报告编号：11011499364-22003-22-0039-01

项目编号：SDXW-DB202204-23-003

网络安全等级保护
ERP 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：北京时代新威信息技术有限公司

报告时间：2022 年 07 月

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	ERP 系统			安全保护等级	第二级（S2A2）
备案证明编号	11011499364-22003				
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	102211
联系人	姓名	王金良	职务/职称	IT 经理	
	所属部门	集团信息管理部	办公电话	010-89774865	
	移动电话	18610116864	电子邮件	Wangjinliang@bjgrc.co	
测评单位					
单位名称	北京时代新威信息技术有限公司			机构代码	SC202127130010039
单位地址	北京市海淀区知春路甲 48 号 2 号楼 12 层 2-5-15C			邮政编码	100086
联系人	姓名	杨玉忠	职务/职称	副总经理	
	所属部门	营销中心	办公电话	010-58732083	
	移动电话	13601264474	电子邮件	yangyuzhong@powertime.cn	
审核批准	编制人		编制日期	2022.07.20	
	审核人		审核日期	2022.07.21	
	批准人		批准日期	2022.07.22	

声明

本报告是“ERP 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。

北京时代新威信息技术有限公司

2022 年 07 月

等级测评结论

测评结论和综合得分			
被测对象名称	ERP 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（国标） □大数据（团标）		
被测对象描述	北京光华荣昌汽车部件有限公司的应用系统承担了供应链、生产、财务、物流、仓库管理系统等业务，建立了一套具有较强的业务处理能力的“ERP 系统”，并对该系统具有信息安全保护责任。 “ERP 系统”采用 C/S 架构部署，使用 HTTP 协议 80 端口进行数据传输，重要数据每天凌晨 2 点进行全量备份。 北京光华荣昌汽车部件有限公司已制定各方面管理制度对“ERP 系统”进行管理，管理制度已覆盖网络、主机、系统、数据、应用层面。		
安全状况描述	本次测评共发现安全问题 40 个，其中，中风险问题 20 个，低风险问题 20 个；选取的测评指标总数为 135 个，不适用指标为 10 个，测评指标符合率为 68.0%，测评指标部分符合率为 22.4%，测评指标不符合率为 9.6%；本次测评的综合得分为 71.21 分，测评结论为中。		
等级测评结论	中	综合得分	71.21 分

总体评价

通过对信息系统基本安全保护状态的分析，北京光华荣昌汽车部件有限公司（以下简称“光华荣昌”）针对“ERP 系统”面临的主要安全威胁采取了相应的安全机制，基本达到保护信息系统重要资产的作用。其中：

在安全物理环境方面：被测系统机房物理位置选择合理，人员访问控制严格，在防盗窃和防破坏、防雷击、防静电、防火、防水和防潮等方面均做了安全防护措施，温湿度控制在合理范围内，具有 UPS 设备，满足短期的备用电力供应。

在安全通信网络方面：被测系统按照方便管理的原则划分了不同的网络区域，系统网络结构合理，重要区域未部署在网络边界处，网络设备的处理能力和网络带宽满足业务高峰期需求，部分安全设备和服务器使用 HTTPS 和 SSH 通信方式保证数据在传输过程中的完整性和保密性。

在安全区域边界方面：互联网边界通过防火墙进行边界访问控制，保证跨越边界的访问和数据流通过受控接口通信。根据各区域访问控制策略，在防火墙上配置了访问控制规则，无多余和无效规则，策略配置合理有效。通过防火墙、Web 应用防护系统和网络入侵防御系统（NIPS）对网络中的入侵行为、恶意代码和恶意流量进行检测和防护。被测系统中安全服务和组件已开启审计功能，配置了日志审计策略，能够对重要的用户行为和重要安全事件进行审计，审计记录备份到日志审计设备上。

在安全计算环境方面：安全产品、服务器、应用系统的身份鉴别措施有效，安全策略配置合理，根据管理人员的职责创建账户，并分配相应的权限；安全产品、服务器、应用系统等具有安全审计功能，能够对重要的用户行为和

重要安全事件进行审计，审计记录定期备份。系统中已部署安全防护软件可对服务器进行恶意代码查杀；管理员已对业务数据进行备份，满足系统数据保护要求。

在安全管理中心方面：通过堡垒机对服务器、网络设备和安全产品进行集中管理，通过日志审计对服务器、网络设备和安全产品的日志进行集中收集、分析；堡垒机和日志审计采取用户名/口令的登录方式对系统管理员、审计管理员和安全管理员进行身份鉴别。

在安全管理制度方面：光华荣昌已制定《信息安全策略总纲》，明确网络安全的总体方针、原则和安全框架等内容；授权集团信息管理部负责制定安全管理制度，管理制度已覆盖网络安全、主机安全、系统安全、数据安全、应用安全等方面的内容。

在安全管理机构方面：光华荣昌授权集团信息管理部为网络安全管理的职能部门，被测单位岗位设置合理，职责明确，人员配备齐全。被测单位制定了授权和审批制度，授权审批事项明确，系统变更、重要操作、物理访问和系统接入等事项严格依照审批流程执行。

在安全管理人员方面：被测单位授权人力资源部负责人员录用和离岗工作，人员录用及离岗流程严格规范，人力资源部负责对各类人员进行安全意识培训及岗位技能培训；建立了外部人员访问管理制度，对外部人员访问受控区域进行严格控制。

在安全建设管理方面：被测系统的定级、备案、测评等工作严格按照等级保护制度要求进行。指定集团信息管理部负责工程实施过程的管理，严格控制项目开发进度、代码编写规范、测试验收及系统交付，并在系统交付后进行网

络安全等级保护测评，被测单位选择的测评机构、产品供应商以及采购的安全产品均符合国家有关规定。

在安全运维管理方面：被测单位对系统变更、恶意代码防范、备份与恢复管理、变更管理、安全事件及应急预案等工作均已制定明确的规章制度。运维人员按照规定的备份周期、备份方式对重要数据进行备份。

综上所述，“ERP 系统”安全措施基本完备，安全策略相对合理，安全管理制度较齐全。本次网络安全等级保护测评的等级测评结论为中，综合得分为 71.21 分。

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，“ERP 系统”存在的主要问题及整改建议如下：

一、安全物理环境

（1）中风险 未采取措施防止地下积水的转移和渗透。

整改建议：建议排查地下积水的转移与渗透情况，及时加强、完善相关防范措施；安装防结露设施，并对主机房和辅助区的温度、露点温度或相对湿度等环境参数加强监测和控制，当环境参数超出设定值时，应报警并及时处置。核心设备区及高密度设备区宜设置机柜微环境监控系统。

二、安全通信网络

（1）中风险 未采用密码技术保证通信过程中数据的完整性；

整改建议：建议采用国家密码管理主管部门认可的密码技术，保护通信过程中数据的完整性。

（2）低风险 未基于可信根对通信设备的引导程序等进行可信验证。

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

三、安全区域边界

（1）低风险 未基于可信根对边界设备的系统引导程序等进行可信验证。

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

四、安全计算环境

（1）中风险 网络中未采用加密协议进行远程管理；

整改建议：建议禁用口令明文传输的服务，如 Telnet 等。

（2）中风险 有关设备、系统未配置登录失败处理功能；

整改建议：建议合理配置非法登录次数、锁定时间和登录连接超时时间。

（3）中风险 日志审计功能不完善；

整改建议：建议配置数据库审核策略，对设备的配置管理操作行为、重要的业务操作等行为进行审计。

（4）中风险 未对管理终端的接入方式或网络地址进行限制；

整改建议：建议修改、完善相关设备或系统配置文件，对管理终端的接入方式和网络地址范围进行限制，如限定网络地址为管理终端 IP 地址等。

（5）中风险 未定期修补漏洞；

整改建议：建议安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装。

（6）中风险 未安装恶意代码防护软件，未采取主动免疫可信验证机制防范恶意代码；

整改建议：建议安装防恶意代码软件，启动防恶意代码引擎，定期升级和更新防恶意代码库，对入侵和病毒行为进行有效阻断；或者安装具备可信验证机制的软件或系统，对系统程序、重要配置文件等进行可信验证，如完整性受到破坏则迅速恢复。

（7）中风险 未采用密码技术进行通信完整性验证；

整改建议：建议升级、完善相关系统，采用国家密码管理主管部门认可的校验技术或密码技术，对传输过程中的重要数据进行完整性保护。

（8）中风险 未将重要数据定时批量传送至异地备份场地；

整改建议：建议利用通信网络将重要数据定时批量传送至异地备份场地，实现重要数据异地备份。

（9）中风险 未提供重要数据的备份恢复测试记录；

整改建议：建议检查相关系统的备份策略设置情况，按照总体安全策略要求，配置合理的备份策略，定期进行备份恢复测试并留存记录。

（10）中风险 未授予不同账户为完成各自承担任务所需的最小权限；

整改建议：建议系统授予不同用户为完成各自承担的任务所需的最小权限，将系统管理员和业务操作员权限分离，并设置独立的安全审计员角色，对各类用户的操作行为进行审计监督。

（11）中风险 安全审计功能不完善；

整改建议：建议为系统增加后台重要操作事件的日志记录功能。

（12）中风险 未对审计记录进行备份；

整改建议：建议为设备配置日志服务器，降低日志遭到非授权删除、修改或覆盖的风险。

（13）中风险 未对身份鉴别信息复杂度进行检查，未强制要求定期更换口令；

整改建议：建议设置口令复杂度策略和合理的口令更换周期，确保只有授权用户方可登录系统。

（14）中风险 未根据不同的管理角色授予不同的权限；

整改建议：建议对所有用户按其职责划分不同的角色，按照权责一致原则授予权限。角色划分情况、授予权限情况应登记备案，或存档备查。

（15）中风险 未重命名系统默认账户；

整改建议：建议重命名系统默认账户。

（16）低风险 未基于可信根对计算设备的引导程序等进行可信验证。

整改建议：建议采取可信验证机制对计算设备的引导程序、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。

五、安全管理制度

（1）低风险 缺乏部分管理操作规程。

整改建议：建议补充、完善相关操作规程，为管理人员或操作人员提供完备的规范性参考文档。

六、安全管理人员

（1）低风险 被录用人员的审查记录缺失；

整改建议：建议规范人员录用程序，明确审查和考核要求，客观、准确记录审查情况和技术技能考核情况，将有关文档纳入人力资源档案管理或存档备查。

（2）低风险 离职人员交接记录缺失；

整改建议：建议加强离岗人员的管理，严控离岗流程，详细记录访问权限的撤销以及证件、信息资产的交还情况，留存相关记录或归档备查。

（3）低风险 外部人员离场后的访问权限清除记录缺失。

整改建议：建议认真落实外部人员访问管理制度，严格管控外部人员访问权限的授予和注销（清除）。外部人员离场后，应及时注销所有权限并详细记录，注销（清除记录）应妥善保管或存档备查。

七、安全建设管理

（1）中风险 系统上线前，未对系统进行安全性测试；

整改建议：建议完善验收管理制度，明确系统上线前的安全性测试要求。应委托第三方测试机构对系统进行安全性测试，取得相关部门或行业认可的测试报告。

（2）中风险 安全整体规划及其配套文件未经过充分论证；

整改建议：建议进一步完善安全整体规划及其配套文件，并组织相关部门和技术专家进行论证和审定，形成论证意见，批准后正式实施。

（3）低风险 未提供软件设计文档和使用指南；

整改建议：建议要求开发单位编制并提供软件设计的相关文档和使用指南，并安排专人管理。

（4）低风险 未编制工程实施方案；

整改建议：建议完善工程实施方面的管理制度，明确工程实施方案编制要求，以及对工程实施过程、进度控制、工程质量等方面进行管控的要求。

（5）低风险 未制定测试验收方案，未依据测试验收方案实施测试验收；

整改建议：建议完善测试验收制度，明确验收前制定测试验收方案,确定参与测试验收的部门、人员、测试验收内容等事项；依据验收方案实施测试验收，记录测试验收过程，形成测试验收报告；测试验收报告报请相关部门审定等内容。

（6）低风险 未制定交付清单；

整改建议：建议补充或重新制定系统交付清单，根据交付清单对所交接的设备、软件和文档等进行再次清点。

（7）低风险 建设过程文档和运行维护文档存在缺失情况；

整改建议：建议完善系统验收、交付等相关管理制度，明确建设过程文档和运行维护文档等编制、交付范围，确保交付质量得到有效控制、满足服务级别协议要求。

（8）低风险 未对外包软件中可能存在的恶意代码进行检测。

整改建议：建议在外包软件交付前，通过第三方检查工具或人工对软件中可能存在的恶意代码进行检测，形成检测报告。检测报告应报相关部门审定或存档备查。

八、安全运维管理

（1）中风险 未提供修复漏洞或消除隐患的操作记录；

整改建议：建议部署必要的技术措施，对发现、识别的安全漏洞和隐患及时评估、修补，确保系统安全并留存相应记录文件。

（2）低风险 外来计算机或存储设备接入系统前未进行恶意代码检查；

整改建议：建议指定专人定期对外来计算机或存储设备进行恶意代码检测并保存检测记录。

（3）低风险 未指定专人负责恶意代码库的升级并进行记录；

整改建议：建议指定专人定期对网络和主机进行恶意代码检测并保存检测记录。

（4）低风险 未指定专人负责恶意代码库的升级并进行分析；

整改建议：建议指定专人定期对网络和主机进行恶意代码检测、保存检测记录，并定期分析。

（5）低风险 未严格落实系统变更管理制度，不具有变更方案评审记录；

整改建议：建议加强运维管理，严格按照变更管理制度要求实施变更；变更需求、变更方案、评审记录及审批记录等应妥善保管或存档备查。

（6）低风险 未提供设备维护记录；

整改建议：建议严格执行设备管理制度，按照设备管理制度对设备进行维护管理，并留存维护记录。

（7）低风险 不具有账户管理记录；

整改建议：建议指定专门的部门或人员进行账户管理，并对申请账户、建立账户、删除账户等相关内容进行审批并记录。

（8）低风险 未制定重要设备的配置和操作手册。

整改建议：建议对重要设备如操作系统、数据库、网络设备、安全设备、应用和组件等建立配置和操作手册，应至少包括操作步骤、维护记录、配置参数、操作风险等内容。在日常运维中，依据手册对设备进行安全配置和优化配置。

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。

北京光华荣昌汽车部件有限公司委托北京时代新威信息技术有限公司（认证证书编号 SC202127130010039）对“ERP 系统”开展网络安全等级测评，通过对目标网络系统的安全技术状态及安全管理状况依据相应网络安全等级保护要求进行测试、评估与分析，并将测评结论作为委托方进一步完善系统安全制度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）GB/T 20984-2007：《信息安全技术 信息安全风险评估规范》

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

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

（4）GB 17859-1999：《计算机信息系统 安全保护等级划分准则》

（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》

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）2022 年 4 月 26 日～4 月 29 日，测评准备过程。

（2）2002 年 5 月 5 日～5 月 7 日，方案编制过程。

（3）2022 年 5 月 9 日～6 月 2 日，现场实施过程。

（4）2022 年 6 月 6 日～7 月 22 日，分析与报告编制过程。

其中，2022 年 4 月 26 日召开了项目启动会议，确定了工作方案及项目人员名单；2022 年 6 月 2 日召开了项目末次会议，确认了测评发现的问题。

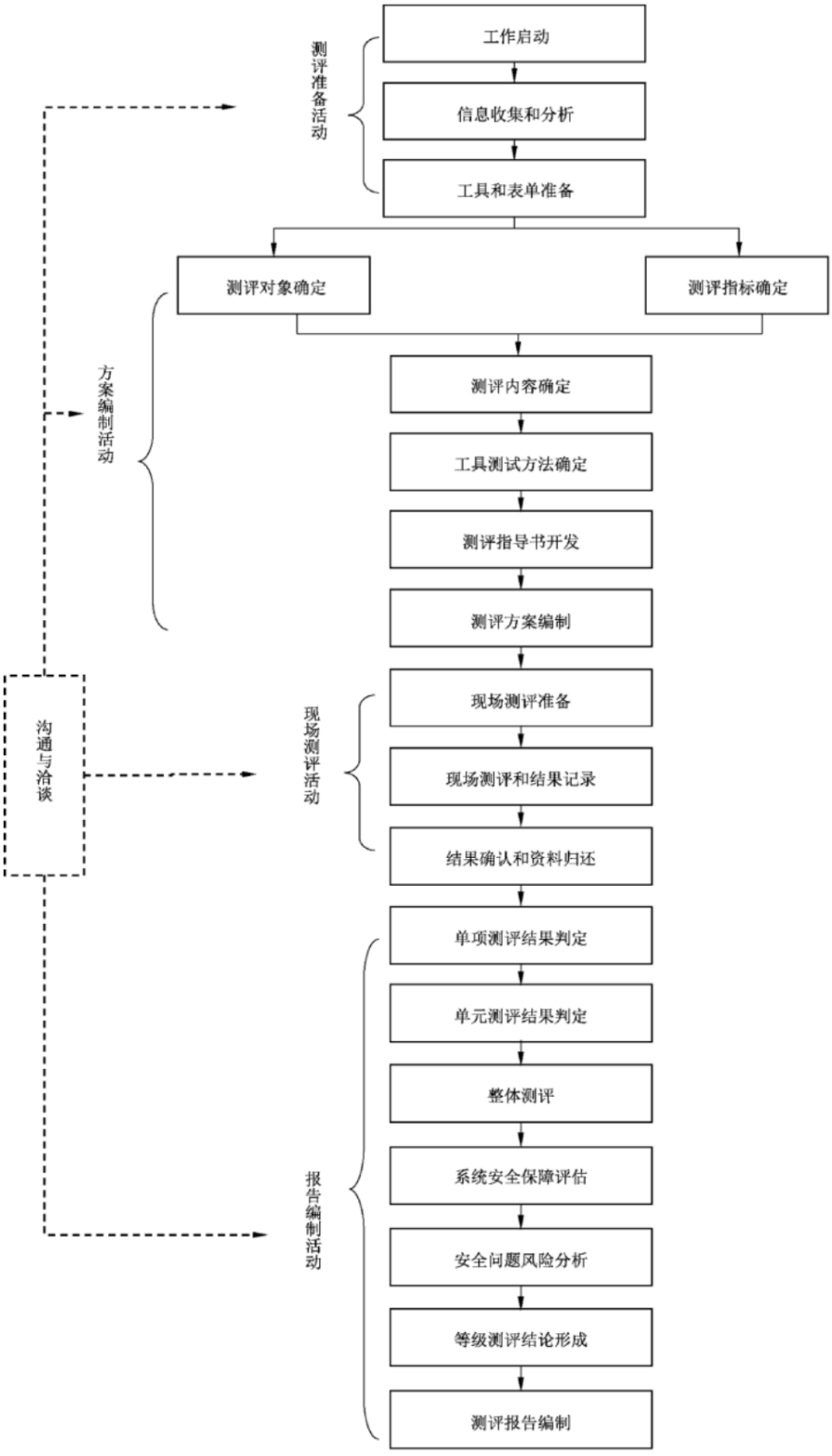

图 1.1 等级保护测评工作流程图

1.4 报告分发范围

等级测评报告正本一式 3 份，其中北京光华荣昌汽车部件有限公司 1 份，北京市公安局昌平分局 1 份，北京时代新威信息技术有限公司 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
ERP 系统	第二级	第二级	第二级

2.1.2 业务和采用的技术

“ERP 系统”主要承载的业务是：为北京光华荣昌汽车部件有限公司提供生产、供应链、财务、物流、仓库管理等业务流程的信息化服务，助力企业高效、快速、低运营成本的开展业务。

“ERP 系统”采用 C/S 架构部署，使用 HTTP 协议 80 端口进行数据传输，重要数据每天凌晨 2 点进行全量备份。

北京光华荣昌汽车部件有限公司已制定各方面管理制度对“ERP 系统”进行管理，管理制度已覆盖网络、主机、系统、数据、应用层面。

2.1.3 网络结构

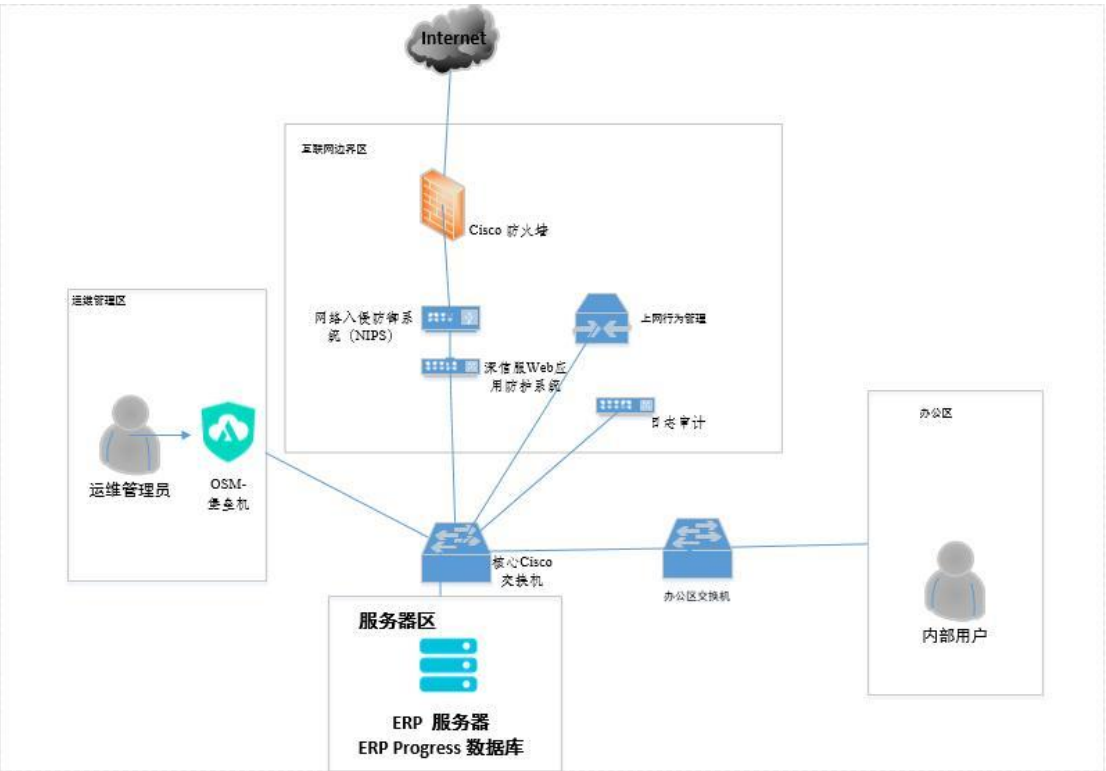

图 2-1 网络结构拓扑图

“ERP 系统”网络拓扑图如图 2.1 所示，“ERP 系统”的网络结构主要包括：互联网边界区、办公区、服务器区、运维管理区。

（1） 互联网边界区

互联网边界区部署了一台 Cisco 5510 防火墙、网络入侵防御系统（NIPS）、深信服 Web 应用防护系统、深信服上网行为管理进行安全防护。

（2） 办公区

通过办公区交换机连接对内部服务进行数据交换。

（3） 服务器区

服务器区通过一台 Redhat Linux 6.9 ERP 服务器装载 Progress3.11 数据库，用于承载业务系统。

（4） 运维管理区

运维管理区前部署了堡垒机，运维人员在北京光华荣昌公司办公楼内通过堡垒机进行运维管理。堡垒机主要用于所有设备的集中运维管理，全程记录用户的操作行为。

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
	恶意代码和垃圾邮件防范	1

[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
	安全审计	3
	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
	沟通和合作	3
	审核和检查	1
安全管理人员	人员录用	2
	人员离岗	1
	安全意识教育和培训	1
	外部人员访问管理	3

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

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			被测系统不涉及密码产品，故此项调整为不适用。
	自行软件开发		被测系统为外包开发，故此项调整为不适用。
			被测系统为外包开发，故此项调整为不适用。
	等级测评		被测系统为首次测评，故此项调整为不适用。
			被测系统未发生重大变更或级别发生变化，故此项调整为不适用。
安全运维管理	密码管理		被测系统不涉及密码产品，故此项调整为不适用。

安全类	控制点	不适用项	不适用原因
		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。	被测系统不涉及密码产品，故此项调整为不适用。
			被测系统目前未发生过网络安全事件，故此项调整为不适用。
	外包运维管理		被测系统为自行运维，故此项调整为不适用。
			被测系统为自行运维，故此项调整为不适用。
不适用指标数			10

2.3 测评对象

2.3.1 测评对象选择方法

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

（1）主机房（包括其环境、设备和设施等）和灾备机房；

（2）存储被测系统重要数据的介质的存放环境；

（3）整个系统的网络拓扑结构；

（4）安全设备，包括防火墙等；

（5）边界网络设备，包括路由器、楼层交换机等；

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

（7）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）；

（8）管理终端和主要应用系统终端；

（9）能够完成系统不同业务使命的业务应用系统；

（10）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；

（11）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安全设备、边界网络设备、网络互联设备、服务器、终端以及备份设备，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	核心机房	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	虚拟设备	系统及版本	品牌及型号	用途	重要程度
1	核心 Cisco 交换机	否	IOS Version12.2	Cisco 3750	业务核心交换	关键

2.3.2.3 安全设备

表 2-8 安全设备

序号	设备名称	虚拟设备	系统及版本	品牌及型号	用途	重要程度
1	Cisco 防火墙	否	IOS Version8.2	Cisco 5510	应用防护、地址划分、边界隔离	关键
2	OSM-堡垒机	否	深信服运维安全管理系统软件 V3.0	深信服 OSM-1000-B1150	功能描述：深信服运维安全管理系统（堡垒机 OSM），将运维人员离散维护主机及网络设备的行为统一到该平台进行	关键
3	网络入侵防御系统 (NIPS)	否	深信服网络入侵防御系统软件 V8.0	深信服 NIPS-1000-B1400	入侵防御、恶意代码防护、漏洞检测和修复、安全基线检查	关键
4	深信服 Web 应用防护系统	否	深信服 Web 应用防护系统软件 V8.0	深信服 WAF-1000-B1200	数据传输安全	关键
5	日志审计	否	深信服日志审计分析管理系统软件 V3.0	深信服 SIP-Logger-A600	服务器运维管理与审计	关键

2.3.2.4 服务器/存储设备

表 2-9 服务器/存储设备

序号	设备名称	所属业务应用系统/平台	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	ERP 服务器	ERP 系统	否	Redhat Linux 6.9	Progress 数据库 3.11	-	关键

2.3.2.5 终端设备

表 2-10 终端设备

序号	设备名称	虚拟设备	操作系统及版本	用途	重要程度
本测评不涉及终端设备					

2.3.2.6 其他设备

表 2-11 其他设备

序号	设备名称	虚拟设备	系统及版本	设备类别/用途	重要程度
本测评不涉及其他设备					

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	虚拟化管理平台	虚拟化管理平台	7.0.3.00300	-	关键
2	ERP Progress 数据库	应用数据库	3.11	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	ERP 系统	该系统主要为北京光华荣昌汽车部件有限公司提供供应链、生产、财务、物流仓库管理系统	V1.0	上海快意信息科技有限公司	关键

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	ERP 系统	保密性、完整性	关键
2	重要业务数据	ERP 系统	保密性、完整性	关键
3	主要配置数据	ERP 系统	保密性、完整性	关键
4	重要个人信息	ERP 系统	保密性、完整性	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	王金良	IT 经理/系统管理员	18610116864	北京光华荣昌汽车部件有限公司
2	庞军伟	IT 管理员/安全管理员	18511780371	北京光华荣昌汽车部件有限公司
3	何高胜	信息总监/审计管理员	18518709008	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	《信息安全岗位职责要求 V1.1》	规定了系统管理员、安全管理员、审计管理员方面的职责要求内容。

序号	文档名称	主要内容
2	《信息安全管理机构 V1.0》	规定了领导层与信息安全部门相关人员内容。
3	《信息安全管理组织职责 V1.0》	规定了领导层与信息安全部门管理职责的内容。
4	《信息系统安全审核和安全检查管理制度》	规定了安全管理员和安全审计员方面的职责要求内容。
5	《安全域划分规范 V1.0》	规定了安全域划分原则方面的内容。
6	《防火墙策略配置规范 V1.0》	规定了防火墙策略配置的内容。
7	《入侵检测系统策略配置规范 V1.0》	规定了入侵防御系统策略配置的内容。
8	《终端安全管理制度 V1.1》	规定了终端计算机总体要求、操作系统核心配置、浏览器核心配置、邮件系统核心配置要求的内容。
9	《关键岗位安全协议 V1.0》	规定了对关键岗位人员安全职责要求的内容。
10	《人员安全管理制度 V1.1》	规定了人员安全教育和培训等方面的管理制度内容。
11	《外部人员访问管理制度 V1.1》	规定了外边人员访问申请的制度内容。
12	《安全方案设计管理制度 V1.1》	对定了安全方案设计过程中职责分工、安全规划、方案设计阶段的内容。
13	《信息安全服务商选择管理办法 V1.1》	规定了信息安全服务商选择要求的内容。
14	《北京光华荣昌汽车部件有限公司办公环境安全管理制度》	规定了办公环境安全管理方面的管理制度内容。
15	《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》	规定了安全事件的报告、处置、响应流程、事件报告和后期恢复方面的管理制度内容。
16	《变更管理制度 V1.0》	规定了系统变更申报、审批、制度变更方案等方面的管理制度内容。
17	《北京光华荣昌汽车部件有限公司变更管理办法》	规定了对信息系统变更要求及变更流程方面的内容。

序号	文档名称	主要内容
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》	规定了防恶意代码（病毒）规范的内容。
19	《北京光华荣昌汽车部件有限公司介质安全管理制度》	规定了介质存储、使用管理方面的管理制度内容。
20	《北京光华荣昌汽车部件有限公司软件开发流程管理制度》	规定了系统软件开发流程要求及规定内容。
21	《北京光华荣昌汽车部件有限公司授权审批管理制度》	规定了授权审批方面的管理要求内容。
22	《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》	规定了数据备份方式、备份频度、存储介质等方面的管理制度内容。
23	《北京光华荣昌汽车部件有限公司网络安全应急预案管理办法》	规定了对公司网络安全应急预案的检测预警、处置原则、应急处置及后期处理的内容。
24	《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》	规定了对公司内部信息网络安全检查的内容。
25	《北京光华荣昌汽车部件有限公司应急预案管理制度》	规定了应急预案框架等相关内容。
26	《机房管理制度》	规定了机房安全方面的管理要求内容。
27	《密码使用管理制度 V1.1》	规定了商用密码产品及信息系统密码的使用管理的内容。
28	《数据恢复应急预案》	规定了对信息系统安全的日常维护及数据恢复应急计划的内容。
29	《数据恢复应急预案演练记录》	规定了对数据恢复应急预案演练记录的内容。
30	《运行维护和监控管理规定 V1.1》	规定了系统在运行和监控方面的要求内容。
31	《资产安全管理制度 V1.1》	规定了资产责任、资产标识、资产使用、资产传输、资产维护、资产报废与处置管理的内容。

序号	文档名称	主要内容
32	《版本控制》	规定了公司发布重要文件的版本、发布日期、发布部门、编写人、更新说明等内容。
33	《信息安全策略总纲V1.1》	规定了机构网络安全工作的总体目标、范围、原则和安全策略等内容。
34	《系统安全管理规定》	规定了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等内容。
35	《制度审批记录》	记录了制度基本信息、制度审核项目、制度审批记录等内容。
36	《信息系统授权审批记录表》	记录了针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程等内容。
37	《会议记录》	记录了各部门之间沟通与协调等内容。
38	《外部合作单位联系表》	记录了包括外联单位名称、合作内容、联系人和联系方式等内容。
39	《安全检查报告及安全检查表》	记录了系统日常运行情况、系统漏洞和数据备份等内容。
40	《安全培训记录表》	记录了对各类人员进行安全意识教育和岗位技能培训等内容。
41	《授权申请表》	记录了外部人员访问申请并批准接入网络的记录等内容。
42	《第三方访问申请表》	记录了外部人员逻辑访问受控区域的登记的记录等内容。
43	《专家评审意见》	记录了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等内容。
44	《培训记录表》	记录了对负责运行维护的技术人员进行相应的技能培训等内容。
45	《人员登记表》	记录了对物理机房进出人员的记录等内容。
46	《机房设备管理记录表》	记录了对物理机房设备进出的记录等内容。
47	《存储介质管理登记表》	记录了对介质的存储和查询的记录等内容。
48	《操作日志》	记录了包括日常巡检工作、运行维护记录、参数的设置和修改等内容。
49	《应急预案培训记录》	记录了定期对系统相关的人员进行应急预案培训等内容。
50	《应急预案演练记录》	记录了定期对系统相关的人员进行应急预案的演练等内容。

序号	文档名称	主要内容
51	《GR-41 采购管理业务程序》	记录了公司内部采购的管理流程和供应商选择规范等内容。
52	《外来人员登记表》	记录了外来人员进出公司的登记记录，包括：来访人员、事由、接待人、来访时间等内容。
53	《设施维护巡检记录》	记录了公司机房的设备日常维护检查的记录等内容。
54	《运行维护和监控管理制度》	记录了公司日常对设备运行维护和集中监控管理的制度等内容。

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

在安全物理环境方面采取了以下安全措施：

物理位置选择：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，所在的大楼具有防震、防风和防雨等能力；

物理访问控制：机房出入口配置电子门禁系统，外来人员访问机房需要提前提交访问人员的信息并提出申请，审核通过后方可进入；

防盗窃和防破坏：机房内重要设备均固定在机柜上，通信线缆铺设在线槽内；

防雷击：机房内各设备均已接地处理，并部署有防雷保护装置；

防火：机房内采用具有耐火等级的建筑材料；

防水和防潮：机房窗户已封闭，墙壁无渗水痕迹，地板下筑有防水坝可防止积水的转移与渗透；

防静电：机房采用防静电地板，工作人员配备有静电手环，可防止静电的产生；

温湿度控制：机房已部署专用的精密空调，能够自动调节温湿度；

电力供应：机房已部署过压保护装置可对主电路电压起到稳压作用，已部署 UPS，UPS 能够在机房断电情况下为设备提供短期电力供应；

电磁防护：机房电源线和通信线缆隔离铺设在不同的线槽内，可避免互相干扰。

3.1.2 主要安全问题汇总分析

安全物理环境存在的安全问题有：

（1）未采取措施防止地下积水的转移和渗透

未采取有效措施防止水蒸气结露，未采取措施防范地下积水的渗透，涉及测评对象**核心机房**。

3.2 安全通信网络

3.2.1 已有安全控制措施汇总分析

在安全通信网络方面采取了以下安全措施：

网络架构：被测系统业务处理能力和带宽可满足高峰期需求，服务器和数据库具有冗余措施；重要业务区未部署在边界处，通过防火墙对所在网络划分互联网边界区、办公区、服务器区、运维管理区等不同网络区域，各区域按照需求分配了各自网段的 IP 地址。

3.2.2 主要安全问题汇总分析

安全通信网络存在的安全问题有：

（1）未采用密码技术保证通信过程中数据的完整性

未采用密码技术保证通信过程中数据的完整性，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引导程序等进行可信验证

未基于可信根对通信设备的引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，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

在安全区域边界方面采取了以下安全措施：

边界防护：被测系统防火墙仅开启了业务需要的端口，配置严格的访问控制策略，限制了内外部用户连接行为；

访问控制：被测系统通过防火墙仅配置了业务需要的访问控制策略，默认均为除非允许否则拒绝所有通信，访问控制策略已优化，不存在相互冲突、包含的情况；

入侵防范和恶意代码防范：被测系统部署了 Web 应用防护系统、网络入侵防御系统（NIPS）、Cisco 防火墙等，在网络关键节点检测和限制内外部发起的网络攻击行为和恶意代码，并开启了平台报警功能；

安全审计：被测系统部署的服务器、网络设备和安全设备审计记录上传至日志审计系统中，保存 180 天，可避免受到未预期的删除、修改或覆盖等。

3.3.2 主要安全问题汇总分析

安全区域边界存在的安全问题有：

（1）未基于可信根对边界设备的系统引导程序等进行可信验证

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，涉及测评对象**内网边界**。

3.4 安全计算环境

3.4.1 网络设备

3.4.1.1 已有安全控制措施汇总分析

在网络设备方面采取了以下安全措施：

身份鉴别：网络设备在用户登录时均采用了用户名/口令的身份鉴别措施；

访问控制：网络设备各用户角色已按最小权限进行权限划分，网络设备不存在多余和过期的账户，不存在多人使用同一账户管理的情况；已重命名默认账户或删除默认账户，已修改默认账户的默认口令；

安全审计：网络设备均开启了审计功能，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，审计日志备份在日志审计设备中，备份策略满足 180 天要求；

入侵防范：通过限制网络地址范围对终端进行接入限制；

数据备份恢复：网络设备已实现数据备份和恢复功能，每次修改配置后由系统管理员进行备份，备份数据保存在管理员电脑上，定期对备份数据进行恢复测试。

3.4.1.2 主要安全问题汇总分析

安全计算环境存在的安全问题有：

（1）网络中未采用加密协议进行远程管理

网络设备开启了 Telnet 服务，口令以明文方式传输，存在网络传输过程中被窃取的风险，涉及测评对象**核心 Cisco 交换机**。

（2）有关设备、系统未配置登录失败处理功能

有关设备、系统未配置登录失败处理功能，未限制登录次数等控制机制，涉及测评对象**核心 Cisco 交换机**。

（3）未定期修补漏洞

未定期修补漏洞，涉及测评对象**核心 Cisco 交换机**。

（4）未采用密码技术进行通信完整性验证

未采用密码技术保证通信过程中数据的完整性，涉及测评对象**核心 Cisco 交换机**。

（5）未将重要数据定时批量传送至异地备份场地

未将重要数据定时批量传送至异地备份场地，涉及测评对象**核心 Cisco 交换机**。

（6）未对身份鉴别信息复杂度进行检查，未强制要求定期更换口令

未对身份鉴别信息复杂度进行检查，未强制要求定期更换口令，涉及测评对象**核心 Cisco 交换机**。

（7）未基于可信根对计算设备的引导程序等进行可信验证

未基于可信根对计算设备的引导程序、系统程序、重要配置参数和应用程序等进行可信验证，涉及测评对象**核心 Cisco 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

在安全设备方面采取了以下安全措施：

身份鉴别：安全设备在用户登录时均采用了用户名/口令的身份鉴别措施，部分安全设备采用 HTTPS 协议进行远程管理，防止鉴别信息在网络传输过程中被窃听；部分安全设备已启用登录失败及超时自动退出功能；

访问控制：安全设备各用户角色已按最小权限进行权限划分，不存在多余和过期的账户，不存在多人使用同一账户管理的情况；已重命名默认账户或删除默认账户，已修改默认账户的默认口令；

安全审计：安全设备启用了安全审计功能，审计覆盖到每个用户，可以对重要用户行为和重要安全事件进行审计，审计日志备份在深信服日志审计系统，备份策略满足 180 天要求；

入侵防范：通过限制网络地址范围对终端进行接入限制，管理员已对 OSM-堡垒机、网络入侵防御系统(NIPS)、深信服 Web 应用防护系统、日志审计进行漏洞扫描，发现漏洞经过评估后进行修补，目前无高危漏洞；

数据完整性：部分安全设备采用 HTTPS 协议通信，保证重要数据在传输过程中的完整性；

数据备份恢复：安全设备已实现数据备份和恢复功能，每次修改配置后由系统管理员进行备份，备份数据保存在管理员电脑上，定期对备份数据进行恢复测试。

3.4.2.2 主要安全问题汇总分析

安全计算环境存在的安全问题有：

（1）网络中未采用加密协议进行远程管理

安全设备开启了 Telnet 服务，口令以明文方式传输，存在网络传输过程中被窃取的风险，涉及测评对象 **Cisco 防火墙**。

（2）有关设备、系统未配置登录失败处理功能

有关设备、系统未配置登录失败处理功能，未限制登录次数等控制机制，涉及测评对象 **Cisco 防火墙**。

（3）未定期修补漏洞

未定期修补漏洞，涉及测评对象 **Cisco 防火墙，OSM-堡垒机，网络入侵防御系统(NIPS)，深信服 Web 应用防护系统，日志审计**。

（4）未采用密码技术进行通信完整性验证

未采用密码技术保证通信过程中数据的完整性，涉及测评对象 **Cisco 防火墙**。

（5）未将重要数据定时批量传送至异地备份场地

未将重要数据定时批量传送至异地备份场地，涉及测评对象 **Cisco 防火墙，OSM-堡垒机，网络入侵防御系统(NIPS)，深信服 Web 应用防护系统，日志审计**。

（6）未对身份鉴别信息复杂度进行检查，未强制要求定期更换口令

未对身份鉴别信息复杂度进行检查，未强制要求定期更换口令，涉及测评对象 **Cisco 防火墙**。

（7）未基于可信根对计算设备的引导程序等进行可信验证

未基于可信根对计算设备的引导程序、系统程序、重要配置参数和应用程序等进行可信验证，涉及测评对象 **Cisco 防火墙，OSM-堡垒机，网络入侵防御系统(NIPS)，深信服 Web 应用防护系统，日志审计**。

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

在服务器方面采取了以下安全措施:

身份鉴别：服务器在用户登录时均采用了用户名/口令的身份鉴别措施;

访问控制：服务器各用户角色已按最小权限进行权限划分，服务器不存在多余和过期的账户，不存在多人使用同一账户管理的情况；

安全审计：服务器均启用了安全审计功能，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，审计日志备份在深信服日志审计系统，备份策略满足 180 天要求；

入侵防范：服务器均遵循最小安装原则，无多余组件和程序，均关闭了非必要的系统服务和默认共享；网络入侵防御系统（NIPS）可对服务器入侵行为进行检测；

数据备份恢复：服务器已采用快照功能进行备份，可通过快照进行恢复，服务器采用虚拟化方式部署；

剩余信息保护：服务器的鉴别信息和敏感数据所在存储空间在被释放或重新分配前已得到完全清除；运维终端已启用“交互式登录：不显示最后的用户名”。

3.4.3.2 主要安全问题汇总分析

安全计算环境存在的安全问题有：

（1）网络中未采用加密协议进行远程管理

操作系统开启了 Telnet 服务，口令以明文方式传输，存在网络传输过程中被窃取的风险，涉及测评对象 **ERP 服务器**。

（2）未定期修补漏洞

未定期修补漏洞，涉及测评对象 **ERP 服务器**。

（3）未安装恶意代码防护软件，未采取主动免疫可信验证机制防范恶意代码

未安装恶意代码防护软件，未采取主动免疫可信验证机制防范恶意代码，涉及测评对象 **ERP 服务器**。

（4）未采用密码技术进行通信完整性验证

未采用密码技术保证通信过程中数据的完整性，涉及测评对象 **ERP 服务器**。

（5）未将重要数据定时批量传送至异地备份场地

未将重要数据定时批量传送至异地备份场地，涉及测评对象 **ERP 服务器**。

（6）未授予不同账户为完成各自承担任务所需的最小权限

系统存在超级管理员用户，且未按照三权分立原则进行权限分离，未授予不同账户为完成各自承担任务所需的最小权限，它们之间未形成相互制约的关系，涉及测评对象 **ERP 服务器**。

（7）未基于可信根对计算设备的引导程序等进行可信验证

未基于可信根对计算设备的引导程序、系统程序、重要配置参数和应用程序等进行可信验证，涉及测评对象 **ERP 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

在系统管理软件方面采取了以下安全措施：

数据库

身份鉴别：Progress 数据库通过用户名/口令方式对登录用户进行身份鉴别，具有身份标识唯一性检查功能，无空口令用户，Progress 数据库已关闭远程管理功能；

访问控制：Progress 数据库默认账户口令已修改，对登录的用户分配了管理员用户和业务用户。不存在多余、过期的账户；

入侵防范：Progress 数据库仅允许通过 OSM-堡垒机登录进行访问；OSM-堡垒机已限制终端 IP 登录地址，仅允许公司内网地址进行访问；

数据完整性 ：Progress 数据库采用 SSH 通信方式进行远程管理，保证重要数据传输过程中的完整性；

数据备份恢复：Progress 数据库每天 9 点进行增量备份到本地；

剩余信息保护：Progress 数据库关闭后及时清除用户鉴别信息，及时释放文件、目录和数据等使用的存储空间；

个人信息保护：Progress 数据库通过管理制度限制用户对个人信息的访问，未被授权的用户不可访问用户个人信息。

虚拟化管理平台

身份鉴别：虚拟化管理平台通过用户名/口令方式对登录用户进行身份鉴别，具有身份标识唯一性检查功能，无空口令用户，已启用口令复杂度配置并定期更换口令，已配置登录失败处理功能，虚拟化管理平台采用加密的 HTTPS 协议进行远程管理，防止鉴别信息在网络传输过程中被窃听；

访问控制：虚拟化管理平台默认账户口令已修改，对登录的用户分配了管理员用户和业务用户的最小权限。不存在多余、过期的账户；

安全审计：虚拟化管理平台已启用安全审计功能，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，审计日志备份在深信服日志审计系统，备份策略满足 180 天要求；

入侵防范：虚拟化管理平台已遵循最小安装的原则，仅安装需要的组件和应用程序；已关闭不需要的系统服务；虚拟化管理平台具备数据有效性检验功能，体现在限制文件类型、字符段大小；

数据完整性：虚拟化管理平台采用 HTTPS 协议进行数据传输，能够保证数据在传输过程中的完整性；

数据备份恢复：虚拟化管理平台每年手动进行全量备份；

剩余信息保护：虚拟化管理平台关闭后及时清除用户鉴别信息，及时释放文件、目录和数据等使用的存储空间，具体措施为退出时清空用户名、口令状态；

个人信息保护：虚拟化管理平台采取系统用户权限策略限制用户对个人信息的访问，未被授权的用户不可访问用户个人信息。

3.4.4.2 主要安全问题汇总分析

安全计算环境存在的安全问题有：

（1）有关设备、系统未配置登录失败处理功能

有关设备、系统未配置登录失败处理功能，未限制登录次数等控制机制，涉及测评对象**虚拟化管理平台，ERP Progress 数据库**。

（2）数据库日志审计功能不完善

数据库日志审计功能不完善，未开启安全事件的审计，涉及测评对象 **ERP Progress 数据库**。

（3）未对管理终端的接入方式或网络地址进行限制

未限制管理终端的接入方式或网络地址，涉及测评对象**虚拟化管理平台**。

（4）未定期修补漏洞

未定期修补漏洞，涉及测评对象**虚拟化管理平台**。

（5）未采用密码技术进行通信完整性验证

未采用密码技术保证通信过程中数据的完整性，涉及测评对象 **ERP Progress 数据库**。

（6）未将重要数据定时批量传送至异地备份场地

未将重要数据定时批量传送至异地备份场地，涉及测评对象**虚拟化管理平台，ERP Progress 数据库**。

（7）未提供重要数据的备份恢复测试记录

未提供重要数据的备份恢复测试记录，涉及测评对象**虚拟化管理平台，ERP Progress 数据库**。

（8）未授予不同账户为完成各自承担任务所需的最小权限

系统存在超级管理员用户，且未按照三权分立原则进行权限分离，未授予不同账户为完成各自承担任务所需的最小权限，它们之间未形成相互制约的关系，涉及测评对象 **ERP Progress 数据库**。

（9）安全审计功能不完善

未对系统后台所有重要操作事件进行日志记录，涉及测评对象 **ERP Progress 数据库**。

（10）未对审计记录进行备份

未对审计记录进行备份，涉及测评对象 **ERP Progress 数据库**。

（11）未对身份鉴别信息复杂度进行检查，未强制要求定期更换口令

未对身份鉴别信息复杂度进行检查，未强制要求定期更换口令，涉及测评对象 **ERP Progress 数据库**。

（12）未根据不同的管理角色授予不同的权限

未划分用户角色，权限分配存在权责不一致的情况，涉及测评对象 **ERP Progress 数据库**。

（13）未重命名系统默认账户

系统已修改了账户的默认口令，但未重命名系统默认账户，涉及测评对象 **ERP Progress 数据库**。

（14）未基于可信根对计算设备的引导程序等进行可信验证

未基于可信根对计算设备的引导程序、系统程序、重要配置参数和应用程序等进行可信验证，涉及测评对象**虚拟化管理平台，ERP Progress 数据库**。

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

在应用系统方面采取了以下安全措施：

身份鉴别：应用系统通过用户名/口令的鉴别方式对用户进行身份鉴别，已配置口令复杂度策略，已配置登录失败处理功能以及登录连接超时自动退出功能；

访问控制：应用系统根据角色划分不同的权限，分为系统管理员、安全管理员、审计管理员、业务管理员等，为不同业务需求和管理需求的用户分配不同角色，应用系统无默认账户，所有账户均未使用默认口令，无多余、过期或共享账户，应用系统管理用户仅授予最小化权限，实现管理用户权限分离；

安全审计：应用系统具有操作日志、人员日志等，可对重要用户行为和重要事件进行审计，审计覆盖所有用户，审计字段包括：用户、时间、事件内容和事件状态等信息；

入侵防范：应用系统具备数据有效性检验功能，通过人机接口或通信接口输入无效数据时应用系统拒绝无效数据；数据有效性检验功能体现在设定了数据格式、大小等要求；

数据备份恢复：应用系统数据每天全量备份至数据库，保存时间 7 天，恢复功能有效可用；

剩余信息保护：应用系统具有完善的剩余信息清除功能，在关闭浏览器或退出系统时会及时清除 Cookie 信息，应用系统产生的临时文件、缓存文件中不存在敏感数据；

个人信息保护：应用系统仅采集和保存业务必需的用户个人信息（手机号），已设定未授权无法访问个人信息。

3.4.5.2 主要安全问题汇总分析

安全计算环境存在的安全问题有：

（1）网络中未采用加密协议进行远程管理

操作系统开启了 Telnet 服务，口令以明文方式传输，存在网络传输过程中被窃取的风险，涉及测评对象 **ERP 系统**。

（2）未定期修补漏洞

未定期修补漏洞，涉及测评对象 **ERP 系统**。

（3）未采用密码技术进行通信完整性验证

未采用密码技术保证通信过程中数据的完整性，涉及测评对象 **ERP 系统**。

（4）未将重要数据定时批量传送至异地备份场地

未将重要数据定时批量传送至异地备份场地，涉及测评对象 **ERP 系统**。

（5）未提供重要数据的备份恢复测试记录

未提供重要数据的备份恢复测试记录，涉及测评对象 **ERP 系统**。

（6）未对身份鉴别信息复杂度进行检查，未强制要求定期更换口令

未对身份鉴别信息复杂度进行检查，未强制要求定期更换口令，涉及测评对象 **ERP 系统**。

（7）未基于可信根对计算设备的引导程序等进行可信验证

未基于可信根对计算设备的引导程序、系统程序、重要配置参数和应用程序等进行可信验证，涉及测评对象 **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

在数据资源方面采取了以下安全措施：

数据备份恢复：应用系统数据每天全量备份至数据库，保存时间 7 天，恢复功能有效可用；

剩余信息保护：应用系统具有完善的剩余信息清除功能，在关闭浏览器或退出系统时会及时清除 Cookie 信息，应用系统产生的临时文件、缓存文件中不存在敏感数据；

个人信息保护：应用系统仅采集和保存业务必需的用户个人信息（手机号），已设定未授权无法访问个人信息。

3.4.6.2 主要安全问题汇总分析

安全计算环境存在的安全问题有：

（1）未采用密码技术进行通信完整性验证

未采用密码技术保证通信过程中数据的完整性，涉及测评对象**鉴别数据，重要业务数据，主要配置数据，重要个人信息**。

（2）未将重要数据定时批量传送至异地备份场地

未将重要数据定时批量传送至异地备份场地，涉及测评对象**鉴别数据，重要业务数据，主要配置数据，重要个人信息**。

（3）未提供重要数据的备份恢复测试记录

未提供重要数据的备份恢复测试记录，涉及测评对象**鉴别数据，重要业务数据，主要配置数据，重要个人信息**。

3.4.7 其他系统或设备

3.4.7.1 已有安全控制措施汇总分析

无。

3.4.7.2 主要安全问题汇总分析

无。

3.5 安全管理中心

3.5.1 已有安全控制措施汇总分析

在安全管理中心方面采取了以下安全措施：

系统管理、审计管理：管理员通过堡垒机对服务器进行远程管理，堡垒机采用用户名/口令的登录方式对系统管理员、审计管理员和安全管理员进行身份鉴别，系统管理员、审计管理员和安全管理员分配各自工作所需的权限。

3.5.2 主要安全问题汇总分析

无。

3.6 安全管理制度

3.6.1 已有安全控制措施汇总分析

在安全管理制度方面采取了以下安全措施：

安全策略：北京光华荣昌汽车部件有限公司制定了信息安全工作的总体方针和安全策略《信息安全策略总纲 V1.1》，阐明了网络安全的总体目标、范围、原则和安全框架等；

管理制度：北京光华荣昌汽车部件有限公司已制定《变更管理制度 V1.0》、《北京光华荣昌汽车部件有限公司介质安全管理制度》、《信息安全管理机构 V1.0》、《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》、《信息安全管理组织职责 V1.0》、《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》、《资产安全管理制度 V1.1》等管理制度，安全管理制度覆盖网络安全、主机安全、系统安全、数据安全、应用安全等方面的内容；

制定和发布：授权集团信息管理部制定、修订管理制度。管理制度版本标识清晰，已通过正规、有效方式发布；

评审和修订：北京光华荣昌汽车部件有限公司规定每年对管理制度至少进行一次评审，由集团信息管理部根据实际情况进行评审和修订。

3.6.2 主要安全问题汇总分析

安全管理制度存在的安全问题有：

（1）缺乏部分管理操作规程

未对日常管理操作建立操作规程或缺失部分日常管理操作规程，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

在安全管理机构方面采取了以下安全措施：

岗位设置：被测单位授权集团信息管理部为网络安全管理工作的职能部门，目前已设立系统管理员、审计管理员、安全管理员等岗位，并定义了其相应的职责；

人员配备：被测单位集团信息管理部目前配备了专职的安全管理员、系统管理员、审计管理员；

授权和审批：被测单位根据各个部门职责的不同，明确了授权审批事项、审批部门和批准人，并对系统变更、重要操作、物理访问和系统接入建立审批程序；

沟通和合作：集团信息管理部积极与网络安全职能部门、各类供应商、业界专家及安全组织进行沟通与合作，已建立《外联单位联系表》，内容包含合作单位、合作范围、联系人姓名、办公电话、手机等信息；

审核和检查：被测单位集团信息管理部定期对信息系统进行常规的安全检查和全面安全检查，形成检查报告，并对检查结果进行通报。

3.7.2 主要安全问题汇总分析

无。

3.8 安全管理人员

3.8.1 已有安全控制措施汇总分析

在安全管理人员方面采取了以下安全措施：

人员录用：人力资源部负责被测单位的人员录用工作，《人员安全管理制度V1.1》明确要求对录用人的身份、背景、专业资格和资质等进行审查；

人员离岗：《人员安全管理制度 V1.1》明确人员离岗前应归还所持有的信息资产，包括笔记本、门禁卡、钥匙、证件、所有工作资料；同时要及时终止该员工的所有访问权限，撤销该员工的账号；

安全意识教育和培训：《人员安全管理制度 V1.1》明确集团信息管理部负责员工的信息安全教育和培训工作，并规定岗位安全责任以及惩戒措施；

外部人员访问管理：《外部人员访问管理制度V1.1》明确外部人员访问受控区域应由部门领导批准后，授予临时权限并由专人陪同，并登记备案。

3.8.2 主要安全问题汇总分析

安全管理人员存在的安全问题有：

（1）被录用人员的审查记录缺失

被录用人员的审查记录缺失，涉及测评对象**安全管理人员**。

（2）离职人员交接记录缺失

离职人员交接记录缺失，涉及测评对象**安全管理人员**。

（3）外部人员离场后的访问权限清除记录缺失

外部人员离场后的访问权限清除记录缺失，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

在安全建设管理方面采取了以下安全措施：

定级和备案：被测单位已制定定级报告以及备案表，说明保护对象的安全保护等级及确定等级的方法和理由；组织专家评审会对定级结果进行论证和审定，并形成评审意见；备案材料已报公安机关进行备案，取得备案证明；

安全方案设计：被测单位已购买防火墙、堡垒机、日志审计、IPS 等安全设备，并根据安全需求配置安全策略；已制定《安全方案设计管理制度》对保护对象的安全保护等级进行安全方案设计；

产品采购和使用：被测单位按照国家有关规定进行安全产品的采购和使用，要求各类安全产品应具有销售许可证书，在产品采购前需对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单；

工程实施：被测单位已提供工程实施方案，指定集团信息管理部负责工程实施过程的管理；

系统交付：系统开发人员已对负责运行维护的技术人员进行相应的技能培训；

等级测评：被测单位委托北京时代新威信息技术有限公司进行网络安全等级保护测评，发现不符合相应等级保护标准要求的安全问题已及时整改，测评机构符合国家有关要求，系统目前未发生过重大变更；

服务供应商选择：被测单位选择的安全服务商为深信服，服务供应商的选择符合国家的有关规定。

3.9.2 主要安全问题汇总分析

安全建设管理存在的安全问题有：

（1）系统上线前，未对系统进行安全性测试

系统上线前，未对系统进行安全性测试验收，涉及测评对象**安全建设管理**。

（2）安全整体规划及其配套文件未经过充分论证

未组织相关部门和技术专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，无论证和审定记录，涉及测评对象**安全建设管理**。

（3）未提供软件设计文档和使用指南

未提供软件设计文档和使用指南，涉及测评对象**安全建设管理**。

（4）未编制工程实施方案

未编制详细的工程实施方案，未对项目实施过程、进度控制、工程质量等方面进行有效管控，涉及测评对象**安全建设管理**。

（5）未制定测试验收方案，未依据测试验收方案实施测试验收

未制定测试验收方案，未依据测试验收方案实施测试验收，涉及测评对象**安全建设管理**。

（6）未制定交付清单

未制定交付清单，涉及测评对象**安全建设管理**。

（7）建设过程文档和运行维护文档存在缺失情况

建设过程文档和运行维护文档存在缺失情况，涉及测评对象**安全建设管理**。

（8）未对外包软件中可能存在的恶意代码进行检测

未对外包软件中可能存在的恶意代码进行检测，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

在安全运维管理方面采取了以下安全措施：

环境管理：被测单位对办公环境和机房环境的安全管理作出了规定，明确应在接待室或对外会议室内接待来访人员，桌面上禁止摆放包含敏感信息的纸质文件、移动介质等；

资产管理：被测单位已指定资产清单，资产清单内容包括：资产责任部门、重要程度和所处位置等；

介质管理：被测单位已制定《北京光华荣昌汽车部件有限公司介质安全管理制度》，对介质在物理传输过程中的人员选择、打包、交付等作出了规定，明确所有介质均需放置于安全的环境中，由安全管理员对存储环境进行管理，并根据存储介质清单定期盘点；

设备维护管理：被测单位指定集团信息管理部对设备、服务器、通信线路以及配套软硬件措施进行维护管理；

网络和系统安全管理：被测单位已制定《信息安全管理组织职责 V1.0》，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了规定；

恶意代码防范管理：被测单位规定集团信息管理部需定期对所有员工进行恶意代码防范意识的教育；

配置管理：被测单位已保存基本的配置信息，内容包括网络拓扑图、IP 地址、软件组件的版本和补丁信息等内容；

变更管理：被测单位已制定《北京光华荣昌汽车部件有限公司变更管理办法》;

备份与恢复管理：被测单位根据数据的重要性，对数据备份类型、方式、频率、存储介质、保存周期等作出了规定;

安全事件处置：被测单位已制定《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》，要求发现安全事件时需及时向安全管理部门报告所发现的安全弱点和可疑事件，明确了对造成系统中断和造成信息泄密等安全事件的响应流程，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;

应急预案管理：被测单位已制定《北京光华荣昌汽车部件有限公司应急预案管理制度》，包括应急处理流程、系统恢复流程等内容。定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。

3.10.2主要安全问题汇总分析

安全运维管理存在的安全问题有:

（1）未提供修复漏洞或消除隐患的操作记录

未提供修复漏洞或消除隐患的操作记录，涉及测评对象**安全运维管理**。

（2）外来计算机或存储设备接入系统前未进行恶意代码检查

未指定专人对外来计算机或存储设备进行恶意代码检测并保存检测记录，涉及测评对象**安全运维管理**。

（3）未指定专人负责恶意代码库的升级并进行记录

未指定专人对网络和主机进行恶意代码检测并保存检测记录，涉及测评对象**安全运维管理**。

（4）未指定专人负责恶意代码库的升级并进行分析

建议指定专人定期对网络和主机进行恶意代码检测、保存检测记录，并定期分析，涉及测评对象**安全运维管理**。

（5）未严格落实系统变更管理制度，不具有变更方案评审记录

未严格落实系统变更管理制度，不具有变更方案评审记录，涉及测评对象**安全运维管理**。

（6）未提供设备维护记录

未提供设备维护记录，涉及测评对象**安全运维管理**。

（7）不具有账户管理记录

不具有账户管理记录，涉及测评对象**安全运维管理**。

（8）未制定重要设备的配置和操作手册

未制定重要设备的配置和操作手册，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

无。

3.11.2主要安全问题汇总分析

无。

3.12 验证测试

3.12.1漏洞扫描

3.12.1.1 漏洞扫描结果统计

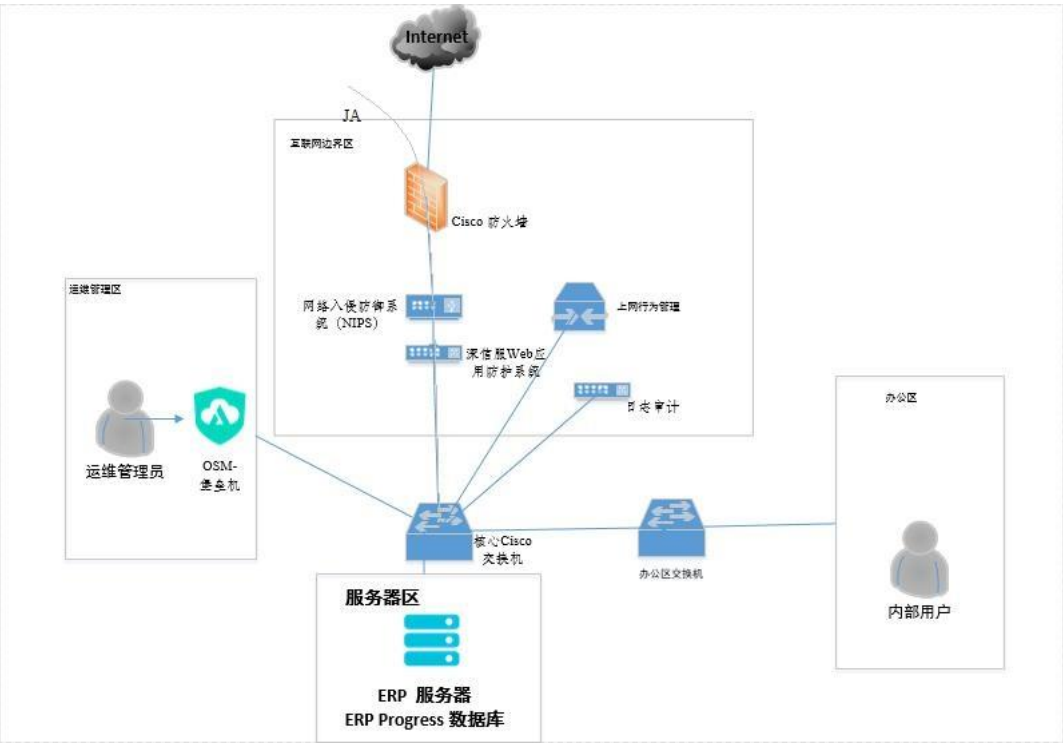

图 3.1 漏洞扫描工具接入测试示意图

对“ERP 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。

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：在办公区交换机接入，主要目的是，模拟内部恶意用户发现操作系统、数据库、Web 应用、第三方产品等安全漏洞的过程，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。

（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	ERP 服务器	Linux6.0、数据库	0	2	8	10
2	核心 Cisco 交换机	IOS Version12.2	0	0	2	2
3	Cisco 防火墙	IOS Version8.2	0	0	1	1
4	网络入侵防御系统(NIPS)	深信服网络入侵防御系统软件 V8.0	0	0	3	3
5	深信服 Web 应用防护系统	深信服 Web 应用防护系统软件 V8.0	0	0	3	3
6	日志审计	深信服日志审计分析管理系统软件 V3.0	0	0	4	4
7	OSM-堡垒机	深信服运维安全管理系统软件 V3.0	0	0	3	3

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，“ERP 系统”存在的主要安全漏洞汇总如下表所示。

表 3-2 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	OpenSSH 用户枚举漏洞(CVE-2018-15473)	ERP 服务器	中风险
2	SSH 服务支持弱加密算法	ERP 服务器	中风险
3	检测到目标 SSL 证书已过期	OSM-堡垒机	低风险
4	OpenSSH CBC 模式信息泄露漏洞(CVE-2008-5161)	ERP 服务器	低风险
5	ICMP timestamp 请求响应漏洞	深信服 Web 应用防护系统、网络入侵防御系统(NIPS)、日志审计、OSM-堡垒机	低风险

6	远端 Web 服务器上存在/robots.txt 文件	ERP 服务器	低风险
7	允许 Traceroute 探测	深信服 Web 应用防护系统、网络入侵防御系统(NIPS)、日志审计、OSM-堡垒机、核心 Cisco 交换机、Cisco 防火墙	低风险
8	检测到远端运行着 Telnet 服务	ERP 服务器	低风险
9	SSH 版本信息可被获取	ERP 服务器	低风险
10	探测到 SSH 服务器支持的算法	ERP 服务器	低风险
11	嵌入式 Web 服务器探测	ERP 服务器	低风险
12	探测到服务器支持的 SSL 加密协议	深信服 Web 应用防护系统、网络入侵防御系统(NIPS)、日志审计	低风险
13	可通过 HTTP 获取远端 WWW 服务信息	ERP 服务器、日志审计	低风险

3.12.2渗透测试

无。

3.13 单项测评小结

3.13.1控制点符合情况汇总

根据单项测评结果汇总控制点符合情况如下表所示。

表 3-3 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	不适用
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	√			

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	不适用
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			恶意代码和垃圾邮件防范	√			
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		安全管理中心	系统管理	√			
31			审计管理	√			
32		安全管理制度	安全策略	√			
33			管理制度		√		
34			制定和发布	√			
35			评审和修订	√			
36		安全管理机构	岗位设置	√			
37			人员配备	√			
38			授权和审批	√			
39			沟通和合作	√			
40			审核和检查	√			
41		安全管理人员	人员录用		√		
42			人员离岗		√		
43			安全意识教育和培训	√			

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	不适用
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				√
安全控制点符合情况数量统计				39	21	5	3

3.13.2安全问题汇总

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

表 3-4 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						
T01	未采取措施防止地下积水的转移和渗透。	核心机房	安全通用要求	安全物理环境	防水和防潮	b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。
T02	未采用密码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。
T03	未基于可信根对通信设备的引导程序等进行可信验证。	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。
T04	未基于可信根对边界设备的系统引导程序等进行可信验证。	内网边界		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。

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
T05	未对身份鉴别信息复杂度进行检查，未强制要求定期更换口令。	核心 Cisco 交换机、Cisco 防火墙、ERP 系统、ERP Progress 数据库		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；
T06	有关设备、系统未配置登录失败处理功能。	核心 Cisco 交换机、Cisco 防火墙、虚拟化管理平台、ERP Progress 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；
T07	使用 Telnet 等口令明文传输的服务。	核心 Cisco 交换机、Cisco 防火墙、ERP 系统、ERP 服务器				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。
T08	未根据不同的管理角色授予不同的权限。	ERP Progress 数据库			访问控制	a）应对登录的用户分配账户和权限；
T09	未重命名系统默认账户。	ERP Progress 数据库				b）应重命名或删除默认账户，修改默认账户的默认口令；
T10	未授予不同账户为完成各自承担任务所需的最小权限。	ERP 服务器、ERP Progress 数据库				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。
T11	数据库日志审计功能不完善。	ERP Progress 数据库			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；

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
T12	安全审计功能不完善。	ERP Progress 数据库				b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
T13	未对审计记录进行备份。	ERP Progress 数据库				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。
T14	未对管理终端的接入方式或网络地址进行限制。	虚拟化管理平台				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；
T15	未定期修补漏洞。	核心 Cisco 交换机、Cisco 防火墙、OSM-堡垒机、网络入侵防御系统(NIPS)、深信服 Web 应用防护系统、日志审计、ERP 系统、虚拟化管理平台、ERP 服务器			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。
T16	未安装恶意代码防护软件，未采取主动免疫可信验证机制防范恶意代码。	ERP 服务器			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。

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
T17	未基于可信根对计算设备的引导程序等进行可信验证	核心 Cisco 交换机、Cisco 防火墙、OSM-堡垒机、网络入侵防御系统(NIPS)、深信服 Web 应用防护系统、日志审计、ERP 系统、虚拟化管理平台、ERP 服务器、ERP Progress 数据库			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。
T18	未采用密码技术进行通信完整性验证。	核心 Cisco 交换机、Cisco 防火墙、ERP 系统、ERP 服务器、ERP Progress 数据库、鉴别数据、重要业务数据、主要配置数据、重要个人信息			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。

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
T19	未提供重要数据的备份恢复测试记录。	ERP 系统、虚拟化管理平台、ERP Progress 数据库、鉴别数据、重要业务数据、主要配置数据、重要个人信息				a）应提供重要数据的本地数据备份与恢复功能；
T20	未将重要数据定时批量传送至异地备份场地。	核心 Cisco 交换机、Cisco 防火墙、OSM-堡垒机、网络入侵防御系统(NIPS)、深信服 Web 应用防护系统、日志审计、ERP 系统、虚拟化管理平台、ERP 服务器、ERP Progress 数据库、鉴别数据、重要业务数据、主要配置数据、重要个人信息			数据备份恢复	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。

问题编号	安全问题	测评对象	通用/扩展	安全类	控制点	测评项
T21	缺乏部分管理操作规程。	安全管理制度		安全管理制度	管理制度	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。
T22	被录用人员的审查记录缺失。	安全管理人员		安全管理人员	人员录用	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。
T23	离职人员交接记录缺失。	安全管理人员			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。
T24	外部人员离场后的访问权限清除记录缺失。	安全管理人员			外部人员访问管理	c）外部人员离场后应及时清除其所有的访问权限。
T25	安全整体规划及其配套文件未经过充分论证。	安全建设管理		安全建设管理	安全方案设计	c）应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。
T26	未对外包软件中可能存在的恶意代码进行检测。	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；
T27	未提供软件设计文档和使用指南。	安全建设管理				b）应保证开发单位提供软件设计文档和使用指南。
T28	未编制工程实施方案。	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	未制定测试验收方案，未依据测试验收方案实施测试验收。	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	系统上线前，未对系统进行安全性测试。	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。

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
T31	未制定交付清单。	安全建设管理			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；
T32	建设过程文档和运行维护文档存在缺失情况。	安全建设管理				c）应提供建设过程文档和运行维护文档。
T33	未提供设备维护记录。	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	未提供修复漏洞或消除隐患的操作记录。	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	不具有账户管理记录。	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	未制定重要设备的配置和操作手册。	安全运维管理				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；
T37	外来计算机或存储设备接入系统前未进行恶意代码检查。	安全运维管理			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；
T38	未指定专人负责恶意代码库的升级并进行记录。	安全运维管理				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；

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
T39	未提供恶意代码防范措施特征库的更新、升级记录。	安全运维管理				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。
T40	未严格落实系统变更管理制度，不具有变更方案评审记录。	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。

安全计算环境层面

在安全计算环境层面，交换机、防火墙、数据库和应用系统未设置口令复杂度要求及定期更换策略，但通过发布管理制度规定口令需满足 8 位以上，由数字、字母、符号组成，并定期更换，且目前已存在账号均满足此要求。综上所述，此问题可酌情降低风险等级为中风险。

在安全计算环境层面，交换机、防火墙、服务器和应用系统未使用加密协议进行远程管理，不能防止通信过程中鉴别信息被窃听或破坏，虽然部分网络设备、安全设备、终端、 应用系统采用未加密的协议进行远程管理，但采用非加密协议传输设备均部署在网络内部，设备处于内网环境，不属于互联网、公共网络环境、开放性办公网络等缺少网络安全管控措施的网络环境，属于可控区域，能在一定程度上防止鉴别信息在传输过程中被窃听。综上所述，此问题可酌情降低风险等级为中风险。

在安全计算环境层面，虚拟化管理平台未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。但设备处于内网环境，不属于互联网、公共网络环境、开放性办公网络等缺少网络安全管控措施的网络环境。非不可控网络环境降低了通信过程中数据被窃听或破坏的风险。已对服务

器远程接入的终端或 IP 地址进行限定，限定对服务器的远程管理方式仅允许通过堡垒机登录。综上所述，此问题可酌情降低风险等级为中风险。

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。

经分析，光华荣昌“ERP 系统”区域间不存在功能增强、补充或削弱等关联项。

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				
T05	未对身份鉴别信息复杂度进行检查，未强制要求定期更换口令。	核心 Cisco 交换机、Cisco 防火墙、ERP 系统、ERP Progress 数据库	未设置口令复杂度要求及定期更换策略，但制度规定了口令需满足 8 位以上，由数字、字母、符号组成，且目前已存在账号均满足此要求。	☐升高 ☑降低
T07	网络中未采用加密协议进行远程管理。	核心 Cisco 交换机、Cisco 防火墙、ERP 系统、ERP 服务器	交换机、防火墙、服务器、应用系统未使用加密协议进行远程管理，不能防止通信过程中鉴别信息被窃听或破坏，虽然部分网络设备、安全设备、终端、 应用系统采用未加密的协议进行远程管理，但采用非加密协议传输设备均部署在网络内部，属于可控区域，能在一定程度上防止鉴别信息在传输过程中被窃听。	☐升高 ☑降低
T14	未对管理终端的接入方式或网络地址进行限制。	虚拟化管理平台	虚拟化管理平台未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。但设备处于内网环境，不属于互联网、公共网络环境、开放性办公网络等缺少网络安全管控措施的网络环境。非不可控网络环境降低了通信过程中数据被窃听或破坏的风险。已对服务器远程接入的终端或 IP 地址进行限定，限定对服务器的远程管理方式仅允许通过堡垒机登录。	☐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	问题编号	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	T01	安全物理环境	未采取措施防止地下积水的转移和渗透。	核心机房	物理环境影响	存在因湿度过高引起设备故障的风险。	中
2	T02	安全通信网络	未采用密码技术保证通信过程中数据的完整性。	安全通信网络	篡改	可能导致重要数据在传输过程中被攻击者劫持、篡改，使传输数据的完整性遭到破坏，可能影响到用户和企业的声誉和经济利益。	中

[3] 如风险值和评价相同，可填写多个关联资产。

序号	问题编号	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
3	T03		未基于可信根对通信设备的引导程序等进行可信验证。	安全通信网络	网络攻击	存在系统引导程序、系统程序、重要配置参数和应用程序在启动和运行中遭受中间人劫持导致重要安全参数被恶意篡改的风险，破坏设备完整性，影响系统安全性。	低
4	T04	安全区域边界	未基于可信根对边界设备的系统引导程序等进行可信验证。	内网边界	软硬件故障	存在系统引导程序、系统程序、重要配置参数和应用程序在启动和运行中遭受中间人劫持导致重要安全参数被恶意篡改的风险。	低
5	T05	安全计算环境	未对身份鉴别信息复杂度进行检查，未强制要求定期更换口令。	核心 Cisco 交换机、Cisco 防火墙、ERP 系统、ERP Progress 数据库	网络攻击	存在口令被恶意用户暴力破解的可能。	中
6	T06		有关设备、系统未配置登录失败处理功能。	核心 Cisco 交换机、Cisco 防火墙、虚拟化管理平台、ERP Progress 数据库	网络攻击	登录口令可能被恶意用户使用暴力猜解方式获得，合法用户身份被仿冒，导致系统被非授权访问。	中
7	T07		使用 Telnet 等口令明文传输的服务。	核心 Cisco 交换机、Cisco 防火墙、ERP 系统、ERP 服务器	泄密、网络攻击、越权或滥用	账号、口令等重要数据可能被嗅探并盗用，导致系统被非授权访问。	中

序号	问题编号	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
8	T08		未根据不同的管理角色授予不同的权限。	ERP Progress 数据库	无作为或操作失误,越权或滥用,抵赖	增大了系统在发生安全事件时无法及时有有效进行追溯的安全风险。	中
9	T09		未重命名系统默认账户。	ERP Progress 数据库	网络攻击、越权或滥用	口令被恶意用户猜测获得，合法用户身份被仿冒，导致数据库被非授权访问。	中
10	T10		未授予不同账户为完成各自承担任务所需的最小权限。	ERP 服务器、ERP Progress 数据库	越权或滥用	管理员权限过大，可能无法对管理员的行为进行监管、制约。	中
11	T11		数据库日志审计功能不完善。	ERP Progress 数据库	抵赖	无法对安全事件进行追溯，同时无法及时了解设备实际运行状况以及存在的安全隐患。	中
12	T12		安全审计功能不完善。	ERP Progress 数据库	抵赖	未对重要用户、重要事件进行日志记录，不便于安全事件的追溯，不利于系统日常的安全运维。	中
13	T13		未对审计记录进行备份。	ERP Progress 数据库	抵赖	可能会受到未预期的删除、修改或覆盖，或无法对安全事件进行追溯，存在一定的安全风险。	中
14	T14		未对管理终端的接入方式或网络地址进行限制。	虚拟化管理平台	越权或滥用,网络攻击	恶意用户可尝试对信息系统设备实施攻击或越权访问。给信息系统的正常运行带来风险。	中

序号	问题编号	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
15	T15		未定期修补漏洞。	核心 Cisco 交换机、Cisco 防火墙、OSM-堡垒机、网络入侵防御系统(NIPS)、深信服 Web 应用防护系统、日志审计、ERP 系统、虚拟化管理平台、ERP 服务器	管理不到位、网络攻击	可能存在未授权人员利用漏洞攻击信息系统的风险。	中
16	T16		未安装恶意代码防护软件，未采取主动免疫可信验证机制防范恶意代码。	ERP 服务器	管理不到位、恶意代码	可能导致信息系统被恶意代码感染，存在信息系统敏感信息泄露的风险。	中
17	T17		未基于可信根对计算设备的引导程序等进行可信验证	核心 Cisco 交换机、Cisco 防火墙、OSM-堡垒机、网络入侵防御系统(NIPS)、深信服 Web 应用防护系统、日志审计、ERP 系统、虚拟化管理平台、ERP 服务器、ERP Progress 数据库	物理环境影响	增大了系统引导程序、系统程序等不可信，导致设备在底层被恶意攻击，进而入侵破坏系统的安全风险。	低

序号	问题编号	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
18	T18		未采用密码技术进行通信完整性验证。	核心 Cisco 交换机、Cisco 防火墙、ERP 系统、ERP 服务器、ERP Progress 数据库、鉴别数据、重要业务数据、主要配置数据、重要个人信息	篡改	可能导致重要数据在传输过程中被攻击者劫持、篡改。	中
19	T19		未提供重要数据的备份恢复测试记录。	ERP 系统、虚拟化管理平台、ERP Progress 数据库、鉴别数据、重要业务数据、主要配置数据、重要个人信息	软硬件故障	系统如出现故障，可能无法及时恢复，或造成重要数据丢失。	中

序号	问题编号	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
20	T20		未将重要数据定时批量传送至异地备份场地。	核心 Cisco 交换机、Cisco 防火墙、OSM-堡垒机、网络入侵防御系统(NIPS)、深信服 Web 应用防护系统、日志审计、ERP 系统、虚拟化管理平台、ERP 服务器、ERP Progress 数据库、鉴别数据、重要业务数据、主要配置数据、重要个人信息	软硬件故障	如机房遭受严重破坏，可能导致数据完全丢失。	中
21	T21	安全管理制度	缺乏部分管理操作规程。	安全管理制度	管理不到位	操作规范缺乏，可能使相关操作过程缺乏规范依据和质量保障，进而影响到信息系统的安全运行。	低
22	T22	安全管理人员	被录用人员的审查记录缺失。	安全管理人员	管理不到位	可能存在人员专业资质、安全技能等方面欠缺等风险。	低
23	T23		离职人员交接记录缺失。	安全管理人员	管理不到位	可能导致离岗员工权限被非授权访问。	低
24	T24		外部人员离场后的访问权限清除记录缺失。	安全管理人员	管理不到位、泄密	可能导致外部人员有意或无意访问机构敏感区域或信息，造成泄密。	低

序号	问题编号	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
25	T25	安全建设管理	安全整体规划及其配套文件未经过充分论证。	安全建设管理	无作为或操作失误,管理不到位,网络攻击	存在安全规划不合理，进而导致系统因非授权操作受到破坏的安全风险。	中
26	T26		未对外包软件中可能存在的恶意代码进行检测。	安全建设管理	恶意代码	存在软件被植入恶意代码的风险。	低
27	T27		未提供软件设计文档和使用指南。	安全建设管理	管理不到位、无作为或操作失误或操作失误	未提供软件设计的相关文档和使用指南，可能存在由于操作不规范或技能不足对系统安全稳定运行带来的风险。	低
28	T28		未编制工程实施方案。	安全建设管理	管理不到位、无作为或操作失误	可能由于缺乏工程实施方案造成工程实施过程管理不到位。	低
29	T29		未制定测试验收方案，未依据测试验收方案实施测试验收。	安全建设管理	管理不到位、无作为或操作失误	可能由于未制定测试验收方案造成测试过程缺乏计划性及操作性，无法保证经过测试验收的系统达到既定的安全性等目标。	低
30	T30		系统上线前，未对系统进行安全性测试。	安全建设管理	管理不到位、无作为或操作失误	可能存在安全隐患在系统上线运行前未被发现的情况。	中
31	T31		未制定交付清单。	安全建设管理	管理不到位、无作为或操作失误	可能导致在系统交付工作中存在疏漏，交付物移交不全面，出现管理不到位。	低

序号	问题编号	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
32	T32		建设过程文档和运行维护文档存在缺失情况。	安全建设管理	无作为或操作失误,管理不到位	信息系统交付时缺少相关的运维手册和建设文档，可能存在由于操作不规范或技能不足对系统安全稳定运行带来的风险。	低
33	T33	安全运维管理	未提供设备维护记录。	安全运维管理	管理不到位	可能存在设备维修、报废管理不到位而造成设备故障或泄密的风险。	低
34	T34		未提供修复漏洞或消除隐患的操作记录。	安全运维管理	管理不到位、网络攻击	可能存在未授权人员利用漏洞攻击信息系统的风险。	中
35	T35		不具有账户管理记录。	安全运维管理	管理不到位	无法对保护对象进行统一监视和控制，当安全事件发生时无法及时对威胁源进行阻断和干预。	低
36	T36		未制定重要设备的配置和操作手册。	安全运维管理	网络攻击	存在系统如出现故障，可能无法及时恢复的风险。	低
37	T37		外来计算机或存储设备接入系统前未进行恶意代码检查。	安全运维管理	管理不到位,恶意代码	可能导致系统恶意代码检测管理不到位，存在信息系统感染恶意代码，从而导致信息泄露风险。	低
38	T38		未指定专人负责恶意代码库的升级并进行记录。	安全运维管理	管理不到位,恶意代码	可能导致系统恶意代码检测管理不到位，存在信息系统感染恶意代码，从而导致信息泄露风险。	低

序号	问题编号	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
39	T39		未提供恶意代码防范措施特征库的更新、升级记录。	安全运维管理	管理不到位,恶意代码	可能导致系统恶意代码检测管理不到位，存在信息系统感染恶意代码，从而导致信息泄露风险。	低
40	T40		未严格落实系统变更管理制度，不具有变更方案评审记录。	安全运维管理	管理不到位、越权或滥用	可能出现变更失败，并且在变更过程中对系统造成软硬件故障或数据丢失等风险。	低

6 等级测评结论

等级测评结论由安全问题风险分析结果和综合得分共同确定，判定依据如下表所示。

表 6-1 等级测评结论判定依据

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

综合得分计算方法如下:

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

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

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

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

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	
ERP 系统	0	20	20	71.21

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“ERP 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：

“ERP 系统”本次等级测评的综合得分为 **71.21** 且不存在高等级风险，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	问题编号	安全类	安全问题	关联资产	整改建议
安全通用要求					
1	T01	安全物理环境	未采取措施防止地下积水的转移和渗透。	核心机房	建议排查地下积水的转移与渗透情况，及时加强、完善相关防范措施；安装防结露设施，并对主机房和辅助区的温度、露点温度或相对湿度等环境参数加强监测和控制，当环境参数超出设定值时，应报警并及时处置。核心设备区及高密度设备区宜设置机柜微环境监控系统。
2	T02	安全通信网络	未采用密码技术保证通信过程中数据的完整性。	安全通信网络	建议采用国家密码管理主管部门认可的密码技术，保护通信过程中数据的完整性。
3	T03		未基于可信根对通信设备的引导程序等进行可信验证。	安全通信网络	建议采取可信验证机制对通信设备的引导程序、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。
4	T04	安全区域边界	未基于可信根对边界设备的系统引导程序等进行可信验证。	内网边界	建议采取可信验证机制对边界设备的引导程序、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。
5	T05	安全计算环境	未对身份鉴别信息复杂度进行检查，未强制要求定期更换口令。	核心 Cisco 交换机、Cisco 防火墙、ERP 系统、ERP Progress 数据库	建议设置口令复杂度策略和合理的口令更换周期，确保只有授权用户方可登录系统。

序号	问题编号	安全类	安全问题	关联资产	整改建议
6	T06		有关设备、系统未配置登录失败处理功能。	核心 Cisco 交换机、Cisco 防火墙、虚拟化管理平台、ERP Progress 数据库	建议合理配置非法登录次数、锁定时间和登录连接超时时间。
7	T07		使用 Telnet 等口令明文传输的服务。	核心 Cisco 交换机、Cisco 防火墙、ERP 系统、ERP 服务器	建议禁用口令明文传输的服务，如 Telnet 等。
8	T08		未根据不同的管理角色授予不同的权限。	ERP Progress 数据库	建议对所有用户按其职责划分不同的角色，按照权责一致原则授予权限。角色划分情况、授予权限情况应登记备案，或存档备查。
9	T09		未重命名系统默认账户。	ERP Progress 数据库	建议重命名系统默认账户。
10	T10		未授予不同账户为完成各自承担任务所需的最小权限。	ERP 服务器、ERP Progress 数据库	建议系统授予不同用户为完成各自承担的任务所需的最小权限，将系统管理员和业务操作员权限分离，并设置独立的安全审计员角色，对各类用户的操作行为进行审计监督。
11	T11		数据库日志审计功能不完善。	ERP Progress 数据库	建议配置数据库审核策略，对设备的配置管理操作行为、重要的业务操作等行为进行审计。
12	T12		安全审计功能不完善。	ERP Progress 数据库	建议为系统增加后台重要操作事件的日志记录功能。
13	T13		未对审计记录进行备份。	ERP Progress 数据库	建议为设备配置日志服务器，降低日志遭到非授权删除、修改或覆盖的风险。
14	T14		未对管理终端的接入方式或网络地址进行限制。	虚拟化管理平台	建议修改、完善相关设备或系统配置文件，对管理终端的接入方式和网络地址范围进行限制，如限定网络地址为管理终端 IP 地址等。

序号	问题编号	安全类	安全问题	关联资产	整改建议
15	T15		未定期修补漏洞。	核心 Cisco 交换机、Cisco 防火墙、OSM-堡垒机、网络入侵防御系统(NIPS)、深信服 Web 应用防护系统、日志审计、ERP 系统、虚拟化管理平台、ERP 服务器	建议安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装。
16	T16		未安装恶意代码防护软件，未采取主动免疫可信验证机制防范恶意代码。	ERP 服务器	建议安装防恶意代码软件，启动防恶意代码引擎，定期升级和更新防恶意代码库，对入侵和病毒行为进行有效阻断；或者安装具备可信验证机制的软件或系统，对系统程序、重要配置文件等进行可信验证，如完整性受到破坏则迅速恢复。
17	T17		未基于可信根对计算设备的引导程序等进行可信验证	核心 Cisco 交换机、Cisco 防火墙、OSM-堡垒机、网络入侵防御系统(NIPS)、深信服 Web 应用防护系统、日志审计、ERP 系统、虚拟化管理平台、ERP 服务器、ERP Progress 数据库	建议采取可信验证机制对计算设备的引导程序、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。

序号	问题编号	安全类	安全问题	关联资产	整改建议
18	T18		未采用密码技术进行通信完整性验证。	核心 Cisco 交换机、Cisco 防火墙、ERP 系统、ERP 服务器、ERP Progress 数据库、鉴别数据、重要业务数据、主要配置数据、重要个人信息	建议升级、完善相关系统，采用国家密码管理主管部门认可的校验技术或密码技术，对传输过程中的重要数据进行完整性保护。
19	T19		未提供重要数据的备份恢复测试记录。	ERP 系统、虚拟化管理平台、ERP Progress 数据库、鉴别数据、重要业务数据、主要配置数据、重要个人信息	建议检查相关系统的备份策略设置情况，按照总体安全策略要求，配置合理的备份策略，定期进行备份恢复测试并留存记录。
20	T20		未将重要数据定时批量传送至异地备份场地。	核心 Cisco 交换机、Cisco 防火墙、OSM-堡垒机、网络入侵防御系统(NIPS)、深信服 Web 应用防护系统、日志审计、ERP 系统、虚拟化管理平台、ERP 服务器、ERP Progress 数据库、鉴别数据、重要业务数据、主要配置数据、重要个人信息	建议利用通信网络将重要数据定时批量传送至异地备份场地，实现重要数据异地备份。
21	T21	安全管理制度	缺乏部分管理操作规程。	安全管理制度	建议补充、完善相关操作规程，为管理人员或操作人员提供完备的规范性参考文档。

序号	问题编号	安全类	安全问题	关联资产	整改建议
22	T22	安全管理人员	被录用人员的审查记录缺失。	安全管理人员	建议规范人员录用程序，明确审查和考核要求，客观、准确记录审查情况和技术技能考核情况，将有关文档纳入人力资源档案管理或存档备查。
23	T23		离职人员交接记录缺失。	安全管理人员	建议加强离岗人员的管理，严控离岗流程，详细记录访问权限的撤销以及证件、信息资产的交还情况，留存相关记录或归档备查。
24	T24		外部人员离场后的访问权限清除记录缺失。	安全管理人员	建议认真落实外部人员访问管理制度，严格管控外部人员访问权限的授予和注销（清除）。外部人员离场后，应及时注销所有权限并详细记录，注销（清除记录）应妥善保管或存档备查。
25	T25	安全建设管理	安全整体规划及其配套文件未经过充分论证。	安全建设管理	建议进一步完善安全整体规划及其配套文件，并组织相关部门和技术专家进行论证和审定，形成论证意见，批准后正式实施。
26	T26		未对外包软件中可能存在的恶意代码进行检测。	安全建设管理	建议在外包软件交付前，通过第三方检查工具或人工对软件中可能存在的恶意代码进行检测，形成检测报告。检测报告应报相关部门审定或存档备查。
27	T27		未提供软件设计文档和使用指南。	安全建设管理	建议要求开发单位编制并提供软件设计的相关文档和使用指南，并安排专人管理
28	T28		未编制工程实施方案。	安全建设管理	建议完善工程实施方面的管理制度，明确工程实施方案编制要求，以及对工程实施过程、进度控制、工程质量等方面进行管控的要求。

序号	问题编号	安全类	安全问题	关联资产	整改建议
29	T29		未制定测试验收方案，未依据测试验收方案实施测试验收。	安全建设管理	建议完善测试验收制度，明确验收前制定测试验收方案,确定参与测试验收的部门、人员、测试验收内容等事项；依据验收方案实施测试验收,记录测试验收过程，形成测试验收报告；测试验收报告报请相关部门审定等内容。
30	T30		系统上线前，未对系统进行安全性测试。	安全建设管理	建议完善验收管理制度，明确系统上线前的安全性测试要求。应委托第三方测试机构对系统进行安全性测试，取得相关部门或行业认可的测试报告。
31	T31		未制定交付清单。	安全建设管理	建议补充或重新制定系统交付清单，根据交付清单对所交接的设备、软件和文档等进行再次清点。
32	T32		建设过程文档和运行维护文档存在缺失情况。	安全建设管理	建议完善系统验收、交付等相关管理制度，明确建设过程文档和运行维护文档等编制、交付范围，确保交付质量得到有效控制、满足服务级别协议要求。
33	T33	安全运维管理	未提供设备维护记录。	安全运维管理	建议严格执行设备管理制度，按照设备管理制度对设备进行维护管理，并留存维护记录。
34	T34		未提供修复漏洞或消除隐患的操作记录。	安全运维管理	建议部署必要的技术措施，对发现、识别的安全漏洞和隐患及时评估、修补，确保系统安全并留存相应记录文件。
35	T35		不具有账户管理记录。	安全运维管理	建议指定专门的部门或人员进行账户管理，并对申请账户、建立账户、删除账户等相关内容进行审批并记录。

序号	问题编号	安全类	安全问题	关联资产	整改建议
36	T36		未制定重要设备的配置和操作手册。	安全运维管理	建议对重要设备如操作系统、数据库、网络设备、安全设备、应用和组件等建立配置和操作手册，应至少包括操作步骤、维护记录、配置参数、操作风险等内容。在日常运维中，依据手册对设备进行安全配置和优化配置。
37	T37		外来计算机或存储设备接入系统前未进行恶意代码检查。	安全运维管理	建议指定专人定期对外来计算机或存储设备进行恶意代码检测并保存检测记录。
38	T38		未指定专人负责恶意代码库的升级并进行记录。	安全运维管理	建议指定专人定期对网络和主机进行恶意代码检测并保存检测记录。
39	T39		未提供恶意代码防范措施特征库的更新、升级记录。	安全运维管理	建议指定专人定期对网络和主机进行恶意代码检测并保存特征库的更新、升级记录。
40	T40		未严格落实系统变更管理制度，不具有变更方案评审记录。	安全运维管理	建议加强运维管理，严格按照变更管理制度要求实施变更；变更需求、变更方案、评审记录及审批记录等应妥善保管或存档备查。

【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	核心机房	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	-

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 Cisco 交换机	否	IOS Version12.2	Cisco 3750	业务核心交换	关键	1
2	交换机	否	-	-	数据交换	一般	1

注：同类型设备在备注中填写设备数量，但确定为测评对象的设备必须单独列出，且设备名称应唯一。

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	Cisco 防火墙	否	IOS Version8.2	Cisco 5510	应用防护、地址划分、边界隔离	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
2	OSM-堡垒机	否	深信服运维安全管理系统软件 V3.0	深信服 OSM-1000-B1150	功能描述：深信服运维安全管理系统（堡垒机 OSM），将运维人员离散维护主机及网络设备的行为统一到该平台进行	关键	1
3	网络入侵防御系统 (NIPS)	否	深信服网络入侵防御系统软件 V8.0	深信服 NIPS-1000-B1400	入侵防御、恶意代码防护、漏洞检测和修复、安全基线检查	关键	1
4	深信服 Web 应用防护系统	否	深信服 Web 应用防护系统软件 V8.0	深信服 WAF-1000-B1200	数据传输安全	关键	1
5	日志审计	否	深信服日志审计分析管理系统软件 V3.0	深信服 SIP-Logger-A600	服务器运维管理与审计	关键	1
6	上网行为管理	否	深信服 AC11.0R2	深信服	对上网行为进行控制	一般	1

注：同类型设备在备注中填写设备数量，但确定为测评对象的设备必须单独列出，且设备名称应唯一。

A.4 服务器/存储设备

附录 A 表-4 服务器/存储设备

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	ERP 服务器	ERP 系统	是	Redhat Linux 6.9	Progress 数据库 3.11	-	关键	1

注：同类型设备在备注中填写设备数量，但确定为测评对象的设备必须单独列出，且设备名称应唯一。

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	否	Windows10	设备运维	一般	1

注：同类型设备在备注中填写设备数量，但确定为测评对象的设备必须单独列出，且设备名称应唯一。

A.6 其他系统或设备

附录 A 表-6 其他设备

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
本次测评不涉及其他设备						

注：同类型设备在备注中填写设备数量，但确定为测评对象的设备必须单独列出，且设备名称应唯一。

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	主要功能	版本	所在设备名称	重要程度	备注
1	虚拟化管理平台	虚拟化管理平台	7.0.3.00300	-	关键	-
2	ERP Progress 数据库	应用数据库	3.11	ERP 服务器	关键	-

注：同类型软件/平台在备注中填写设备数量，但确定为测评对象的设备必须单独列出。

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	ERP 系统	该系统主要为北京光华荣昌汽车部件有限公司提供供应链、生产、财务、物流仓库管理系统	V1.0	上海快意信息科技有限公司	关键	-

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	ERP 系统	保密性、完整性	关键
2	重要业务数据	ERP 系统	保密性、完整性	关键
3	主要配置数据	ERP 系统	保密性、完整性	关键
4	重要个人信息	ERP 系统	保密性、完整性	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
本次测评不涉及密码产品						

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	王金良	IT 经理/系统管理员	18610116864	北京光华荣昌汽车部件有限公司
2	庞军伟	IT 管理员/安全管理员	18511780371	北京光华荣昌汽车部件有限公司
3	何高胜	信息总监/审计管理员	18518709008	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	《信息安全岗位职责要求 V1.1》	规定了系统管理员、安全管理员、审计管理员方面的职责要求内容。
2	《信息安全管理机构 V1.0》	规定了领导层与信息安全部门相关人员内容。
3	《信息安全管理组织职责 V1.0》	规定了领导层与信息安全部门管理职责的内容。
4	《信息系统安全审核和安全检查管理制度》	规定了安全管理员和安全审计员方面的职责要求内容。
5	《安全域划分规范 V1.0》	规定了安全域划分原则方面的内容。
6	《防火墙策略配置规范 V1.0》	规定了防火墙策略配置的内容。
7	《入侵检测系统策略配置规范 V1.0》	规定了入侵防御系统策略配置的内容。
8	《终端安全管理制度 V1.1》	规定了终端计算机总体要求、操作系统核心配置、浏览器核心配置、邮件系统核心配置要求的内容。
9	《关键岗位安全协议 V1.0》	规定了对关键岗位人员安全职责要求的内容。
10	《人员安全管理制度 V1.1》	规定了人员安全教育和培训等方面的管理制度内容。
11	《外部人员访问管理制度 V1.1》	规定了外边人员访问申请的制度内容。
12	《安全方案设计管理制度 V1.1》	对定了安全方案设计过程中职责分工、安全规划、方案设计阶段的内容。
13	《信息安全服务商选择管理办法 V1.1》	规定了信息安全服务商选择要求的内容。
14	《北京光华荣昌汽车部件有限公司办公环境安全管理制度》	规定了办公环境安全管理方面的管理制度内容。
15	《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》	规定了安全事件的报告、处置、响应流程、事件报告和后期恢复方面的管理制度内容。
16	《变更管理制度 V1.0》	规定了系统变更申报、审批、制度变更方案等方面的管理制度内容。
17	《北京光华荣昌汽车部件有限公司变更管理办法》	规定了对信息系统变更要求及变更流程方面的内容。
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》	规定了防恶意代码（病毒）规范的内容。
19	《北京光华荣昌汽车部件有限公司介质安全管理制度》	规定了介质存储、使用管理方面的管理制度内容。

序号	文档名称	主要内容
20	《北京光华荣昌汽车部件有限公司软件开发流程管理制度》	规定了系统软件开发流程要求及规定内容。
21	《北京光华荣昌汽车部件有限公司授权审批管理制度》	规定了授权审批方面的管理要求内容。
22	《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》	规定了数据备份方式、备份频度、存储介质等方面的管理制度内容。
23	《北京光华荣昌汽车部件有限公司网络安全应急预案管理办法》	规定了对公司网络安全应急预案的检测预警、处置原则、应急处置及后期处理的内容。
24	《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》	规定了对公司内部信息网络安全检查的内容。
25	《北京光华荣昌汽车部件有限公司应急预案管理制度》	规定了应急预案框架等相关内容。
26	《机房管理制度》	规定了机房安全方面的管理要求内容。
27	《密码使用管理制度 V1.1》	规定了商用密码产品及信息系统密码的使用管理的内容。
28	《数据恢复应急预案》	规定了对信息系统安全的日常维护及数据恢复应急计划的内容。
29	《数据恢复应急预案演练记录》	规定了对数据恢复应急预案演练记录的内容。
30	《运行维护和监控管理规定 V1.1》	规定了系统在运行和监控方面的要求内容。
31	《资产安全管理制度 V1.1》	规定了资产责任、资产标识、资产使用、资产传输、资产维护、资产报废与处置管理的内容。
32	《版本控制》	规定了公司发布重要文件的版本、发布日期、发布部门、编写人、更新说明等内容。
33	《信息安全策略总纲 V1.1》	规定了机构网络安全工作的总体目标、范围、原则和安全策略等内容。
34	《系统安全管理规定》	规定了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等内容。
35	《制度审批记录》	记录了制度基本信息、制度审核项目、制度审批记录等内容。
36	《信息系统授权审批记录表》	记录了针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程等内容。
37	《会议记录》	记录了各部门之间沟通与协调等内容。
38	《外部合作单位联系表》	记录了包括外联单位名称、合作内容、联系人和联系方式等内容。

序号	文档名称	主要内容
39	《安全检查报告及安全检查表》	记录了系统日常运行情况、系统漏洞和数据备份等内容。
40	《安全培训记录表》	记录了对各类人员进行安全意识教育和岗位技能培训等内容。
41	《授权申请表》	记录了外部人员访问申请并批准接入网络的记录等内容。
42	《第三方访问申请表》	记录了外部人员逻辑访问受控区域的登记的记录等内容。
43	《专家评审意见》	记录了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等内容。
44	《培训记录表》	记录了对负责运行维护的技术人员进行相应的技能培训等内容。
45	《人员登记表》	记录了对物理机房进出人员的记录等内容。
46	《机房设备管理记录表》	记录了对物理机房设备进出的记录等内容。
47	《存储介质管理登记表》	记录了对介质的存储和查询的记录等内容。
48	《操作日志》	记录了包括日常巡检工作、运行维护记录、参数的设置和修改等内容。
49	《应急预案培训记录》	记录了定期对系统相关的人员进行应急预案培训等内容。
50	《应急预案演练记录》	记录了定期对系统相关的人员进行应急预案的演练等内容。
51	《GR-41 采购管理业务程序》	记录了公司内部采购的管理流程和供应商选择规范等内容。
52	《外来人员登记表》	记录了外来人员进出公司的登记记录，包括：来访人员、事由、接待人、来访时间等内容。
53	《设施维护巡检记录》	记录了公司机房的设备日常维护检查的记录等内容。
54	《运行维护和监控管理制度》	记录了公司日常对设备运行维护和集中监控管理的制度等内容。

附录B 上次测评问题整改情况说明

本次测评为北京光华荣昌汽车部件有限公司“ERP 系统”首次测评，不涉及上次测评问题整改。

附录C 单项测评结果汇总

C.1 安全物理环境

附录 C 表-1 安全物理环境单项测评结果汇总（安全通用要求）

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	核心机房	符合	2	1	2	1	2	1	1	1	2	1
		部分符合	0	0	0	0	0	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 个，符合项 14 个，部分符合项 1 个，不符合项 0 个，不适用项 0 个												

C.2 安全通信网络

附录 C 表-2 安全通信网络单项测评结果汇总（安全通用要求）

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 个，符合项 2 个，部分符合项 1 个，不符合项 1 个，不适用项 0 个					

C.3 安全区域边界

附录 C 表-3 安全区域边界单项测评结果汇总（安全通用要求）

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	恶意代码和垃圾邮件防范	安全审计	可信验证
1	内网边界	符合	1	4	1	1	3	0
		部分符合	0	0	0	0	0	0
		不符合	0	0	0	0	0	1
		不适用	0	0	0	0	0	0
总计测评项 11 个，符合项 10 个，部分符合项 0 个，不符合项 1 个，不适用项 0 个								

C.4 安全计算环境

C.4.1 网络设备

附录 C 表-4 网络设备单项测评结果汇总（安全通用要求）

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Cisco交换机	符合	0	4	3	1	-	0	0	1	-	-
		部分符合	1	0	0	1	-	0	0	0	-	-
		不符合	2	0	0	0	-	1	1	1	-	-
		不适用	0	0	0	3	-	0	0	0	-	-
总计测评项 19 个，符合项 9 个，部分符合项 2 个，不符合项 5 个，不适用项 3 个												

C.4.2 安全设备

附录 C 表-5 安全设备单项测评结果汇总（安全通用要求）

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	Cisco防火墙	符合	0	4	3	1	-	0	0	1	-	-
		部分符合	1	0	0	1	-	0	0	0	-	-
		不符合	2	0	0	0	-	1	1	1	-	-
		不适用	0	0	0	3	-	0	0	0	-	-
2	OSM-堡垒机	符合	3	4	3	1	-	0	1	1	-	-
		部分符合	0	0	0	1	-	0	0	0	-	-
		不符合	0	0	0	0	-	1	0	1	-	-
		不适用	0	0	0	3	-	0	0	0	-	-
3	网络入侵防御系统(NIPS)	符合	3	4	3	1	-	0	1	1	-	-
		部分符合	0	0	0	1	-	0	0	0	-	-
		不符合	0	0	0	0	-	1	0	1	-	-
		不适用	0	0	0	3	-	0	0	0	-	-
4	深信	符合	3	4	3	1	-	0	1	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
	服Web应用防护系统	部分符合	0	0	0	1	-	0	0	0	-	-
		不符合	0	0	0	0	-	1	0	1	-	-
		不适用	0	0	0	3	-	0	0	0	-	-
5	日志审计	符合	3	4	3	1	-	0	1	1	-	-
		部分符合	0	0	0	1	-	0	0	0	-	-
		不符合	0	0	0	0	-	1	0	1	-	-
		不适用	0	0	0	3	-	0	0	0	-	-
总计测评项 95 个，符合项 61 个，部分符合项 6 个，不符合项 13 个，不适用项 15 个												

C.4.3 服务器和终端

附录 C 表-6 服务器和终端单项测评结果汇总（安全通用要求）

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服务器	符合	2	3	3	3	0	0	0	1	1	-
		部分符合	1	0	0	1	0	0	1	0	0	-
		不符合	0	1	0	0	1	1	0	1	0	-
		不适用	0	0	0	1	0	0	0	0	0	-
总计测评项 21 个，符合项 13 个，部分符合项 3 个，不符合项 4 个，不适用项 1 个												

C.4.4 系统管理软件/平台

附录 C 表-7 系统管理软件/平台单项测评结果汇总（安全通用要求）

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	虚拟化管理平台	符合	2	4	3	3	-	0	1	0	1	2
		部分符合	1	0	0	0	-	0	0	1	0	0
		不符合	0	0	0	2	-	1	0	1	0	0
		不适	0	0	0	0	-	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
		用										
2	ERP Progress 数据库	符合	1	1	0	2	-	0	0	0	1	2
		部分符合	1	2	0	0	-	0	1	1	0	0
		不符合	1	1	3	0	-	1	0	1	0	0
		不适用	0	0	0	3	-	0	0	0	0	0
总计测评项 44 个，符合项 23 个，部分符合项 7 个，不符合项 11 个，不适用项 3 个												

C.4.5 业务应用系统/平台

附录 C 表-8 业务应用系统/平台单项测评结果汇总（安全通用要求）

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	1	-	0	0	1	0	0
		不符合	1	0	0	0	-	1	1	1	0	0
		不适用	0	0	0	3	-	0	0	0	0	0
总计测评项 22 个，符合项 12 个，部分符合项 3 个，不符合项 4 个，不适用项 3 个												

C.4.6 数据资源

附录 C 表-9 数据资源单项测评结果汇总（安全通用要求）

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	2
		部分符合	-	-	-	-	-	-	0	1	0	0
		不符合	-	-	-	-	-	-	1	1	0	0
		不适用	-	-	-	-	-	-	0	0	0	0
2	重要业务数据	符合	-	-	-	-	-	-	0	0	1	2
		部分符合	-	-	-	-	-	-	0	1	0	0
		不符	-	-	-	-	-	-	1	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
		合										
		不适用	-	-	-	-	-	-	0	0	0	0
3	主要配置数据	符合	-	-	-	-	-	-	0	0	1	2
		部分符合	-	-	-	-	-	-	1	1	0	0
		不符合	-	-	-	-	-	-	0	1	0	0
		不适用	-	-	-	-	-	-	0	0	0	0
4	重要个人信息	符合	-	-	-	-	-	-	0	0	1	2
		部分符合	-	-	-	-	-	-	0	1	0	0
		不符合	-	-	-	-	-	-	1	1	0	0
		不适用	-	-	-	-	-	-	0	0	0	0
总计测评项 24 个，符合项 12 个，部分符合项 5 个，不符合项 7 个，不适用项 0 个												

C.5 安全管理中心

附录 C 表-10 安全管理中心单项测评结果汇总（安全通用要求）

序号	测评对象	符合情况	安全通用要求	
			系统管理	审计管理
1	安全管理中心	符合	2	2
		部分符合	0	0
		不符合	0	0
		不适用	0	0
总计测评项 4 个，符合项 4 个，部分符合项 0 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-11 安全管理制度单项测评结果汇总（安全通用要求）

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	1	2	1
		部分符合	0	1	0	0
		不符合	0	0	0	0
		不适用	0	0	0	0
总计测评项 6 个，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-12 安全管理机构单项测评结果汇总（安全通用要求）

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	3	1
		部分符合	0	0	0	0	0
		不符合	0	0	0	0	0
		不适用	0	0	0	0	0
总计测评项 9 个，符合项 9 个，部分符合项 0 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-13 安全管理人员单项测评结果汇总（安全通用要求）

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	1	0	1	2
		部分符合	1	1	0	1
		不符合	0	0	0	0
		不适用	0	0	0	0
总计测评项 7 个，符合项 4 个，部分符合项 3 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-14 安全建设管理单项测评结果汇总（安全通用要求）

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	2	1	0	0	1	0	1	1	2
		部分符合	0	0	0	0	1	0	0	0	0	0
		不符合	0	1	0	0	1	1	2	2	0	0
		不适用	0	0	1	2	0	0	0	0	2	0
总计测评项 25 个，符合项 12 个，部分符合项 1 个，不符合项 7 个，不适用项 5 个												

C.10安全运维管理

附录 C 表-15 安全运维管理单项测评结果汇总（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	3	0	1	0	0	3	2	2	0
		部分符合	0	0	0	1	1	2	3	0	0	1	0	0	0	0
		不符合	0	0	0	0	0	0	0	0	0	0	0	0	0	0
		不适用	0	0	0	0	0	0	0	0	2	0	0	1	0	2
总计测评项 31 个，符合项 18 个，部分符合项 8 个，不符合项 0 个，不适用项 5 个																

C.11其他安全要求指标

无。

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 核心机房

安全控制点	测评指标	结果记录	符合程度
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。	经访谈系统管理员，核查物理机房，机房不在建筑物顶层或地下。	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。	符合

安全控制点	测评指标	结果记录	符合程度
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、自动报警但未开启自动灭火功能。具有自动灭火功能，但是为防止误报，设置成手动灭火。	符合
	b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。	经访谈系统管理员，核查物理机房，机房采用耐火的建筑材料，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。	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

安全控制点	测评指标	结果记录	符合程度
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。	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

安全控制点	测评指标	结果记录	符合程度
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；	经访谈系统管理员，核查拓扑图、防火墙， 1）网络拓扑与实际运行环境一致； 2）网络划分了不同的安全区域，具体区域和 VLAN 划分：互联网边界区、办公区、服务器区、运维管理区。	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。	经访谈系统管理员，核查拓扑图、防火墙， 1）网络拓扑与实际运行环境一致； 2）重要的网络区域未部署在边界处； 3）网络区域间采取了技术隔离手段； 4）网络边界和区域间采取的技术隔离措施为：VLAN 隔离。	符合

安全控制点	测评指标	结果记录	符合程度
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。	经访谈系统管理员，核查网络设备、安全设备、服务器、应用，测试网络设备、安全设备、服务器、应用， 1）数据通信过程中，采用的完整性校验技术是：部分安全设备使用 HTTPS 协议进行传输；服务器使用 SSH/Telnet 协议进行传输；防火墙使用 Telnet 协议传输；应用使用 80 端口进行传输； 2）经现场测试验证，部分设备采用的完整性校验措施是真实有效。	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。	经访谈系统管理员，核查设备，未通过技术手段对通信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。	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 内网边界

安全控制点	测评指标	结果记录	符合程度
边界防护	a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	经访谈系统管理员，核查防火墙，测试 ACL 策略， 1）网络中有明确的网络边界设备，已明确边界设备端口； 2）网络路由信息与实际的端口配置匹配，端口及路由匹配信息如下：限制通过 50、130、111、102 端口进行访问； 3）通过网管系统及无线嗅探器未发现非授权网络出口。	符合
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	经访谈系统管理员，核查防火墙， 1）网络边界或区域之间已部署访问控制设备，已启用访问控制策略； 2）访问控制设备已采用白名单机制，仅允许授权的访问行为通过； 3）访问控制策略已在实际应用的端口启用，起到了安全防护作用。	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；	经访谈系统管理员，核查防火墙， 1）访问控制需求已与访问控制策略保持一致； 2）访问控制策略优先级配置合理； 3）访问控制策略中已禁止全通策略或授权范围过大的策略； 4）访问控制策略已进行合理的优化，无相互重复、包含的策略。	符合

安全控制点	测评指标	结果记录	符合程度
	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；	经访谈系统管理员，核查防火墙，关键节点的访问控制设备已配置了严格的访问控制策略，严格限制策略的源地址、目的地址、源端口、目的端口和协议。	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。	经访谈系统管理员，核查防火墙，网络中关键节点处防火墙设备为状态检测防火墙，能够根据会话状态信息为进出数据流提供明确的允许或拒绝访问的能力。	符合
入侵防范	a）应在关键网络节点处监视网络攻击行为。	经访谈系统管理员，核查入侵防御系统， 1）当检测到攻击行为时，设备记录了网络攻击行为，如目标服务器、攻击类型、攻击次数、攻击来源等信息； 2）在发生严重入侵事件时，采用系统通知方式进行告警。	符合
恶意代码和垃圾邮件防范	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。	经访谈系统管理员，核查入侵防御系统， 1）在关键网络节点处部署入侵防御系统，具备恶意代码防护功能； 2）恶意代码库更新时间：2022 年 5 月，设备设置了自动更新。	符合

安全控制点	测评指标	结果记录	符合程度
安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经访谈审计管理员，核查入侵防御系统、堡垒机、日志审计， 1）网络边界处部署了入侵防御系统、日志审计，已启用相关设备上的日志审计功能； 2）审计范围：网络中的关键网络设备、关键安全设备、关键主机设备（包括操作系统、数据库等），重要用户行为和重要安全事件； 3）审计内容：网络流量审计、网络安全事件审计和入侵防御系统对异常数据的分析等。	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；	经访谈审计管理员，核查日志审计，审计记录包含时间、源 IP、描述、用户名、操作信息。	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。	经访谈审计管理员，核查日志留存记录，测试日志审计， 1）部署审计系统对审计记录进行保护； 2）对审计记录进行定期备份，备份机制是：保存 180 天。	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。	经访谈系统管理员，核查设备，未通过技术手段对通信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。	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 Cisco 交换机

安全控制点	测评指标	结果记录	符合程度
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；	经访谈系统管理员，核查交换机， 1）设备使用用户名/口令鉴别机制对登录用户进行身份标识和鉴别； 2）用户身份标识具有唯一性； 3）设备不具有口令复杂度策略； 4）未限制口令长度，未启用由数字、大小写字母和特殊字符中的两种以上组成的口令策略，未启用定期更改口令的策略； 5）采用管理制度限制使用具有数字、大小写字母和特殊字符的复杂度口令、口令最小长度 8 位，每 90 天进行定期更换。	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；	经访谈管理员，核查交换机， 1）设备未启用登录失败处理功能。 2）设备未启用远程登录连接超时并自动退出功能。	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。	经访谈系统管理员，核查交换机， 1）设备开启了远程管理。 2）网络中未采用加密协议对设备进行数据传输，无法防止鉴别信息在网络中被窃听。	不符合

安全控制点	测评指标	结果记录	符合程度
访问控制	a）应对登录的用户分配账户和权限；	经访谈系统管理员，核查交换机，设备已对登录的用户分配账户和权限，禁用或限制匿名、默认账户的访问权限。	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；	经访谈系统管理员，核查交换机， 1）设备已重命名默认账户或删除默认账户； 2）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；	经访谈系统管理员，核查交换机，设备的用户列表不存在多余或过期账户、共享用户。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	经访谈系统管理员，核查交换机， 1）设备的系统用户已进行角色划分； 2）系统中的账户分为管理员、审计员、安全员三类，管理用户的权限进行了分离，并为其工作任务所需的最小权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经访谈审计管理员，核查交换机， 1）设备已开启审计功能； 2）设备的审计范围已覆盖到每个用户； 3）设备已对重要的用户行为和重要安全事件进行审计。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经访谈审计管理员，核查交换机，设备的日志信息中包含用户名、主机 IP、操作对象、操作、日期时间等与审计相关的信息。	符合

安全控制点	测评指标	结果记录	符合程度
	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。	经访谈审计管理员，核查交换机， 1）设备已对审计记录进行备份。具体方式导出到硬盘，日志保存时间不少于 180 天； 2）设备采用权限控制措施防止审计记录受到未预期的删除、修改和覆盖。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	非网络设备测评项，故此项调整为不适用。	不适用
	b）应关闭不需要的系统服务、默认共享和高危端口；	非网络设备测评项，故此项调整为不适用。	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；	经访谈系统管理员，核查交换机， 1）设备已对终端接入范围进行限制； 2）具体限制措施为设定允许访问网络地址范围； 3）终端接入方式为仅允许通过堡垒机登录。	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；	非网络设备测评项，故此项调整为不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经访谈系统管理员，核查交换机，测试漏洞扫描， 1）设备已进行定期漏洞扫描，具体周期为两年一次； 2）管理员未定期修补漏洞； 3）经现场漏洞扫描设备不存在高风险漏洞。	部分符合

安全控制点	测评指标	结果记录	符合程度
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。	经访谈系统管理员，核查设备，未通过技术手段对通信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。	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。	经访谈系统管理员，核查交换机，被测设备未采用加密协议进行数据传输，无法保证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；	经访谈系统管理员，核查交换机， 1）设备已提供数据的本地备份与恢复功能； 2）设备的备份与恢复方式为：设备每次修改配置后由管理员进行备份，数据备份保存在管理员电脑上，定期对备份数据进行恢复测试。	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。	经访谈系统管理员，核查交换机，设备未提供异地数据备份功能。	不符合

D.4.1.2 安全设备

D.4.1.2.1 Cisco 防火墙

安全控制点	测评指标	结果记录	符合程度
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；	经访谈系统管理员，核查防火墙， 1）设备使用用户名/口令鉴别机制对登录用户进行身份标识和鉴别； 2）用户身份标识具有唯一性； 3）设备不具有口令复杂度策略； 4）口令长度 5 位以上，未启用由数字、大小写字母和特殊字符中的两种以上组成的口令策略，未启用定期更改口令的策略； 5）采用管理制度限制使用具有数字、大小写字母和特殊字符的复杂度口令、口令最小长度 8 位，每 90 天进行定期更换。	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；	经访谈系统管理员，核查防火墙， 1）设备未启用登录失败处理功能； 2）设备未启用远程登录连接超时并自动退出功能。	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。	经访谈系统管理员，核查防火墙，网络中未采用加密协议对设备进行数据传输，无法防止鉴别信息在网络中被窃听。	不符合
访问控制	a）应对登录的用户分配账户和权限；	经访谈系统管理员，核查防火墙，设备已对登录的用户分配账户和权限，禁用或限制匿名、默认账户的访问权限。	符合

安全控制点	测评指标	结果记录	符合程度
	b）应重命名或删除默认账户，修改默认账户的默认口令；	经访谈系统管理员，核查防火墙， 1）设备已重命名默认账户或删除默认账户； 2）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；	经访谈系统管理员，核查防火墙，设备的用户列表不存在多余或过期账户、共享用户。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	经访谈系统管理员，核查防火墙， 1）设备的系统用户已进行角色划分； 2）系统中的账户分为管理员、审计员、安全员三类，管理用户的权限进行了分离，并为其工作任务所需的最小权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经访谈审计管理员，核查防火墙， 1）设备已开启审计功能； 2）设备的审计范围已覆盖到每个用户； 3）设备已对重要的用户行为和重要安全事件进行审计。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经访谈审计管理员，核查防火墙，设备的日志信息中包含用户名、主机 IP、操作对象、操作、日期时间等与审计相关的信息。	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。	经访谈审计管理员，核查防火墙， 1）设备已对审计记录进行备份。具体方式导出到硬盘，日志保存时间不少于 180 天； 2）设备采用权限控制措施防止审计记录受到未预期的删除、修改和覆盖。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	非安全设备测评项，故此项调整为不适用。	不适用

安全控制点	测评指标	结果记录	符合程度
	b）应关闭不需要的系统服务、默认共享和高危端口；	非安全设备测评项，故此项调整为不适用。	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；	经访谈系统管理员，核查设备登录方式， 1）设备已对终端接入范围进行限制； 2）具体限制措施为设定允许访问网络地址范围； 3）终端接入方式为仅允许通过堡垒机登录。	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；	非安全设备测评项，故此项调整为不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经访谈系统管理员，核查防火墙，测试漏洞扫描， 1）设备已进行定期漏洞扫描，具体周期为两年一次； 2）管理员未定期修补漏洞； 3）经现场漏洞扫描设备不存在高风险漏洞。	部分符合
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。	经访谈系统管理员，核查设备，未通过技术手段对通信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。	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。	经访谈系统管理员，核查防火墙，设备采用 Telnet 进行数据传输，不能够保证数据在传输过程中的完整性。	不符合

安全控制点	测评指标	结果记录	符合程度
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；	经访谈系统管理员，核查防火墙， 1）设备已提供数据的本地备份与恢复功能； 2）设备的备份与恢复方式为设备每次修改配置后由管理员进行备份，数据备份保存在管理员电脑上，定期对备份数据进行恢复测试。	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。	经访谈系统管理员，核查防火墙，设备未提供异地数据备份功能。	不符合

D.4.1.2.2 OSM-堡垒机

安全控制点	测评指标	结果记录	符合程度
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；	经访谈系统管理员，核查堡垒机， 1）设备使用用户名/口令鉴别机制对登录用户进行身份标识和鉴别； 2）用户身份标识具有唯一性； 3）设备具有口令复杂度策略； 4）口令长度 10 位以上，启用由数字、大小写字母和特殊字符中的两种以上组成的口令策略，启用定期更改口令的策略，更改周期为 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；	经访谈系统管理员，核查堡垒机， 1）设备已启用登录失败处理功能，方式为结束会话和限制登录次数； 2）登录失败 5 次，锁定用户 10 分钟； 3）设备已启用远程登录连接超时并自动退出功能，时间为 5 分钟。	符合

安全控制点	测评指标	结果记录	符合程度
	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。	经访谈系统管理员，核查堡垒机， 1）设备开启了远程管理； 2）网络中采用 HTTPS 协议对设备进行数据传输，防止鉴别信息在网络中被窃听。	符合
访问控制	a）应对登录的用户分配账户和权限；	经访谈系统管理员，核查堡垒机，设备已对登录的用户分配账户和权限，禁用或限制匿名、默认账户的访问权限。	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；	经访谈系统管理员，核查堡垒机， 1）设备已重命名默认账户或删除默认账户； 2）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；	经访谈系统管理员，核查堡垒机，设备的用户列表不存在多余或过期账户、共享用户。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	经访谈系统管理员，核查堡垒机， 1）设备的系统用户已进行角色划分； 2）系统中的账户分为系统管理员、安全管理员和审计管理员三类，管理用户的权限进行了分离，并为其工作任务所需的最小权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经访谈审计管理员，核查堡垒机， 1）设备已开启审计功能； 2）设备的审计范围已覆盖到每个用户； 3）设备已对重要的用户行为和重要安全事件进行审计。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经访谈审计管理员，核查堡垒机，设备的日志信息中包含起始时间、结束时间、登录地址、目标地址、用户名称等与审计相关的信息。	符合

安全控制点	测评指标	结果记录	符合程度
	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。	经访谈审计管理员，核查堡垒机， 1）设备已对审计记录进行备份。具体方式为转发至日志审计，日志保存时间不少于180 天； 2）设备采用权限控制措施防止审计记录受到未预期的删除、修改和覆盖。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	非安全设备测评项，故此项调整为不适用。	不适用
	b）应关闭不需要的系统服务、默认共享和高危端口；	非安全设备测评项，故此项调整为不适用。	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；	经访谈系统管理员，核查堡垒机， 1）设备已对终端接入范围进行限制； 2）具体限制措施为设定允许访问网络地址范围。	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；	非安全设备测评项，故此项调整为不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经访谈系统管理员，核查交堡垒机，测试漏洞扫描， 1）设备已进行定期漏洞扫描，具体周期为两年一次； 2）管理员未定期修补漏洞； 3）经现场漏洞扫描设备不存在高风险漏洞。	部分符合
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。	经访谈系统管理员，核查设备，未通过技术手段对通信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。	不符合

安全控制点	测评指标	结果记录	符合程度
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。	经访谈系统管理员，核查堡垒机，设备采用 HTTPS 协议进行数据传输，能够保证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；	经访谈系统管理员，核查堡垒机， 1）设备已提供数据的本地数据备份与恢复功能； 2）设备的备份与恢复方式为如设备每次修改配置后由管理员进行备份，数据备份保存在管理员电脑上，定期对备份数据进行恢复测试。	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。	经访谈系统管理员，核查堡垒机，设备未提供异地数据备份功能。	不符合

D.4.1.2.3 网络入侵防御系统(NIPS)

安全控制点	测评指标	结果记录	符合程度
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；	经访谈系统管理员，核查入侵防御系统， 1）设备使用用户名/口令鉴别机制对登录用户进行身份标识和鉴别； 2）用户身份标识具有唯一性； 3）设备具有口令复杂度策略； 4）口令长度 8 位以上，启用由数字、大小写字母和特殊字符中的两种以上组成的口令策略，启用定期更改口令的策略，更改周期为 90 天。	符合

安全控制点	测评指标	结果记录	符合程度
	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；	经访谈系统管理员，核查入侵防御系统， 1）设备已启用登录失败处理功能，方式为结束会话和限制登录次数； 2）登录失败 5 次，锁定用户 10 分钟； 3）设备已启用远程登录连接超时并自动退出功能，时间为 10 分钟。	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	经访谈系统管理员，核查入侵防御系统， 1）设备开启了远程管理； 2）网络中采用 HTTPS 协议对设备进行数据传输，防止鉴别信息在网络中被窃听。	符合
访问控制	a）应对登录的用户分配账户和权限；	经访谈系统管理员，核查入侵防御系统，设备已对登录的用户分配账户和权限，禁用或限制匿名、默认账户的访问权限。	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；	经访谈系统管理员，核查入侵防御系统， 1）设备已重命名默认账户或删除默认账户； 2）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；	经访谈系统管理员，核查入侵防御系统，设备的用户列表不存在多余或过期账户、共享用户。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	经访谈系统管理员，核查入侵防御系统， 1）设备的系统用户已进行角色划分； 2）系统中的账户分为系统管理员、安全管理员和审计管理员三类，管理用户的权限进行了分离，并为其工作任务所需的最小权限。	符合

安全控制点	测评指标	结果记录	符合程度
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；	经访谈审计管理员，核查入侵防御系统， 1）设备已开启审计功能； 2）设备的审计范围已覆盖到每个用户； 3）设备已对重要的用户行为和重要安全事件进行审计。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经访谈审计管理员，核查入侵防御系统，设备的日志信息中包含用户名、主机 IP、操作对象、操作、日期时间等与审计相关的信息。	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。	经访谈审计管理员，核查入侵防御系统， 1）设备已对审计记录进行备份。具体方式导出到硬盘，日志保存时间不少于 180 天； 2）设备采用权限控制措施防止审计记录受到未预期的删除、修改和覆盖。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	非安全设备测评项，故此项调整为不适用。	不适用
	b）应关闭不需要的系统服务、默认共享和高危端口；	非安全设备测评项，故此项调整为不适用。	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；	经访谈系统管理员，核查入侵防御系统， 1）设备已对终端接入范围进行限制； 2）具体限制措施为设置黑白名单； 3）终端接入方式为仅允许通过堡垒机登录。	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；	非安全设备测评项，故此项调整为不适用。	不适用

安全控制点	测评指标	结果记录	符合程度
	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。	经访谈系统管理员，核查入侵防御系统，测试漏洞扫描， 1）设备已进行定期漏洞扫描，具体周期为两年一次； 2）管理员未定期修补漏洞； 3）经现场漏洞扫描设备不存在高风险漏洞。	部分符合
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。	经访谈系统管理员，核查设备，未通过技术手段对通信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。	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。	经访谈系统管理员，核查入侵防御系统，设备采用 HTTPS 协议进行数据传输，能够保证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；	经访谈系统管理员，核查入侵防御系统， 1）设备已提供数据的本地数据备份与恢复功能； 2）设备的备份与恢复方式为由管理员进行定期备份，数据备份保存在管理员电脑上，定期对备份数据进行恢复测试。	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。	经访谈系统管理员，核查入侵防御系统，设备未提供异地数据备份功能。	不符合

D.4.1.2.4 深信服 Web 应用防护系统

安全控制点	测评指标	结果记录	符合程度
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；	经访谈系统管理员，核查 Web 应用防护系统， 1）设备使用用户名/口令鉴别机制对登录用户进行身份标识和鉴别； 2）用户身份标识具有唯一性； 3）设备具有口令复杂度策略； 4）口令长度 8 位以上，启用由数字、大小写字母和特殊字符中的两种以上组成的口令策略，启用定期更改口令的策略，更改周期为 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；	经访谈系统管理员，核查 Web 应用防护系统， 1）设备已启用登录失败处理功能，方式为结束会话和限制登录次数； 2）登录失败 5 次，锁定用户 10 分钟； 3）设备已启用远程登录连接超时并自动退出功能，时间为 10 分钟。	符合
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	经访谈系统管理员，核查 Web 应用防护系统， 1）设备开启了远程管理； 2）网络中采用 HTTPS 协议对设备进行数据传输，防止鉴别信息在网络中被窃听。	符合
访问控制	a）应对登录的用户分配账户和权限；	经访谈系统管理员，核查 Web 应用防护系统，设备已对登录的用户分配账户和权限，禁用或限制匿名、默认账户的访问权限。	符合

安全控制点	测评指标	结果记录	符合程度
	b）应重命名或删除默认账户，修改默认账户的默认口令；	经访谈系统管理员，核查 Web 应用防护系统， 1）设备已重命名默认账户或删除默认账户； 2）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；	经访谈系统管理员，核查 Web 应用防护系统，设备的用户列表不存在多余或过期账户、共享用户。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	经访谈系统管理员，核查 Web 应用防护系统， 1）设备的系统用户已进行角色划分； 2）系统中的账户分为系统管理员、安全管理员和审计管理员三类，管理用户的权限进行了分离，并为其工作任务所需的最小权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经访谈审计管理员，核查 Web 应用防护系统， 1）设备已开启审计功能； 2）设备的审计范围已覆盖到每个用户； 3）设备已对重要的用户行为和重要安全事件进行审计。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经访谈审计管理员，核查 Web 应用防护系统，设备的日志信息中包含时间、威胁类型、威胁等级、源 IP、目的 IP 等与审计相关的信息。	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。	经访谈审计管理员，核查 Web 应用防护系统， 1）设备已对审计记录进行备份。具体方式导出到硬盘，日志保存时间不少于 180 天； 2）设备采用权限控制措施防止审计记录受到未预期的删除、修改和覆盖。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	非安全设备测评项，故此项调整为不适用。	不适用

安全控制点	测评指标	结果记录	符合程度
	b）应关闭不需要的系统服务、默认共享和高危端口；	非安全设备测评项，故此项调整为不适用。	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；	经访谈系统管理员，核查 Web 应用防护系统， 1）设备已对终端接入范围进行限制； 2）具体限制措施为网络地址范围； 3）终端接入方式为仅允许通过堡垒机登录。	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；	非安全设备测评项，故此项调整为不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经访谈系统管理员，核查 Web 应用防护系统，测试漏洞扫描， 1）设备已进行定期漏洞扫描，具体周期为两年一次； 2）管理员未定期修补漏洞； 3）经现场漏洞扫描设备不存在高风险漏洞。	部分符合
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。	经访谈系统管理员，核查设备，未通过技术手段对通信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。	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。	经访谈系统管理员，核查 Web 应用防护系统，设备采用 HTTPS 协议进行数据传输，能够保证数据在传输过程中的完整性。	符合

安全控制点	测评指标	结果记录	符合程度
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；	经访谈系统管理员，核查Web 应用防护系统， 1）设备已提供数据的本地数据备份与恢复功能； 2）设备的备份与恢复方式为设备每次修改配置后由管理员进行备份，数据备份保存在管理员电脑上，定期对备份数据进行恢复测试。	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。	经访谈系统管理员，核查Web 应用防护系统，设备未提供异地数据备份功能。	不符合

D.4.1.2.5 日志审计

安全控制点	测评指标	结果记录	符合程度
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；	经访谈系统管理员，核查日志审计， 1）设备使用用户名/口令鉴别机制对登录用户进行身份标识和鉴别； 2）用户身份标识具有唯一性； 3）设备具有口令复杂度策略； 4）口令长度 8 位以上，启用由数字、大小写字母和特殊字符中的两种以上组成的口令策略，启用定期更改口令的策略，更改周期为 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；	经访谈系统管理员，核查日志审计， 1）设备已启用登录失败处理功能，方式为结束会话和限制登录次数； 2）登录失败 5 次，锁定用户 10 分钟； 3）设备已启用远程登录连接超时并自动退出功能，时间为 10 分钟。	符合

安全控制点	测评指标	结果记录	符合程度
	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。	经访谈系统管理员，核查日志审计， 1）设备开启了远程管理； 2）网络中采用 HTTPS 协议对设备进行数据传输，防止鉴别信息在网络中被窃听。	符合
访问控制	a）应对登录的用户分配账户和权限；	经访谈系统管理员，核查日志审计，设备已对登录的用户分配账户和权限，禁用或限制匿名、默认账户的访问权限。	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；	经访谈系统管理员，核查日志审计， 1）设备已重命名默认账户或删除默认账户； 2）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；	经访谈系统管理员，核查日志审计，设备的用户列表不存在多余或过期账户、共享用户。	符合
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	经访谈系统管理员，核查日志审计， 1）设备的系统用户已进行角色划分； 2）系统中的账户分为系统管理员、安全管理员和审计管理员三类，管理用户的权限进行了分离，并为其工作任务所需的最小权限。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经访谈审计管理员，核查日志审计， 1）设备已开启审计功能； 2）设备的审计范围已覆盖到每个用户； 3）设备已对重要的用户行为和重要安全事件进行审计。	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经访谈审计管理员，核查日志审计，设备的日志信息中包含时间、描述、源 IP、用户名、操作等与审计相关的信息。	符合

安全控制点	测评指标	结果记录	符合程度
	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。	经访谈审计管理员，核查日志审计， 1）设备已对审计记录进行备份。具体方式导出到硬盘，日志保存时间不少于 180 天； 2）设备采用权限控制措施防止审计记录受到未预期的删除、修改和覆盖。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	非安全设备测评项，故此项调整为不适用。	不适用
	b）应关闭不需要的系统服务、默认共享和高危端口；	非安全设备测评项，故此项调整为不适用。	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；	经访谈系统管理员，核查日志审计， 1）设备已对终端接入范围进行限制； 2）具体限制措施为 IP 白名单； 3）终端接入方式为仅允许通过堡垒机登录。	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；	非安全设备测评项，故此项调整为不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经访谈系统管理员，核查日志审计，测试漏洞扫描， 1）设备已进行定期漏洞扫描，具体周期为两年一次； 2）管理员未定期修补漏洞； 3）经现场漏洞扫描设备不存在高风险漏洞。	部分符合

安全控制点	测评指标	结果记录	符合程度
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。	经访谈系统管理员，核查设备，未通过技术手段对通信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。	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。	经访谈系统管理员，核查日志审计，设备采用 HTTPS 协议进行数据传输，能够保证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；	经访谈系统管理员，核查日志审计， 1）设备已提供数据的本地数据备份与恢复功能； 2）设备的备份与恢复方式为如设备每次修改配置后由管理员进行备份，数据备份保存在管理员电脑上，定期对备份数据进行恢复测试。	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。	经访谈系统管理员，核查日志审计，设备未提供异地数据备份功能。	不符合

D.4.1.3 服务器和终端

D.4.1.3.1 ERP 服务器

安全控制点	测评指标	结果记录	符合程度
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；	经访谈系统管理员，核查服务器， 1）用户在登录 Linux 系统时，已采用身份鉴别措施，用户登录方式：用户名/口令； 2）当采用的用户名口令方式进行身份认证时，用户名是具有唯一性； 3）口令构成方式为单一构成，记录口令复杂度配置参数信息： PASS_MAX_DAYS = 9999； PASS_MIN_LEN=5； PASS_WARN_AGE=7； dcredit=0； ucredit=0； lcredit=0； ocredit=0； 未设置口令复杂度，其中口令组成为数字、字母混合组成，口令更换周期未限制，口令最小长度 5 位； 4）采用管理制度限制使用具有数字、大小写字母和特殊字符的复杂度口令、口令最小长度 8 位，每 90 天进行定期更换。	符合
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	经访谈系统管理员，核查服务器， 1）对用户进行身份认证时，Linux 已启用了登录失败处理功能； 2）Linux 系统本地连接失败配置参数： pam_tally.so deny = 5，TIMEOUT = 600。	符合

安全控制点	测评指标	结果记录	符合程度
	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。	经访谈系统管理员，核查服务器，Linux 系统启用 Telnet 与 SSH 协议进行远程管理，Telnet 属于明文传输协议，不符合对传输加密。	部分符合
访问控制	a）应对登录的用户分配账户和权限；	经访谈系统管理员，核查服务器，Linux 系统已对登录的用户分配账户和权限，禁用或限制匿名、默认账户的访问权限。	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；	经访谈系统管理员，核查服务器， 1）Linux 系统不存在默认用户； 2）默认口令已修改。	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；	经访谈系统管理员，核查服务器， 1）Linux 系统不存在多余、过期账户； 2）不存在共享账户情况。	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。	经访谈系统管理员，核查服务器， 1）Linux 系统管理员账户有 root； 2）管理员账户并非最小授权； 3）管理员账户未与其他账户权限分离，具体分配情况。	不符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经访谈审计管理员，核查服务器， 1）服务器已开启审计功能； 2）服务器采取 audit、rsyslog 措施实现了审计功能； 3）服务器的审计范围已覆盖到每个用户； 4）服务器能对重要的用户行为和重要安全事件进行审计。	符合

安全控制点	测评指标	结果记录	符合程度
	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；	经访谈审计管理员，核查服务器，服务器的日志信息中包含事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	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。	经访谈审计管理员，核查服务器， 1）服务器已对审计记录进行备份。具体方式转发至日志审计设备，日志保存时间不少于 180 天； 2）服务器采用权限控制措施防止审计记录受到未预期的删除、修改和覆盖。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	经访谈系统管理员，核查服务器， 1）检查应用和组件，应用和组件的安装已遵循最小安装原则； 2）在保证正常应用情况下，不存在非必要的组件或程序。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	经访谈系统管理员，核查端口及服务，服务器已关闭了不必要的端口及服务。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	经访谈系统管理员，核查设备登录方式， 1）服务器已对 Linux 服务器远程接入的终端或 IP 地址进行限定； 2）限定对 Linux 系统远程管理的方式仅允许通过堡垒机登录。	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；	非服务器测评项，故此项调整为不适用。	不适用

安全控制点	测评指标	结果记录	符合程度
	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。	经访谈系统管理员，核查服务器，测试漏洞扫描， 1）设备已进行定期漏洞扫描，具体周期为两年一次； 2）管理员未定期修补漏洞； 3）经现场漏洞扫描设备不存在高风险漏洞。	部分符合
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。	经访谈系统管理员，核查服务器，主机未部署恶意代码防范软件。	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。	经访谈系统管理员，核查设备，未通过技术手段对通信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。	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。	经访谈系统管理员，核查服务器，设备采用 Telnet 与 SSH 协议进行数据传输，不能完全保证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；	经访谈系统管理员，核查服务器， 1）设备已提供数据的本地数据备份与恢复功能； 2）设备的备份与恢复方式为设备每次修改配置后由管理员进行备份，数据备份保存在管理员电脑上，定期对备份数据进行恢复测试。	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。	经访谈系统管理员，核查服务器，设备未提供异地数据备份功能。	不符合

安全控制点	测评指标	结果记录	符合程度
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。	经访谈系统管理员，核查服务器，被测服务器用户退出系统后会自动清除用户名、鉴别信息等缓存信息。	符合

D.4.1.4 系统管理软件/平台

D.4.1.4.1 虚拟化管理平台

安全控制点	测评指标	结果记录	符合程度
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；	经访谈系统管理员，核查虚拟化管理平台， 1）用户在登录时系统已提供身份鉴别措施； 2）在未登录状态下不可进行页面访问； 3）系统提供了用户身份唯一性标识：用户名/口令； 4）系统提供了口令复杂度限制，口令长度不低于 8 位，需由数字、大小写字母、特殊字符组成，强制 90 天修改一次； 5）空口令用户不可以登录系统。	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；	经访谈系统管理员，核查虚拟化管理平台， 1）系统未提供超时结束会话时间限制； 2）用户登录连续口令错误时，系统提供登录失败处理功能； 3）用户登录口令连续错误 5 次，锁定该用户需管理员解锁。	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。	经访谈系统管理员，核查虚拟化管理平台， 1）虚拟化管理平台已启用加密协议进行远程管理； 2）采用的具体措施 HTTPS 协议。	符合

安全控制点	测评指标	结果记录	符合程度
访问控制	a）应对登录的用户分配账户和权限；	经访谈系统管理员，核查虚拟化管理平台， 1） 虚拟化管理平台提供访问控制功能； 2）虚拟化管理平台的访问控制功能为用户权限限制； 3） 经验证不同角色用户拥有不同的权限。	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；	经访谈系统管理员，核查虚拟化管理平台，系统内不存在权限不受限制的超级管理用户。	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；	经访谈系统管理员，核查虚拟化管理平台， 1）系统已及时删除或停用过期、多余账户； 2）过期账户不能够登录系统； 3）管理员用户和账户之间是一一对应。	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。	经访谈系统管理员，核查虚拟化管理平台， 1）管理用户不具有业务操作权限； 2） 不同角色管理用户仅拥有其工作所需的最小权限； 3） 管理用户权限情况 NsxAdministraors 管理员、NsxAuditors 审核管理员。	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；	经访谈审计管理员，核查虚拟化管理平台， 1） 虚拟化管理平台提供了安全审计功能； 2） 审计范围覆盖到每个用户； 3） 审计内容包括重要的用户行为和重要安全事件； 4）系统实际审计内容包括：日期、任务名称、对象、状态、详细信息、启动者、排队时间。	符合

安全控制点	测评指标	结果记录	符合程度
	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；	经访谈审计管理员，核查虚拟化管理平台设备的日志信息中包含日期、任务名称、对象、状态、详细信息、启动者、排队时间与审计相关的信息。	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。	经访谈审计管理员，核查虚拟化管理平台， 1） 定期对审计记录进行备份； 2） 虚拟化管理平台具有审计记录的删除、修改或导入功能； 3） 虚拟化管理平台具备对审计记录进行保护的措施； 4）虚拟化管理平台对审计记录的保护措施为导出至外部硬盘中存储。	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；	经访谈系统管理员，核查虚拟化管理平台，被测系统已遵循最小安装的原则，仅安装需要的组件和应用程序。	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	经访谈系统管理员，核查虚拟化管理平台，被测系统已关闭不需要的系统服务。	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	经访谈系统管理员，核查虚拟化管理平台，被测系统未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。	不符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	经访谈系统管理员，核查虚拟化管理平台， 1） 虚拟化管理平台具备数据有效性检验功能； 2） 通过人机接口或通信接口输入无效数据，虚拟化管理平台拒绝无效数据； 3）数据有效性检验功能体现在限制文件类型、字符段大小。	符合

安全控制点	测评指标	结果记录	符合程度
	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。	经访谈系统管理员，核查虚拟化管理平台，测试漏洞扫描，设备未进行定期漏洞扫描。	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。	经访谈系统管理员，核查虚拟化管理平台，经访谈系统管理员，核查设备，未通过技术手段对通信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。	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。	经访谈系统管理员，核查虚拟化管理平台，被测系统采用 HTTPS 协议进行数据传输能够保证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；	经访谈系统管理员，核查虚拟化管理平台， 1）提供本地数据备份措施和恢复措施； 2）数据备份周期和方式为每年手动进行备份； 3）无近期数据恢复测试记录； 4）查看备份文件，备份结果与策略一致。	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。	经访谈系统管理员，核查虚拟化管理平台，未提供异地定时数据备份。	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。	经访谈系统管理员，核查虚拟化管理平台， 1）用户的鉴别信息所在的存储空间被释放或重新分配前得到了完全清除； 2）具体措施为退出时清空用户名、口令状态。	符合

安全控制点	测评指标	结果记录	符合程度
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；	经访谈系统管理员，核查虚拟化管理平台， 1）系统采集了用户个人信息； 2）系统所采集的个人信息均为系统内功能和业务所需的信息； 3）系统采集的个人信息为用户名、口令、描述。	符合
	b）应禁止未授权访问和非法使用用户个人信息。	经访谈系统管理员，核查虚拟化管理平台， 1）系统采用了技术措施限制对用户个人信息的访问和使用； 2）未授权用户不可访问用户个人信息； 3）制定了有关用户个人信息保护的管理制度和流程； 4）采取的技术措施为：系统用户权限策略。	符合

D.4.1.4.2 ERP Progress 数据库

安全控制点	测评指标	结果记录	符合程度
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；	经访谈系统管理员，核查数据库， 1）用户在登录 Progress 数据库时，已采用身份鉴别措施； 2）采用用户名/口令的方式对身份进行认证； 3）采用的用户名口令方式进行身份认证时，用户名已具有唯一性； 4）未对数据库用户的口令最小长度、复杂度限制、定期更换进行限制； 5）采用管理制度限制使用具有数字、大小写字母和特殊字符的复杂度口令、口令最小长度 8 位，每 90 天进行定期更换。	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；	经访谈系统管理员，核查数据库， 1）对用户进行身份认证时，Progress 数据库未配置连接失败； 2）Progress 数据库未配置远程连接超时退出功能。	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。	经访谈系统管理员，核查数据库， 1）数据库已开启远程管理； 2）远程管理数据库时，采用加密协议为：SSH。	符合
访问控制	a）应对登录的用户分配账户和权限；	经访谈系统管理员，核查数据库， 1）Progress 数据库已为不同的用户分配了不同的账号和权限； 2）Progress 数据库分配的账号有管理账户； 3）未分配用户权限。	部分符合

安全控制点	测评指标	结果记录	符合程度
	b）应重命名或删除默认账户，修改默认账户的默认口令；	经访谈系统管理员，核查数据库， 1） 通过查看用户列表，Progress 数据库存在未禁用的默认用户，默认账户的使用情况为数据库中只有管理账户； 2）默认口令已修改。	部分符合
	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；	经访谈系统管理员，核查数据库， 1） Progress 数据库不存在多余、过期账户； 2）不存在共享账户情况。	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。	经访谈系统管理员，核查数据库， 1）管理员账户有所有权限； 2）未对管理员账户授予最小授权； 3）管理员账户与其他账户权限未分离，未设置安全管理员。	不符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	经访谈审计管理员，核查数据库， 数据库未开启审计功能，只允许管理员通过堡垒机登录数据库进行远程管理，可以对重要用户行为进行记录。	不符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	经访谈审计管理员，核查数据库， 数据库未开启审计功能，只允许管理员通过堡垒机登录数据库进行远程管理，可以对重要用户行为进行记录。	不符合

安全控制点	测评指标	结果记录	符合程度
	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。	经访谈审计管理员，核查数据库，数据库未开启审计功能，只允许管理员通过堡垒机登录数据库进行远程管理，可以对重要用户行为进行记录。堡垒机记录的用户行为会定期备份，避免受到未预期的删除、修改或覆盖。	不符合
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；	非数据库测评项，故此项调整为不适用。	不适用
	b）应关闭不需要的系统服务、默认共享和高危端口；	非数据库测评项，故此项调整为不适用。	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；	经访谈系统管理员，核查数据库， 1）已对 Progress 数据库远程接入的终端或 IP 地址进行限定； 2）限定对 Progress 数据库管理的方式：仅允许通过远程连接应用服务器登录； 3）经测试验证，未被授权的终端或 IP 地址不可连接到 Progress 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；	非数据库测评项，故此项调整为不适用。	不适用
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	经访谈系统管理员，核查数据库，测试漏洞扫描， 1）Progress 数据库版本 3.11； 2）已对 Progress 数据库进行定期漏扫；上一次漏扫时间为 2022 年 5 月； 3）未发现数据库漏洞。	符合

安全控制点	测评指标	结果记录	符合程度
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。	经访谈系统管理员，核查设备，未通过技术手段对通信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。	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。	经访谈系统管理员，核查数据库，应用服务器采用 Telnet 与 SSH 协议进行数据传输，不能完全保证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；	经访谈系统管理员，核查数据库， 1）已对本地数据进行定期备份，具体备份策略为每日 9 点进行备份，能查看到备份文件记录，是增量备份； 2）无近期恢复测试记录。	部分符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	经访谈系统管理员，核查数据库，设备未提供异地数据备份功能。	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。	经访谈系统管理员，核查数据库， 1）用户的鉴别信息所在的存储空间被释放或重新分配前得到了完全清除； 2）具体措施为不记录上次用户登录名称。	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；	经访谈系统管理员，核查数据库， 1）数据库未采集用户个人信息； 2）数据库所采集的个人信息均为系统内功能和业务所需的信息； 3）数据库采集的个人信息为用户名、口令、部门。	符合

安全控制点	测评指标	结果记录	符合程度
	b）应禁止未授权访问和非法使用用户个人信息。	经访谈系统管理员，核查数据库，测试非授权用户登录， 1） 数据库采取技术措施限制对用户个人信息的访问和使用； 2）未授权用户不可访问用户个人信息； 3） 制定了有关用户个人信息保护的管理制度和流程； 4） 采取的技术措施为通过访问控制限制信息访问。	符合

D.4.1.5 业务应用系统/平台

D.4.1.5.1 ERP 系统

安全控制点	测评指标	结果记录	符合程度
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；	经访谈系统管理员，核查应用系统， 1） 用户在登录时系统已提供身份鉴别措施； 2） 在未登录状态下不可进行页面访问； 3） 系统提供了用户身份唯一性标识：用户名/口令； 4） 系统提供口令复杂度限制，口令长度不低于 10 位，需由数字、大小写字母、特殊字符组成，定期无修改一次； 5） 空口令用户不可以登录系统。	部分符合

安全控制点	测评指标	结果记录	符合程度
	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；	经访谈系统管理员，核查应用系统， 1）系统提供超时结束会话时间限制，系统 60 分钟结束超时会话，再次使用系统需重新进行身份认证； 2）用户登录连续口令错误时，系统提供登录失败处理功能； 3）用户登录口令连续错误 1 次，锁定该用户由管理员直接 解锁。	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。	经访谈系统管理员，核查应用系统，应用系统未启用加密协议进行远程管理；	不符合
访问控制	a）应对登录的用户分配账户和权限；	经访谈系统管理员，核查应用系统， 1）应用系统提供访问控制功能； 2）应用系统的访问控制功能为； 3）经验证不同角色用户拥有不相同的权限。	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；	经访谈系统管理员，核查应用系统，系统内不存在权限不受限制的超级管理用户。	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；	经访谈系统管理员，核查应用系统， 1）系统已及时删除或停用过期、多余账户； 2）过期账户不能够登录系统； 3）管理员用户和账户之间是一一对应。	符合

安全控制点	测评指标	结果记录	符合程度
	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。	经访谈系统管理员，核查 ERP 系统， 1）管理用户不具有业务操作权限； 2）不同角色管理用户仅拥有其工作所需的最小权限； 3）管理用户权限情况操作管理员、安全管理员、系统管理员。	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；	经访谈审计管理员，核查应用系统， 1）应用系统提供了安全审计功能； 2）审计范围覆盖到每个用户； 3）审计内容包括重要的用户行为和重要安全事件。 4）系统实际审计内容包括：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。	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；	经访谈审计管理员，核查应用系统，设备的日志信息中包含事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	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。	经访谈审计管理员，核查应用系统、日志审计设备， 1）定期对审计记录进行备份； 2）应用系统具有审计记录的删除、修改或导入功能； 3）应用系统具备对审计记录进行保护的措施； 4）应用系统服务器对审计记录的保存措施为保存镜像文件在本机，保存时间不少于 180 天。	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；	非应用系统测评项，故此项调整为不适用。	不适用

安全控制点	测评指标	结果记录	符合程度
	b）应关闭不需要的系统服务、默认共享和高危端口；	非应用系统测评项，故此项调整为不适用。	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；	非应用系统测评项，故此项调整为不适用。	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；	经访谈系统管理员，核查应用系统，测试漏洞扫描， 1）应用系统具备数据有效性检验功能； 2）通过人机接口或通信接口输入无效数据，应用系统拒绝无效数据； 3）数据有效性检验功能体现在设定了数据格式、大小等要求。	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。	经访谈系统管理员，核查服务器，测试漏洞扫描， 1）设备已进行定期漏洞扫描，具体周期为两年一次； 2）管理员未定期修补漏洞； 3）经现场漏洞扫描设备不存在高风险漏洞。	部分符合
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。	经访谈系统管理员，核查设备，未通过技术手段对通信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。	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。	经访谈系统管理员，核查应用系统，系统未采用校验技术或密码技术保证重要数据在传输过程中的完整性。	不符合

安全控制点	测评指标	结果记录	符合程度
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；	经访谈系统管理员，核查应用系统， 1）提供本地数据备份措施和恢复措施； 2）数据备份周期和方式为每天凌晨 2 点进行全量备份； 3）无近期恢复测试记录； 4） 查看备份文件，备份结果与策略一致。	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。	经访谈系统管理员，核查应用系统，设备未提供异地数据备份功能。	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。	经访谈系统管理员，核查应用系统， 1） 用户的鉴别信息所在的存储空间被释放或重新分配前得到了完全清除； 2） 具体措施为登录框清空。	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；	经访谈系统管理员，核查应用系统， 1）系统采集了用户个人信息； 2）系统所采集的个人信息均为系统内功能和业务所需的信息； 3）系统采集的个人信息为用户名、口令、部门。	符合
	b）应禁止未授权访问和非法使用用户个人信息。	经访谈系统管理员，核查应用系统，测试数据库存储数据， 1）系统采用了技术措施限制对用户个人信息的访问和使用； 2）未授权用户不可访问用户个人信息； 3）制定了有关用户个人信息保护的管理制度和流程； 4）采取的技术措施为禁止非授权用户登录。	符合

D.4.1.6 数据资源

D.4.1.6.1 鉴别数据

安全控制点	测评指标	结果记录	符合程度
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。	经访谈系统管理员，核查应用系统，系统未采用校验技术或密码技术保证重要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；	经访谈系统管理员，核查应用系统， 1）提供本地数据备份措施和恢复措施； 2）数据备份周期和方式为每天凌晨 2 点进行全量备份； 3）无近期恢复测试记录； 4）查看备份文件，备份结果与策略一致。	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。	经访谈系统管理员，核查应用系统，设备未提供异地数据备份功能。	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。	经访谈系统管理员，核查应用系统， 1）用户的鉴别信息所在的存储空间被释放或重新分配前得到了完全清除； 2）具体措施为登录框清空。	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；	经访谈系统管理员，核查应用系统， 1）系统采集了用户个人信息； 2）系统所采集的个人信息均为系统内功能和业务所需的信息； 3）系统采集的个人信息为用户名、口令、部门。	符合

安全控制点	测评指标	结果记录	符合程度
	b）应禁止未授权访问和非法使用用户个人信息。	经访谈系统管理员，核查应用系统，测试数据库存储数据， 1）系统采用了技术措施限制对用户个人信息的访问和使用； 2）未授权用户不可访问用户个人信息； 3）制定了有关用户个人信息保护的管理制度和流程； 4）采取的技术措施为禁止非授权用户登录。	符合

D.4.1.6.2 重要业务数据

安全控制点	测评指标	结果记录	符合程度
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。	经访谈系统管理员，核查应用系统，系统未采用校验技术或密码技术保证重要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；	经访谈系统管理员，核查应用系统， 1）提供本地数据备份措施和恢复措施； 2）数据备份周期和方式为每天凌晨 2 点进行全量备份； 3）无近期恢复测试记录； 4）查看备份文件，备份结果与策略一致。	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。	经访谈系统管理员，核查应用系统，设备未提供异地数据备份功能。	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。	经访谈系统管理员，核查应用系统， 1）用户的鉴别信息所在的存储空间被释放或重新分配前得到了完全清除； 2）具体措施为登录框清空。	符合

安全控制点	测评指标	结果记录	符合程度
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；	经访谈系统管理员，核查应用系统， 1）系统采集了用户个人信息； 2）系统所采集的个人信息均为系统内功能和业务所需的信息； 3）系统采集的个人信息为用户名、口令、部门。	符合
	b）应禁止未授权访问和非法使用用户个人信息。	经访谈系统管理员，核查应用系统，测试数据库存储数据， 1）系统采用了技术措施限制对用户个人信息的访问和使用； 2）未授权用户不可访问用户个人信息； 3）制定了有关用户个人信息保护的管理制度和流程； 4）采取的技术措施为禁止非授权用户登录。	符合

D.4.1.6.3 主要配置数据

安全控制点	测评指标	结果记录	符合程度
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。	经访谈系统管理员，核查数据库，应用服务器采用 Telnet 与 SSH 协议进行数据传输，不能完全保证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；	经访谈系统管理员，核查数据库， 1）已对本地数据进行定期备份，具体备份策略为每日 9 点进行备份，能查看到备份文件记录，是增量备份； 2）无近期恢复测试记录。	部分符合
	b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	经访谈系统管理员，核查数据库，设备未提供异地数据备份功能。	不符合

安全控制点	测评指标	结果记录	符合程度
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。	经访谈系统管理员，核查数据库， 1） 用户的鉴别信息所在的存储空间被释放或重新分配前得到了完全清除； 2） 具体措施为不记录上次用户登录名称。	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；	经访谈系统管理员，核查数据库， 1）数据库未采集用户个人信息； 2）数据库所采集的个人信息均为系统内功能和业务所需的信息； 3）数据库采集的个人信息为用户名、口令、部门。	符合
	b）应禁止未授权访问和非法使用用户个人信息。	经访谈系统管理员，核查数据库，测试非授权用户登录， 1） 数据库采取技术措施限制对用户个人信息的访问和使用； 2）未授权用户不可访问用户个人信息； 3） 制定了有关用户个人信息保护的管理制度和流程； 4） 采取的技术措施为通过访问控制限制信息访问。	符合

D.4.1.6.4 重要个人信息

安全控制点	测评指标	结果记录	符合程度
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。	经访谈系统管理员，核查应用系统，系统未采用校验技术或密码技术保证重要数据在传输过程中的完整性。	不符合

安全控制点	测评指标	结果记录	符合程度
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；	经访谈系统管理员，核查应用系统， 1）提供本地数据备份措施和恢复措施； 2）数据备份周期和方式为每天凌晨 2 点进行全量备份； 3）无近期恢复测试记录； 4）查看备份文件，备份结果与策略一致。	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。	经访谈系统管理员，核查应用系统，设备未提供异地数据备份功能。	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。	经访谈系统管理员，核查应用系统， 1）用户的鉴别信息所在的存储空间被释放或重新分配前得到了完全清除； 2）具体措施为登录框清空。	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；	经访谈系统管理员，核查应用系统， 1）系统采集了用户个人信息； 2）系统所采集的个人信息均为系统内功能和业务所需的信息； 3）系统采集的个人信息为用户名、口令、部门。	符合
	b）应禁止未授权访问和非法使用用户个人信息。	经访谈系统管理员，核查应用系统，测试数据库存储数据， 1）系统采用了技术措施限制对用户个人信息的访问和使用； 2）未授权用户不可访问用户个人信息； 3）制定了有关用户个人信息保护的管理制度和流程； 4）采取的技术措施为禁止非授权用户登录。	符合

D.5 安全管理中心

D.5.1 安全通用要求部分

安全控制点	测评指标	结果记录	符合程度
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；	经访谈系统管理员，核查网络设备、安全设备、服务器、数据库、应用系统，测试系统管理员账户， 1）网络层面采用用户名/口令方式对系统管理员进行身份鉴别； 2）主机层面采用用户名/口令方式对系统管理员进行身份鉴别； 3）应用层面采用用户名/口令方式对系统管理员进行身份鉴别； 4）被测系统通过系统对各层面系统管理员的操作进行审计。	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。	经访谈系统管理员，核查网络设备、安全设备、服务器、数据库、应用系统，测试系统管理员账户， 1）各层面已实现对系统管理员权限划分； 2）仅系统管理员具备查看用户身份、系统资源配置等操作权限。	符合

安全控制点	测评指标	结果记录	符合程度
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；	经访谈审计管理员，核查网络设备、安全设备、服务器、数据库、应用系统，测试审计管理员账户， 1）网络层面采用用户名/口令方式对审计管理员进行身份鉴别； 2）主机层面采用用户名/口令方式对审计管理员进行身份鉴别； 3）应用层面采用用户名/口令方式对审计管理员进行身份鉴别； 4）被测系统通过系统对各层面审计管理员的操作进行审计。	符合
	b）应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	经访谈审计管理员，核查网络设备、安全设备、服务器、数据库、应用系统，测试审计管理员账户， 1）各层面实现了对审计管理员权限划分； 2）仅审计管理员具备审计分析权限。	符合

D.6 安全管理制度

D.6.1 安全通用要求部分

安全控制点	测评指标	结果记录	符合程度
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。	经访谈系统管理员，核查相关制度， 1）具有信息安全总体方针策略文件； 2）文件名：《信息安全策略总纲 V1.1》； 3）文件内容：机构网络安全工作的总体目标、范围、原则和安全策略等。	符合

安全控制点	测评指标	结果记录	符合程度
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；	经访谈系统管理员，核查相关制度， 1）制定了《变更管理制度 V1.0》、《北京光华荣昌汽车部件有限公司介质安全管理制度》、《信息安全管理机构 V1.0》、《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》、《信息安全管理组织职责 V1.0》、《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》、《资产安全管理制度 V1.1》等管理制度； 2）安全管理制度覆盖：物理、网络、主机系统、数据、应用、建设和运维等层面的管理内容。	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。	经访谈系统管理员，核查相关制度， 1）制定了《防火墙策略配置规范 V1.0》、《安全域划分规范 V1.0》、《入侵检测系统策略配置规范 V1.0》、《终端安全管理制度 V1.1》等操作规程； 2）操作规程覆盖：物理、网络、主机系统等层面的重要操作内容，未覆盖数据、应用、建设和运维等层面的重要操作内容。	部分符合
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；	经访谈系统管理员，核查相关制度，负责制定管理制度的部门或人员是：集团信息管理部。	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。	经访谈系统管理员，核查相关制度， 1）各项安全管理制度文档的发布方式发布印刷版； 2）安全管理制度文件具有版本标识。	符合

安全控制点	测评指标	结果记录	符合程度
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。	经访谈系统管理员，核查相关制度， 1）具有安全管理制度的核查记录或评审记录； 2）核查记录或评审记录：《制度审批记录》； 3）具有修订版本的安全管理制度； 4）修订内容与评审记录中一致。	符合

D.7 安全管理机构

D.7.1 安全通用要求部分

安全控制点	测评指标	结果记录	符合程度
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；	经访谈系统管理员，核查相关制度， 1）网络安全管理职能部门：集团信息管理部； 2）指定了各方面负责人：系统运维负责人、系统建设负责人等； 3）职责文件：《信息安全岗位职责要求 V1.1》。	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。	经访谈系统管理员，核查相关制度， 1）设立的岗位：系统管理员、审计管理员、安全管理员等； 2）职责文档：《信息安全岗位职责要求 V1.1》。	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。	经访谈系统管理员，核查相关制度， 1）系统管理员数量：1 人； 2）审计管理员数量：1 人； 3）安全管理员数量：1 人。	符合

安全控制点	测评指标	结果记录	符合程度
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；	经访谈系统管理员，核查相关制度， 1）需要进行审批的信息系统活动：系统变更、设备维修、设备上线等； 2）审批记录和职责文件描述一致。	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。	经访谈系统管理员，核查相关制度， 1）系统变更、物理访问和系统介入等重要操作的审批流程文档：《北京光华荣昌汽车部件有限公司授权审批管理制度》； 2）审批记录：《信息系统授权审批记录表》。	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；	经访谈系统管理员，核查相关制度， 1）会议记录：《会议记录》； 2）会议记录内容：会议内容、会议时间、参加人员和会议结果等。	符合
	b）应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；	经访谈系统管理员，核查相关制度， 1）日常沟通方式：提交工单、电话沟通； 2）已提供手机中的日常沟通记录。	符合
	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。	经访谈系统管理员，核查相关制度， 1）外联单位联系列表：《外部合作单位联系表》； 2）外联单位联系列表内容：合作单位、合作范围、联系人姓名、办公电话、手机。	符合

安全控制点	测评指标	结果记录	符合程度
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。	经访谈系统管理员，核查相关制度， 1）安全检查覆盖的内容：系统日常运行情况、系统漏洞和数据备份等； 2）检查记录：《安全检查报告及安全检查表》。	符合

D.8 安全管理人员

D.8.1 安全通用要求部分

安全控制点	测评指标	结果记录	符合程度
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；	经访谈系统管理员，核查相关制度，负责人员录用的部门或人员是：人力资源部。	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。	经访谈系统管理员，核查相关制度， 1）人员录用管理文档已说明不同岗位录用人员的条件，如学历要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等； 2）人员录用的审查记录：未提供人员录用的相关审查记录； 3）人员录用的技能考核记录：未提供人员录用的技能考核记录。	部分符合

安全控制点	测评指标	结果记录	符合程度
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。	经访谈系统管理员，核查相关制度， 1）明确及时终止离岗人员的所有访问权限。人员管理文档是《人员安全管理制度 V1.1》，内容包括：明确人员离岗前应归还所持有的信息资产，包括笔记本、门禁卡、钥匙、证件、软硬件设备等；并及时终止离岗人员的访问权限； 2）未提供人员离职记录文档。	部分符合
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。	经访谈系统管理员，核查相关制度， 1）安全意识教育和岗位技能培训相关的文档名称是：《信息安全管理组织职责》； 2）网络安全教育和技能培训记录名称是：《安全培训记录表》，内容包括：培训对象、培训方式、培训内容和考核方式等； 3）安全责任和惩戒措施文档名称是：《人员安全管理制度 V1.1》。	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；	经访谈系统管理员，核查相关制度， 1）外部人员访问受控区域管理文档名称是：《外部人员访问管理制度 V1.1》； 2）外部人员访问受控区域申请并批准进入的记录名称是：《外部人员访问管理制度 V1.1》； 3）外部人员访问受控区域的登记记录的名称是：《外来人员登记表》； 4）登记记录的内容包括：区域名称、进入时间、离开时间、访问区域及陪同人等。	符合

安全控制点	测评指标	结果记录	符合程度
	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；	经访谈系统管理员，核查相关制度， 1）外部人员逻辑访问受控网络系统的审批要求的文档名称是：《外部人员访问管理制度 V1.1》； 2）外部人员访问申请并批准接入网络的记录名称是：《授权申请表》； 3）外部人员逻辑访问受控区域的登记的记录名称是：《第三方访问申请表》。	符合
	c）外部人员离场后应及时清除其所有的访问权限。	经访谈系统管理员，核查相关制度， 1）外部人员离场后清除其权限的要求的文档名称是：《外部人员访问管理制度 V1.1》； 2）未提供清除访问权限的记录。	部分符合

D.9 安全建设管理

D.9.1 安全通用要求部分

安全控制点	测评指标	结果记录	符合程度
定级和备案	a）应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；	经访谈系统管理员，核查相关制度，被测单位 ERP 系统网络安全等级保护定级报告明确了本系统的安全等级 S2A2G2 分别从业务信息和系统服务说明定级理由。	符合
	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；	经访谈系统管理员，核查相关制度， 1）组织的论证和审定会议是：北京光华荣昌汽车部件有限公司专家评审会； 2）定级结果和论证文件是：系统级别定为二级，论证文件为专家评审意见。	符合

安全控制点	测评指标	结果记录	符合程度
	c）应保证定级结果经过相关部门的批准；	经访谈系统管理员，核查相关制度， 1）单位内部管理部门是：集团信息管理部； 2）已提供单位内部管理部门的审批意见。	符合
	d）应将备案材料报主管部门和相应公安机关备案。	经访谈系统管理员，核查相关制度， 1）被测单位无上级主管部门； 2）备案机关是：北京市公安局昌平分局，备案编号是：11011499364-22003。	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；	经访谈系统管理员，核查相关制度， 1）系统等级是：第二级； 2）风险分析或评估的结果补充安全控制措施是：购买防火墙、堡垒机、日志审计、IPS 等安全设备，并根据安全需求配置安全策略； 3）核查的文档是：《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》。	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；	经访谈系统管理员，核查相关制度， 1）保护对象的总体规划和安全设计文档：《安全方案设计管理制度》； 2）文档主要内容包括：职责分工、安全规划、方案设计等。	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。	经访谈系统管理员，未提供规划和建设文档。	不符合

安全控制点	测评指标	结果记录	符合程度
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；	经访谈系统管理员，核查相关制度， 1）产品的采购流程是：按照《GR-41 采购管理业务程序》进行管理； 2）销售许可标编号是：0405220244、0404220286、0402210356、0404211668。	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。	被测系统不涉及密码产品，故此项调整为不适用。	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；	被测系统为外包开发，故此项调整为不适用。	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。	被测系统为外包开发，故此项调整为不适用。	不适用
外包软件开发	a）应在软件交付前检测其中可能存在的恶意代码；	经访谈系统管理员，核查相关制度， 1）负责软件恶意代码检测的部门或人员是：集团信息管理部； 2）未提供恶意代码检测报告。	部分符合
	b）应保证开发单位提供软件设计文档和使用指南。	经访谈系统管理员，未提供软件设计文档和使用指南。	不符合
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；	经访谈系统管理员，核查相关制度， 1）负责部门或人员是：集团信息管理部； 2）岗位职责文件名称是：《北京光华荣昌汽车部件有限公司软件开发流程管理制度》。	符合
	b）应制定安全工程实施方案控制工程实施过程。	经访谈信息总监，未提供工程实施方案。	不符合

安全控制点	测评指标	结果记录	符合程度
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；	经访谈信息总监，未提供验收管控流程。	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。	经访谈系统管理员，核查相关制度，未提供安全性测试报告。	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；	经访谈系统管理员，核查相关制度，未提供交付清单。	不符合
	b）应对负责运行维护的技术人员进行相应的技能培训；	经访谈系统管理员，核查相关制度， 1）培训文档名称是：《培训记录表》； 2）内容包括：培训内容、培训时间、培训人员等。	符合
	c）应提供建设过程文档和运行维护文档。	经访谈系统管理员，核查相关制度，未提供建设过程的管控措施。	不符合
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；	被测系统为首次测评，故此项调整为不适用。	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；	被测系统未发生重大变更或级别发生变化，故此项调整为不适用。	不适用
	c）应确保测评机构的选择符合国家有关规定。	经访谈系统管理员，测评机构名称是：北京时代新威信息技术有限公司。	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；	经访谈系统管理员，核查相关情况， 1）选择服务商的控制措施是：制定并执行《GR-41 采购管理业务程序》； 2）服务商名称是：深信服科技股份有限公司。	符合

安全控制点	测评指标	结果记录	符合程度
	b）应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。	经访谈系统管理员，核查相关情况， 1）对服务供应商的管控措施是：合同约束； 2）服务协议和内容包括：服务周期、服务内容等。	符合

D.10安全运维管理

D.10.1 安全通用要求部分

安全控制点	测评指标	结果记录	符合程度
环境管理	a）应指定专门的部门或人员负责机房安全，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；	经访谈系统管理员，核查相关制度， 1）负责机房安全管理工作的部门和人员是：集团信息管理部的王金良； 2）具有来访人员登记记录； 3）登记记录名称：《人员登记表》，内容包括：序号、人员、单位、进入时间、离开时间、备注； 4）具有设施维护记录； 5）设施维护记录名称：《设施维护巡检记录》，内容包括：序号、日期、设备名称、备注、维护人员。	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；	经访谈系统管理员，核查相关制度， 1）具有机房安全管理制度； 2）文件名：《机房管理制度》，内容包括：物理访问、常规检查与维护，内容覆盖测评项的要求； 3）具有机房物理访问、物品带进带出机房和机房环境安全等相关记录； 4）记录名称：《机房设备管理记录表》，记录与制度相符。	符合

安全控制点	测评指标	结果记录	符合程度
	c）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	经访谈系统管理员，核查相关制度， 1）具有办公环境的安全管理制度； 2）文件名称：《北京光华荣昌汽车部件有限公司办公环境安全管理制度》，内容已明确来访人员的接待区域； 3）员工的办公桌面上不存在包含敏感信息的纸质文件和移动介质。	符合
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。	经访谈系统管理员，核查相关制度， 1）具有资产清单； 2）资产清单内容包括：资产责任部门、重要程度和所处位置等，内容覆盖全面。	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； 4）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。	经访谈系统管理员，核查相关制度，经访谈系统管理员，核查相关制度， 1）具有介质在物理传输时的管理要求； 2）文件名：《北京光华荣昌汽车部件有限公司介质安全管理制度》； 3）具有物理介质传输的管理记录，管理记录：《存储介质管理登记表》，内容包括序号、介质名称、介质编号、使用时间、使用人、介质测试/更换时间。	符合

安全控制点	测评指标	结果记录	符合程度
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、维修过程的监督控制等。	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、维修过程的监督控制等； 3）未提供维修和服务的审批、维修过程等记录。	部分符合
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。	经访谈系统管理员，核查相关制度， 1）具有发现安全漏洞和隐患的措施； 2）措施是：通过入侵防御系统和防火墙识别隐患； 3）未提供识别安全漏洞和隐患的安全报告或记录； 4）未提供修复漏洞或消除隐患的操作记录。	部分符合
网络和系统安全管理	a）应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；	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

安全控制点	测评指标	结果记录	符合程度
	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； 3）未提供设备操作记录。	部分符合
	e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。	经访谈系统管理员，核查相关制度， 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。	符合

安全控制点	测评指标	结果记录	符合程度
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，外来计算机或存储设备接入系统前未进行恶意代码检查。	部分符合
	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）不具有检查恶意代码防范措施执行记录； 3）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。	部分符合
	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。	经访谈系统管理员，核查相关制度， 1）已进行恶意代码防范； 2）不具有恶意代码防范检测记录、分析报告； 3）运维人员手动更新恶意代码库措施对恶意代码特征库进行更新； 4）未提供恶意代码防范措施特征库的更新、升级记录。	部分符合

安全控制点	测评指标	结果记录	符合程度
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；	被测系统不涉及密码产品，故此项调整为不适用。	不适用
	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。	被测系统不涉及密码产品，故此项调整为不适用。	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

安全控制点	测评指标	结果记录	符合程度
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

安全控制点	测评指标	结果记录	符合程度
安全事件处置	a）应及时向安全管理部门报告所发现的安全弱点和可疑事件；	经访谈系统管理员，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》。	符合
	b）应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；	经访谈系统管理员，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。	被测系统目前未发生过网络安全事件，故此项调整为不适用。	不适用

安全控制点	测评指标	结果记录	符合程度
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，并进行应急预案的演练。	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； 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、培训地点等； 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。	符合
外包运维管理	a）应确保外包运维服务商的选择符合国家的有关规定；	被测系统为自行运维，故此项调整为不适用。	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。	被测系统为自行运维，故此项调整为不适用。	不适用

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
1	中风险	OpenSSH 用户枚举漏洞(CVE-2018-15473)	192.168.0.206
2	中风险	SSH 服务支持弱加密算法	192.168.0.206
3	低风险	检测到目标 SSL 证书已过期	192.168.5.254
4	低风险	OpenSSH CBC 模式信息泄露漏洞(CVE-2008-5161)	192.168.0.206
5	低风险	ICMP timestamp 请求响应漏洞	192.168.0.206、192.168.0.1、192.168.5.251、192.168.5.252、192.168.5.253、192.168.5.254
6	低风险	远端 Web 服务器上存在/robots.txt 文件	192.168.0.206
7	低风险	允许 Traceroute 探测	192.168.10.1、192.168.0.1、192.168.5.251、192.168.5.252、192.168.5.253、192.168.5.254
8	低风险	检测到远端运行着 Telnet 服务	192.168.0.206
9	低风险	SSH 版本信息可被获取	192.168.0.206
10	低风险	探测到 SSH 服务器支持的算法	192.168.0.206
11	低风险	嵌入式 Web 服务器探测	192.168.0.206
12	低风险	探测到服务器支持的 SSL 加密协议	192.168.5.251、192.168.5.252、192.168.5.253
13	低风险	可通过 HTTP 获取远端 WWW 服务信息	192.168.0.206、192.168.5.253

附录F 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	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等问题
2	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
3	无作为或操作失误	应该执行而没有执行相应的操作，或无意执行了错误的操作
4	管理不到位	安全管理无法落实或不到位，从而破坏信息系统正常有序运行
5	恶意代码	故意在计算机系统上执行恶意任务的程序代码
6	越权或滥用	通过采用一些措施，超越自己的权限访问了本来无权访问的资源，或者滥用自己的权限，做出破坏信息系统的行为
7	网络攻击	利用工具和技术通过网络对信息系统进行攻击和入侵
8	物理攻击	通过物理的接触造成对软件、硬件、数据的破坏
9	泄密	信息泄露给不应了解的他人
10	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
11	抵赖	不承认收到的信息和所作的操作和交易
12	资源不足	系统重要设备负载较高，不满足业务需求，一旦设备因负载较高而出现故障将影响业务连续性
13	敏感信息泄漏	敏感信息包括用户信息、 公民信息、地理信息，数量级 0~1 万、1~10 万、10~100 万、100 万以上
14	网页篡改	针对连接互联网的网站面临被篡改的可能性较大