汽车部件有限公司

A.12 安全管理文档

附录 A 表-12 安全管理文档

序号	文档名称	主要内容
1	《个人信息管理制度》	明确个人信息的收集范围和目的，确保在合法、合理、必要的情况下收集和使用个人信息，并遵守相关的法律法规。
2	《信息安全策略总纲 V1.1》	主要包含了方针、目标、原则、总体安全策略、制度的制定与发布、制度的评审和修订等内容。
3	《信息安全岗位职责要求 V1.1》	主要包含了技能安全培训要求、信息安全主管岗位职责、安全管理员岗位职责、系统管理员岗位职责、审计管理员岗位职责等内容。
4	《机房管理制度》	主要包含了机房管理制度、机房的常规检查和维护、机房消防系统等内容。
5	《运行维护和监控管理规定 V1.1》	主要包含了组织及岗位职责、系统运行维护和监控管理等内容。
6	《防火墙策略配置规范 v1.0》	主要包含了防火墙的策略配置要求等内容。
7	《外联单位联系列表》	列出了与外部单位建立联系和沟通所需的单位名称、联系人以及联系方式等。
8	《信息系统安全审核和安全检查管理制度》	主要包含了安全审核和安全检查等内容。
9	《人员安全管理制度 V1.1》	主要包含了人员录用、人员转岗和离岗、人员

序号	文档名称	主要内容
		考核、人员惩戒、人员教育和培训等内容。
10	《外部人员访问管理制度 V1.1》	主要包含了外部人员访问安全管理等内容。
11	《光华荣昌智能数字化平台系统网络安全等级保护定级报告》	主要包含光华荣昌智能数字化平台系统的定级系统描述、网络结构、业务描述、系统安全等级确认等。
12	《光华荣昌智能数字化平台系统网络安全等级保护定级评审意见》	主要包含民防图像信息管理平台业务信息安全保护等级和系统服务安全保护等级的描述和专家评审意见。
13	《软件设计说明书》	详细描述软件设计的技术规范、功能需求和设计思路。
14	《系统操作手册》	指导用户如何操作和使用办公信息系统或软件的手册。
15	《北京光华荣昌汽车部件有限公司办公环境安全管理制度》	主要包含了办公场所安全管理规定、办公场所消防安全要求等内容。
16	《资产安全管理制度》	主要包含了资产责任制度、资产标识管理、资产使用管理、资产传输管理、资产维护管理、资产报废与处置管理等内容。
17	《运行维护和监控管理制度》	主要包含了组织及岗位职责、系统运行维护和监控管理等内容。
18	《北京光华荣昌汽车部件有限公司恶意代码防范管理制度》	主要包含了恶意代码（病毒）防范具体要求。
19	《北京光华荣昌汽车部件有限公司变更管理办法》	主要包含了变更的分类和界定、变更管理等内容。

附录B 上次测评问题整改情况说明

本次测评为被测对象的首次测评。

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	2	1	2	1	1	1	1	1	2	1
		部分符合	0	0	0	0	1	1	0	0	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
总计测评项 15，符合项 13，部分符合项 2，不符合项 0 个，不适用项 0 个												

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
本报告不涉及安全扩展指标		

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	0	0
		部分符合	0	1	0
		不符合	0	0	1
		不适用	0	0	0
总计测评项 4，符合项 2 个，部分符合项 1 个，不符合项 1 个，不适用项 0 个					

附录 C 表-4 安全通信网络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
本报告不涉及安全扩展指标		

C.3 安全区域边界

附录 C 表- 5 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	互联网接入区	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
总计测评项 **11**，符合项 **10** 个，部分符合项 **0** 个，不符合项 **1** 个，不适用项 **0** 个								

附录 C 表- 6 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
本报告不涉及安全扩展指标		

C.4 安全计算环境

C.4.1 网络设备

附录 C 表-7 网络设备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	2	2	3	3	-	0	1	0	-	-
		部分符合	1	2	0	0	-	0	0	1	-	-
		不符合	0	0	0	1	-	1	0	1	-	-

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	1	-	0	0	0	-	-
总计测评项 19，符合项 11 个，部分符合项 4 个，不符合项 3 个，不适用项 1 个												

附录 C 表- 8 网络设备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
本报告不涉及安全扩展指标		

C.4.2 安全设备

附录 C 表-9 安全设备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	VPN	符合	3	2	3	3	-	0	1	0	-	-
		部分符合	0	2	0	0	-	0	0	1	-	-
		不符	0	0	0	1	-	1	0	1	-	-

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
		合										
		不适用	0	0	0	1	-	0	0	0	-	-
2	网络入侵防御系统	符合	3	2	3	3	-	0	1	0	-	-
		部分符合	0	2	0	0	-	0	0	1	-	-
		不符合	0	0	0	1	-	1	0	1	-	-
		不适用	0	0	0	1	-	0	0	0	-	-
3	上网行为管理	符合	3	2	3	3	-	0	1	0	-	-
		部分符合	0	2	0	0	-	0	0	1	-	-
		不	0	0	0	1	-	1	0	1	-	-

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
		符合										
		不适用	0	0	0	1	-	0	0	0	-	-
4	边界防火墙	符合	3	2	3	3	-	0	1	0	-	-
		部分符合	0	2	0	0	-	0	0	1	-	-
		不符合	0	0	0	1	-	1	0	1	-	-
		不适用	0	0	0	1	-	0	0	0	-	-
5	WEB 应用防火墙	符合	3	2	3	3	-	0	1	0	-	-
		部分符合	0	2	0	0	-	0	0	1	-	-

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
		不符合	0	0	0	1	-	1	0	1	-	-
		不适用	0	0	0	1	-	0	0	0	-	-
6	日志分析管理系统	符合	3	2	3	3	-	0	1	0	-	-
		部分符合	0	2	0	0	-	0	0	1	-	-
		不符合	0	0	0	1	-	1	0	1	-	-
		不适用	0	0	0	1	-	0	0	0	-	-
7	运维安全管理系统	符合	3	4	3	3	-	0	1	0	-	-
		部分符	0	0	0	0	-	0	0	1	-	-

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
		合										
		不符合	0	0	0	1	-	1	0	1	-	-
		不适用	0	0	0	1	-	0	0	0	-	-
总计测评项 133，符合项 86 个，部分符合项 19 个，不符合项 21 个，不适用项 7 个												

附录 C 表- 10 安全设备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
本报告不涉及安全扩展指标		

C.4.3 服务器和终端

附录 C 表-11 服务器和终端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	BPM 数	符	3	3	2	3	1	0	1	0	1	-

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
	据库服务器	合										
		部分符合	0	1	1	0	0	0	0	1	0	-
		不符合	0	0	0	1	0	1	0	1	0	-
		不适用	0	0	0	1	0	0	0	0	0	-
2	BPM 服务器	符合	2	3	2	3	1	0	1	0	1	-
		部分符合	1	1	1	0	0	0	0	1	0	-
		不符合	0	0	0	1	0	1	0	1	0	-
		不适用	0	0	0	1	0	0	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
3	ERP 服务器	符合	1	2	3	3	0	0	1	0	1	-
		部分符合	2	2	0	0	0	0	0	1	0	-
		不符合	0	0	0	1	1	1	0	1	0	-
		不适用	0	0	0	1	0	0	0	0	0	-
4	运维终端	符合	2	4	3	2	0	0	0	0	1	-
		部分符合	0	0	0	0	0	0	0	0	0	-
		不符合	0	0	0	1	1	1	0	0	0	-
		不适	1	0	0	2	0	0	1	2	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
		用										
5	办公终端	符合	2	4	3	2	0	0	0	0	1	-
		部分符合	0	0	0	0	0	0	0	0	0	-
		不符合	0	0	0	1	1	1	0	0	0	-
		不适用	1	0	0	2	0	0	1	2	0	-
总计测评项 105，符合项 62 个，部分符合项 12 个，不符合项 16 个，不适用项 15 个												

附录 C 表- 12 服务器和终端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
本报告不涉及安全扩展指标		

C.4.4 系统管理软件/平台

附录 C 表- 13 系统管理软件/平台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	BMP 系统数据库	符合	3	2	3	1	-	0	1	1	1	2
		部分符合	0	2	0	0	-	0	0	0	0	0
		不符合	0	0	0	1	-	1	0	1	0	0
		不适用	0	0	0	3	-	0	0	0	0	0
2	ERP 系统数据库	符合	1	2	3	1	-	0	1	0	1	2
		部分符合	1	2	0	0	-	0	0	1	0	0
		不符合	1	0	0	1	-	1	0	1	0	0
		不适用	0	0	0	3	-	0	0	0	0	0
3	中间件	符合	0	0	3	0	-	0	1	0	0	0
		部分符合	0	0	0	0	-	0	0	1	0	0
		不符合	0	0	0	1	-	1	0	1	0	0
		不适用	3	4	0	4	-	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
总计测评项 66，符合项 29 个，部分符合项 7 个，不符合项 10 个，不适用项 20 个												

附录 C 表- 14 系统管理软件/平台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
本报告不涉及安全扩展指标		

C.4.5 业务应用系统/平台

附录 C 表- 15 业务应用系统/平台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	ERP 系统	符合	1	4	3	1	-	0	0	0	1	2
		部分符合	1	0	0	0	-	0	0	1	0	0
		不符合	1	0	0	1	-	1	1	1	0	0
		不适用	0	0	0	3	-	0	0	0	0	0
2	BPM 系统	符合	0	1	3	1	-	0	0	1	1	2
		部分符合	2	3	0	0	-	0	0	0	0	0
		不符合	1	0	0	1	-	1	1	1	0	0
		不适用	0	0	0	3	-	0	0	0	0	0
总计测评项 44，符合项 21 个，部分符合项 7 个，不符合项 10 个，不适用项 6 个												

附录 C 表- 16 业务应用系统/平台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
本报告不涉及安全扩展指标		

C.4.6 数据资源

附录 C 表- 17 数据资源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	鉴别数据	符合	-	-	-	-	-	-	0	0	1	0
		部分符合	-	-	-	-	-	-	1	0	0	0
		不符合	-	-	-	-	-	-	0	0	0	0
		不适用	-	-	-	-	-	-	0	2	0	2
2	业务数据	符合	-	-	-	-	-	-	0	0	0	0
		部分符合	-	-	-	-	-	-	0	1	0	0
		不符合	-	-	-	-	-	-	1	1	0	0
		不适用	-	-	-	-	-	-	0	0	1	2
3	审计数据	符合	-	-	-	-	-	-	0	0	0	0
		部分符合	-	-	-	-	-	-	1	0	0	0
		不符合	-	-	-	-	-	-	0	0	0	0
		不适用	-	-	-	-	-	-	0	2	1	2
4	配置数据	符合	-	-	-	-	-	-	0	0	0	0
		部分符合	-	-	-	-	-	-	1	1	0	0
		不符合	-	-	-	-	-	-	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	1	2
5	个人信息	符合	-	-	-	-	-	-	0	0	0	2
		部分符合	-	-	-	-	-	-	0	0	0	0
		不符合	-	-	-	-	-	-	1	0	0	0
		不适用	-	-	-	-	-	-	0	2	1	0
总计测评项 30，符合项 3 个，部分符合项 5 个，不符合项 4 个，不适用项 18 个												

附录 C 表- 18 数据资源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
本报告不涉及安全扩展指标		

C.4.7 其他系统或设备

附录 C 表- 19 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
本次测评不涉及其他系统或设备												

附录 C 表- 20 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
本报告不涉及安全扩展指标		

C.5 安全管理中心

附录 C 表- 21 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	0
		部分符合	0	2
		不符合	0	0
		不适用	0	0
总计测评项 4，符合项 2 个，部分符合项 2 个，不符合项 0 个，不适用项 0 个				

C.6 安全管理制度

附录 C 表- 22 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	安全管理制度	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
总计测评项 6，符合项 5 个，部分符合项 1 个，不符合项 0 个，不适用项 0 个						

C.7 安全管理机构

附录 C 表- 23 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	安全管理机构	符合	2	1	2	2	0
		部分符合	0	0	0	1	1
		不符合	0	0	0	0	0
		不适用	0	0	0	0	0
总计测评项 9，符合项 7 个，部分符合项 2 个，不符合项 0 个，不适用项 0 个							

C.8 安全管理人员

附录 C 表- 24 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	安全管理人员	符合	2	1	1	2
		部分符合	0	0	0	1
		不符合	0	0	0	0
		不适用	0	0	0	0
总计测评项 7，符合项 6 个，部分符合项 1 个，不符合项 0 个，不适用项 0 个						

C.9 安全建设管理

附录 C 表- 25 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	安全建设管理	符合	4	1	1	0	1	1	0	1	2	2
		部分符合	0	0	0	0	0	0	0	2	0	0
		不符合	0	2	0	0	1	1	2	0	0	0
		不适用	0	0	1	2	0	0	0	0	1	0
总计测评项 25，符合项 13 个，部分符合项 2 个，不符合项 6 个，不适用项 4 个												

附录 C 表- 26 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
本报告不涉及安全扩展指标		

C.10 安全运维管理

附录 C 表- 27 安全运维管理单项测评结果汇总表（安全通用要求）

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	安全运维管理	符合	3	1	2	1	0	4	3	1	1	0	3	3	2	0
		部分符合	0	0	0	1	0	1	0	0	0	1	0	0	0	0
		不符合	0	0	0	0	1	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
总计测评项 31，符合项 24 个，部分符合项 3 个，不符合项 1 个，不适用项 3 个																

附录 C 表- 28 安全运维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
本报告不涉及安全扩展指标		

C.11 其他安全要求指标

附录 C 表- 29 其他指标单项测评结果汇总表

序号	测评对象	符合情况
本报告不涉及其他安全指标		

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
安全通用要求			
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；	经访谈系统管理员，核查物理机房， 1)机房具有建筑物抗震设防审批验收文件； 2)机房不存在天花板、窗台下的水渗漏现象； 3)机房有窗户； 4)机房内安装的窗户具有防护措施； 5)机房不存在屋顶、墙体、门窗和地面等开裂的情况。	符合
	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。	经访谈和核查，机房位于北京市昌平区流村镇工业园区北京光华荣昌公司院内一层，未在建筑物的顶层或地下室，周边无用水设施。	符合
物理访问控制	a) 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。	经访谈系统管理员，核查物理机房， 1)机房具有电子门禁； 2)机房已安排专人值守； 3)电子门禁系统可以正常工作，能对进出人员进行鉴别； 4)专人值守能对进出人员进行鉴别。	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；	经访谈系统管理员，核查物理机房， 1)机房内设备放置在机柜或机架上，并已采取固定措施； 2)设备或主要部件具有不易除去的标识、标志。	符合
	b) 应将通信线缆铺设在隐蔽安全处。	经访谈系统管理员，核查物理机房，机房内通信线缆铺设在线槽中，线缆不易损坏。	符合
防雷击	a) 应将各类机柜、设施和设备等通过接地系统安全接地。	经访谈系统管理员，核查物理机房，机房内所有机柜、设施和设备等已采取接地控制措施。	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；	经访谈系统管理员，核查物理机房， 1)机房内具有火灾自动消防系统； 2)自动消防系统能自动检测火情、自动报警但不能自动灭火。	部分符合

控制点	测评项	结果记录	符合情况
		3）有自动灭火功能，但是为防止误报，设置成手动灭火。	
	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。	经访谈系统管理员，核查物理机房，机房采用耐火的建筑材料，并设置了防火墙体。	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；	经访谈系统管理员，核查物理机房，机房具有防雨水渗透措施，设置了墙壁防水层、双层玻璃，并对窗口进行了防护措施。	符合
	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。	经访谈系统管理员，核查物理机房， 1)机房具有防止水蒸气结露的措施，设置了机房空调、除湿器； 2)机房不具有排水措施，未采取措施防止地下积水的转移和渗透。	部分符合
防静电	a) 应采用防静电地板或地面并采用必要的接地防静电措施。	经访谈系统管理员，核查物理机房， 1)机房内具有防静电地板； 2)机房内采取了接地措施。	符合
温湿度控制	a) 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。	经访谈系统管理员，核查物理机房， 1)机房内配有专用的精密空调； 2)机房内温度:22℃至 23℃，湿度:45%至 55%。	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；	经访谈系统管理员，核查物理机房， 1)机房具有稳压器和过电压防护设备； 2)现场观测时稳压器和过电压防护设备处于正常工作状态。	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。	经访谈系统管理员，核查物理机房， 1)具有 UPS 后备电源系统； 2)UPS 满足短期断电时的供电要求（2 小时）。	符合
电磁防护	a) 电源线和通信线缆应隔离铺设，避免互相干扰。	经访谈系统管理员，核查物理机房，电源线缆和通信线缆隔离铺设在线槽里。	符合

D.2 安全通信网络

D.2.1 安全通用要求部分

控制点	测评项	结果记录	符合情况
安全通用要求			

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；	经访谈并核查得知，1）已按照重要性原则划分了边界防护区、运维管理区、服务器区等区域，并为各区域分配了地址；2）网络拓扑图区域划分情况与实际运行环境一致。	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。	经访谈并核查得知，1）被测系统具有与实际网络运行情况相符的网络拓扑图；2）重要网络区域未部署在网络边界处；3）区域之间采用 VLAN 隔离技术进行区域间的逻辑隔离。	符合
通信传输	a) 应采用校验技术保证通信过程中数据的完整性。	经核查，1）网络设备、安全设备采用 HTTPS 协议进行远程管理；2）BPM 服务器、BPM 数据库服务器、ERP 服务器分别采用 SSL（TLS1.0）、RDP、SSH 协议进行远程管理；3）数据库通过所在服务器进行管理；4）以上设备可以保证数据在传输过程中的完整性。5）但 BPM 系统、ERP 系统未采用加密协议进行远程管理，不能保证数据在传输过程中的完整性。	部分符合
可信验证	a) 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。	经核查，安全通信网络无可信验证环境。	不符合

D.3 安全区域边界

D.3.1 安全通用要求部分

D.3.1.1 互联网接入区

控制点	测评项	结果记录	符合情况
安全通用要求			
边界防护	a) 应保证跨越边界的访问和数据流通过	经核查，系统在网络边界处部署了边界防火墙，配置了双向的访问控制策	符合

控制点	测评项	结果记录	符合情况
	边界设备提供的受控接口进行通信。	略，策略指定通过特定端口进行通信，保证了网络边界访问的安全性，并且每条访问控制规则均有明确的源 IP 地址、目的 IP 地址以及协议端口等。	
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，网络边界处部署了边界防火墙进行访问控制，配置了合理的访问控制规则，防火墙为隐式拒绝防火墙，默认最后一条为拒绝所有通信。	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，边界防火墙中的访问控制规则已进行相关的优化，不存在多余的、无效的访问控制规则，访问控制规则之间的逻辑关系和前后排序合理，不存在矛盾的地方，并且访问控制规则的数量达到了最小化。	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，防火墙通过配置访问控制策略，对源地址、目的地址、源端口、目的端口和服务协议等进行检查，允许或拒绝数据包进出。经测试，未经授权的 IP 或端口无法访问系统设备，访问控制策略的配置参数有效。	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，边界防火墙能够根据会话状态检测表追踪连接会话状态，并结合前后会话关系综合判断，能够为进出的数据流提供明确的允许/拒绝的能力。	符合
入侵防范	a) 应在关键网络节点处监视网络攻击行为。	经核查，网络边界处部署有网络入侵防御系统，可以用于检测和限制从外部发起的网络攻击行为，网络入侵防御系统的安全防护策略覆盖了网络中的所有关键节点，网络入侵防御系统的热门威胁库规则库已更新到最新版本（2024-10-16）。	符合
恶意代码防范	a) 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，网络边界处部署有网络入侵防御系统，可以对网络环境中的恶意代码进行检测和清除，漏洞攻击特征识别库已更新到最新版本（2024-8-14）。经测试，网络入侵防御系统的安全防护策略处于有效运行状态。	符合
安全审计	a) 应在网络边界、重要网络节点进行安	经核查，网络设备、安全设备、服务器、数据库和应用系统均启用了安全	符合

控制点	测评项	结果记录	符合情况
	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；	审计功能，可以对登录事件、操作事件和相关安全事件进行审计，审计覆盖到每个用户。	
	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，网络入侵防御系统的审计记录包括事件的序号、攻击者 IP、归属地、严重等级、影响业务/服务器、事件描述、攻击事件、操作等审计相关信息。	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、网络入侵防御系统、WEB 应用防火墙、上网行为管理等关键计算节点设备产生的日志定时推送到日志分析管理系统（192.168.5.253）中，审计日志留存时间满足 6 个月。	符合
可信验证	a) 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，边界设备未有可信验证机制。	不符合

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
安全通用要求			
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，网络设备采用“用户名+静态口令”方式对用户进行身份标识和鉴别；查看用户列表得知，身份标识具有唯一性，不存在空口令用户；已启用口令复杂度策略，要求口令最小长度 8 位，口令由数字、大写字母、小写字母、特殊字符中的两种组成，未	部分符合

控制点	测评项	结果记录	符合情况
		配置口令定期更换。	
	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，网络设备启用了登录失败处理功能和登录连接超时自动退出功能，连续登录失败 3 次锁定账号 5 分钟，登录后无操作 20 分钟，设备自动退出登录状态。	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，网络设备采用 HTTPS 协议进行远程管理，可以防止鉴别信息在网络传输中被窃听。	符合
访问控制	a) 应对登录的用户分配账户和权限；	经核查，已对登录的用户分配了账号和权限，但未限制默认账户 admin 的访问权限。	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，网络设备已修改默认账户的默认口令。	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，网络设备不存在多余或过期账户，且管理员用户与账户之间一一对应，不存在多人使用同一账户的情况。	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，网络设备划分了系统管理员 admin，并为其分配了权限或角色，但未划分安全管理员、审计管理员账号，未禁用或限制默认账户 admin 的访问控制权限。	部分符合
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，网络设备已开启安全审计功能，可以对登录事件、操作事件等重要用户行为和重要安全事件进行审计，审计覆盖到每个账户。	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，网络设备的审计记录包括事件的日志时间、日志模块、日志级别、日志助记符、日志内容等审计相关信息。	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，网络设备产生的日志每月进行本地备份，审计日志留存时间满足 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	经核查，网络设备安装的组件均为业务所需，已遵循最小安装原则。	符合

控制点	测评项	结果记录	符合情况
	的组件和应用程序；		
	b) 应关闭不需要的系统服务、默认共享和高危端口；	经核查，网络设备关闭了非必要的系统服务和高危端口。	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，已对终端接入方式进行限制，交换机通过运维安全管理系统进行登录管理。	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；	经核查，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对网络设备无相关判定需求，故此项为不适用项。	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，未定期对网络设备进行漏洞扫描，不能发现可能存在的已知漏洞。	不符合
可信验证	a) 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，网络设备无可信验证环境。	不符合
数据完整性	a) 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，网络设备采用 HTTPS 协议进行通信传输，可以保证鉴别数据、重要配置数据、重要审计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，网络设备在重大变更前/后进行本地配置备份，备份策略合理，备份结果与备份策略一致，但未定期对备份文件进行恢复测试。	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，网络设备的配置数据未进行异地定时备份。	不符合

D.4.1.2 安全设备

D.4.1.2.1 VPN

控制点	测评项	结果记录	符合情况
安全通用要求			
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，安全设备采用“用户名+静态口令”方式对用户进行身份标识和鉴别；查看用户列表得知，身份标识具有唯一性，不存在空口令用户；已启用口令复杂度策略，要求口令最小长度 8 位，口令由数字、大写字母、小写字母、特殊字符中的两种组成，并配置了口令每隔 90 天更换一次。	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，安全设备启用了登录失败处理功能和登录连接超时自动退出功能，连续登录失败 5 次锁定账号 30 分钟，登录后无操作 10 分钟，设备自动退出登录状态。	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，安全设备采用 HTTPS 协议进行远程管理，可以防止鉴别信息在网络传输中被窃听。	符合
访问控制	a) 应对登录的用户分配账户和权限；	经核查，已对登录的用户分配了账号和权限，但未限制默认账户 admin 的访问权限。	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，安全设备已修改默认账户的默认口令。	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，安全设备不存在多余或过期账户，且管理员用户与账户之间一一对应，不存在多人使用同一账户的情况。	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，安全设备划分了系统管理员 admins，并为其分配了权限或角色，但未划分安全管理员、审计管理员账号，未禁用或限制默认账户 admin 的访问控制权限。	部分符合
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	经核查，安全设备已开启安全审计功能，可以对登录事件、操作事件等重要用户行为和重要安全事件进行审	符合

控制点	测评项	结果记录	符合情况
	户行为和重要安全事件进行审计；	计，审计覆盖到每个账户。	
	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，安全设备的审计记录包括事件的用户名、IP 地址、操作权限、操作时间、配置类型、操作过程、操作结果等审计相关信息。	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，安全设备产生的日志每月进行本地备份，审计日志留存时间满足 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；	经核查，安全设备安装的组件均为业务所需，已遵循最小安装原则。	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，安全设备关闭了非必要的系统服务和高危端口。	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，已对终端接入方式进行限制，安全设备通过运维安全管理系统（192.168.5.254）进行登录管理。	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；	经核查，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对安全设备无相关判定需求，故此项为不适用项。	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，未定期对安全设备进行漏洞扫描，不能发现可能存在的已知漏洞。	不符合
可信验证	a) 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，安全设备无可信验证环境。	不符合

控制点	测评项	结果记录	符合情况
数据完整性	a) 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，安全设备采用 HTTPS 协议进行通信传输，可以保证鉴别数据、重要配置数据、重要审计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，安全设备在重大变更前/后进行本地配置备份，备份策略合理，备份结果与备份策略一致，但未定期对备份文件进行恢复测试。	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，安全设备的配置数据未进行异地定时备份。	不符合

D.4.1.2.2 网络入侵防御系统

控制点	测评项	结果记录	符合情况
安全通用要求			
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，安全设备采用“用户名+静态口令+图形验证码”方式对用户进行身份标识和鉴别；查看用户列表得知，身份标识具有唯一性，不存在空口令用户；已启用口令复杂度策略，要求口令最小长度 8 位，口令由数字、字母、特殊字符中的两种组成，并配置了口令每隔 90 天更换一次。	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，安全设备启用了登录失败处理功能和登录连接超时自动退出功能，连续登录失败 5 次锁定账号，需手动解锁，登录后无操作 10 分钟，设备自动退出登录状态。	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，安全设备采用 HTTPS 协议进行远程管理，可以防止鉴别信息在网络传输中被窃听。	符合
访问控制	a) 应对登录的用户分配账户和权限；	经核查，已对登录的用户分配了账号和权限，但未限制默认账户 admin 的访问权限。	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，安全设备已修改默认账户的默认口令。	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，安全设备不存在多余或过期账户，且管理员用户与账户之间一一对应，不存在多人使用同一账户的情况。	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，安全设备已按照三权分立原则，划分了系统管理员 sysadmin、安全管理员 secadmin、审计管理员 audadmin，并为其分配了不同权限或角色，但未禁用或限制默认账户 admin 的访问控制权限。	部分符合
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，安全设备已开启安全审计功能，可以对登录事件、操作事件等重要用户行为和重要安全事件进行审计，审计覆盖到每个账户。	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，安全设备的审计记录包括事件的序号、用户名、主机 IP、操作对象、操作、日期时间、描述等审计相关信息。	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，安全设备产生的日志定时推送到日志分析管理系统（192.168.5.253）中，审计日志留存时间满足 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；	经核查，安全设备安装的组件均为业务所需，已遵循最小安装原则。	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，安全设备关闭了非必要的系统服务和高危端口。	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，已对终端接入方式进行限制，安全设备通过运维安全管理系统（192.168.5.254）进行登录管理。	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；	经核查，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对安全设备无相关判定需求，故此项为不适用项。	不适用
	e) 应能发现可能存	经核查，未定期对安全设备进行漏洞	不符合

控制点	测评项	结果记录	符合情况
	在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；	扫描，不能发现可能存在的已知漏洞。	
可信验证	a) 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，安全设备无可信验证环境。	不符合
数据完整性	a) 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，安全设备采用 HTTPS 协议进行通信传输，可以保证鉴别数据、重要配置数据、重要审计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，安全设备在重大变更前/后进行本地配置备份，备份策略合理，备份结果与备份策略一致，但未定期对备份文件进行恢复测试。	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，安全设备的配置数据未进行异地定时备份。	不符合

D.4.1.2.3 上网行为管理

控制点	测评项	结果记录	符合情况
安全通用要求			
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，安全设备采用“用户名+静态口令”方式对用户进行身份标识和鉴别；查看用户列表得知，身份标识具有唯一性，不存在空口令用户；已启用口令复杂度策略，要求口令最小长度 8 位，口令由数字、字母、特殊字符中的两种组成，并配置了口令每隔 90 天更换一次。	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	经核查，安全设备启用了登录失败处理功能和登录连接超时自动退出功能，连续登录失败 5 次锁定账号 1 分	符合

控制点	测评项	结果记录	符合情况
	非法登录次数和当登录连接超时自动退出等相关措施；	钟，登录后无操作 60 分钟，设备自动退出登录状态。	
	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，安全设备采用 HTTPS 协议进行远程管理，可以防止鉴别信息在网络传输中被窃听。	符合
访问控制	a) 应对登录的用户分配账户和权限；	经核查，已对登录的用户分配了账号和权限，但未限制默认账户 admin 的访问权限。	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，安全设备已修改默认账户的默认口令。	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，安全设备不存在多余或过期账户，且管理员用户与账户之间一一对应，不存在多人使用同一账户的情况。	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，安全设备划分了系统管理员 sangfor，并为其分配了权限或角色，但未划分安全管理员、审计管理员账号，未禁用或限制默认账户 admin 的访问控制权限。	部分符合
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，安全设备已开启安全审计功能，可以对登录事件、操作事件等重要用户行为和重要安全事件进行审计，审计覆盖到每个账户。	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，安全设备的审计记录包括事件的序号、来源、类型、时间、详细信息等审计相关信息。	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，安全设备产生的日志定时推送到日志分析管理系统（192.168.5.253）中，审计日志留存时间满足 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；	经核查，安全设备安装的组件均为业务所需，已遵循最小安装原则。	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，安全设备安装的组件均为业务所需，已遵循最小安装原则。	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，已对终端接入方式进行限制，安全设备通过运维安全管理系统（192.168.5.254）进行登录管理。	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；	经核查，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对安全设备无相关判定需求，故此项为不适用项。	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，未定期对安全设备进行漏洞扫描，不能发现可能存在的已知漏洞。	不符合
可信验证	a) 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，安全设备无可信验证环境。	不符合
数据完整性	a) 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，安全设备采用 HTTPS 协议进行通信传输，可以保证鉴别数据、重要配置数据、重要审计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，安全设备在重大变更前/后进行本地配置备份，备份策略合理，备份结果与备份策略一致，但未定期对备份文件进行恢复测试。	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，安全设备的配置数据未进行异地定时备份。	不符合

D.4.1.2.4 边界防火墙

控制点	测评项	结果记录	符合情况
安全通用要求			
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，安全设备采用“用户名+静态口令”方式对用户进行身份标识和鉴别；查看用户列表得知，身份标识具有唯一性，不存在空口令用户；已启用口令复杂度策略，要求口令最小长度 8 位，口令由数字、大写字母、小写字母、特殊字符中的三种组成，并配置了口令每隔 90 天更换一次。	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，安全设备启用了登录失败处理功能和登录连接超时自动退出功能，连续登录失败 3 次锁定账号 30 分钟，登录后无操作 60 分钟，设备自动退出登录状态。	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，安全设备采用 HTTPS 协议进行远程管理，可以防止鉴别信息在网络传输中被窃听。	符合
访问控制	a) 应对登录的用户分配账户和权限；	经核查，已对登录的用户分配了账号和权限，但未限制默认账户 admin 的访问权限。	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，安全设备已修改默认账户的默认口令。	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，安全设备不存在多余或过期账户，且管理员用户与账户之间一一对应，不存在多人使用同一账户的情况。	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，安全设备划分了系统管理员 admins，并为其分配了权限或角色，但未划分安全管理员、审计管理员账号，未禁用或限制默认账户 admin 的访问控制权限。	部分符合
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，安全设备已开启安全审计功能，可以对登录事件、操作事件等重要用户行为和重要安全事件进行审计，审计覆盖到每个账户。	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	经核查，安全设备的审计记录包括事件的时间、管理员、登录 IP 地址、内容、虚拟系统等审计相关信息。	符合

控制点	测评项	结果记录	符合情况
	件是否成功及其他与审计相关的信息；		
	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，安全设备产生的日志每月进行本地备份，审计日志留存时间满足 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；	经核查，安全设备安装的组件均为业务所需，已遵循最小安装原则。	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，安全设备关闭了非必要的系统服务和高危端口。	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，已对终端接入方式进行限制，安全设备通过运维安全管理系统（192.168.5.254）进行登录管理。	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；	经核查，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对安全设备无相关判定需求，故此项为不适用项。	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，未定期对安全设备进行漏洞扫描，不能发现可能存在的已知漏洞。	不符合
可信验证	a) 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，安全设备无可信验证环境。	不符合
数据完整性	a) 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，安全设备采用 HTTPS 协议进行通信传输，可以保证鉴别数据、重要配置数据、重要审计数据在传输过程中的完整性。	符合
数据备	a) 应提供重要数据	经核查，安全设备在重大变更前/后进	部分符合

控制点	测评项	结果记录	符合情况
份恢复	的本地数据备份与恢复功能；	行本地配置备份，备份策略合理，备份结果与备份策略一致，但未定期对备份文件进行恢复测试。	
	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，安全设备的配置数据未进行异地定时备份。	不符合

D.4.1.2.5 WEB 应用防火墙

控制点	测评项	结果记录	符合情况
安全通用要求			
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，安全设备采用“用户名+静态口令+图形验证码”方式对用户进行身份标识和鉴别；查看用户列表得知，身份标识具有唯一性，不存在空口令用户；已启用口令复杂度策略，要求口令最小长度 8 位，口令由数字、大写字母、小写字母、特殊字符中的三种组成，并配置了口令每隔 90 天更换一次。	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，安全设备启用了登录失败处理功能和登录连接超时自动退出功能，连续登录失败 5 次锁定账号，登录后无操作 10 分钟，设备自动退出登录状态。	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，安全设备采用 HTTPS 协议进行远程管理，可以防止鉴别信息在网络传输中被窃听。	符合
访问控制	a) 应对登录的用户分配账户和权限；	经核查，已对登录的用户分配了账号和权限，但未限制默认账户 admin 的访问权限。	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，安全设备已修改默认账户的默认口令。	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，安全设备不存在多余或过期账户，且管理员用户与账户之间一一对应，不存在多人使用同一账户的情况。	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，安全设备已按照三权分立原则，划分了系统管理员 systemadmin、安全管理员 securityadmin、审计管理员 auditadmin，并为其分配了不同权限或角色，但未禁用或限制默认账户 admin 的访问控制权限。	部分符合
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，安全设备已开启安全审计功能，可以对登录事件、操作事件等重要用户行为和重要安全事件进行审计，审计覆盖到每个账户。	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，安全设备的审计记录包括事件的序号、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，安全设备产生的日志定时推送到日志分析管理系统（192.168.5.253）中，审计日志留存时间满足 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；	经核查，安全设备安装的组件均为业务所需，已遵循最小安装原则。	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，安全设备关闭了非必要的系统服务和高危端口。	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，已对终端接入方式进行限制，安全设备通过运维安全管理系统（192.168.5.254）进行登录管理。	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；	经核查，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对安全设备无相关判定需求，故此项为不适用项。	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，未定期对安全设备进行漏洞扫描，不能发现可能存在的已知漏洞。	不符合

控制点	测评项	结果记录	符合情况
可信验证	a) 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，安全设备无可信验证环境。	不符合
数据完整性	a) 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，安全设备采用 HTTPS 协议进行通信传输，可以保证鉴别数据、重要配置数据、重要审计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，安全设备在重大变更前/后进行本地配置备份，备份策略合理，备份结果与备份策略一致，但未定期对备份文件进行恢复测试。	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，安全设备的配置数据未进行异地定时备份。	不符合

D.4.1.2.6 日志分析管理系统

控制点	测评项	结果记录	符合情况
安全通用要求			
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，安全设备采用“用户名+静态口令+图形验证码”方式对用户进行身份标识和鉴别；查看用户列表得知，身份标识具有唯一性，不存在空口令用户；已启用口令复杂度策略，要求口令最小长度 8 位，口令由数字、大写字母、小写字母、特殊字符中的三种组成，并配置了口令每隔 90 天更换一次。	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	经核查，安全设备启用了登录失败处理功能和登录连接超时自动退出功能，连续登录失败 5 次锁定账号 10 分钟，登录后无操作 10 分钟，设备自动退出登录状态。	符合

控制点	测评项	结果记录	符合情况
	等相关措施；		
	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，安全设备采用 HTTPS 协议进行远程管理，可以防止鉴别信息在网络传输中被窃听。	符合
访问控制	a) 应对登录的用户分配账户和权限；	经核查，已对登录的用户分配了账号和权限，但未限制默认账户 admin 的访问权限。	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，安全设备已修改默认账户的默认口令。	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，安全设备不存在多余或过期账户，且管理员用户与账户之间一一对应，不存在多人使用同一账户的情况。	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，安全设备已按照三权分立原则，划分了系统管理员 sysadmin、安全管理员 secadmin、审计管理员 audtadmin，并为其分配了不同权限或角色，但未禁用或限制默认账户 admin 的访问控制权限。	部分符合
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，安全设备已开启安全审计功能，可以对登录事件、操作事件等重要用户行为和重要安全事件进行审计，审计覆盖到每个账户。	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，安全设备的审计记录包括事件的序号、告警、描述、创建时间、最后更新时间、详情等审计相关信息。	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，安全设备产生的日志每天本地备份，审计日志留存时间满足 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；	经核查，安全设备安装的组件均为业务所需，已遵循最小安装原则。	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，安全设备关闭了非必要的系统服务和高危端口。	符合
	c) 应通过设定终端	经核查，已对终端接入方式进行限	符合

控制点	测评项	结果记录	符合情况
	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；	制，安全设备通过运维安全管理系统（192.168.5.254）进行登录管理。	
	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，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对安全设备无相关判定需求，故此项为不适用项。	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，未定期对安全设备进行漏洞扫描，不能发现可能存在的已知漏洞。	不符合
可信验证	a) 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，安全设备无可信验证环境。	不符合
数据完整性	a) 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，安全设备采用 HTTPS 协议进行通信传输，可以保证鉴别数据、重要配置数据、重要审计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，安全设备在重大变更前/后进行本地配置备份，备份策略合理，备份结果与备份策略一致，但未定期对备份文件进行恢复测试。	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，安全设备的配置数据未进行异地定时备份。	不符合

D.4.1.2.7 运维安全管理系统

控制点	测评项	结果记录	符合情况
安全通用要求			

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，安全设备采用“用户名+静态口令”方式对用户进行身份标识和鉴别；查看用户列表得知，身份标识具有唯一性，不存在空口令用户；已启用口令复杂度策略，要求口令最小长度 10 位，口令由数字、大写字母、小写字母、特殊字符组成，每种类型至少 1 位，并配置了口令每隔 90 天更换一次。	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，安全设备启用了登录失败处理功能和登录连接超时自动退出功能，连续登录失败 5 次锁定账号 10 分钟，登录后无操作 5 分钟，设备自动退出登录状态。	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，安全设备采用 HTTPS 协议进行远程管理，可以防止鉴别信息在网络传输中被窃听。	符合
访问控制	a) 应对登录的用户分配账户和权限；	经核查，已对登录的用户分配了账号和权限，已限制默认账户 admin 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，安全设备已修改默认账户的默认口令。	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，安全设备不存在多余或过期账户，且管理员用户与账户之间一一对应，不存在多人使用同一账户的情况。	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，安全设备已按照三权分立原则，划分了系统管理员 sysadmin、安全管理员 secadmin、审计管理员 audadmin，并为其分配了不同权限或角色，已限制默认账户 admin 的访问控制权限。	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，安全设备已开启安全审计功能，可以对登录事件、操作事件等重要用户行为和重要安全事件进行审计，审计覆盖到每个账户。	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	经核查，安全设备的审计记录包括事件的序号、时间、账号、登录地址、用户、模块、操作、操作结果等审计	符合

控制点	测评项	结果记录	符合情况
	件是否成功及其他与审计相关的信息；	相关信息。	
	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，安全设备产生的日志定时推送到日志分析管理系统（192.168.5.253）中，审计日志留存时间满足 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；	经核查，安全设备安装的组件均为业务所需，已遵循最小安装原则。	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，安全设备关闭了非必要的系统服务和高危端口。	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，已对终端接入方式进行限制，安全设备通过特定 IP 或网段访问管理，如 VPN（192.168.12.254）。	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；	经核查，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对安全设备无相关判定需求，故此项为不适用项。	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，未定期对安全设备进行漏洞扫描，不能发现可能存在的已知漏洞。	不符合
可信验证	a) 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，安全设备无可信验证环境。	不符合
数据完整性	a) 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，安全设备采用 HTTPS 协议进行通信传输，可以保证鉴别数据、重要配置数据、重要审计数据在传输过程中的完整性。	符合
数据备	a) 应提供重要数据	经核查，安全设备每天进行本地配置	部分符合

控制点	测评项	结果记录	符合情况
份恢复	的本地数据备份与恢复功能；	备份，备份策略合理，备份结果与备份策略一致，但未定期对备份文件进行恢复测试。	
	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，安全设备的配置数据未进行异地定时备份。	不符合

D.4.1.3 服务器和终端

D.4.1.3.1 BPM 数据库服务器

控制点	测评项	结果记录	符合情况
安全通用要求			
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，通过 Win+R（运行）输入 netplwiz 命令得知，已勾选“要使用本计算机，用户必须输入用户名和密码”；通过 Win+R（运行）输入 lusrmgr.msc 命令，点击用户得知，每个账户身份标识具有唯一性；无空口令用户；通过 Win+R（运行）输入 secpol.msc 命令，点击密码策略得知，密码必须符合复杂性要求：已启用，密码长度最小值：8 个字符，密码最长使用期限：90 天；已启用口令复杂度要求，用户口令最小长度 8 位，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，通过 Win+R（运行）输入 secpol.msc 命令，点击账户锁定策略得知，账户锁定时间：30 分钟，账户锁定阈值：5 次无效登录，重置账户锁定计数器：30 分钟；通过 Win+R（运行）输入 secpol.msc 命令，点击本地策略→安全选项得知，“交互式登录：计算机不活动限制”安全设置为 1800 秒，非活动时间超过 30 分钟锁定会话。	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，通过 Win+R（运行）输入 gpedit.msc 命令，点击计算机配置→管理模板→Windows 组件→远程桌面服务→远程桌面会话主机→安全得	符合

控制点	测评项	结果记录	符合情况
		知，已启用“远程（RDP）连接要求使用指定的安全层”，安全层为 RDP。	
访问控制	a) 应对登录的用户分配账户和权限；	经核查，通过 Win+R（运行）输入 secpol.msc 命令，点击本地策略→用户权限分配得知，已对用户或用户组权限进行合理分配；访问 C 盘的 Program Files 文件夹，右键属性→安全得知，已对不同的组和用户名进行合理授权；已限制默认账户 Administrator 的访问控制权限。	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，已禁用默认账户 Guest，已修改默认账户 administrator 的默认口令。	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，通过 Win+R（运行）输入 lusrmgr.msc 命令，点击用户得知，不存在多余或过期账户，且管理员用户与账户之间一一对应，不存在多人使用同一账户的情况。	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，通过 Win+R（运行）输入 secpol.msc 命令，点击本地策略→用户权限分配以及查看管理员账户隶属组得知，划分了系统管理员，并为其分配了组或权限，但未划分安全管理员、审计管理员账号，不能实现管理用户的权限分离。	部分符合
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，通过 Win+R（运行）输入 secpol.msc 命令，点击本地策略→审核策略得知，审核策略安全设置未全部配置为（成功，失败），审计策略不完善。	部分符合
	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，通过 Win+R（运行）输入 eventvwr.msc 命令，点击 Windows 日志得知，审计记录包括日志名称、来源、事件 ID、级别、用户、操作代码、记录时间、任务类别、关键字、计算机等审计相关信息。	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，服务器已设置“日志满时将其存档，不覆盖事件”，系统产生的日志每月本地备份，审计日志留存时间满足 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；	经核查，通过 Win+R（运行）输入 dcomcnfg 命令，点击组件服务→计算机→我的电脑→COM+应用程序得	符合

控制点	测评项	结果记录	符合情况
		知，无多余组件；通过 win+R（运行）输入 appwiz.cpl 命令得知，无多余应用程序。	
	b) 应关闭不需要的系统服务、默认共享和高危端口；	经核查，通过 Win+R（运行）输入 services.msc 命令得知，无多余系统服务；通过 cmd 输入 net share 命令得知，未开启默认共享；通过 cmd 输入 netstat -an 命令得知，开启了 135、445 等高危端口，已在主机防火墙入站规则中制定了高危端口阻断策略，策略名为禁用 135、139、445。	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，已对终端接入方式进行限制，服务器通过运维安全管理系统进行登录管理。	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；	经核查，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对服务器无相关判定需求，故此项为不适用项。	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，未定期对服务器进行漏洞扫描，不能发现可能存在的已知漏洞。	不符合
恶意代码防范	a) 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，服务器安装了 360 安全卫士，可以识别恶意代码和病毒行为并进行阻断，特征库已更新至最新版本（2024-09-26）。	符合
可信验证	a) 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，服务器无可信验证环境。	不符合
数据完整性	a) 应采用校验技术保证重要数据在传输	经核查，服务器已启用“远程（RDP）连接要求使用指定的安全层”，安全层	符合

控制点	测评项	结果记录	符合情况
	过程中的完整性。	为 RDP，可以保证鉴别数据、重要配置数据、重要审计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，服务器在重大变更前/后进行本地配置备份，备份策略合理，备份结果与备份策略一致，但未定期对备份文件进行恢复测试。	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，服务器的配置数据未进行异地定时备份。	不符合
剩余信息保护	a) 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，通过 Win+R（运行）输入 secpol.msc 命令，点击本地策略→安全选项得知，“交互式登录：不显示最后的用户名”安全设置为已启用状态，能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。	符合

D.4.1.3.2 BPM 服务器

控制点	测评项	结果记录	符合情况
安全通用要求			
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，通过 Win+R（运行）输入 netplwiz 命令得知，已勾选“要使用本计算机，用户必须输入用户名和密码”；通过 Win+R（运行）输入 lusrmgr.msc 命令，点击用户得知，每个账户身份标识具有唯一性；无空口令用户；通过 Win+R（运行）输入 secpol.msc 命令，点击密码策略得知，密码必须符合复杂性要求：已启用（口令需包含数字、小写字母、大写字母、特殊字符中的三类），密码长度最小值：8 个字符；密码最长使用期限：29 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，通过 Win+R（运行）输入 secpol.msc 命令，点击账户锁定策略得知，账户锁定时间：30 分钟，账户锁定阈值：4 次无效登录，重置账户锁定计数器：30 分钟；通过“设置活动但空闲的远程桌面会话的时间限制”	部分符合

控制点	测评项	结果记录	符合情况
		得知，已启用登录连接超时自动退出功能，空闲会话限制时间为从不。	
	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，通过 Win+R（运行）输入 gpedit.msc 命令，点击计算机配置→管理模板→Windows 组件→远程桌面服务→远程桌面会话主机→安全得知，已启用“远程（RDP）连接要求使用指定的安全层”，安全层为 SSL（TLS1.0），可以保证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，通过 Win+R（运行）输入 secpol.msc 命令，点击本地策略→用户权限分配得知，已对用户或用户组权限进行合理分配；访问 C 盘的 Program Files 文件夹，右键属性→安全得知，已对不同的组和用户名进行合理授权；已限制默认账户 Administrator 的访问控制权限。	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，已禁用默认账户 Guest，已修改默认账户 Administrator 的默认口令。	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，通过 Win+R（运行）输入 lusrmgr.msc 命令，点击用户得知，不存在多余或过期账户，且管理员用户与账户之间一一对应，不存在多人使用同一账户的情况。	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，通过 Win+R（运行）输入 secpol.msc 命令，点击本地策略→用户权限分配以及查看管理员账户隶属组得知，划分了系统管理员，并为其分配了组或权限，但未划分安全管理员、审计管理员账号，不能实现管理用户的权限分离。	部分符合
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，通过 Win+R（运行）输入 secpol.msc 命令，点击本地策略→审核策略得知，审核策略安全设置未全部配置为（成功，失败），审计策略不完善。	部分符合
	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，通过 Win+R（运行）输入 eventvwr.msc 命令，点击 Windows 日志得知，审计记录包括日志名称、来源、事件 ID、级别、用户、操作代码、记录时间、任务类别、关键字、	符合

控制点	测评项	结果记录	符合情况
		计算机等审计相关信息。	
	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，服务器产生的日志定时推送到日志分析管理系统中，审计日志留存时间满足 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；	经核查，通过 Win+R（运行）输入 dcomcnfg 命令，点击组件服务→计算机→我的电脑→COM+应用程序得知，无多余组件；通过 win+R（运行）输入 appwiz.cpl 命令得知，无多余应用程序。	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，通过 Win+R（运行）输入 services.msc 命令得知，无多余系统服务；通过 cmd 输入 net share 命令得知，未开启默认共享；通过 cmd 输入 netstat -an 命令得知，开启了 135、139、445 等高危端口，已在主机防火墙入站规则中制定了高危端口阻断策略，策略名为禁用 135、139、445。	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，已对终端接入方式进行限制，服务器通过运维安全管理系统进行登录管理。	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；	经核查，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对服务器无相关判定需求，故此项为不适用项。	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，未定期对服务器进行漏洞扫描，不能发现可能存在的已知漏洞。	不符合
恶意代码防范	a) 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，服务器安装了火绒安全软件，可以识别恶意代码和病毒行为并进行阻断，特征库已更新至最新版本（2024-10-16 18:22）。	符合
可信验证	a) 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	经核查，服务器无可信验证环境。	不符合

控制点	测评项	结果记录	符合情况
	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	a) 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，服务器已启用“远程（RDP）连接要求使用指定的安全层”，安全层为 SSL（TLS1.0），可以保证鉴别数据、重要配置数据、重要审计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，服务器在重大变更前/后进行本地配置备份，备份策略合理，备份结果与备份策略一致，但未定期对备份文件进行恢复测试。	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，服务器的配置数据未进行异地定时备份。	不符合
剩余信息保护	a) 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，通过 Win+R（运行）输入 secpol.msc 命令，点击本地策略→安全选项得知，“交互式登录：不显示最后的用户名”安全设置为已启用状态，能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。	符合

D.4.1.3.3 ERP 服务器

控制点	测评项	结果记录	符合情况
安全通用要求			
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，1）服务器采用“用户名+静态口令”方式对用户进行身份标识和鉴别；2）账号身份标识（UID）具有唯一性，不存在空口令用户；3）通过“cat /etc/security/pwquality”命令得知，未配置口令复杂度要求；4）通过“cat /etc/login.defs”命令得知，未配置口令定期更换。	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	经核查，1）通过“cat /etc/profile”命令得知，空闲超时退出时间（TMOUT）为 30 分钟；2）通过“cat	部分符合

控制点	测评项	结果记录	符合情况
	非法登录次数和当登录连接超时自动退出等相关措施；	/etc/pam.d/system-auth”命令得知，未配置登录失败处理功能。	
	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，服务器采用 SSH 协议进行远程管理，可以防止鉴别信息在网络传输中被窃听。	符合
访问控制	a) 应对登录的用户分配账户和权限；	经核查，1）通过“cat /etc/group”命令得知，已对登录的用户分配了账号和用户组，/etc/passwd、/etc/shadow、/etc/rsyslog.conf 等重要文件权限不高于 644；2）通过“cat /etc/ssh/sshd_config”命令得知，未限制默认账户 root 直接远程登录服务器。	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，已修改默认账户 root 的默认口令。	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，1）通过“cat /etc/passwd”命令得知，不存在多余或过期账户，且管理员用户与账户之间一一对应，不存在多人使用同一账户的情况。	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，1）通过“cat /etc/passwd”、“cat /etc/group”命令得知，已按照三权分立原则，划分了系统管理员、安全管理员、审计管理员；2）已为管理用户分配了不同组或权限，实现了管理用户的权限分离；3）未禁用或限制默认账户 root 的访问控制权限。	部分符合
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，通过“systemctl status auditd”和“systemctl status rsyslog”命令得知，已开启 audit 和 rsyslog 服务，审计覆盖到每个用户，能够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，通过“cat /var/log/audit/audit.log”和“cat /var/log/messages”命令得知，审计记录包括日期/时间、对象、路径、相关系统调用、用户 ID、用户组 ID、命令、可执行文件路径等审计相关信息。	符合
	c) 应对审计记录进行保护，定期备份，	经核查，非授权账户无法访问审计日志，系统产生的日志定时推送到日志	符合

控制点	测评项	结果记录	符合情况
	避免受到未预期的删除、修改或覆盖等。	分析管理系统（192.168.5.253）中，审计日志留存时间满足 6 个月。	
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，通过“uname -a”和“yum list installed”命令得知，服务器无多余组件和应用程序，已遵循最小安装原则。	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，通过“systemctl | grep running”和“ss -tnlu”命令得知，不存在多余的系统服务和端口。	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，已对终端接入方式进行限制，服务器通过运维安全管理系统进行登录管理。	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；	经核查，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对服务器无相关判定需求，故此项为不适用项。	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，未定期对服务器进行漏洞扫描，不能发现可能存在的已知漏洞。	不符合
恶意代码防范	a) 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，未安装防恶意代码软件，无法识别恶意代码和病毒行为并进行阻断。	不符合
可信验证	a) 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，服务器无可信验证环境。	不符合
数据完整性	a) 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，服务器采用 SSH 协议进行远程管理，可以保证鉴别数据、重要配置数据、重要审计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，服务器在重大变更前/后进行本地配置备份，备份策略合理，备份结果与备份策略一致，但未定期对备份文件进行恢复测试。	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，服务器的配置数据未进行异地定时备份。	不符合
剩余信息保护	a) 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，服务器自身具有剩余信息处理机制，用户注销后，系统会进行相关的剩余信息处理，可以完全清除鉴别信息所处的存储空间。	符合

D.4.1.3.4 运维终端

控制点	测评项	结果记录	符合情况
安全通用要求			
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，通过 Win+R（运行）输入 netplwiz 命令得知，已勾选“要使用本计算机，用户必须输入用户名和密码”；通过 Win+R（运行）输入 lusrmgr.msc 命令，点击用户得知，每个账户身份标识具有唯一性；无空口令用户；通过 Win+R（运行）输入 secpol.msc 命令，点击密码策略得知，密码必须符合复杂性要求：已启用，密码长度最小值：8 个字符，密码最长使用期限：90 天；已启用口令复杂度要求，用户口令最小长度 8 位，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，通过 Win+R（运行）输入 secpol.msc 命令，点击账户锁定策略得知，账户锁定时间：30 分钟，账户锁定阈值：10 次无效登录，重置账户锁定计数器：30 分钟；查看“屏幕保护程序设置”得知，等待时间为 10 分钟，已勾选“在恢复时显示登录屏幕”。	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	经核查，终端仅采用本地方式进行管理，不涉及此项内容，故此项不适用。	不适用

控制点	测评项	结果记录	符合情况
	传输过程中被窃听。		
访问控制	a) 应对登录的用户分配账户和权限；	经核查，通过 Win+R（运行）输入 secpol.msc 命令，点击本地策略→用户权限分配得知，已对用户或用户组权限进行合理分配；访问 C 盘的 Program Files 文件夹，右键属性→安全得知，已对不同的组和用户名进行合理授权；已限制默认账户 Administrator 的访问控制权限。	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，已修改默认账户 Administrator 的默认口令。	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，通过 Win+R（运行）输入 lusrmgr.msc 命令，点击用户得知，不存在多余或过期账户，且管理员用户与账户之间一一对应，不存在多人使用同一账户的情况。	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，通过 Win+R（运行）输入 secpol.msc 命令，点击本地策略→用户权限分配以及查看管理员账户隶属组得知，已按照三权分立原则，划分了系统管理员、安全管理员、审计管理员，并为其分配了不同组或权限，实现了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，通过 Win+R（运行）输入 secpol.msc 命令，点击本地策略→审核策略得知，审核策略更改、审核登录事件、审核对象访问、审核进程跟踪、审核目录服务访问、审核特权使用、审核系统事件、审核账户登录事件、审核账户管理安全设置均为（成功，失败），审计能够覆盖到每个账户，可以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，通过 Win+R（运行）输入 eventvwr.msc 命令，点击 Windows 日志得知，审计记录包括日志名称、来源、事件 ID、级别、用户、操作代码、记录时间、任务类别、关键字、计算机等审计相关信息。	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	经核查，非授权账户无法访问审计日志，终端产生的日志每月本地备份，审计日志留存时间满足 6 个月。	符合

控制点	测评项	结果记录	符合情况
	除、修改或覆盖等。		
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，通过 Win+R（运行）输入 dcomcnfg 命令，点击组件服务→计算机→我的电脑→COM+应用程序得知，无多余组件；通过 win+R（运行）输入 appwiz.cpl 命令得知，无多余应用程序。	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，通过 Win+R（运行）输入 services.msc 命令得知，无多余系统服务；通过 cmd 输入 net share 命令得知，未开启默认共享；通过 cmd 输入 netstat -an 命令得知，开启了 135、139、445 等高危端口，已在防火墙中制定了高危端口阻断策略，阻断 135-139、445 等高危端口。	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，终端只能通过本地进行管理，禁止其他远程登录方式，不涉及此项内容，故此项为不适用项。	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，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对终端无相关判定需求，故此项为不适用项。	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，未定期对服务器进行漏洞扫描，不能发现可能存在的已知漏洞。	不符合
恶意代码防范	a) 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，终端未安装防恶意代码软件，无法识别恶意代码和病毒行为并进行阻断。	不符合
可信验证	a) 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，终端无可信验证环境。	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	a) 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，终端只能通过本地进行管理，禁止其他远程登录方式，鉴别数据、重要审计数据和重要配置数据未在网络环境中进行传输，不涉及此项内容，此项为不适用项。	不适用
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，设备损坏不影响业务系统的正常使用，并且终端不存储应用系统的业务数据等重要数据，没有重要数据备份和恢复需求，故此项为不适用项。	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，设备损坏不影响业务系统的正常使用，并且终端不存储应用系统的业务数据等重要数据，没有异地备份需求，故此项为不适用项。	不适用
剩余信息保护	a) 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，通过 Win+R（运行）输入 secpol.msc 命令，点击本地策略→安全选项得知，“交互式登录：不显示最后的用户名”安全设置为已启用状态，能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。	符合

D.4.1.3.5 办公终端

控制点	测评项	结果记录	符合情况
安全通用要求			
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，通过 Win+R（运行）输入 netplwiz 命令得知，已勾选“要使用本计算机，用户必须输入用户名和密码”；通过 Win+R（运行）输入 lusrmgr.msc 命令，点击用户得知，每个账户身份标识具有唯一性；无空口令用户；通过 Win+R（运行）输入 secpol.msc 命令，点击密码策略得知，密码必须符合复杂性要求：已启用，密码长度最小值：8 个字符，密码最长使用期限：90 天；已启用口令复杂度要求，用户口令最小长度 8 位，口令更换周期为 90 天。	符合
	b) 应具有登录失败	经核查，通过 Win+R（运行）输入	符合

控制点	测评项	结果记录	符合情况
	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；	secpol.msc 命令，点击账户锁定策略得知，账户锁定时间：30 分钟，账户锁定阈值：10 次无效登录，重置账户锁定计数器：30 分钟；查看“屏幕保护程序设置”得知，等待时间为 10 分钟，已勾选“在恢复时显示登录屏幕”。	
	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，终端仅采用本地方式进行管理，不涉及此项内容，故此项不适用。	不适用
访问控制	a) 应对登录的用户分配账户和权限；	经核查，通过 Win+R（运行）输入 secpol.msc 命令，点击本地策略→用户权限分配得知，已对用户或用户组权限进行合理分配；访问 C 盘的 Program Files 文件夹，右键属性→安全得知，已对不同的组和用户名进行合理授权；已限制默认账户 Administrator 的访问控制权限。	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，已修改默认账户 Administrator 的默认口令。	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，通过 Win+R（运行）输入 lusrmgr.msc 命令，点击用户得知，不存在多余或过期账户，且管理员用户与账户之间一一对应，不存在多人使用同一账户的情况。	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，通过 Win+R（运行）输入 secpol.msc 命令，点击本地策略→用户权限分配以及查看管理员账户隶属组得知，已按照三权分立原则，划分了系统管理员、安全管理员、审计管理员，并为其分配了不同组或权限，实现了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，通过 Win+R（运行）输入 secpol.msc 命令，点击本地策略→审核策略得知，审核策略更改、审核登录事件、审核对象访问、审核进程跟踪、审核目录服务访问、审核特权使用、审核系统事件、审核账户登录事件、审核账户管理安全设置均为（成功，失败），审计能够覆盖到每个账户，可以对重要的用户行为和重要安	符合

控制点	测评项	结果记录	符合情况
		全事件进行审计。	
	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；	经核查，通过 Win+R（运行）输入 eventvwr.msc 命令，点击 Windows 日志得知，审计记录包括日志名称、来源、事件 ID、级别、用户、操作代码、记录时间、任务类别、关键字、计算机等审计相关信息。	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，非授权账户无法访问审计日志，终端产生的日志每月本地备份，审计日志留存时间满足 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；	经核查，通过 Win+R（运行）输入 dcomcnfg 命令，点击组件服务→计算机→我的电脑→COM+应用程序得知，无多余组件；通过 win+R（运行）输入 appwiz.cpl 命令得知，无多余应用程序。	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，通过 Win+R（运行）输入 services.msc 命令得知，无多余系统服务；通过 cmd 输入 net share 命令得知，未开启默认共享；通过 cmd 输入 netstat -an 命令得知，开启了 135、139、445 等高危端口，已在防火墙中制定了高危端口阻断策略，阻断 135-139、445 等高危端口。	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，终端只能通过本地进行管理，禁止其他远程登录方式，不涉及此项内容，故此项为不适用项。	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，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对终端无相关判定需求，故此项为不适用项。	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，未定期对服务器进行漏洞扫描，不能发现可能存在的已知漏洞。	不符合
恶意代码防范	a) 应安装防恶意代码软件或配置具有相应功能的软件，并定	经核查，终端未安装防恶意代码软件，无法识别恶意代码和病毒行为并进行阻断。	不符合

控制点	测评项	结果记录	符合情况
	期进行升级和更新防恶意代码库。		
可信验证	a) 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，终端无可信验证环境。	不符合
数据完整性	a) 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，终端只能通过本地进行管理，禁止其他远程登录方式，鉴别数据、重要审计数据和重要配置数据未在网络环境中进行传输，不涉及此项内容，此项为不适用项。	不适用
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，设备损坏不影响业务系统的正常使用，并且终端不存储应用系统的业务数据等重要数据，没有重要数据备份和恢复需求，故此项为不适用项。	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，设备损坏不影响业务系统的正常使用，并且终端不存储应用系统的业务数据等重要数据，没有异地备份需求，故此项为不适用项。	不适用
剩余信息保护	a) 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，通过 Win+R（运行）输入 secpol.msc 命令，点击本地策略→安全选项得知，“交互式登录：不显示最后的用户名”安全设置为已启用状态，能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。	符合

D.4.1.4 其他系统或设备

本次测评未涉及其他系统或设备。

D.4.1.5 系统管理软件/平台

D.4.1.5.1 BMP 系统数据库

控制点	测评项	结果记录	符合情况
安全通用要求			
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，数据库采用 SQL Server 和 Windows 身份验证模式进行身份标识和鉴别，用户名具有唯一性，勾选了“强制实施密码策略”已引用所在服务器身份鉴别策略（密码必须符合复杂性要求：已启用，密码长度最小值：8 个字符），密码最长使用期限：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，数据库采用 SQL Server 和 Windows 身份验证模式进行身份鉴别，数据库所在服务器已启用登录失败处理功能，账户锁定时间：30 分钟，账户锁定阈值：5 次无效登录，重置账户锁定计数器：30 分钟；通过查看“远程服务器连接→远程查询超时值”得知，空闲查询超时退出时间为 600 秒。	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，数据库只能通过所在的服务器进行管理，服务器已启用“远程（RDP）连接要求使用指定的安全层”，安全层为 RDP，可以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，管理员根据数据库业务情况和用户需求，划分了合理的账户和权限，数据库不存在匿名账户，但是未限制默认账户 sa 等的访问权限。	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，已修改默认账户 sa 的默认口令。	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，数据库不存在多余的、过期的账户，不存在多人使用同一账户的情况。	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，数据库划分了系统管理员、安全管理员、审计管理员并为其分配了相应权限，但未禁用或限制默认账户 sa 的访问控制权限。	部分符合
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	经核查，数据库启用了安全审计功能，审计覆盖到每个用户，已设置登录审核策略为“失败和成功的登录”，	符合

控制点	测评项	结果记录	符合情况
	户行为和重要安全事件进行审计；	并启用“C2 审核跟踪”，可以对登录事件、操作事件等进行审计。	
	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；	经核查，数据库的审计记录包括事件时间、源、信息和事件结果等信息。	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，数据库审计日志存放在数据库中，数据库每天全量备份，数据库的审计日志可以保存 6 个月以上。	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，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对数据库管理系统无相关判定需求，故此项为不适用项。	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，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对数据库管理系统无相关判定需求，故此项为不适用项。	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；	经核查，数据库对管理员的登录地址进行了限制，只允许通过所在服务器本地登录数据库。	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；	经核查，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对数据库管理系统无相关判定需求，故此项为不适用项。	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，未定期对数据库进行漏洞扫描，不能发现可能存在的已知漏洞。	不符合
可信验证	a) 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	经核查，数据库未有可信验证机制。	不符合

控制点	测评项	结果记录	符合情况
	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	a) 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，数据库只能通过所在的服务器进行管理，服务器已启用“远程（RDP）连接要求使用指定的安全层”，安全层为 RDP，可以保证鉴别数据、重要审计数据、重要配置数据、重要业务数据和个人信息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，数据库在重大变更前/后进行本地配置备份，业务数据每天进行全量备份，备份策略合理，备份结果与备份策略一致，每 1-2 个月对备份文件进行恢复测试。	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，数据库的配置数据未进行异地定时备份。	不符合
剩余信息保护	a) 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，数据库退出登录后，不存在残留用户鉴别信息，可以完全清除鉴别信息所处的存储空间。	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业务必需的用户个人信息，如用户姓名、单位等，未收集其他多余信息，并且单位制定了《个人信息管理制度》对个人信息采集、保存等内容进行规定。	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，数据库禁止未授权访问和非法使用用户个人信息，并且单位制定了《个人信息管理制度》对个人信息的访问授权、使用等内容进行了规定。	符合

D.4.1.5.2 ERP 系统数据库

控制点	测评项	结果记录	符合情况
安全通用要求			
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	经核查，数据库采用“用户名+静态口令”方式对用户进行身份标识和鉴别；查看用户列表得知，身份标识具有唯	部分符合

控制点	测评项	结果记录	符合情况
	一性，身份鉴别信息具有复杂度要求并定期更换；	一性，不存在空口令用户；未配置口令复杂度和口令定期更换。	
	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，数据库未启用登录失败处理功能和登录连接超时自动退出功能。	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，数据库只能通过所在的服务器进行管理，服务器采用 SSH 协议进行远程管理，可以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，已对登录的用户分配了账号和权限，但未限制默认账户的访问权限。	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，数据库已修改默认账户的默认口令。	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，数据库不存在多余或过期账户，且管理员用户与账户之间一一对应，不存在多人使用同一账户的情况。	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，数据库划分了系统管理员、审计管理员，并为其分配了不同权限或角色，但未划分安全管理员账号，且未限制默认账户的访问权限。	部分符合
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，数据库已开启安全审计功能，可以对登录事件、操作事件等重要用户行为和重要安全事件进行审计，审计覆盖到每个账户。	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，数据库的审计记录包括事件的日期和时间、用户、事件类型、事件是否成功等审计相关信息。	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，数据库审计日志存放在数据库中，数据库每天全量备份，数据库的审计日志可以保存 6 个月以上。	符合
入侵防	a) 应遵循最小安装	经核查，依据《信息安全技术 网络安	不适用

控制点	测评项	结果记录	符合情况
范	的原则，仅安装需要的组件和应用程序；	全等级保护测评要求》（GB/T28448-2019），此测评项对数据库管理系统无相关判定需求，故此项为不适用项。	
	b) 应关闭不需要的系统服务、默认共享和高危端口；	经核查，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对数据库管理系统无相关判定需求，故此项为不适用项。	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；	经核查，数据库对管理员的登录地址进行了限制，只允许通过所在服务器本地登录数据库。	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；	经核查，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对数据库管理系统无相关判定需求，故此项为不适用项。	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，未定期对数据库进行漏洞扫描，不能发现可能存在的已知漏洞。	不符合
可信验证	a) 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，数据库无可信验证环境。	不符合
数据完整性	a) 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，数据库只能通过所在的服务器进行管理，服务器采用 SSH 协议进行远程管理，可以保证鉴别数据、重要审计数据、重要配置数据、重要业务数据和个人信息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，数据库在重大变更前/后进行本地配置备份，备份策略合理，备份结果与备份策略一致，但未定期对备	部分符合

控制点	测评项	结果记录	符合情况
		份文件进行恢复测试。	
	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，数据库的配置数据未进行异地定时备份。	不符合
剩余信息保护	a) 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，数据库退出登录后，不存在残留用户鉴别信息，可以完全清除鉴别信息所处的存储空间。	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业务必需的用户个人信息，如用户姓名、单位等，未收集其他多余信息，并且单位制定了《个人信息管理制度》对个人信息采集、保存等内容进行规定。	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，数据库禁止未授权访问和非法使用用户个人信息，并且单位制定了《个人信息管理制度》对个人信息的访问授权、使用等内容进行了规定。	符合

D.4.1.5.3 中间件

控制点	测评项	结果记录	符合情况
安全通用要求			
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；	IIS 中间件的身份鉴别功能由 Windows 操作系统实现，故此项为不适用项。	不适用
	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；	IIS 中间件的身份鉴别功能由 Windows 操作系统实现，故此项为不适用项。	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。	IIS 中间件的身份鉴别功能由 Windows 操作系统实现，故此项为不适用项。	不适用
访问控	a) 应对登录的用户	IIS 中间件的访问控制功能由 Windows	不适用

控制点	测评项	结果记录	符合情况
制	分配账户和权限；	操作系统实现，故此项为不适用项。	
	b) 应重命名或删除默认账户，修改默认账户的默认口令；	IIS 中间件的访问控制功能由 Windows 操作系统实现，故此项为不适用项。	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；	IIS 中间件的访问控制功能由 Windows 操作系统实现，故此项为不适用项。	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。	IIS 中间件的访问控制功能由 Windows 操作系统实现，故此项为不适用项。	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，通过“BPM 应用系统站点属性”得知，中间件已开启安全审计功能，可以对访问事件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，日志格式为 W3C，审计记录包括发出请求时候的日期、客户端 IP 地址、用户名、服务名、服务器的名称、服务器的 IP 地址、为服务配置的服务器端口号、请求中使用的 HTTP 方法、URI 资源、URI 资源、协议状态等审计相关信息。	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，非授权用户无法访问审计日志，审计日志每天进行本地归档备份，日志留存时间满足 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；	经核查，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对中间件无相关判定需求，故此项为不适用项。	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，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对中间件无相关判定需求，故此项为不适用项。	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；	经核查，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对中间件无相关判定需求，故此项为不适用项。	不适用
	d) 应提供数据有效	经核查，中间件无 WEB 管理界面，	不适用

控制点	测评项	结果记录	符合情况
	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；	无文件上传接口模块，故此项为不适用项。	
	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，未定期对中间件进行漏洞扫描，不能发现可能存在的已知漏洞。	不符合
可信验证	a) 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，中间件无可信验证环境。	不符合
数据完整性	a) 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，IIS 中间件的身份鉴别功能由 Windows 操作系统实现，中间件所在的服务器采用 RDP（安全层为 SSL（TLS1.0））协议进行通信传输，能够保证鉴别数据、重要配置数据和重要审计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，中间件在重大变更前/后进行本地配置备份，备份策略合理，备份结果与备份策略一致，但未定期对备份文件进行恢复测试。	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，中间件的配置数据未进行异地定时备份。	不符合
剩余信息保护	a) 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，IIS 中间件的身份鉴别功能由 Windows 操作系统实现，自身无鉴别信息，故此项为不适用项。	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，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对中间件无相关判定需求，故此项为不适用项。	不适用
	b) 应禁止未授权访	经核查，依据《信息安全技术 网络安	不适用

控制点	测评项	结果记录	符合情况
	问和非法使用用户个人信息。	全等级保护测评要求》（GB/T28448-2019），此测评项对中间件无相关判定需求，故此项为不适用项。	

D.4.1.6 业务应用系统/平台

D.4.1.6.1 ERP 系统

控制点	测评项	结果记录	符合情况
安全通用要求			
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，应用系统采用“用户名+静态口令”方式对用户进行身份标识和鉴别；查看用户列表得知，身份标识具有唯一性，不存在空口令用户；已启用口令复杂度策略，要求口令最小长度 19 位，口令由数字、大/小写字母组成，未配置口令定期更换。	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，应用系统启用了登录失败处理功能和登录连接超时自动退出功能，连续登录失败 3 次锁定账号，由管理员解锁，登录后无操作 60 分钟，设备自动退出登录状态。	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，应用系统未采用加密协议进行远程管理，不能防止鉴别信息在网络传输中被窃听。	不符合
访问控制	a) 应对登录的用户分配账户和权限；	经核查，应用系统由系统管理员进行角色划分与权限分配，基于权限列表对登录的账户进行模块化授权，并删除了默认账户。	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，应用系统已修改默认账户的默认口令。	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，应用系统不存在多余或过期账户，且管理员用户与账户之间一一对应，不存在多人使用同一账户的情况。	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，应用系统已按照三权分立原则，划分了系统管理员、安全管理员、审计管理员，并为其分配了不同权限或角色，实现了管理用户的权限	符合

控制点	测评项	结果记录	符合情况
		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，应用系统已开启安全审计功能，可以对登录事件、操作事件等重要用户行为和重要安全事件进行审计，审计覆盖到每个账户。	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，应用系统的审计记录包括事件的日期和时间、用户、事件类型、事件是否成功等审计相关信息。	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，应用系统审计日志存放在数据库中，数据库每天对审计日志进行全量备份，审计日志留存时间满足 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；	经核查，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对应用系统无相关判定需求，故此项为不适用项。	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，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对应用系统无相关判定需求，故此项为不适用项。	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；	经核查，应用系统自身无终端接入控制功能，网络层限制会造成业务访问困难，故此项为不适用项。	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，应用系统提供了数据有效性检验功能，对文本输入框进行了格式和长度限制，如输入包含特殊字符的语句时，系统进行了字符转义，可以正常处理请求。	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，未定期对应用系统进行漏洞扫描，不能发现可能存在的已知漏洞。	不符合
可信验证	a) 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	经核查，应用系统无可信验证环境。	不符合

控制点	测评项	结果记录	符合情况
	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	a) 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，应用系统未采用加密协议进行通信传输，不能保证鉴别数据、重要配置数据、重要审计数据和重要业务数据在传输过程中的完整性。	不符合
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，应用系统在重大变更前/后进行本地配置备份，业务数据每天进行全量备份，备份策略合理，备份结果与备份策略一致，但未定期对备份文件进行恢复测试。	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，应用系统的配置数据、业务数据未进行异地定时备份。	不符合
剩余信息保护	a) 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，应用系统退出登录后无法通过复制链接直接访问应用系统，需要重新进行登录验证，应用系统的临时文件未有残留的用户鉴别信息，可以保证鉴别信息所处的存储空间被释放或重新分配前得到完全清除。	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；	经核查，应用系统仅采集和保存业务必需的用户个人信息，如用户姓名、单位等，未收集其他多余信息，并且单位制定了《个人信息管理制度》对个人信息采集、保存等内容进行规定。	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，应用系统禁止未授权访问和非法使用用户个人信息，并且单位制定了《个人信息管理制度》对个人信息的访问授权、使用等内容进行了规定。	符合

D.4.1.6.2 BPM 系统

控制点	测评项	结果记录	符合情况
安全通用要求			

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，应用系统采用“用户名+静态口令”方式对用户进行身份标识和鉴别；查看用户列表得知，身份标识具有唯一性，不存在空口令用户；口令长度大于等于 3 位，不超过 16 位，口令复杂度较低，未配置口令定期更换。	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，应用系统启用了登录失败处理功能，连续登录失败 5 次锁定账号 2 分钟，登录后无操作 24 小时，设备自动退出登录状态，空闲超时退出时间过长。	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在网络传输过程中被窃听。	经核查，应用系统采用 HTTP 协议进行远程管理，不能防止鉴别信息在网络传输中被窃听。	不符合
访问控制	a) 应对登录的用户分配账户和权限；	经核查，应用系统由系统管理员进行角色划分与权限分配，基于权限列表对登录的账户进行模块化授权，但未限制默认账户 SA 的访问权限。	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，应用系统已修改默认账户的默认口令。	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，应用系统管理员用户与账户之间一一对应，不存在多人使用同一账户的情况，但存在多余账户（test1、test1109、test77、test88）。	部分符合
	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，应用系统已按照三权分立原则，划分了系统管理员、安全管理员、审计管理员，并为其分配了不同权限或角色，但未禁用或限制默认账户 SA 的访问控制权限。	部分符合
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，应用系统已开启安全审计功能，可以对登录事件、操作事件等重要用户行为和重要安全事件进行审计，审计覆盖到每个账户。	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，应用系统的审计记录包括事件的 ID、UserID、User、IP、place、时间日期等审计相关信息。	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，应用系统审计日志存放在数据库中，数据库每天对审计日志进行全量备份，审计日志留存时间满足 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；	经核查，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对应用系统无相关判定需求，故此项为不适用项。	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，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项对应用系统无相关判定需求，故此项为不适用项。	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；	经核查，应用系统为互联网前台页面，面向互联网访问，故此项为不适用项。	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，应用系统提供了数据有效性检验功能，对文本输入框进行了格式和长度限制，如输入包含特殊字符的语句时，系统进行了字符转义，可以正常处理请求。	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，未定期对应用系统进行漏洞扫描，不能发现可能存在的已知漏洞。	不符合
可信验证	a) 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，应用系统无可信验证环境。	不符合
数据完整性	a) 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，应用系统采用 HTTP 协议进行通信传输，不能保证鉴别数据、重要配置数据、重要审计数据、重要业务数据和重要个人信息在传输过程中的完整性。	不符合
数据备	a) 应提供重要数据	经核查，应用系统在重大变更前/后进	符合

控制点	测评项	结果记录	符合情况
份恢复	的本地数据备份与恢复功能；	行本地配置备份，业务数据每天进行全量备份，备份策略合理，备份结果与备份策略一致，每 1-2 个月对备份文件进行恢复测试。	
	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，应用系统的配置数据、业务数据未进行异地定时备份。	不符合
剩余信息保护	a) 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，应用系统退出登录后无法通过复制链接直接访问应用系统，需要重新进行登录验证，应用系统的临时文件未有残留的用户鉴别信息，可以保证鉴别信息所处的存储空间被释放或重新分配前得到完全清除。	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；	经核查，应用系统仅采集和保存业务必需的用户个人信息，如用户姓名、单位等，未收集其他多余信息，并且单位制定了《个人信息管理制度》对个人信息采集、保存等内容进行规定。	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，应用系统禁止未授权访问和非法使用用户个人信息，并且单位制定了《个人信息管理制度》对个人信息的访问授权、使用等内容进行了规定。	符合

D.4.1.7 数据资源

D.4.1.7.1 鉴别数据

控制点	测评项	结果记录	符合情况
安全通用要求			
数据完整性	a) 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，1）网络设备采用 HTTPS 协议进行远程管理；2）安全设备采用 HTTPS 协议进行远程管理；3）Windows 服务器已启用“远程（RDP）连接要求使用指定的安全层”，安全层为 SSL/RDP；4）数据库通过所在服务器进行管理；5）以上设备/系统可以保证鉴别数据在传输过程中的完整性；6）应用系统采用 HTTP 协议进行	部分符合

控制点	测评项	结果记录	符合情况
		管理，不能保证鉴别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，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项仅针对配置数据和业务数据，当前测评对象为鉴别数据，故此项为不适用项。	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，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项仅针对配置数据和业务数据，当前测评对象为鉴别数据，故此项为不适用项。	不适用
剩余信息保护	a) 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，1）Windows 服务器已开启“交互式登录：不显示最后的用户名”能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；2）Linux 服务器自身具有剩余信息处理机制，用户注销后，系统会进行相关的剩余信息处理，可以完全清除鉴别信息所处的存储空间；3）数据库用户在退出或注销时会自动清除鉴别信息所在的存储空间，不会残留用户鉴别信息；4）应用系统退出登录后无法通过复制链接直接访问应用系统，需要重新进行登录验证，应用系统的临时文件未有残留的用户鉴别信息。	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，此测评项仅针对个人信息，当前测评对象为鉴别数据，故此项为不适用项。	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，此测评项仅针对个人信息，当前测评对象为鉴别数据，故此项为不适用项。	不适用

D.4.1.7.2 业务数据

控制点	测评项	结果记录	符合情况
安全通用要求			
数据完整性	a) 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，应用系统采用 HTTP 协议进行远程管理，不能保证业务数据在传输过程中的完整性。	不符合
数据备份恢复	a) 应提供重要数据的本地数据备份与恢	经核查，业务数据每天进行全量备份，备份策略合理，备份结果与备份	部分符合

控制点	测评项	结果记录	符合情况
	复功能；	策略一致，BPM 系统每 1-2 个月对备份文件进行恢复测试，但 ERP 系统未定期对备份文件进行恢复测试。	
	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，应用系统的业务数据未进行异地定时备份。	不符合
剩余信息保护	a) 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，此测评项仅针对鉴别数据，当前测评对象为业务数据，故此项为不适用项。	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，此测评项仅针对个人信息，当前测评对象为业务数据，故此项为不适用项。	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，此测评项仅针对个人信息，当前测评对象为业务数据，故此项为不适用项。	不适用

D.4.1.7.3 审计数据

控制点	测评项	结果记录	符合情况
安全通用要求			
数据完整性	a) 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，1）网络设备采用 HTTPS 协议进行远程管理；2）安全设备采用 HTTPS 协议进行远程管理；3）Windows 服务器已启用“远程（RDP）连接要求使用指定的安全层”，安全层为 SSL/RDP；4）数据库通过所在服务器进行管理；5）以上设备/系统可以保证审计数据在传输过程中的完整性；6）应用系统采用 HTTP 协议进行管理，不能保证审计数据在传输过程中的完整性。	部分符合
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，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项仅针对配置数据和业务数据，当前测评对象为审计数据，故此项为不适用项。	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	经核查，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项仅针对配置数据和	不适用

控制点	测评项	结果记录	符合情况
	批量传送至备用场地。	业务数据，当前测评对象为审计数据，故此项为不适用项。	
剩余信息保护	a) 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，此测评项仅针对鉴别数据，当前测评对象为审计数据，故此项为不适用项。	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，此测评项仅针对个人信息，当前测评对象为审计数据，故此项为不适用项。	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，此测评项仅针对个人信息，当前测评对象为审计数据，故此项为不适用项。	不适用

D.4.1.7.4 配置数据

控制点	测评项	结果记录	符合情况
安全通用要求			
数据完整性	a) 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，1）网络设备采用 HTTPS 协议进行远程管理；2）安全设备采用 HTTPS 协议进行远程管理；3）Windows 服务器已启用“远程（RDP）连接要求使用指定的安全层”，安全层为 SSL/RDP；4）数据库通过所在服务器进行管理；5）以上设备/系统可以保证配置数据在传输过程中的完整性；6）应用系统采用 HTTP 协议进行管理，不能保证配置数据在传输过程中的完整性。	部分符合
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，网络设备、安全设备、服务器、数据库和应用系统在重大变更前/后进行本地配置备份，备份策略合理，备份结果与备份策略一致，但未定期对备份文件进行恢复测试。	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，网络设备、安全设备、服务器、数据库和应用系统的配置数据未进行异地定时备份。	不符合
剩余信息保护	a) 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，此测评项仅针对鉴别数据，当前测评对象为配置数据，故此项为不适用项。	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；	经核查，此测评项仅针对个人信息，当前测评对象为配置数据，故此项为不适用项。	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，此测评项仅针对个人信息，当前测评对象为配置数据，故此项为不适用项。	不适用

D.4.1.7.5 个人信息

控制点	测评项	结果记录	符合情况
安全通用要求			
数据完整性	a) 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，应用系统采用 HTTP 协议进行远程管理，不能保证个人信息在传输过程中的完整性。	不符合
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，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项仅针对配置数据和业务数据，当前测评对象为个人信息，故此项为不适用项。	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，依据《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019），此测评项仅针对配置数据和业务数据，当前测评对象为个人信息，故此项为不适用项。	不适用
剩余信息保护	a) 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，此测评项仅针对鉴别数据，当前测评对象为个人信息，故此项为不适用项。	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，应用系统仅采集和保存业务必需的用户个人信息，如用户姓名、单位等，未收集其他多余信息，并且单位制定了《个人信息管理制度》对个人信息采集、保存等内容进行规定。	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，应用系统禁止未授权访问和非法使用用户个人信息，并且单位制定了《个人信息管理制度》对个人信息的访问授权、使用等内容进行了规定。	符合

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
安全通用要求			
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，网络设备、安全设备、服务器通过运维安全管理系统进行登录，堡垒机和各设备已划分系统管理员账号，已对系统管理员进行了身份鉴别；设备均开启了日志审计功能，可以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，网络设备、安全设备、服务器已划分系统管理员，系统管理员的管理和操作权限有别于审计管理员和安全管理员，指定由系统管理员对设备的资源和运行进行配置、控制和管理，其中包括账户创建、系统资源配置和重要数据的备份与恢复等。	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，部分安全设备、部分服务器划分了审计管理员账户，已对审计管理员账户进行了身份鉴别；设备均开启了日志审计功能，可以对审计管理员的操作行为进行审计。但网络设备、部分安全设备、部分服务器未划分审计管理员账户，无法对审计管理员进行身份鉴别、授权、操作审计等。	部分符合
	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，部分安全设备、部分服务器划分了审计管理员账户，审计管理员的管理和操作权限有别于系统管理员和安全管理员，并且指定由审计管理员对设备和数据库的审计日志进行存储管理和分析，分析结果汇总成报告的形式进行上报。但网络设备、部分安全设备、部分服务器未划分审计管理员账户，不能通过审计管理员对审计记录进行分析。	部分符合

D.6 安全管理制度

D.6.1 安全通用要求部分

控制点	测评项	结果记录	符合情况
安全通用要求			
安全策略	a) 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，该单位已制定《信息安全策略总纲 V1.1》明确了该单位的信息安全建设原则、总体方针和各类安全策略，如物理安全策略、网络安全策略、系统安全策略等，明确了安全工作的目标、范围和原则等。	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，该单位已经建立了完善的安全管理制度，有《信息安全策略总纲 V1.1》、《信息安全岗位职责要求 V1.1》、《机房管理制度》等，其内容涵盖了全体单位人员、物理环境、安全建设、安全运维等方面。	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，该单位已提供《运行维护和监控管理规定 V1.1》、《防火墙策略配置规范 v1.0》。	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，该单位已制定《信息安全策略总纲 V1.1》明确了由第信息管理部负责实施和制定具体的安全要求和流程，并形成相应的管理制度。	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，该单位在《信息安全策略总纲 V1.1》→制度的制定与发布中，明确了安全管理制度的制定应具有统一的格式，对制度进行了编号和版本控制；安全管理制度经信息安全领导小组讨论通过，由信息安全领导小组负责人审批发布，并且在其中注明了相应的发布范围。	符合
评审和修订	a) 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，该单位在《信息安全策略总纲 V1.1》→制度的评审和修订中，每年定期进行一次安全管理制度审查，修订和完善当前的管理制度内容，所有信息安全管理制度的制定和修订均由指定和授权的部门或人员进行，但未提供信息安全管理制度评审与修订记录。	部分符合

D.7 安全管理机构

D.7.1 安全通用要求部分

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，该单位设立了信息安全领导小组，已制定《信息安全策略总纲 V1.1》明确了信息安全领导小组的构成情况和工作职责，其最高领导由单位主管领导委任。	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，该单位设立了信息安全部负责网络安全管理工作，已制定《信息安全岗位职责要求 V1.1》明确安全主管、安全管理各个方面的负责人的岗位和职责。	符合
人员配备	a) 应配备一定数量的系统管理员、审计管理员和安全管理员等。	经核查，该单位已制定《信息安全岗位职责要求 V1.1》明确设立安全管理员、系统管理员、审计管理员等，提供了信息安全人员名单，配备了安全管理员、系统管理员、审计管理员各一名。	符合
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，该单位已制定《信息安全策略总纲 V1.1》明确了信息安全领导小组负责信息系统的所有安全管理活动相关事宜，第一审批人为单位主管领导，关键安全管理活动一律由第一审批人或授权责任人审批，并且已经提供了《变更申请表》等审批记录表单。	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，该单位已制定《信息安全策略总纲 V1.1》明确了对于信息系统中发生的重大及关键安全管理活动的授权和审批过程，已建立了完善的逐级审批程序，要求必须通过部门负责人和单位主管领导的双重审批，并且《变更申请表》等记录表单的审批结果和管理制度要求一致。	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，该单位已制定《信息安全策略总纲 V1.1》明确了该单位内部沟通的机制和流程，该单位原则上每年召开一次信息安全沟通会议，由信息安全部组织，信息安全各部门负责人参加，但未提供《信息安全沟通会议记录表》。	部分符合
	b) 应加强与网络安全职能部门、各类供	经核查，该单位已制定《信息安全策略总纲 V1.1》明确了与单位外部沟通	符合

控制点	测评项	结果记录	符合情况
	应商、业界专家及安全组织的合作与沟通；	的机制和流程，包括与各类设备供应商、业界专家等的沟通，并且提供了腾讯会议记录，会议主题明确了会议内容。	
	c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	经核查，该单位提供了《外联单位联系列表》，列表包含了外联单位名称、合作内容、联系人和联系方式等内容。	符合
审核和检查	a) 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，该单位已制定《信息系统安全审核和安全检查管理制度》明确了安全管理员每年进行一次信息系统的常规性安全检查，但未提供常规性安全检查记录。	部分符合

D.8 安全管理人员

D.8.1 安全通用要求部分

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；	经核查及访谈，该单位已制定《人员安全管理制度 V1.1》明确了由人力资源部负责人员招聘、录用和离职等工作。	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，《人员安全管理制度 V1.1》明确要求负责人员从候选简历中挑选出初步符合所招岗位的人员进行面试、笔试和复试，并对其身份、背景、专业资格和资质进行审查。提供了《录用人员审查表》明确了录用人员的学习简历、工作经历、单位意见、考核结果等内容。	符合
人员离岗	a) 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，该单位已制定《人员安全管理制度 V1.1》明确了当人员离职时，按照单位离职流程，归还所持有的信息资产，归还所有的物理安全设备，包括笔记本、门禁卡、钥匙和证件等，终止该员工的所有访问权限，撤销该员工的账号，收回该员工曾掌握过的密码或密钥，并确认密码或密钥的正确性。	符合

控制点	测评项	结果记录	符合情况
安全意识教育和培训	a) 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，该单位已制定《人员安全管理制度 V1.1》明确了安全培训的各项内容以及安全职责、惩戒措施等相关内容；每年至少进行一次安全意识和岗位技能培训，已提供《培训签到表》明确了培训内容和参与人员。	符合
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《外部人员访问管理规定》规范了外部人员的来访流程，明确了外包人员的访问范围、进入条件等。制定了《外来人员进出机房申请表》，由单位接待人员填写后，经单位领导审批通过后，还必须由接待人员陪同，陪同人员填写《机房人员进出登记表》后才能进入机房进行访问。提供了《外来人员进出机房申请表》明确了审批人签字等内容；提供了《机房人员进出登记表》明确了人员的进出时间、陪同人员等内容。	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，该单位已制定《外部人员访问管理制度 V1.1》明确了外部人员访问系统前应告知其相关的安全责任，并登记备案，由信息管理部审批后，方可访问系统网络；要求对外部人员的访问操作内容进行记录。未提供外部人员访问申请记录。	部分符合
	c) 外部人员离场后应及时清除其所有的访问权限。	经核查，该单位已制定《外部人员访问管理制度 V1.1》明确了外部人员离场后应及时清除其所有的访问权限。运维安全管理系统可以查看到访问权限被清除的时间以及相关账号等。	符合

D.9 安全建设管理

D.9.1 安全通用要求部分

控制点	测评项	结果记录	符合情况
安全通用要求			
定级和备案	a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；	经核查，《光华荣昌智能数字化平台系统网络安全等级保护定级报告》文档内容已经明确该系统的安全保护等级以及定级的方法和理由。	符合

控制点	测评项	结果记录	符合情况
	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，该单位已组织相关部门和技术专家对定级结果的合理性和正确性进行论证和审定，并提供了《光华荣昌智能数字化平台系统网络安全等级保护定级评审意见》。	符合
	c) 应保证定级结果经过相关部门的批准；	经核查，该系统的定级结果已获得相关部门批准，并取得备案证明。	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，该单位已将系统备案材料上传至北京市公安局昌平分局进行备案，并取得备案证明，备案证编号：11011499364-24001。	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，《光华荣昌智能数字化平台系统网络安全等级保护定级报告》已明确系统安全保护等级为第二级；被测单位已按照第二级保护需求进行了安全加固和调整。	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，该单位无相关的安全规划设计类文档和被测系统安全方案设计文档。	不符合
	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，该单位未提供整体安全规划和安全方案设计的专家论证文档和批准意见。	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，该单位的相关网络安全产品采购和使用已符合国家的有关规定，具有销售许可证明。	符合
	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，该单位未有密码产品，此项不适用。	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，该系统为外包开发，此项不适用。	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，该系统为外包开发，此项不适用。	不适用

控制点	测评项	结果记录	符合情况
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，该单位无相关恶意代码检测报告。	不符合
	b) 应保证开发单位提供软件设计文档和使用指南。	经核查，该单位已提供《软件设计说明书》、《系统操作手册》等。	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，该单位由信息安全部负责对工程实施过程进行监督和管理。	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，该单位未制定工程实施方面的管理制度以及控制方法。	不符合
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，该单位未有相关的测试验收方案和测试验收报告。	不符合
	b) 应进行上线前的安全性测试，并出具安全测试报告。	经核查，该单位未提供上线前的安全性测试报告。	不符合
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，该单位提供了《系统交付清单》明确了系统资产、项目阶段文档等内容。	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，该单位未提供相关技术培训记录文档。	部分符合
	c) 应提供建设过程文档和运行维护文档。	经核查，该单位已提供《软件设计说明书》、《系统操作手册》，但未提供《项目测试验收报告》、《运维培训记录表》等记录表单。	部分符合
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，该系统为首次等级测评，不适用。	不适用
	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，该系统暂无发生过重大变更或级别发生变化，在《信息安全策略总纲 V1.1》中，规定系统发生重大变更或者系统等级发生变化后，将相关修订实施细则报信息安全办公室进行	符合

控制点	测评项	结果记录	符合情况
		备案，并开展等级测评。	
	c) 应确保测评机构的选择符合国家有关规定。	经核查，该单位已选取符合国家有关规定的测评机构开展等级测评工作。本次等级测评选取的测评机构为国源天顺科技产业集团有限公司，该测评机构已获得公安部第三研究所（国家认证认可委员会批准的认证机构）认证发放的《网络安全等级测评与检测评估机构服务认证证书》，认证证书编号为 SC202127130010050。	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；	经核查及访谈，该单位选择的服务供应商（国源天顺科技产业集团有限公司、深信服科技股份有限公司）具备相应的安全服务资质，符合国家有关规定。	符合
	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，该单位已与选定的服务供应商签订了合同协议，明确约定了相关责任、技术培训、服务承诺、服务期限等内容。	符合

D.10 安全运维管理

D.10.1 安全通用要求部分

控制点	测评项	结果记录	符合情况
安全通用要求			
环境管理	a) 应指定专门的部门或人员负责机房安全，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；	经核查及访谈，该单位已制定《机房管理制度》明确了由机房管理员对机房的环境安全和网络通信等进行管理；提供了《机房设备运行及维护记录》明确了设备参数、用途和设备运行是否正常等。	符合
	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，该单位已制定《机房管理制度》覆盖了机房的物理环境、物理访问、物品进出、人员出入等内容的管理，提供了《机房人员出入登记表》明确了来访人员、来访时间、携带物品等内容。	符合
	c) 应不在重要区域接待来访人员，不随	经核查，该单位已制定《北京光华荣昌汽车部件有限公司办公环境安全管	符合

控制点	测评项	结果记录	符合情况
	意放置含有敏感信息的纸档文件和移动介质等。	理制度》明确了办公区应设置专门的接待区域，由接待人员统一处理外来人员的出入申请，在受访者陪同下进入办公区域；办公区内不得随意存放涉及单位管理、技术、财务、人力资源等部门机密信息。	
资产管理	a) 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，该单位已制定《北京光华荣昌汽车部件有限公司办公环境安全管理制度》明确了资产管理员应制定和维护所管辖的资产清单，提供了《信息设备资产清单》明确了资产类别、责任部门、所处地点、存放形式等内容。	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；	经访谈系统管理员，核查相关制度， 1)当前使用的存储介质形态是：硬盘； 2)存放环境是：系统管理员保存，负责的部门或人员是：系统管理员； 3)定期盘点记录；盘点记录：《存储介质管理登记表》，内容包括：介质名称、介质数量、盘点人、盘点时间。	符合
	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。	经核查及访谈，该单位已制定《存储介质管理规定》明确了对介质的传输过程进行控制，资产管理员对存储介质的转移和支配必须进行登记，填写《信息系统存储介质使用清单》，对存储介质传递过程需要有记录并定期对登记记录进行复核；提供了《信息系统存储介质使用清单》明确了介质的使用情况、归还情况等内容。	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；	经访谈系统管理员，核查相关制度， 1)系统管理员负责对各类设备进行定期维护； 2)具有明确设备维护管理责任部门的文件； 3)文件名：《资产安全管理制度》，制度要求和访谈结果一致。	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	经访谈系统管理员，核查相关制度， 1)具有设备维护管理制度文件； 2)文件名：《运行维护和监控管理制度》，内容包括：明确维护人员的责任、维修和服务的审批、维修过程的	部分符合

控制点	测评项	结果记录	符合情况
	程的监督控制等。	监督控制等； 3)未提供维修和服务的审批、维修过程等记录。	
漏洞和风险管理	a) 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，该单位未定期对设备等进行漏洞扫描，无相关漏洞扫描报告。	不符合
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，明确各个角色的责任和权限；	经访谈系统管理员，核查相关制度， 1)具有管理员职责文档； 2)职责文件名：《信息安全管理组织职责》，文件明确各个角色的责任和权限，包括网络管理员、系统管理员、安全管理员、审计管理员等角色； 3)与技术测评人员核实，网络和系统的运维管理人员和职责文件定义一致。	符合
	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；	经访谈系统管理员，核查相关制度， 1)负责账户的管理工作的部门或人员是：系统管理员； 2)具有管理员职责文档； 3)职责文件名：《信息安全管理组织职责》，文件明确由系统管理员负责账户管理，与访谈结果一致； 4)不具有账户管理记录。	部分符合
	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；	经访谈系统管理员，核查相关制度， 1)具有网络和系统安全管理制度； 2)文件名：《信息系统安全审核和安全检查管理制度》； 3)制度内容包括：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，内容覆盖全面。	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；	经访谈系统管理员，核查相关制度， 1)具有重要设备的配置和操作手册； 2)文件名：《防火墙策略配置规范》、《安全域划分规范》、《入侵检测系统策略配置规范》、《终端安全管理制度》，手册内容包括操作步骤、维护记录、参数配置等；	符合
	e) 应详细记录运维	经访谈系统管理员，核查相关制度，	符合

控制点	测评项	结果记录	符合情况
	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。	1)具有对系统进行日常操作、运维管理等工作记录； 2)记录名：《操作日志》内容包括日常巡检工作、运行维护记录、参数的设置和修改等。	
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；	经访谈系统管理员，核查相关制度， 1)采取定期培训方式提升员工的防恶意代码意识； 2)具有提升员工防恶意代码意识的培训记录或宣贯记录； 3)记录名：《安全培训记录表》； 4)制定了《北京光华荣昌汽车部件有限公司恶意代码防范管理制度》，对恶意代码检查作出了规定，对外来计算机或存储设备接入系统前进行恶意代码检查。	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、恶意代码的定期查杀等；	经访谈系统管理员，核查相关制度， 1)具有恶意代码防范措施，已制定《北京光华荣昌汽车部件有限公司恶意代码防范管理制度》； 2)具有恶意代码防范措施特征库的更新记录，内容包括主程序版本、病毒库日期。	符合
	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。	经核查及访谈，该单位已定期对安全设备的恶意代码库进行升级，并且对截获的恶意代码进行分析和汇总上报，已经提供了《恶意代码库升级记录》和《恶意代码分析报告》。	符合
配置管理	a) 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。	经访谈系统管理员，核查相关制度， 1)具有对配置信息进行保存的记录； 2)记录名：《北京光华荣昌汽车部件有限公司信息网络安全检查实施细则》，内容包括应记录和保存基本配置信息，包括网络拓扑结构、IP 地址、软件组件的版本和补丁信息等，已提供相关的配置信息记录，覆盖全面。	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，《信息安全策略总纲 V1.1》中明确要求安全管理员在密码管理过程中必须遵循密码相关标准和规定，要求重要数据的传输和存储必须使用安全的加密算法。	符合
	b) 应使用国家密码	经核查，该单位未使用相关的密码产	不适用

控制点	测评项	结果记录	符合情况
	管理主管部门认证核准的密码技术和产品。	品，不涉及此项内容，不适用。	
变更管理	a) 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。	经访谈系统管理员，核查相关制度， 1)以往发生过的系统变更均制定变更方案； 2)变更方案名：《北京光华荣昌汽车部件有限公司变更管理办法》，内容包括提交变更申请、审核变更申请、变更可用性、批准变更、实施变更等； 3)不具有变更方案评审记录。	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；	经访谈系统管理员，核查相关制度， 1)具有定期备份的重要业务信息、系统数据及软件系统的备份记录； 2)备份重要业务信息的周期是每天增量备份、每周全量备份，备份记录清单名称是《存储介质管理登记表》； 3)备份系统数据的周期是每天增量备份、每周全量备份，备份记录清单名称是《存储介质管理登记表》； 4)备份软件系统的周期是每天增量备份、每周全量备份，备份记录清单名称是《存储介质管理登记表》。	符合
	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；	经访谈系统管理员，核查相关制度， 1)具有备份与恢复管理制度； 2)文件名：《北京光华荣昌汽车部件有限公司数据备份与恢复管理办法》，内容包括：对应用系统、操作系统、数据库系统、网络系统等的业务数据和系统数据进行定期备份，每天增量备份，每周全量备份，备份数据保留在硬盘中，备份保留 1 年，内容覆盖全面。	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。	经访谈系统管理员，核查相关制度， 1)具有备份恢复策略和程序； 2)文件名：《北京光华荣昌汽车部件有限公司数据备份与恢复管理办法》，内容包括：明确数据备份策略和恢复策略、备份程序和恢复程序等，内容根据数据的重要程度制定。	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	经访谈系统管理员，核查相关制度， 1)具有明确告知用户在发现安全弱点	符合

控制点	测评项	结果记录	符合情况
	安全弱点和可疑事件；	和可疑事件时应及时向安全管理部门报告的文件； 2)文件名：《北京光华荣昌汽车部件有限公司信息安全事件报告和处置管理制度》； 3)具有安全弱点和可疑事件对应的报告或记录； 4)报告或记录：《安全检查报告及安全检查表》。	
	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；	经访谈系统管理员，核查相关制度， 1)具有安全事件管理制度； 2)文件名：《北京光华荣昌汽车部件有限公司信息安全事件报告和处置管理制度》，内容包括：明确安全事件的报告、处置和响应流程，并且规定安全事件的现场处理、事件报告，内容覆盖全面； 3)具有安全事件报告的模板文件； 4)模板文件名：《安全检查报告及安全检查表》。	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《安全事件报告和处置管理制度 V1.1》规范安全事件报告和响应处理流程，要求事件调查组利用合法手段在安全事件现场收取证据，向信息系统使用或维护单位了解事件发生经过，收集相关资料，查明事件发生的原因、危害程度及造成的损失等情况，检查预防和控制事件发生的措施以及事件发生后应急预案是否得当并得到落实，确定事件的级别和性质，查明相关责任并提出处理建议，提出防止类似事件再次发生的措施和建议。	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；	经访谈系统管理员，核查相关制度， 1)具有重要事件的专项应急预案，针对机房(供电、火灾、漏水等)、系统(病毒爆发、数据泄露等)、网络(断网、拥塞等)等各个层面； 2)具有专项事件应急预案，内容包含：应急处理流程、恢复流程。	符合
	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	经访谈系统管理员，核查相关制度， 1)定期对系统相关的人员进行应急预案培训和演练：	符合

控制点	测评项	结果记录	符合情况
	预案的演练。	2)每年组织次应急预案培训和演练，演练内容：通过演练发现应急工作体系和工作机制存在的问题，不断完善应急预案，提高应急处置能力； 3)具有应急预案的培训记录、演练记录； 4)应急预案的培训记录：《应急预案培训记录》，内容包括：培训人员、培训时间、培训内容、培训地点； 5)应急预案演练记录：《应急预案演练记录》，内容包括：演练方式、演练目的、演练内容、整改措施。	
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，该单位未有外包运维服务情况，不涉及此项内容，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，该单位未有外包运维服务情况，不涉及此项内容，不适用。	不适用

D.11 其他安全要求

暂无其他安全要求。

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	危险程度	漏洞名称	影响 IP	漏洞修复建议
1	低	获取 SSL 证书中的 hostname【原理扫描】	192.168.0.1 192.168.0.5 192.168.10.218	解决方案： 无需修复，仅仅为信息获取
2	低	获取目标 SSL 证书过期时间【原理扫描】	192.168.0.1 192.168.10.218	仅用作信息收集，无需修复
3	低	检测到目标主机加密通信支持的 SSL 加密算法【原理扫描】	192.168.0.1 192.168.10.218	该漏洞仅仅是一个信息获取的漏洞，可以不做修复。
4	低	SMTP 服务器版本信息可被获取	192.168.0.1 192.168.0.5 192.168.0.204 192.168.0.16 192.168.12.254 192.168.5.93	NSFOCUS 建议您采取以下措施以降低威胁： * 修改源代码或者配置文件改变缺省 banner 信息。
5	低	探测到服务器支持的 SSL 加密协议【原理扫描】	192.168.0.1 192.168.0.5	该漏洞仅仅是一个信息获取的漏洞，可以不做修复。
6	低	可通过 HTTP 获取远端 WWW 服务信息	192.168.0.1 192.168.0.5 192.168.0.16	该漏洞仅是为了信息获取，建议隐藏敏感信息。如果 banner 未包含敏感信息，则表明该漏洞已经不具备暴露敏感信息风险，可以不用修复。
7	中	检测到目标 SSL 证书已过期【原理扫描】	192.168.0.5	修复建议： 及时购买或生成一个新的 SSL 证书以取代现有的证书
8	中	服务器支持 TLS Client-initiated 重协商攻击(CVE-2011-1473)【原理扫描】	192.168.0.5	使用 SSL 开启重协商的服务都会受该漏洞影响 Apache 解决办法： 升级到 Apache 2.2.15 以后版本 IIS 解决办法： IIS 5.0 启用 SSL 服务时，也会受影响。可以升级 IIS 6.0 到更高的版本。

序号	危险程度	漏洞名称	影响 IP	漏洞修复建议
				Lighttpd 解决办法： 建议升级到 lighttpd 1.4.30 或者更高，并设置 ssl.disable-client-renegotiation = "enable"。 http://download.lighttpd.net/lighttpd/releases-1.4.x/ Nginx 解决办法： 0.7.x 升级到 nginx 0.7.64 0.8.x 升级到 0.8.23 以及更高版本。 http://nginx.org/en/download.html Tomcat 解决办法： 1、使用 NIO connector 代替 BIO connector，因为 NIO 不支持重协商，参考如下配置： <Connector protocol="org.apache.coyote.http11.Http11NioProtocol">（可能会影响 Tomcat 性能）； 2、配置 Nginx 反向代理，在 Nginx 中修复 OpenSSL 相关问题。 参考链接: https://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html https://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html http://tomcat.apache.org/security-7.html#Not_a_vulnerability_in_Tomcat

序号	危险程度	漏洞名称	影响 IP	漏洞修复建议
				https://tomcat.apache.org/tomcat-6.0-doc/config/http.html#Connector_Comparison Squid 解决办法: 升级到 3.5.24 以及以后版本 http://www.squid-cache.org/Versions/ 缓解或者修复建议: 1、建议关闭重协商，举例：ssl renegotiation disable 2、无法禁用重新协商策略的建议: a)则仅允许安全重新协商并限制 SSL 握手的次数，或者通过添加 SSL 加速器之类的产品来升级服务器资源。不支持不安全的重新协商 b)请限制 SSL 握手的次数，或者通过添加 SSL 加速器之类的产品来升级服务器资源。 c)增加防火墙规则，限制端口访问等策略 d)使用 iptable 规则，限制每个 ip 地址的请求数 如果扫描器跟目标机之间存在 WAF，请优先检查 WAF 配置。
9	低	使用了自签名证书【原理扫描】	192.168.0.5	解决方案: 购买证书。
10	低	SSL 证书链不完整【原理扫描】	192.168.0.5	解决方案: 购买证书。
11	低	SSL 证书无法受到信任【原理扫描】	192.168.0.5	解决方案: 购买证书。
12	低	Oracle Database Server 安全漏洞(CVE-2014-2478)	192.168.0.5	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接: http://www.oracle.com/technet

序号	危险程度	漏洞名称	影响 IP	漏洞修复建议
				work/topics/security/cpuoct2014-1972960.html
13	低	Oracle Enterprise Manager Grid Control Enterprise Manager for Oracle Database 组件安全漏洞(CVE-2014-6488)	192.168.0.5	厂商补丁： Oracle ------ 目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
14	低	Oracle Database Server Core RDBMS 组件安全漏洞(CVE-2013-3790)	192.168.0.5	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
15	低	远端 VMWARE SERVER 服务正在运行	192.168.0.5	NSFOCUS 建议您采取以下措施以降低威胁： * 在您的防火墙上限制对端口 TCP 902 的访问； * 如果你不需要该服务，请关掉它。
16	低	Oracle tnslsnr 的版本可以查询	192.168.0.5	NSFOCUS 强烈您使用防火墙屏蔽非信任 IP 对该端口的的访问。同时也建议使用此软件的用户随时关注并从厂商的主页获取最新版本： http://www.oracle.com
17	低	服务器允许 SSL 会话恢复【原理扫描】	192.168.0.5 192.168.5.253 192.168.10.218	该漏洞仅仅是对 SSL 会话恢复的检测，可以不修复。
18	低	工作站服务正在运行	192.168.0.5	
19	低	远程主机计算机名检测	192.168.0.5 192.168.0.16	该漏洞仅是为了信息获取，建议隐藏敏感信息。
20	低	远程桌面服务(RDS)协议探测	192.168.0.5 192.168.0.16	无需修复。
21	中	伪来源 IP 地址的 DNS 远程攻击漏洞(CVE-	192.168.10.218	解决方案： 1.建议对于无意义的查询，

序号	危险程度	漏洞名称	影响 IP	漏洞修复建议
		2006-0987)【原理扫描】		不回复任何响应。 2.限制 ip 访问 3.禁用 DNS 递归查询， 4.针对 bind ，配置 ACL 策略，参考链接： https://kb.isc.org/docs/aa-00269

22	中	远端 DNS 服务允许递归查询	192.168.10.218	NSFOCUS 建议您采取以下措施以降低威胁：
				
				* 限制这台主机的递归查询
				
				具体方法为：
				
				1. 如果你使用 bind 8，可以在“named.conf”文件（缺省路径是/etc/named.conf）的“options”里使用“allow-recursion”来进行限制。
				
				例如，您可以只允许自己本地主机以及内部主机进行递归查询，其他主机则不允许递归查询：
				
				options {
				allow-recursion
				{ 192.168.196.0/24;
				localhost; };
				};
				
				注意：在修改完配置文件之后，需要重新启动 named。
				
				2. 如果您使用的是 Windows DNS Server，可以通过修改注册表来将其配置为非递归 DNS Server。
				只要将注册表中 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\DNS\Parameters 的 RecursionNO 的值设定为

序号	危险程度	漏洞名称	影响 IP	漏洞修复建议
				ture.默认是 false。 当有合法的解析器使用 DNS 服务器，或其它合法的 DNS 服务器将这个 DNS 服务器作为传递服务器（forwarder）时，不应关闭递归查询，如果不能关闭递归查询，就需要进行对进行递归查询的 IP 地址作出限制。如果递归查询请求来自不允许的 IP 地址，则 DNS 服务器将此查询以非递归查询对待。 3. 如果使用其它版本的 Name Server，请参考相应的文档。
23	低	检测到远端 DNS 服务正在运行中	192.168.10.218	NSFOCUS 建议您使用专用 DNS 服务，并禁用自己架设的 DNS 服务。

附录F 渗透测试结果记录

被测系统安全保护等级为第二级（S2A2），不涉及渗透测试。

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。