报告编号：4403161303000001-16-4411-01

信息系统安全等级测评报告

系统名称：你我金融信息服务系统

委托单位：深圳市你我金融信息服务股份有限公司

测评单位：深圳市网安计算机安全检测技术有限公司

报告时间：2016 年 6 月 17 日

信息系统等级测评基本信息表

<table>
<tr><td colspan="7">信息系统</td></tr>
<tr><td>系统名称</td><td colspan="2">你我金融信息服务系统</td><td colspan="2">安全保护等级</td><td colspan="2">第三级</td></tr>
<tr><td>备案证明编号</td><td colspan="2">440316-13030-00001</td><td colspan="2">测评结论</td><td colspan="2">基本符合</td></tr>
<tr><td colspan="7">被测单位</td></tr>
<tr><td>单位名称</td><td colspan="6">深圳市你我金融信息服务股份有限公司</td></tr>
<tr><td>单位地址</td><td colspan="3">深圳市南山区乌石头路天明科技大厦主楼 10/11 楼</td><td>邮政编码</td><td colspan="2">518000</td></tr>
<tr><td rowspan="3">联 系 人</td><td>姓　　名</td><td>刘忠宇</td><td>职务/职称</td><td colspan="3">数据库运维经理</td></tr>
<tr><td>所属部门</td><td>技术中心</td><td>办公电话</td><td colspan="3">0755-86653710</td></tr>
<tr><td>移动电话</td><td>13823396610</td><td>电子邮件</td><td colspan="3">liuzhongyu@tuandai.com</td></tr>
<tr><td colspan="7">测评单位</td></tr>
<tr><td>单位名称</td><td colspan="3">深圳市网安计算机安全检测技术有限公司</td><td>单位代码</td><td colspan="2">（粤）-005</td></tr>
<tr><td>通信地址</td><td colspan="3">深圳市南山区学苑大道 1001 号南山智园 C1 栋 13 楼</td><td>邮政编码</td><td colspan="2">518055</td></tr>
<tr><td rowspan="3">联 系 人</td><td>姓　　名</td><td>石松奇</td><td>职务/职称</td><td colspan="3">副总经理</td></tr>
<tr><td>所属部门</td><td>行政部</td><td>办公电话</td><td colspan="3">0755-83764999</td></tr>
<tr><td>移动电话</td><td>13714833734</td><td>电子邮件</td><td colspan="3">root@szcert.org</td></tr>
<tr><td rowspan="3">审核批准</td><td>编 制 人</td><td></td><td>编制日期</td><td colspan="3"></td></tr>
<tr><td>审 核 人</td><td></td><td>审核日期</td><td colspan="3"></td></tr>
<tr><td>批 准 人</td><td></td><td>批准日期</td><td colspan="3"></td></tr>
</table>

声明

本报告是深圳市你我金融信息服务股份有限公司你我金融信息服务系统等级测评报告。

本报告测评结论的有效性建立在被测评单位提供相关证据的真实性基础之上。

本报告中给出的测评结论仅对被测信息系统当时的安全状态有效。当测评工作完成后，由于信息系统发生变更而涉及到的系统构成组件（或子系统）都应重新进行等级测评，本报告不再适用。

本报告中给出的测评结论不能作为对信息系统内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。

深圳市网安计算机安全检测技术有限公司

2016 年 6 月

等级测评结论表

测评结论与综合得分			
系统名称	你我金融信息服务系统	**保护等级**	第三级
系统简介	你我金融信息服务系统是以客户为中心，借款人、担保人、投资人依托此平台进行资金交易，通过担保分散，投资分散，将风险分散化做到极致，同时利用众保的风险管控模式，对资金安全性进行保障，真正实现运用互联网的特性做到风险碎片化，在体系进行风险的化解。		
测评过程简介	本次测评是按照《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2008）三级信息系统安全要求进行安全测评。本测评项目的开展经历了测评准备阶段、方案编制阶段、现场实施阶段、分析与报告编制阶段四个阶段，历时一个月左右,投入测评人员 6 人，使用了多种测评设备/工具。测评内容涵盖等级保护安全技术要求的 5 个层面和安全管理要求的 5 个层面，涉及测评分类 73 类。		
测评结论	基本符合	**综合得分**	89.2

总体评价

本次对被测系统实施的等级测评工作包含两个方面的内容：单元测评和整体测评。单元测评主要测评《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2008）所要求的基本安全控制在被测单位中的实施和配置情况。整体测评主要测评分析信息系统的整体安全性。汇总第 5 和第 6 章的内容，对被测系统实施单元测评和整体测评分析后，可以得到如下测评结果：

被测系统的物理布局、网络结构和业务逻辑等在整体结构上合理、安全。在物理上，机房出入口安排专人值守，控制、鉴别和记录进入的人员；机房设置灭火设备和火灾自动报警系统；关键设备采用必要的接地防静电措施；机房设置温、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。在网络上，应保证关键网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；对网络系统中的网络设备运行状况、网络流量等进行日志记录；在网络边界部署访问控制设备，启用访问控制功能。操作系统、应用系统、数据库等各种业务应用平台都采取了基本的身份鉴别、访问控制、审计、资源控制等安全措施。在入侵防范和恶意代码防护上，采用防火墙、防病毒软件等安全措施。在数据备份方面，重要数据每日备份。总体来看，安全技术方面具有基本安全保障能力。

在安全管理方面，制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；对安全管理活动中的重要管理内容建立安全管理制度；定期对安全管理制度进行评审，对存在不足或需要改进的安全管理制度进行修订；被测系统所属单位已经建立了基本的信息安全管理体系，建立了相应的安全组织。信息系统日常运行维护，如外来人员访问管理、系统安全管理和网络安全管理等方面，拥有较完善的流程和规范。总体来看，安全管理方面具有基本安全保障能力。

被测单位对其中立即整改类建议实施了整改，对需要持续整改的意见，制定了信息系统整改方案，并在方案中制定了整改的具体计划。整改计划中，被测单位对测评中发现信息系统存在的问题采取了相应的安全控制措施，经过测评单位参照等

级保护中相应安全控制要求对整改方案进行了分析，得出被测单位按计划实施整改计划后，可以满足等级保护基本要求的结论。

综合上述评价结果，可以看到信息系统中存在安全问题，但不会导致信息系统面临高等级安全风险。因此，本次等级测评结论为：**基本符合**。

主要安全问题

通过本次等级测评，发现被测系统仍存在一些安全问题，主要包括：

1）网络安全层面：被测单位未采用审计工具对管理员的操作记录进行日志记录；网络设备只采用用户名密码一种鉴别技术对管理员进行身份鉴别。

2）安全管理机构层面：被测单位未配备专职的安全管理员；没有定期审查、更新审批项目；未聘请信息安全专家作为常年的安全顾问；目前没有内部人员或上级单位对信息系统进行全面安全检查；没有制定安全检查列表；没有制定安全审核和安全检查制度。

3）人员安全管理层面：被测单位没有建立安全教育和培训计划；没有安全教育和培训记录。

4）系统建设管理层面：被测单位没有由总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案形成的配套文件；未制定代码编写规范；未委托第三方进行安全性测试，没有安全性测试报告；未选定安全服务商。

5）系统运维管理层面：被测单位没有制定信息分类与标识文档；未对存储介质进行定期盘点；重要介质中的数据和软件未采取加密存储；没有对系统监控记录进行分析评审；存在两名管理员共用同一个账号的情况；没有定期对运行日志和审计结果进行分析；没有定期检查信息系统内各种产品的恶意代码库的升级情况，没有书面的报表和总结汇报;没有建立建立中止变更并从失败变更中恢复的文件化程序；没有定期执行备份恢复测试；对造成系统中断和造成信息泄密的安全事件未制定相应的处理程序和报告程序；没有进行应急预案培训和演练；未对应急预案定期进行审查。

6)工具测试：漏洞扫描发现较多中高危漏洞。

问题处置建议

针对被测系统存在的问题，提出如下主要安全建设整改建议：

1）网络安全层面：采用审计工具对管理员的操作记录进行日志记录；采用两种或两种以上鉴别技术对管理员进行身份鉴别。

2）安全管理机构层面：配备专职的安全管理员；授权专人定期对重要审批事项进行审查，发现不适用的审批程序应及时修订；聘请信息安全专家作为常年的安全顾问；信息安全领导层或管理层组织定期进行安全管理评审，检查内容包括检测所采取的安全技术措施是否有效、安全配置和安全策略是否一致、安全管理制度的执行情况等；根据相关的安全标准、企业信息安全战略目标制定详细的安全检查列表，详细记录检查情况，形成检查报告；制定安全审核和安全检查制度，明确要求安全检查和审核过程中的行为规范，确保审核和检查没有遗漏和降低审核和检查所带来的风险。

3）人员安全管理层面：根据不同岗位的安全要求制定培训计划，定期对各岗位进行安全培训，包括信息安全基础知识、岗位安全技能、岗位操作规程等。

4）系统建设管理层面：根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件；制定代码编写安全规范，要求开发人员参照规范编写代码；委托第三方测试机构对信息系统进行独立的安全性测试，并出具相应测试报告；所选择的安全服务商应符合国家的有关规定。

5）系统运维管理层面：制定信息分类文档，内容应明确信息分类标识的原则和方法；根据介质的目录清单对介质的使用现状进行定期检查，定期对其完整性（数据是否损坏或丢失）和可用性（介质是否受到物理破坏）进行检查；应根据所承载数据和软件的重要性对介质进行分类和标识管理，对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理；定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施；存指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权

限、责任和风险，权限设定应当遵循最小授权原则；定期对运行日志和审计结果进行分析，并出具分析报告；定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报；建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练；定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复；系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序；应急预案的培训应至少每年举办一次；定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期；定期审查应急预案的管理规定，明确应急预案中需要定期审查和根据实际情况更新的内容，并存档应急预案的审查记录。

6）工具测试：建议评估业务的影响后对中高危漏洞进行修复。

目录

1 测评项目概述

1.1 测评目的

本测评项目的对象是深圳市你我金融信息服务股份有限公司核心业务——你我金融信息服务系统。业务信息安全保护等级为第三级，系统服务安全保护等级为第三级，安全保护等级为第三级。

本测评的委托单位是深圳市你我金融信息服务股份有限公司。你我金融 APP 是一款移动社交金融 APP，由东莞团贷网互联网科技服务有限公司（团贷网）的全资子公司深圳市你我金融信息服务股份有限公司（以下简称你我金融）推出。你我金融 APP 将传统金融的担保、保险概念运用于大数据、移动互联网技术中，再加入社交思维，创建出一套完整的在线金融生态体系。在该体系中，借款人、担保人、投资人依托你我金融的平台进行资金交易，通过担保分散、投资分散，将风险分散化做到极致，同时加入保险的概念，对资金安全性进行保障，真正实现运用互联网的特性做到风险碎片化，在体系中进行风险的消解。

本测评项目的测评单位是深圳市网安计算机安全检测技术有限公司（以下简称网安公司）。网安公司是深圳市计算机网络公共安全协会的技术支撑单位，是专业的网络安全应急服务提供商和网络安全风险管理服务提供商，具有多年的信息系统安全运维和信息系统安全等级保护测评的经验。网安公司是公安部授权的等级测评机构，同时拥有广东省公安厅认可的安全服务资质。网安公司也是深圳地区唯一具有等级测评资质的第三方商业机构，拥有一支由博士后、博士带队的经验丰富、理论知识深厚的测评队伍，每年为超过 150 家单位和机构的近 400 个信息系统提供等级测评服务，测评质量得到了等级保护主管机构和广大客户的高度认可。

本次测评的目的是通过对被测系统在安全技术和安全管理方面的测评，对被测系统的安全状态做出判断，明确被测系统在安全技术和安全管理方面与其相应安全保护等级要求之间的差距，提出信息系统安全整改建议，给出等级测评结论。测评结果将为委托方进一步完善系统安全策略、采取适当的安全保护措施提供依据。

1.2 测评依据

- 基线标准
  - 《信息安全技术 信息系统安全等级保护基本要求》(GB/T 22239-2008)；
  - 《信息安全技术 信息系统安全等级保护测评要求》(GB/T 28448-2012)；
- 辅助标准
  - 《信息安全等级保护实施指南》(GB/T 25058-2010)；
  - 《计算机信息系统安全保护等级划分准则》(GB 17859-1999)；
  - 《信息系统等级保护等级定级指南》(GB/T 22240-2008)；
  - 《信息安全技术 信息安全风险评估规范》(GB/T 20984-2007)；
- 文件
  - 《信息安全等级保护管理办法》(公通字[2007]43 号)；
  - 《广东省公安厅关于计算机信息系统安全保护的实施办法》(粤公通字[2008]228 号)；
  - 被测信息系统《信息安全等级保护定级报告》；
  - 等级测评任务书/测评合同等。

1.3 测评过程

等级测评工作流程分为四个阶段：测评准备阶段、方案编制阶段、现场实施阶段、分析与报告编制阶段。

测评准备阶段是开展现场测评工作的前提和基础，是整个等级测评过程有效性的保证。测评准备工作是否充分直接关系到现场测评工作能否顺利开展。本阶段的主要工作是掌握被测系统的详细情况和为实施现场测评作好方案、文档及测试工具等方面的准备。

方案编制阶段是根据测评准备阶段收集的信息编制出项目实施方案，是项目实施的方向和准则。本阶段的主要工作是测评对象确定、测评指标确定、测评内容确定、工具测试方法确定、测评作业指导书开发及测评方案编制。

现场实施阶段是开展等级测评工作的关键阶段。本阶段的主要工作是按照测评

方案的总体要求，严格执行作业指导书，分步实施所有测评项目，包括单项测评和系统整体测评两个方面，以了解系统的真实保护情况，获取足够证据，发现系统存在的安全问题。

分析与报告编制阶段是等级测评工作的重要环节，是对被测系统整体安全保护能力的综合评价过程。主要工作是根据现场测评结果和《信息系统安全等级保护基本要求》的有关要求，通过单项测评结果判定和系统整体测评分析等方法，分析整个系统的安全保护现状与相应等级的保护要求之间的差距，给出测评结论，提出修改建议并编制测评报告等。

本次等级测评的工作流程各阶段完成的关键任务和具体时间节点如下表：

阶段	工作内容	对象	日期
实施准备阶段	项目启动	项目甲乙双方	2016.03.21 ~ 2016.03.25
	信息收集与分析	调研表	
	工具、文档、表单准备	测评工具、测评授权书、文档交接单	
方案编制阶段	确定测评对象、指标等	测评方案-对象列表	2016.03.28 ~ 2016.03.29
	开发作业指导书	测评作业指导书	
	编制方案	测评方案	
现场实施阶段	安全管理访谈	被测单位人员	2016.03.30 ~ 2016.04.01
	安全管理文档检查	安全管理制度、规范、运维管理记录等	
	物理安全测评	机房	
	网络安全测评	网络安全设备、网络设备	
	应用安全测评	业务应用系统	
	主机 OS 测评	主机操作系统	
	主机 DB 测评	主机数据库	
	工具测试	网络、主机、数据库、应用	
分析与报告编制阶段	单项结果判定	测评报告	2016.04.04 ~ 2016.06.17
	整体测评		
	风险分析		

阶段	工作内容	对象	日期
	形成初步结论		
	给出整改建议		
	编制报告		

1.4 报告分发范围

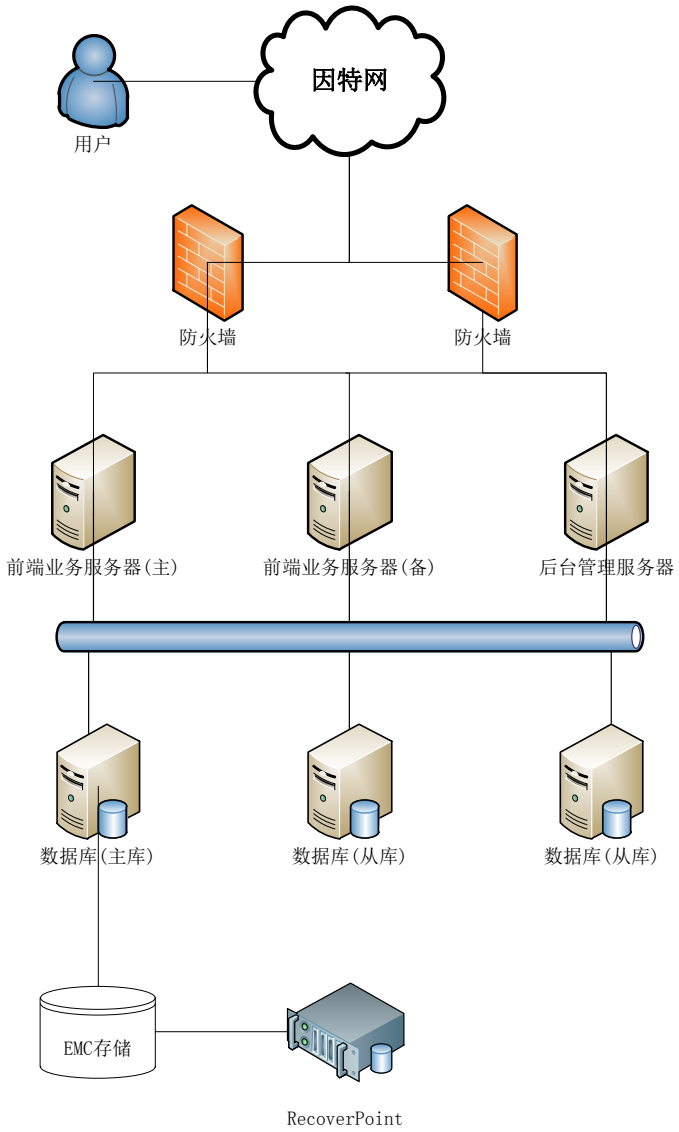
依据测评要求，本次测评应交付等级测评报告一式四份，两份提交测评委托单位，一份提交深圳市信息安全等级保护工作协调领导小组办公室，一份由测评单位留存。

2 被测信息系统表

2.1 承载的业务情况

你我金融信息服务系统是以客户为中心，借款人、担保人、投资人依托此平台进行资金交易，通过担保分散，投资分散，将风险分散化做到极致，同时利用众保的风险管控模式，对资金安全性进行保障，真正实现运用互联网的特性做到风险碎片化，在体系进行风险的化解。

2.2 网络结构



2.3 系统资产

2.3.1 机房

序号	机房名称	物理位置
1	中国电信东莞东城 IDC 机房(托管)	广东省东莞市东城主山塘边头中国电信大楼 6 楼

2.3.2 网络设备

序号	设备名称	品牌	型号	用途	数量（台/套）	重要程度
1	交换机	思科	思科 WS-C2960-24TC-L	路由器	2	5

2.3.3 安全设备

序号	设备名称	品牌	型号	用途	数量（台/套）	重要程度
1	防火墙 1	Juniper	Juniper SRX550	防火墙	2	5

2.3.4 服务器/存储设备

序号	设备名称	操作系统/数据库管理系统	IP	业务应用软件	数量（台/套）	重要程度
1	后台管理服务器	LINUX	192.168.10.14	你我金融信息服务系统	1	5
2	API 服务器	LINUX	192.168.10.15	你我金融信息服务系统	1	5
3	数据库服务器	LINUX	192.168.10.34	你我金融信息服务系统	1	5
4	mysql	MYSQL	192.168.10.34	你我金融信息服务系统	1	5

2.3.5 业务应用软件

序号	软件名称	主要功能	开发厂商	重要程度
1	你我金融信息服务系统	你我金融信息服务系统是以客户为中心，借款人、担保人、投资人依托此平台进行资金交易，通过担保分散，投资分散，将风险分散化做到极致，同时利用众保的风险管控模式，对资金安全性进行保障，真正实现运用互联网的特性做到风险碎片化，在体系进行风险的化解	自行开发	5

2.3.6 关键数据类别

序号	数据类别	所属业务应用	安全防护需求	重要程度
1	客户基本信息	你我金融信息服务系统	完整性、机密性	5

2.3.7 安全相关人员

序号	姓名	岗位/角色	联系方式
1	刘忠宇	数据库运维经理	略
2	陈敏	人力资源部	略
3	梁绍秦	运维工程师	略
4	黄小鑫	运维工程师	略
5	刘魁	数据库管理员	略

2.3.8 安全管理文档

序号	文档名称	主要内容

序号	文档名称	主要内容
1	《你我金融信息安全方针》	为了保护深圳市你我金融信息服务股份有限公司(以下简称：你我金融）自有的信息资产，积极预防安全事件的发生，最小化信息安全事件的影响，以确保你我金融业务活动的持续性，赢得客户的信任，增强你我金融全员的信息安全意识，贯彻落实信息安全方针及各项控制措施，提高公司竞争力特制定本方针。信息安全管理体系的建立，旨在保护你我金融所有的信息资产，包括属于你我金融配置的信息，客户数据、各类软件硬件、通信、供电设施等。
2	《你我金融信息安全组织建设制度》	为了完善深圳市你我金融信息服务股份有限公司信息安全的组织架构，明确信息安全组织职责，保障信息安全相关政策的贯彻实施，特制定本组织建设说明。
3	《你我金融计算机安全管理制度》	主要内容包括计算机设备安全、计算机软件系统安全、移动存储介质安全、计算机网络安全、电子邮件系统安全、数据备份、计算机病毒防治等。
4	《你我金融存储介质管理制度》	为了明确信息资产存储介质的管理职责、管理规程，防止信息资产由于未授权的泄露、修改、移动或销毁而导致的损失，特制订本细则，以规范信息资产中的各类介质的管理、控制、物理保护等工作。
5	《你我金融电脑设备管理制度》	为加强公司电脑设备管理，提高设备利用率，延长设备使用寿命，合理配置各种设备，控制营运成本，特制定本管理办法。行政管理部是公司电脑设备管理监督部门，统一负责公司电脑设备管理工作。
6	《你我金融计算机病毒防范管理制度》	为了加强公司计算机系统病毒的防范管理，保证计算机系统安全运行，有效防范风险，根据《信息技术管理制度》等相关制度，制定本办法。计算机病毒防范遵循预防为主，事后处理为辅的原则。
7	《你我金融开发上	本流程只要目的旨在定义敏捷实施的整体流程和规范和指

序号	文档名称	主要内容
	线实施流程》	导敏捷实施团队具体执行流程和活动。主要内容包括整体开发模型、需求分析、开发流程、测试管理、上线管理等。
8	《你我金融数据备份管理制度》	为切实贯彻和落实公司信息安全管理制度，实现公司内部部分重要数据的备份、系统的的安全配置、日常维护以及异常处理、建立合理的操作流程，充分发挥数据备份系统软件的作用，保证数据存储的安全，特制定本办法。
9	《你我金融网络安全管理制度》	制定本标准的目的是为了保障深圳市你我金融信息服务股份有限公司(以下简称：你我金融）业务系统安全稳定的运行，加强公司计算机用户网络使用的安全管理。
10	《你我金融系统运行管理制度》	为规范系统运维管理工作，确保系统的安全可靠运行，切实提高生产效率和服务质量，使系统更好的服务与生产运营和管理，特制订本管理办法。系统的维护内容在生产操作层面又分为机房环境维护、计算机硬件平台维护、配套网络维护、基础软件维护、应用软件维护等五部分。
11	《你我金融系统运行整体应急预案》	为了规范对系统异常、安全等突发事件的预防及处置，最大限度地预防和减少信息安全突发事件及其造成的损害和影响，保障基础网络和系统的安全稳定运行，维护正常的生产秩序，特制订本文档。坚持“安全第一、预防为主”，立足安全防护，加强预警，技术中心要重点保护基础信息网络和核心业务系统，按照“谁主管、谁负责，谁运营、谁负责”的要求，实行“统一领导、分级负责、各司其职、协调配合”。
12	《你我金融信息系统变更管理制度》	本办法应用于所有对公司信息系统进行改动的行为，包括系统的软件升级和变更、系统设置变更、操作规程变更等。任何可能使得公司信息系统发生变化的行为，包括硬件设备和软件的变更，包括子系统的增加、打补丁、升级、运行模式改变等。所有可能导致信息系统变化的行为，都需

序号	文档名称	主要内容
		要进行技术评估、测试，才能上线操作。
13	《你我金融应用服务日常管理制度》	本细则作为《你我金融网络安全管理制度.doc》的补充文档。明确规定公司所有对互联网提供应用服务的开放和管理原则；适用于 WWW、API、后台管理、天秤系统服务等等在内的所有提供应用的服务、所有正式运行系统、测试系统以及其他临时使用的系统服务以及公司自有应用系统，以及所有托管、合作单位的业务系统。
14	《你我金融员工信息安全管理制度》	为了保障深圳市你我金融信息服务股份有限公司（以下简称本公司）的计算机信息系统安全，规范办公环境中的计算机使用行为，编制本手册。编制《员工信息安全手册》目的在于使每位员工了解本公司信息系统安全相关规定。
15	《你我金融数据库日常管理制度》	为规范深圳市你我金融信息服务股份有限公司技术中心数据运维组数据库系统的日常工作，确保数据库系统安全稳定运行，特制订本规范。内容主要是数据维护服务、数据环境服务等的管理要求。

2.4 安全服务

序号	安全服务名称	安全服务商
1	无	无

2.5 安全环境威胁评估

描述被测信息系统的运行环境中与安全相关的部分，并以列表形式给出被测信息系统的威胁列表。

序号	威胁种类	威胁分(子）类	描述
1	物理环境威胁	断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等	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

2	物理攻击	物理破坏、盗窃等	通过物理的接触造成对设备的破坏以及实施盗窃造成的影响
3	软硬件故障	设备硬件故障、传输设备故障、存储媒体故障、系统软件故障、应用软件故障、数据库软件故障、开发环境故障等	由于设备硬件故障、通讯链路中断、系统本身或软件 BUG 导致对业务稳定运行的影响
4	误操作	维护错误、操作失误等	在正常工作或使用过程中，由于操作不当而造成的影响
5	恶意代码	病毒、后门、窃听软件等	受到病毒、蠕虫、逻辑炸弹、木马后门等恶意代码的攻击可能造成的影响
6	越权或滥用	非授权访问网络资源、非授权访问系统资源、滥用权限非正常修改系统配置或数据、滥用权限泄露秘密信息等	没有权限的用户试图非法访问，或者较低权限的用户试图越权访问，从而做出破坏系统的行为
7	黑客攻击技术	网络探测和信息采集、漏洞探测、嗅探（帐号、口令、权限等）	利用黑客攻击工具和技术，对系统进行攻击和入侵
8	蓄意泄密	用户身份伪造和欺骗、用户或业务数据的窃取和破坏、系统运行的控制和破坏等	有意造成的机密信息外泄
9	非法篡改	篡改网络配置或系统配置信息、篡改安全配置信息、篡改用户身份信息或业务数据信息等	破坏信息的完整性
10	抵赖	接收者抵赖、发送者抵赖	用户否认其行为，无法确认其责任性
11	社会工程学攻击	流氓软件、网络钓鱼、垃圾邮件、诈骗等	利用人为的漏洞缺陷并采用欺骗手段进行攻击的手段
12	拒绝服务	黑客攻击、带宽不足、性能不足等	由于系统处理能力、网络带宽能力以及黑客攻击，可能造成系统无法提供正常服务

2.6 前次测评情况

本次测评是被测系统的第一次等级测评。

3 等级测评范围与方法表

3.1 测评指标

测评指标包括基本指标和特殊指标两部分。

3.1.1 基本指标

依据信息系统确定的业务信息安全保护等级和系统服务安全保护等级，选择《基本要求》中对应级别的安全要求作为等级测评的基本指标，以表格形式在表 3-1 中列出。

表 3-1 基本指标

安全分类	安全子类	测评项数	安全分类	安全子类	测评项数
物理安全	物理位置选择	2	安全管理制度	管理制度	4
	物理访问控制	4		制定和发布	5
	防盗窃和防破坏	6		评审和修订	2
	防雷击	3	安全管理机构	岗位设置	4
	防火	3		人员配备	3
	防水和防潮	4		授权和审批	4
	防静电	2		沟通和合作	5
	温湿度控制	1		审核和检查	4
	电力供应	4	人员安全管理	人员录用	4
	电磁防护	3		人员离岗	3
网络安全	结构安全	7		人员考核	3
	访问控制	8		安全意识教育和培训	4
	安全审计	4		外部人员访问管理	2

安全分类	安全子类	测评项数	安全分类	安全子类	测评项数
	边界完整性检查	2	系统建设管理	系统定级	4
	入侵防范	2		安全方案设计	5
	恶意代码防范	2		产品采购和使用	4
	网络设备防护	8		自行软件开发	5
主机安全	身份鉴别	6		外包软件开发	4
	访问控制	7		工程实施	3
	安全审计	6		测试验收	5
	剩余信息保护	2		系统交付	5
	入侵防范	3		系统备案	3
	恶意代码防范	3		等级测评	4
	资源控制	5		安全服务商选择	3
应用安全	身份鉴别	5	系统运维管理	环境管理	4
	访问控制	6		资产管理	4
	安全审计	4		介质管理	6
	剩余信息保护	2		设备管理	5
	通信完整性	1		监控管理和安全管理中心	3
	通信保密性	2		网络安全管理	8
	抗抵赖	2		系统安全管理	7
	软件容错	2		恶意代码防范管理	4
	资源控制	7		密码管理	1
数据安全及备份恢复	数据完整性	2		变更管理	4
	数据保密性	2		备份与恢复管理	5
	备份和恢复	4		安全事件处置	6
	—	—		应急预案管理	5

3.1.2 不适用指标

鉴于信息系统的复杂性和特殊性，《基本要求》的某些要求项可能不适用于整个信息系统，对于这些不适用项应在表后给出不适用原因。

表 3-2 不适用指标

安全层面	安全控制点	不适用项	原因说明
网络安全-全局	访问控制	h）应限制具有拨号访问权限的用户数量。	无拨号访问用户。
主机安全 OS	访问控制	f）应对重要信息资源设置敏感标记；	API 服务器: 操作系统不支持强制访问控制策略，故此项不适用。 后台管理服务器: 操作系统不支持强制访问控制策略，故此项不适用。 数据库服务器: 操作系统不支持强制访问控制策略，故此项不适用。
主机安全 OS	访问控制	g）应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。	API 服务器: 操作系统不支持强制访问控制策略，故此项不适用。 后台管理服务器: 操作系统不支持强制访问控制策略，故此项不适用。 数据库服务器: 操作系统不支持强制访问控制策略，故此项不适用。

安全层面	安全控制点	不适用项	原因说明
主机安全 OS	恶意代码防范	a)应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；	API 服务器: 操作系统为 LINUX，没有适用的防恶意代码软件。 后台管理服务器: 操作系统为 LINUX，没有适用的防恶意代码软件。 数据库服务器: 操作系统为 LINUX，没有适用的防恶意代码软件。
主机安全 OS	恶意代码防范	b）主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；	API 服务器: 操作系统为 LINUX，没有适用的防恶意代码软件。 后台管理服务器: 操作系统为 LINUX，没有适用的防恶意代码软件。 数据库服务器: 操作系统为 LINUX，没有适用的防恶意代码软件。
主机安全 OS	恶意代码防范	c）应支持恶意代码防范的统一管理。	API 服务器: 操作系统为 LINUX，没有适用的防恶意代码软件。 后台管理服务器: 操作系统为 LINUX，没有适用的防恶意代码软件。 数据库服务器: 操作系统为 LINUX，没有适用的防恶意代码软件。

安全层面	安全控制点	不适用项	原因说明
主机安全 OS	资源控制	d）应限制单个用户对系统资源的最大或最小使用限度；	API 服务器: 被测服务器用户量少，无需限制单个用户对资源最大或最小消耗。 后台管理服务器: 被测服务器用户量少，无需限制单个用户对资源最大或最小消耗。 数据库服务器: 被测服务器用户量少，无需限制单个用户对资源最大或最小消耗。
主机安全 DB	身份鉴别	c)启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；	mysql: 被测数据库不支持登录失败处理功能，但跳板机上已启用登录失败处理功能。
主机安全 DB	访问控制	f）应对重要信息资源设置敏感标记；	mysql: 数据库不支持强制访问控制策略，故此项不适用。
主机安全 DB	访问控制	g）应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。	mysql: 数据库不支持强制访问控制策略，故此项不适用。
主机安全 DB	资源控制	d）应限制单个用户对系统资源的最大或最小使用限度；	mysql: 被测数据库用户单一，无需对单个用户最大或最小资源消耗进行限制。
应用安全	访问控制	e）应具有对重要信息资源设置敏感标记的功能；	你我金融信息服务系统: 此项不适用
应用安全	资源控制	g）应提供服务优先级设定功能，并在安装后根据安全策略设定访问帐户或请求进程的优先级，根据优先级分配系统资源。	你我金融信息服务系统: 无优先级

安全层面	安全控制点	不适用项	原因说明
系统建设管理	安全方案设计	a）应根据系统的安全保护等级选择基本安全措施，并依据风险分析的结果补充和调整安全措施；	本次测评为被测单位第一次测评，已承诺依据风险分析结果补充和调整安全措施。
系统建设管理	产品采购和使用	b）应确保密码产品采购和使用符合国家密码主管部门的要求；	未使用密码产品
系统建设管理	外包软件开发	a）应根据开发需求检测软件质量；	无外包软件开发的情况
系统建设管理	外包软件开发	b）应在软件安装之前检测软件包中可能存在的恶意代码；	无外包软件开发的情况
系统建设管理	外包软件开发	c）应要求开发单位提供软件设计的相关文档和使用指南；	无外包软件开发的情况
系统建设管理	外包软件开发	d）应要求开发单位提供软件源代码，并审查软件中可能存在的后门。	无外包软件开发的情况
系统运维管理	密码管理	a）应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。	未使用密码产品

3.1.3 特殊指标

结合被测评单位要求、被测信息系统的实际安全需求以及安全最佳实践经验，以列表形式给出《基本要求》（或行业标准）未覆盖或者高于《基本要求》（或行业标准）的安全要求。

安全层面	安全控制点	特殊要求描述	测评项数
-	-	-	-

3.2 测评对象

3.2.1 测评对象选择方法

依据 GB/T 28449-2012 信息系统安全等级保护测评过程指南的测评对象确定原则和方法，结合资产重要程度赋值结果，描述本报告中测评对象的选择规则和方法。

3.2.2 测评对象选择结果

1）机房

序号	机房名称	物理位置	重要程度
1	中国电信东莞东城 IDC 机房（托管）	广东省东莞市东城主山塘边头中国电信大楼 6 楼	5

2）网络设备

序号	设备名称	型号	用途	重要程度
1	交换机	思科 WS-C2960-24TC-L	路由器	5

3）安全设备

序号	设备名称	型号	用途	重要程度
1	防火墙	Juniper SRX550	边界防护	5

4）服务器/存储设备

序号	设备名称	操作系统/数据库管理系统	IP	重要程度
1	后台管理服务器	LINUX	192.168.10.14	5
2	API 服务器	LINUX	192.168.10.15	5
3	数据库服务器	LINUX	192.168.10.34	5

5）数据库管理系统

序号	数据库系统名称	数据库管理系统类型	IP	重要程度
1	mysql	MYSQL	192.168.10.34	5

6）业务应用软件

序号	软件名称	主要功能	开发厂商	重要程度
1	你我金融信息服务系统	你我金融信息服务系统是以客户为中心，借款人、担保人、投资人依托此平台进行资金交易，通过担保分散，投资分散，将风险分散化做到极致，同时利用众保的风险管控模式，对资金安全性进行保障，真正实现运用互联网的特性做到风险碎片化，在体系进行风险的化解。	自行开发	5

7）访谈人员

序号	姓名	岗位/职责
1	刘忠宇	数据库运维经理
2	陈敏	人力资源部
3	梁绍秦	运维工程师
4	黄小鑫	运维工程师
5	刘魁	数据库管理员

8）安全管理文档

序号	文档名称	主要内容
1	《你我金融信息安全方针》	为了保你我金融自有的信息资产，积极预防安全事件的发生，最小化信息安全事件的影响，以确保你我金融业务活动的持续性，赢得客户的信任，增强你我金融全员的信息安全意识，贯彻落实信息安全方针及各项控制措施，提高公司竞争力特制定本方针。信息安全管理体系的建立，旨

序号	文档名称	主要内容
		在保护你我金融所有的信息资产，包括属于你我金融配置的信息，客户数据、各类软件硬件、通信、供电设施等。
2	《你我金融信息安全组织建设制度》	为了完善深圳市你我金融信息服务股份有限公司信息安全的组织架构，明确信息安全组织职责，保障信息安全相关政策的贯彻实施，特制定本组织建设说明。
3	《你我金融计算机安全管理制度》	主要内容包括计算机设备安全、计算机软件系统安全、移动存储介质安全、计算机网络安全、电子邮件系统安全、数据备份、计算机病毒防治等。
4	《你我金融存储介质管理制度》	为了明确信息资产存储介质的管理职责、管理规程，防止信息资产由于未授权的泄露、修改、移动或销毁而导致的损失，特制订本细则，以规范信息资产中的各类介质的管理、控制、物理保护等工作。
5	《你我金融电脑设备管理制度》	为加强公司电脑设备管理，提高设备利用率，延长设备使用寿命，合理配置各种设备，控制营运成本，特制定本管理办法。行政管理部是公司电脑设备管理监督部门，统一负责公司电脑设备管理工作。
6	《你我金融计算机病毒防范管理制度》	为了加强公司计算机系统病毒的防范管理，保证计算机系统安全运行，有效防范风险，根据《信息技术管理制度》等相关制度，制定本办法。计算机病毒防范遵循预防为主，事后处理为辅的原则。
7	《你我金融开发上线实施流程》	本流程只要目的旨在定义敏捷实施的整体流程和规范和指导敏捷实施团队具体执行流程和活动。主要内容包括整体开发模型、需求分析、开发流程、测试管理、上线管理等。
8	《你我金融数据备份管理制度》	为切实贯彻和落实公司信息安全管理制度，实现公司内部部分重要数据的备份、系统的的安全配置、日常维护以及异常处理、建立合理的操作流程，充分发挥数据备份系统软件的作用，保证数据存储的安全，特制定本办法。

序号	文档名称	主要内容
9	《你我金融网络安全管理制度》	制定本标准的目的是为了保障深圳市你我金融信息服务股份有限公司(以下简称：你我金融）业务系统安全稳定的运行，加强公司计算机用户网络使用的安全管理。
10	《你我金融系统运行管理制度》	为规范系统运维管理工作，确保系统的安全可靠运行，切实提高生产效率和服务质量，使系统更好的服务与生产运营和管理，特制订本管理办法。系统的维护内容在生产操作层面又分为机房环境维护、计算机硬件平台维护、配套网络维护、基础软件维护、应用软件维护等五部分。
11	《你我金融系统运行整体应急预案》	为了规范对系统异常、安全等突发事件的预防及处置，最大限度地预防和减少信息安全突发事件及其造成的损害和影响，保障基础网络和系统的安全稳定运行，维护正常的生产秩序，特制订本文档。坚持“安全第一、预防为主”，立足安全防护，加强预警，技术中心要重点保护基础信息网络和核心业务系统，按照“谁主管、谁负责，谁运营、谁负责”的要求，实行“统一领导、分级负责、各司其职、协调配合”。
12	《你我金融信息系统变更管理制度》	本办法应用于所有对公司信息系统进行改动的行为，包括系统的软件升级和变更、系统设置变更、操作规程变更等。任何可能使得公司信息系统发生变化的行为，包括硬件设备和软件的变更，包括子系统的增加、打补丁、升级、运行模式改变等。所有可能导致信息系统变化的行为，都需要进行技术评估、测试，才能上线操作。
13	《你我金融应用服务日常管理制度》	本细则作为《你我金融网络安全管理制度.doc》的补充文档。明确规定公司所有对互联网提供应用服务的开放和管理原则；适用于 WWW、API、后台管理、天秤系统服务等等在内的所有提供应用的服务、所有正式运行系统、测试系统以及其他临时使用的系统服务以及公司自有应用系统，

序号	文档名称	主要内容
		以及所有托管、合作单位的业务系统。
14	《你我金融员工信息安全管理制度》	为了保障深圳市你我金融信息服务股份有限公司（以下简称本公司）的计算机信息系统安全，规范办公环境中的计算机使用行为，编制本手册。编制《员工信息安全手册》目的在于使每位员工了解本公司信息系统安全相关规定。
15	《你我金融数据库日常管理制度》	为规范深圳市你我金融信息服务股份有限公司技术中心数据运维组数据库系统的日常工作，确保数据库系统安全稳定运行，特制订本规范。内容主要是数据维护服务、数据环境服务等的管理要求。

3.3 测评方法

安全测评的主要方法有：访谈、检查和测试。

a） 访谈

访谈是指测评人员通过与信息系统有关人员（个人/群体）进行交流、讨论等活动，获取相关证据以表明信息系统安全保护措施是否有效落实的一种方法。在访谈范围上，应基本覆盖所有的安全相关人员类型，在数量上可以抽样。

b） 检查

检查是指测评人员通过对测评对象进行观察、查验、分析等活动，获取相关证据以证明信息系统安全保护措施是否有效实施的一种方法。在检查范围上，应基本覆盖所有的对象种类（设备、文档、机制等），数量上可以抽样。

c） 测试

测试是指测评人员针对测评对象按照预定的方法/工具使其产生特定的响应,通过查看和分析响应的输出结果，获取证据以证明信息系统安全保护措施是否得以有效实施的一种方法。在测试范围上，应基本覆盖不同类型的机制，在数量上可以抽样。

主要使用到的测评工具有：扫描工具、嗅探工具等。具体描述如下表所示：

序号	工具名称	工具描述
1	绿盟安全评估系统 RSAS	可以对操作系统，网络设备和数据库的等多种设备的扫描规则库，漏洞库遵循 CVE，CAN 和 MS 等国际标准。
2	网络侦听工具集	网络数据包侦听工具。

4 单元测评

单元测评内容包括“3.1.1 基本指标”以及“3.1.3 特殊指标”中涉及的安全层面，内容由问题分析和结果汇总等两个部分构成，详细结果记录及符合程度参见报告附录 A。

4.1 物理安全

4.1.1 结果汇总

针对不同安全控制点对单个测评对象在物理安全层面的单项测评结果进行汇总和统计。

表 4-1 物理安全-单元测评结果汇总表

序号	测评对象	符合情况	安全控制点									
			物理位置的选择	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	中国电信东莞东城 IDC 机房（托管）	符合	2	4	6	3	3	4	2	1	4	3
		部分符合	0	0	0	0	0	0	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

4.1.2 结果分析

被测系统在物理安全层面满足《信息安全技术 信息系统安全等级保护基本要求》中对应级别的安全要求。

4.2 网络安全

4.2.1 结果汇总

针对不同安全控制点对单个测评对象在网络安全层面的单项测评结果进行汇总和统计。

表 4-2 网络安全-单元测评结果汇总表

序号	测评对象	符合情况	安全控制点						
			结构安全	访问控制	安全审计	边界完整性检查	入侵防范	恶意代码防范	网络设备防护
1	网络全局	符合	7	7	3	2	2	2	-
		部分符合	0	0	1	0	0	0	-
		不符合	0	0	0	0	0	0	-
		不适用	0	1	0	0	0	0	-
1	防火墙	符合	-	-	-	-	-	-	7
		部分符合	-	-	-	-	-	-	0
		不符合	-	-	-	-	-	-	1
		不适用	-	-	-	-	-	-	0
2	交换机	符合	-	-	-	-	-	-	7
		部分符合	-	-	-	-	-	-	0
		不符合	-	-	-	-	-	-	1
		不适用	-	-	-	-	-	-	0

4.2.2 结果分析

1）安全审计

a）项部分符合。

被测单位未采用审计工具对管理员的操作记录进行日志记录。

2）网络设备防护

d）项不符合。

网络设备只采用用户名密码一种鉴别技术对管理员进行身份鉴别。

4.3 主机安全 OS

4.3.1 结果汇总

针对不同安全控制点对单个测评对象在主机安全层面的单项测评结果进行汇总和统计。

表 4-3 主机安全 OS-单元测评结果汇总表

序号	测评对象	符合情况	安全控制点						
			身份鉴别	访问控制	安全审计	剩余信息保护	入侵防范	恶意代码防范	资源控制
1	API 服务器	符合	6	5	6	2	3	0	4
		部分符合	0	0	0	0	0	0	0
		不符合	0	0	0	0	0	0	0
		不适用	0	2	0	0	0	3	1
2	后台管理服务器	符合	6	5	6	2	3	0	4
		部分符合	0	0	0	0	0	0	0
		不符合	0	0	0	0	0	0	0
		不适	0	2	0	0	0	3	1

序号	测评对象	符合情况	安全控制点						
			身份鉴别	访问控制	安全审计	剩余信息保护	入侵防范	恶意代码防范	资源控制
		用							
3	数据库服务器	符合	6	5	6	2	3	0	4
		部分符合	0	0	0	0	0	0	0
		不符合	0	0	0	0	0	0	0
		不适用	0	2	0	0	0	3	1

4.3.2 结果分析

被测系统在主机安全(OS）层面满足《信息安全技术 信息系统安全等级保护基本要求》中对应级别的安全要求。

4.4 主机安全 DB

4.4.1 结果汇总

针对不同安全控制点对单个测评对象在主机安全层面的单项测评结果进行汇总和统计。

表 4-4 主机安全 DB-单元测评结果汇总表

序号	测评对象	符合情况	安全控制点						
			身份鉴别	访问控制	安全审计	剩余信息保护	入侵防范	恶意代码防范	资源控制
1	mysql	符合	5	5	6	-	-	-	4
		部分符合	0	0	0	-	-	-	0
		不符合	0	0	0	-	-	-	0
		不适用	1	2	0	-	-	-	1

4.4.2 结果分析

被测系统在主机安全(DB）层面满足《信息安全技术 信息系统安全等级保护基本要求》中对应级别的安全要求。

4.5 应用安全

4.5.1 结果汇总

表 4-5 应用安全-单元测评结果汇总表

序号	测评对象	符合情况	安全控制点								
			身份鉴别	访问控制	安全审计	剩余信息保护	通信完整性	通信保密性	抗抵赖	软件容错	资源控制
1	你我金融信息服务系统	符合	5	4	4	2	1	2	2	2	6
		部分符合	0	0	0	0	0	0	0	0	0
		不符合	0	0	0	0	0	0	0	0	0
		不适用	0	2	0	0	0	0	0	0	1

4.5.2 结果分析

被测系统在应用安全层面满足《信息安全技术 信息系统安全等级保护基本要求》中对应级别的安全要求。

4.6 数据安全及备份恢复

4.6.1 结果汇总

表 4-6 数据安全-单元测评结果汇总表

序号	符合情况	安全控制点		
		数据完整性	数据保密性	备份与恢复

序号	符合情况	安全控制点		
		数据完整性	数据保密性	备份与恢复
1	符合	2	2	4
	部分符合	0	0	0
	不符合	0	0	0
	不适用	0	0	0

4.6.2 结果分析

被测系统在数据安全及备份恢复层面满足《信息安全技术 信息系统安全等级保护基本要求》中对应级别的安全要求。

4.7 安全管理制度

4.7.1 结果汇总

表 4-7 安全管理制度-单元测评结果汇总表

序号	符合情况	安全控制点		
		管理制度	制定和发布	评审和修订
1	符合	4	5	2
	部分符合	0	0	0
	不符合	0	0	0
	不适用	0	0	0

4.7.2 结果分析

被测系统在安全管理制度层面满足《信息安全技术 信息系统安全等级保护基本要求》中对应级别的安全要求。

4.8 安全管理机构

4.8.1 结果汇总

表 4-8 安全管理机构-单元测评结果汇总表

序号	符合情况	安全控制点				
		岗位设置	人员配备	授权和审批	沟通和合作	审核和检查
1	符合	4	2	3	4	1
	部分符合	0	0	0	0	0
	不符合	0	1	1	1	3
	不适用	0	0	0	0	0

4.8.2 结果分析

1）人员配备

b）项不符合。

被测单位没有配备专职的安全管理员。

2）授权和审批

c）项不符合。

被测单位没有定期对审批事项进行审查。

3）沟通和合作

e）项不符合。

被测单位没有聘请信息安全专家作为常年的安全顾问。

4）审核和检查

b）、c）、d）项不符合。

被测单位目前没有内部人员或上级单位对信息系统进行全面安全检查；没有制定安全检查列表；没有制定安全审核和安全检查制度。

4.9 人员安全管理

4.9.1 结果汇总

表 4-9 人员安全管理-单元测评结果汇总表

序号	符合情况	安全控制点				
		人员录用	人员离岗	人员考核	安全意识培训和教育	外部人员访问管理
1	符合	4	3	3	2	2
	部分符合	0	0	0	0	0
	不符合	0	0	0	2	0
	不适用	0	0	0	0	0

4.9.2 结果分析

1）安全意识教育和培训

c）、d）项不符合。

被测单位没有建立安全教育和培训计划；无法提供安全教育和培训记录。

4.10 系统建设管理

4.10.1 结果汇总

表 4-10 系统建设管理-单元测评结果汇总表

序号	符合情况	安全控制点										
		系统定级	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	系统备案	等级测评	安全服务商选择
1	符合	4	2	4	4	3	3	4	5	3	4	0

序号	符合情况	安全控制点										
		系统定级	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	系统备案	等级测评	安全服务商选择
	部分符合	0	0	0	0	0	0	0	0	0	0	0
	不符合	0	3	0	1	0	0	1	0	0	0	3
	不适用	0	0	0	0	1	0	0	0	0	0	0

4.10.2 结果分析

1）安全方案设计

c）、d）、e）项不符合。

被测单位没有由总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案形成的配套文件。

2）自行软件开发

c）项不符合。

目前没有制定代码编写规范。

3）测试验收

a）项不符合。

仅有研发技术人员进行功能和性能测试，未委托第三方进行安全性测试，没有安全性测试报告。

4）安全服务商选择

a）、b）、c）项不符合。

被测单位没有选择安全服务商。

4.11 系统运维管理

4.11.1 结果汇总

表 4-11 系统运维管理-单元测评结果汇总表

序号	符合情况	安全控制点												
		环境管理	资产管理	介质管理	设备管理	监控管理和安全管理中心	网络安全管理	系统安全管理	恶意代码防范管理	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
1	符合	4	3	4	5	2	8	5	3	1	3	4	5	2
	部分符合	0	0	0	0	1	0	0	0	0	0	0	0	0
	不符合	0	1	2	0	0	0	2	1	0	1	1	1	3
	不适用	0	0	0	0	0	0	0	0	0	0	0	0	0

4.11.2 结果分析

1）资产管理

d）项不符合。

被测单位没有制定信息分类与标识文档。

2）介质管理

c）、f）项不符合。

被测单位未对存储介质进行定期盘点；重要介质中的数据和软件未采取加密存储。

3）监控管理和安全管理中心

b）项部分符合。

被测单位没有对系统监控记录进行分析评审。

4）系统安全管理

e）、g）项不符合。

存在两名管理员共用同一个账号的情况；没有定期对运行日志和审计结果进行分析。

5）恶意代码防范管理

d）项不符合。

没有定期检查信息系统内各种产品的恶意代码库的升级情况，没有书面的报表和总结汇报。

6）变更管理

d）项不符合。

没有建立建立中止变更并从失败变更中恢复的文件化程序。

7）备份与恢复管理

e）项不符合。

没有定期执行备份恢复测试。

8）安全事件处置

f）项不符合。

对造成系统中断和造成信息泄密的安全事件未制定相应的处理程序和报告程序。

9）应急预案管理

c）、d）、e）项不符合。

被测单位没有进行应急预案培训和演练；未对应急预案定期进行审查。

4.12 单元测评小结

4.12.1 控制点符合情况汇总

以表格形式汇总测评结果，表格以不同颜色对测评结果进行区分，部分符合（安全控制点得分在 0 分和 5 分之间，不等于 0 分或 5 分）的安全控制点采用黄色标识，不符合（安全控制点得分为 0 分）的安全控制点采用红色标识。

表 4-12 单元测评结果分类统计表

序号	安全层面	安全控制点	安全控制点得分	符合情况			
				符合	部分符合	不符合	不适用
1	物理安全	物理位置的选择	5.0	2	0	0	0
2		物理访问控制	5.0	4	0	0	0
3		防盗窃和防破坏	5.0	6	0	0	0
4		防雷击	5.0	3	0	0	0
5		防火	5.0	3	0	0	0
6		防水和防潮	5.0	4	0	0	0
7		防静电	5.0	2	0	0	0
8		温湿度控制	5.0	1	0	0	0
9		电力供应	5.0	4	0	0	0
10		电磁防护	5.0	3	0	0	0
11	网络安全	结构安全	5.0	7	0	0	0
12		访问控制	5.0	7	0	0	1
13		安全审计	4.0	3	1	0	0
14		边界完整性检查	5.0	2	0	0	0
15		入侵防范	5.0	2	0	0	0
16		恶意代码防范	5.0	2	0	0	0
17		网络设备防护	4.0	7	0	1	0
18	主机安全	身份鉴别	5.0	6	0	0	0
19		访问控制	5.0	5	0	0	2
20		安全审计	5.0	6	0	0	0

序号	安全层面	安全控制点	安全控制点得分	符合情况			
				符合	部分符合	不符合	不适用
21	OS	剩余信息保护	5.0	2	0	0	0
22		入侵防范	5.0	3	0	0	0
23		恶意代码防范	-	0	0	0	3
24		资源控制	5.0	4	0	0	1
25	主机安全DB	身份鉴别	5.0	5	0	0	1
26		访问控制	5.0	5	0	0	2
27		安全审计	5.0	6	0	0	0
28		剩余信息保护	-	-	-	-	-
29		入侵防范	-	-	-	-	-
30		恶意代码防范	-	-	-	-	-
31		资源控制	5.0	4	0	0	1
32	应用安全	身份鉴别	5.0	5	0	0	0
33		访问控制	5.0	4	0	0	2
34		安全审计	5.0	4	0	0	0
35		剩余信息保护	5.0	2	0	0	0
36		通信完整性	5.0	1	0	0	0
37		通信保密性	5.0	2	0	0	0
38		抗抵赖	5.0	2	0	0	0
39		软件容错	5.0	2	0	0	0
40		资源控制	5.0	6	0	0	1
41	数据安全	数据完整性	5.0	2	0	0	0
42		数据保密性	5.0	2	0	0	0
43		备份和恢复	5.0	4	0	0	0
44	安	管理制度	5.0	4	0	0	0

序号	安全层面	安全控制点	安全控制点得分	符合情况			
				符合	部分符合	不符合	不适用
45	全管理制度	制定和发布	5.0	5	0	0	0
46		评审和修订	5.0	2	0	0	0
47	安全管理机构	岗位设置	5.0	4	0	0	0
48		人员配备	3.8	2	0	1	0
49		授权和审批	4.1	3	0	1	0
50		沟通和合作	4.2	4	0	1	0
51		审核和检查	2.0	1	0	3	0
52	人员安全管理	人员录用	5.0	4	0	0	0
53		人员离岗	5.0	3	0	0	0
54		人员考核	5.0	3	0	0	0
55		安全意识教育和培训	2.5	2	0	2	0
56		外部人员访问管理	5.0	2	0	0	0
57	系统建设管理	系统定级	5.0	4	0	0	0
58		安全方案设计	2.1	2	0	3	0
59		产品采购和使用	5.0	4	0	0	0
60		自行软件开发	4.3	4	0	1	0
61		外包软件开发	5.0	0	0	0	4
62		工程实施	5.0	3	0	0	0
63		测试验收	3.1	4	0	1	0
64		系统交付	5.0	5	0	0	0
65		系统备案	5.0	3	0	0	0
66		等级测评	5.0	4	0	0	0
67		安全服务商选择	0.0	0	0	3	0
68	系	环境管理	5.0	4	0	0	0

序号	安全层面	安全控制点	安全控制点得分	符合情况			
				符合	部分符合	不符合	不适用
69	统运维管理	资产管理	3.2	3	0	1	0
70		介质管理	3.3	4	0	2	0
71		设备管理	5.0	5	0	0	0
72		监控管理和安全管理中心	4.3	2	1	0	0
73		网络安全管理	5.0	8	0	0	0
74		系统安全管理	3.9	5	0	2	0
75		恶意代码防范管理	4.1	3	0	1	0
76		密码管理	5.0	1	0	0	0
77		变更管理	3.2	3	0	1	0
78		备份与恢复管理	4.4	4	0	1	0
79		安全事件处置	4.4	5	0	1	0
80		应急预案管理	1.9	2	0	3	0
统计			341.0	268	3	28	15

4.12.2 安全问题汇总

针对单元测评结果中存在的部分符合项或不符合项加以汇总，形成安全问题列表并计算其严重程度值。依其严重程度取值为 1~5，最严重的取值为 5。安全问题严重程度值是基于对应的测评项权重并结合附录 A 中对应测评项的符合程度进行的。具体计算公式如下：

安全问题严重程度值=（5-测评项符合程度得分）×测评项权重。

表 4-4 安全问题汇总表

问题编号	测评对象	安全层面	安全控制点	测评项	测评项权重	问题严重程度值
1	你我金融信息服务系统	网络安全-全局	安全审计	a）应对网络系统中的网络设备运行状	1.0	3.0

问题编号	测评对象	安全层面	安全控制点	测评项	测评项权重	问题严重程度值
				况、网络流量、用户行为等进行日志记录；		
2	你我金融信息服务系统	网络安全	网络设备防护	d）主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；	1.0	5.0
3	你我金融信息服务系统	应用安全	访问控制	e）应具有对重要信息资源设置敏感标记的功能；	1.0	5.0
4	你我金融信息服务系统	应用安全	访问控制	f）应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。	1.0	5.0
5	你我金融信息服务系统	应用安全	资源控制	g）应提供服务优先级设定功能，并在安装后根据安全策略设定访问帐户或请求进程的优先级，根据优先级分配系统资源。	0.5	2.5
6	你我金融信息服务系统	安全管理机构	人员配备	b）应配备专职安全管理员，不可兼任；	0.5	2.5
7	你我金融信息服务系统	安全管理机构	人员配备	c）关键事务岗位应配备多人共同管理。	0.5	0.5

问题编号	测评对象	安全层面	安全控制点	测评项	测评项权重	问题严重程度值
8	你我金融信息服务系统	安全管理机构	授权和审批	c）应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；	0.2	1.0
9	你我金融信息服务系统	安全管理机构	沟通和合作	e）应聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。	0.2	1.0
10	你我金融信息服务系统	安全管理机构	审核和检查	b）应由内部人员或上级单位定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；	0.5	2.5
11	你我金融信息服务系统	安全管理机构	审核和检查	c）应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报；	0.5	2.5

问题编号	测评对象	安全层面	安全控制点	测评项	测评项权重	问题严重程度值
12	你我金融信息服务系统	安全管理机构	审核和检查	d）应制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动。	0.5	2.5
13	你我金融信息服务系统	人员安全管理	安全意识教育和培训	c）应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训；	1.0	5.0
14	你我金融信息服务系统	人员安全管理	安全意识教育和培训	d）应对安全教育和培训的情况和结果进行记录并归档保存。	0.5	2.5
15	你我金融信息服务系统	系统建设管理	安全方案设计	c）应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成	1.0	5.0

问题编号	测评对象	安全层面	安全控制点	测评项	测评项权重	问题严重程度值
				配套文件；		
16	你我金融信息服务系统	系统建设管理	安全方案设计	d）应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施；	0.5	2.5
17	你我金融信息服务系统	系统建设管理	安全方案设计	e）应根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。	0.5	2.5
18	你我金融信息服务系统	系统建设管理	自行软件开发	c）应制定代码编写安全规范，要求开发人员参照规范编写代码；	0.5	2.5
19	你我金融信	系统建设	外包软件开	a）应根据开发需求	1.0	5.0

问题编号	测评对象	安全层面	安全控制点	测评项	测评项权重	问题严重程度值
	息服务系统	管理	发	检测软件质量；		
20	你我金融信息服务系统	系统建设管理	测试验收	a）应委托公正的第三方测试单位对系统进行安全性测试，并出具安全性测试报告；	0.5	2.5
21	你我金融信息服务系统	系统建设管理	安全服务商选择	a）应确保安全服务商的选择符合国家的有关规定；	0.2	1.0
22	你我金融信息服务系统	系统建设管理	安全服务商选择	b）应与选定的安全服务商签订与安全相关的协议，明确约定相关责任；	0.5	2.5
23	你我金融信息服务系统	系统建设管理	安全服务商选择	c）应确保选定的安全服务商提供技术培训和服务承诺，必要的与其签订服务合同。	0.2	1.0
24	你我金融信息服务系统	系统运维管理	资产管理	d）应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。	0.5	2.5
25	你我金融信息服务系统	系统运维管理	介质管理	c）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，	0.2	1.0

问题编号	测评对象	安全层面	安全控制点	测评项	测评项权重	问题严重程度值
				对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点；		
26	你我金融信息服务系统	系统运维管理	介质管理	f）应对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理。	0.5	2.5
27	你我金融信息服务系统	系统运维管理	监控管理和安全管理中心	b）应组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施；	1.0	2.0
28	你我金融信息服务系统	系统运维管理	系统安全管理	e）应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则；	0.5	2.5
29	你我金融信	系统运维	系统安全管	g）应定期对运行日	0.5	2.5

问题编号	测评对象	安全层面	安全控制点	测评项	测评项权重	问题严重程度值
	息服务系统	管理	理	志和审计数据进行分析，以便及时发现异常行为。		
30	你我金融信息服务系统	系统运维管理	恶意代码防范管理	d）应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。	0.2	1.0
31	你我金融信息服务系统	系统运维管理	变更管理	d）应建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。	0.5	2.5
32	你我金融信息服务系统	系统运维管理	备份与恢复管理	e）应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间	0.2	1.0

问题编号	测评对象	安全层面	安全控制点	测评项	测评项权重	问题严重程度值
				内完成备份的恢复。		
33	你我金融信息服务系统	系统运维管理	安全事件处置	f）对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。	0.5	2.5
34	你我金融信息服务系统	系统运维管理	应急预案管理	c）应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次；	1.0	5.0
35	你我金融信息服务系统	系统运维管理	应急预案管理	d）应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期；	1.0	5.0
36	你我金融信息服务系统	系统运维管理	应急预案管理	e）应规定应急预案需要定期审查和根据实际情况更新的内容，并按照执行。	0.5	2.5

5 整体测评

从安全控制间、层面间、区域间和验证测试等方面对单元测评的结果进行验证、分析和整体评价。

具体内容参见《GB/T 28448 信息安全技术信息系统安全等级保护测评要求》。

5.1 安全控制间安全测评

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。安全功能上的削弱可能会使一个安全控制的引入影响另一个安全控制的功能发挥或者给其带来新的脆弱性，使其在特定环境中不能达到该等级信息系统的安全要求。

特别需要考虑到测评安全控制间的削弱作用。在测评安全控制间的削弱作用时，根据安全控制的具体实现方式和部署方式以及信息系统的实际环境，分析物理安全、网络安全、主机系统安全、应用安全和数据安全等同一层面内的哪些安全技术控制间可能会存在安全功能上的削弱作用。最后根据测评分析结果，综合判断安全控制间的相互作用是否会制约到安全控制的功能发挥或者给其带来新的脆弱性，使其功能削弱。

5.1.1 物理安全

5.1.1.1 物理位置的选择与防水、防潮、防雷击

被测单位机房托管在中国电信东莞东城 IDC 机房，机房环境条件能够满足信息系统业务需求和安全管理需求；未设置对外窗户；未发生过机房和办公场地环境条件引发的安全事件或安全隐患；托管机房具备基本的防震、防风和防雨等能力。

被测机房建筑已部署避雷针等措施，机房通过精密空调来自动调节机房内温湿度的变化，防止机房内水蒸气结露，机房地面铺设有防水围堰，防止地下积水的转移和渗透。

测评结果显示，被测单位机房物理位置的环境条件符合机房选址要求，不易发生自然灾害，对防雷、防水、防潮等控制项起到增强作用。

5.1.1.2 物理访问控制与防盗窃和防破坏

被测机房部署控制人员进出机房的保护措施包括：电子门禁系统、来访全程陪同等；进出机房人员需在机房管理员处身份证信息登记，机房内部署了视频监控系统，进行无死角监控，机房 24 小时值守，值守人员认真执行有关机房出入的管理规定。

被测单位主要设备均放置在机房内并每天巡检。机房内设置了视频监控系统和光电报警系统，当检测到机房内环境和基础设施出现异常，会向管理员及时发出报警信息，摄像头监控范围已覆盖机房所有通道和入口。

测评结果显示，机房的物理访问控制措施安全、可靠，采取的物理访问控制措施能有效防止设备被盗窃、被破坏，并且能够通过电子门禁系统和视频监控系统追溯事故责任，物理访问控制对防盗窃、防破坏起到增强作用。

5.1.2 网络安全

5.1.2.1 结构安全与访问控制

被测系统主要的网络设备的业务处理能力和网络带宽满足高峰期的需要，并具有一定的冗余空间。使用静态路由建立安全的访问路径，并且划分网段。重要网段与其他网段之间使用防火墙进行隔离。

被测系统在防火墙上配置网络访问控制，对数据流进行严格控制，粒度为端口级。网络应用层的信息内容，如 HTTP、TELNET 等协议控制信息实现过滤。会话结束后自动结束会话，根据应用情况配置长连接会话。

测评结果显示，网络访问控制的措施对网络结构安全起到增强作用。

5.1.2.2 安全审计与边界完整性检查

被测单位部署了防火墙对非授权设备私自联到内部网络的行为进行检查和阻断。

被测单位使用 zabbix 监控平台对网络设备运行状况和网络流量进行记录，但未采用技术措施对管理员的操作行为进行日志记录。

测评结果显示，安全审计的控制措施不足对边界完整性检查起到削弱作用。

5.1.3 主机安全

5.1.3.1 身份鉴别、访问控制与安全审计

被测单位管理员使用 Xshell 连接服务器，采用用户名密码+动态密码进行身份鉴别。系统设置了强制密码策略限制密码的长度、复杂度和更换周期。并已启用登录失败处理功能，连接服务器时使用 ssh 协议，具有加密功能，能够防止鉴别信息在传输过程中被窃听。

被测服务器用户权限分配合理，仅授予管理员所需的最小权限。系统管理员和数据库管理员由不同的人员担任，使用不同的帐户进行管理。员工离职后管理员会及时删除帐户，不存在共享帐户。

被测服务器已启用安全审计功能，安全审计能够覆盖登录服务器的所有用户。定期分析审计记录并生成审计报表，采取措施保护审计进程不被中断，并采取措施保护审计记录。

测评结果显示，主机层面的安全审计与身份鉴别、访问控制的安全控制措施之间起到了增强作用。

5.1.4 应用安全

5.1.4.1 身份鉴别与安全审计

应用系统提供了专用的登录模块，使用用户名密码手机验证码双因子身份进行身份标识和鉴别，采用了强制密码策略。

应用系统提供实时日志记录，可查看用户的操作行为。能够对审计记录数据进行统计、分析及生成审计报表。

测评结果显示，身份鉴别的控制措施对安全审计起到了增强作用。

5.2 层面间安全测评

层面间的安全测评主要考虑同一区域内的不同层面之间存在的功能增强、补充和削弱等关联作用。安全功能上的增强和补充可以使两个不同层面上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。安全功能上的削弱会使一个层面上的安全控制影响另一个层面安全控制的功能发挥或者给其带来新的脆弱性。

特别需要考虑到测评层面间的削弱作用。在测评层面间的功能削弱作用时，先根据层面的整合集成方式和信息系统的实际环境，分析哪些安全技术层面间和安全管理方面可能存在安全功能上的削弱作用。根据测评分析结果，综合判断不同层面整合后，一个层面是否影响另一个层面安全功能的发挥或者给其带来新的脆弱性，使其功能削弱。

5.2.1 网络安全、主机安全与应用安全、数据安全

被测单位的主要网络设备和通信线路负载均较低，能够保证高峰的需要，保证系统的高可用性，并且部署了防火墙设备。防火墙上只开放需要访问外部网络的主机指定的应用端口。开启了防火墙的入侵防御模块，对端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等进行监视。

服务器主机上部署了杀毒软件并及时更新病毒库，定期对服务进行扫描，能够及时清除服务器上的病毒。

测评结果显示，网络安全、主机安全的有效措施对应用安全、数据安起到了增强作用。

5.3 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。安全功能上的增强和补充可以使两个不同区域上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。安全功能上的削弱会使一个区域上的安全功能影响另一个区域安全功能的发挥或者给其带来新的脆弱性。

特别需要考虑到测评区域间的削弱作用。在测评区域间的功能削弱作用时，先根据区域间互连互通的集成方式和信息系统的实际环境，特别是区域间的数据流流向和控制方式，分析哪些区域间可能会存在安全功能上的削弱作用。根据测评分析结果，综合判断不同区域互连互通后，一个区域是否影响另一个区域安全功能的发挥或者给其带来新的脆弱性，使其功能削弱。

被测系统主要有广域网接入区、生产网络区、关联业务区及管理区域。

5.4 验证测试

验证测试包括漏洞扫描，渗透测试等，验证测试发现的安全问题对应到相应的测评项的结果记录中。详细验证测试报告见报告附录 B。

若由于用户原因无法开展验证测试，应将用户签章的“自愿放弃验证测试声明”作为报告附件。

5.5 整体测评结果汇总

根据整体测评结果，修改安全问题汇总表中的问题严重程度值及对应的修正后测评项符合程度得分，并形成修改后的安全问题汇总表（仅包括有所修正的安全问题）。可根据整体测评安全控制措施对安全问题的弥补程度将修正因子设为0.5~0.9。

修正后问题严重程度值[1]=修正前的问题严重程度值×修正因子。

修正后测评项符合程度=5-修正后问题严重程度值/测评项权重

表 5-1 修正后的安全问题汇总表

序号	问题编号[2]	安全问题描述	测评项权重	整体测评描述	修正因子	修正后问题严重程度值	修正后测评项符合程度
-	-	-	-	-	-	-	-

6 总体安全状况分析

6.1 系统安全保障评估

以表格形式汇总被测信息系统已采取的安全保护措施情况，并综合附录 A 中的测评项符合程度得分以及 5.5 章节中的修正后测评项符合程度得分（有修正的测评项以 5.5 章节中的修正后测评项符合程度得分带入计算），以算术平均法合并多个测评对象在同一测评项的得分，得到各测评项的多对象平均分。

根据测评项权重（见附件《测评项权重赋值表》，其他情况的权重赋值另行发布），以加权平均合并同一安全控制点下的所有测评项的符合程度得分，并按照控制点得分计算公式得到各安全控制点的 5 分制得分。计算公式为：

[1]问题严重程度值最高为 5。

[2]该处编号与 4.12.2 安全问题汇总表中的问题编号一一对应。

控制点得分=$\frac{\sum_{k=1}^{n}\text{测评项的多对象平均分}\times\text{测评项权重}}{\sum_{k=1}^{n}\text{测评项权重}}$，n 为同一控制点下的测评项数，不含不适用的控制点和测评项。

以算术平均合并同一安全层面下的所有安全控制点得分，并转换为安全层面的百分制得分。根据表格内容描述被测信息系统已采取的有效保护措施和存在的主要安全问题情况。

表 6-1 系统安全保障情况得分表

序号	安全层面	安全控制点	安全控制点得分	安全层面得分
1	物理安全	物理位置的选择	5.0	100.0
2		物理访问控制	5.0	
3		防盗窃和防破坏	5.0	
4		防雷击	5.0	
5		防火	5.0	
6		防水和防潮	5.0	
7		防静电	5.0	
8		温湿度控制	5.0	
9		电力供应	5.0	
10		电磁防护	5.0	
11	网络安全	结构安全	5.0	89.7
12		访问控制	5.0	
13		安全审计	4.0	
14		边界完整性检查	5.0	
15		入侵防范	5.0	
16		恶意代码防范	5.0	
17		网络设备防护	4.0	
18	主机安全(OS）	身份鉴别	5.0	100.0
19		访问控制	5.0	

序号	安全层面	安全控制点	安全控制点得分	安全层面得分
20		安全审计	5.0	
22		剩余信息保护	5.0	
23		入侵防范	5.0	
24		恶意代码防范	-	
25		资源控制	5.0	
26	主机安全(DB）	身份鉴别	5.0	100.0
27		访问控制	5.0	
29		安全审计	5.0	
31		剩余信息保护	-	
32		入侵防范	-	
33		恶意代码防范	-	
34		资源控制	5.0	
35	应用安全	身份鉴别	5.0	100.0
36		访问控制	5.0	
38		安全审计	5.0	
40		剩余信息保护	5.0	
41		通信完整性	5.0	
42		通信保密性	5.0	
43		抗抵赖	5.0	
44		软件容错	5.0	
45		资源控制	5.0	
46	数据安全及备份恢复	数据完整性	5.0	100.0
47		数据保密性	5.0	
48		备份和恢复	5.0	
49	安全管理制度	管理制度	5.0	100.0

序号	安全层面	安全控制点	安全控制点得分	安全层面得分
50		制定和发布	5.0	
51		评审和修订	5.0	
52	安全管理机构	岗位设置	5.0	76.2
53		人员配备	3.8	
54		授权和审批	4.1	
55		沟通和合作	4.2	
56		审核和检查	2.0	
57	人员安全管理	人员录用	5.0	90.0
58		人员离岗	5.0	
59		人员考核	5.0	
60		安全意识教育和培训	2.5	
61		外部人员访问管理	5.0	
62	系统建设管理	系统定级	5.0	80.9
63		安全方案设计	2.1	
64		产品采购和使用	5.0	
65		自行软件开发	4.3	
66		外包软件开发	5.0	
67		工程实施	5.0	
68		测试验收	3.1	
69		系统交付	5.0	
70		系统备案	5.0	
71		等级测评	5.0	
72		安全服务商选择	0.0	
73	系统运维管理	环境管理	5.0	81.1
74		资产管理	3.2	
75		介质管理	3.3	

序号	安全层面	安全控制点	安全控制点得分	安全层面得分
76		设备管理	5.0	
77		监控管理和安全管理中心	4.3	
78		网络安全管理	5.0	
79		系统安全管理	3.9	
80		恶意代码防范管理	4.1	
81		密码管理	5.0	
82		变更管理	3.2	
83		备份与恢复管理	4.4	
84		安全事件处置	4.4	
85		应急预案管理	1.9	

6.2 安全问题风险评估

依据信息安全标准规范，采用风险分析的方法进行危害分析和风险等级判定。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危害，找出可能对信息系统、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严重程度进一步确定信息系统面临的风险等级，结果为“高”、“中”或“低”。并以列表形式给出等级测评发现安全问题以及风险分析和评价情况，参见表 6-2。

其中，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 6-2 信息系统安全问题风险分析表

问题编号	安全层面	问题描述	关联资产[1]	关联威胁[2]	危害分析结果	风险等级
-	-	-	-	-	-	-

[1] 如风险值和评价相同，可填写多个关联资产。

[2]对于多个威胁关联同一个问题的情况，应分别填写。

6.3 等级测评结论

综合上述几章节的测评与风险分析结果，根据符合性判别依据给出等级测评结论，并计算信息系统的综合得分。

等级测评结论应表述为“**符合**、“**基本符合**”或者“**不符合**”。

结论判定及综合得分计算方式见下表：

测评结论	符合性判别依据	综合得分计算公式
符合	信息系统中未发现安全问题，等级测评结果中所有测评项得分均为 5 分。	100 分
基本符合	信息系统中存在安全问题，但不会导致信息系统面临高等级安全风险。	$\frac{\sum_{k=1}^{p} \text{测评项的多对象平均分×测评项权重}}{\sum_{k=1}^{p} \text{测评项权重}} \times 20$，$p$ 为总测评项数，不含不适用的控制点和测评项，有修正的测评项以 5.5 章节中的修正后测评项符合程度得分带入计算。
不符合	信息系统中存在安全问题，而且会导致信息系统面临高等级安全风险。	$60 - \frac{\sum_{j=1}^{l} \text{修正后问题严重程度值}}{\sum_{k=1}^{p} \text{测评项权重}} \times 12$，$l$ 为安全问题数，p 为总测评项数，不含不适用的控制点和测评项。
注：修正后问题严重程度赋值结果取多对象中针对同一测评项的最大值。		

也可根据特殊指标重要程度为其赋予权重，并参照上述方法和综合得分计算公式，得出综合基本指标与特殊指标测评结果的综合得分。

7 问题处置建议

针对被测系统在本次等级测评过程中发现的安全问题，我们提出系统安全建设、整改类建议。整改类建议分为立即整改和持续改进两类。

立即整改类建议表明被测系统存在相应方面的问题，这些问题对信息系统的安全保护能力有较大影响，亟待解决，建议在接收到本报告后，尽可能快地组织人员，研究解决方案和相关技术路线，进行合理、稳妥和有效地改进。

持续改进类建议表明被测系统存在相应方面的问题，但是这些问题目前来说对信息系统的安全保护能力影响不是很大，或者对被测系统来说当前还不是很容易解决，建议在接收到本报告后，选择适当的时机，进行逐步整改、解决。

7.1 物理安全

通过对测评结果的综合分析，结合被测系统的实际情况，本次测评中物理方面未发现不满足要求的问题，因此目前未提出整改类建议，仅提出一般类建议：建议深圳市你我金融信息服务股份有限公司坚持并持续加强物理安全方面的控制措施。

7.2 网络安全

通过对测评结果的全面分析，结合被测系统的实际情况，网络安全方面目前主要存在并有待解决的问题如下：

- 被测单位未采用审计工具对管理员的操作记录进行日志记录；
- 网络设备只采用用户名密码一种鉴别技术对管理员进行身份鉴别。

针对以上问题，我们提出以下改进建议：

持续改进类：

- 采用审计工具对管理员的操作记录进行日志记录；
- 采用两种或两种以上鉴别技术对管理员进行身份鉴别。

7.3 主机安全（OS）

通过对测评结果的综合分析，结合被测系统的实际情况，本次测评中主机安全(OS）方面未发现不满足要求的问题，因此目前未提出整改类建议，仅提出一般类建议：建议深圳市你我金融信息服务股份有限公司坚持并持续加强主机安全(OS）方面的控制措施。

7.4 主机安全（DB）

通过对测评结果的综合分析，结合被测系统的实际情况，本次测评中主机安全(DB）方面未发现不满足要求的问题，因此目前未提出整改类建议，仅提出一般类建议：建议深圳市你我金融信息服务股份有限公司坚持并持续加强主机安全(DB）

方面的控制措施。

7.5 应用安全

通过对测评结果的综合分析，结合被测系统的实际情况，本次测评中应用安全方面未发现不满足要求的问题，因此目前未提出整改类建议，仅提出一般类建议：建议深圳市你我金融信息服务股份有限公司坚持并持续加强应用安全方面的控制措施。

7.6 数据安全

通过对测评结果的综合分析，结合被测系统的实际情况，本次测评中数据安全方面未发现不满足要求的问题，因此目前未提出整改类建议，仅提出一般类建议：建议深圳市你我金融信息服务股份有限公司坚持并持续加强主机安全(DB）方面的控制措施。

7.7 安全管理

通过对测评结果的全面分析，结合被测系统的实际情况，网络安全方面目前主要存在并有待解决的问题如下：

- 被测单位未配备专职的安全管理员；
- 没有定期审查、更新审批项目；
- 未聘请信息安全专家作为常年的安全顾问；
- 目前没有内部人员或上级单位对信息系统进行全面安全检查；
- 没有制定安全检查列表；
- 没有制定安全审核和安全检查制度；
- 被测单位没有建立安全教育和培训计划，没有安全教育和培训记录；
- 被测单位没有由总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案形成的配套文件；
- 未制定代码编写规范；
- 未委托第三方进行安全性测试，没有安全性测试报告；
- 未选定安全服务商；

- 被测单位没有制定信息分类与标识文档；
- 未对存储介质进行定期盘点；
- 重要介质中的数据和软件未采取加密存储；
- 没有对系统监控记录进行分析评审；
- 存在两名管理员共用同一个账号的情况；
- 没有定期对运行日志和审计结果进行分析；
- 没有定期检查信息系统内各种产品的恶意代码库的升级情况，没有书面的报表和总结汇报；
- 没有建立建立中止变更并从失败变更中恢复的文件化程序；
- 没有定期执行备份恢复测试；
- 对造成系统中断和造成信息泄密的安全事件未制定相应的处理程序和报告程序；
- 没有进行应急预案培训和演练；
- 未对应急预案定期进行审查。

针对以上问题，我们提出以下改进建议：

持续改进类：

- 配备专职的安全管理员；
- 授权专人定期对重要审批事项进行审查，发现不适用的审批程序应及时修订；
- 聘请信息安全专家作为常年的安全顾问；
- 信息安全领导层或管理层组织定期进行安全管理评审，检查内容包括检测所采取的安全技术措施是否有效、安全配置和安全策略是否一致、安全管理制度的执行情况等；
- 根据相关的安全标准、企业信息安全战略目标制定详细的安全检查列表，详细记录检查情况，形成检查报告；
- 制定安全审核和安全检查制度，明确要求安全检查和审核过程中的行为规范，确保审核和检查没有遗漏和降低审核和检查所带来的风险；
- 根据不同岗位的安全要求制定培训计划，定期对各岗位进行安全培训，包

括信息安全基础知识、岗位安全技能、岗位操作规程等。

- 根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件；
- 制定代码编写安全规范，要求开发人员参照规范编写代码；
- 委托第三方测试机构对信息系统进行独立的安全性测试，并出具相应测试报告；
- 选择安全服务商；
- 制定信息分类文档，内容应明确信息分类标识的原则和方法；
- 根据介质的目录清单对介质的使用现状进行定期检查，定期对其完整性（数据是否损坏或丢失）和可用性（介质是否受到物理破坏）进行检查；
- 应根据所承载数据和软件的重要性对介质进行分类和标识管理，对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理；
- 定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施；
- 存指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则；
- 定期对运行日志和审计结果进行分析，并出具分析报告；
- 定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报；
- 建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练；
- 定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复；
- 系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序；
- 应急预案的培训应至少每年举办一次；

- 定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期；定期审查应急预案的管理规定，明确应急预案中需要定期审查和根据实际情况更新的内容，并存档应急预案的审查记录。

[正文完]

附录 A 等级测评结果记录

以表格形式给出现场测评结果。符合程度根据被测信息系统实际保护状况进行赋值，完全符合项赋值为 5，其他情况根据被测系统在该测评指标的符合程度赋值为 0~4（取整数值）。

A.1 物理安全

中国电信东莞东城 IDC 机房（托管）

安全控制点	测评指标	结果记录	符合程度
物理位置的选择	a）机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内；	1.机房是否具有基本的防震、防风和防雨等能力： √是 □否 2.是否存在因机房和办公场地环境条件引发的安全事件或安全隐患： □是 √否	5
	b） 机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。	1.机房位于第 6 层。 2.机房场地是否在建筑物的顶层或地下室： □是，采取的补偿性控制措施有：_____ √否 3.机房场地是否在用水设备的下层或隔壁： □是，采取防水措施有：_____ √否	5
物理访问控制	a）机房出入口应安排专人值守，控制、鉴别和记录进入的人员；	1.是否对进入机房人员的身份进行鉴别： √是 □否 2.机房出入口是否安排专人 24 小时值守： √是 □否 3.机房出入口是否部署视频监控系统： √是 □否 4.机房出入口是否部署门禁系统： √是，产品为：电子门禁系统 □否 5.是否对进入机房的人员记录在案： √是，记录内容为：身份证登记	5

安全控制点	测评指标	结果记录	符合程度
		□否	
	b）需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围；	1.是否有来访人员进入机房的申请和审批记录： √是，记录内容为：身份证信息 □否 2.审批记录是否包括来访人员的访问范围： √是 □否	5
	c）应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域；	1.是否对机房进行了划分区域管理： √是 □否 2.是否在机房重要区域前设置交付或安装等过渡区域： √是 □否 3.是否在机房重要区域间设置了有效的物理隔离装置： √是 □否	5
	d）重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。	1.重要区域是否配置的电子门禁系统： √是 □否 2.电子门禁系统目前能否正常工作： √是 □否	5
防盗窃和防破坏	a） 应将主要设备放置在机房内；	1.主要设备是否集中放置在机房内： √是 □否	5
	b）应对设备或主要部件进行固定，并设置明显的无法除去的标记；	1.设备或主要部件是否进行了固定（不易被移动或被搬走）： √是 □否 2.设备或主要部件是否进行了标记： √是，标记内容有：IP 信息 □否 3.设备或主要部件的标记是否明显的不易除去： √是，标记方法是：标签 □否	5
	c）应将通信线缆铺设在隐蔽处，如铺设在地	1.通信线缆是否铺设在隐蔽处： √是，上空架设的管槽内	5

安全控制点	测评指标	结果记录	符合程度
	下或管道中等；	□否_____	
	d）应对介质分类标识，存储在介质库或档案室中；	1.介质是否进行了分类标识： √是 □否 2.介质是否存放在介质库或档案室内进行管理： √是，存放位置是：在线存储 □否	5
	e）应利用光、电等技术设置机房的防盗报警系统，以防进入机房的盗窃和破坏行为；	1.是否利用光、电等技术设置机房的防盗报警系统： √是，产品为：红外声光报警器 □否 2.是否对机房安装的防盗报警系统定期进行维护检查： √是 □否	5
	f）应对机房设置监控报警系统	1.机房是否安装监控报警系统： √是，产品为：视频监控系统 □否 2.是否对机房安装的监控报警系统定期进行维护检查： √是 □否	5
防雷击	a） 机房建筑应设置避雷装置；	1.机房建筑是否设置了避雷装置： √是 □否 2.是否通过验收或国家有关部门的技术检测： √是 □否 3.机房计算机系统接地是否设置了专用地线： √是 □否	5
	b）应设置防雷保安器，防止感应雷；	1.是否设置防雷保安器，在电源和信号线上安装避雷装置： √是 □否 2.该产品是否通过验收或国家有关部门的技术检测： √是 □否	5

安全控制点	测评指标	结果记录	符合程度
		3.是否定期检测防雷装置能否正常工作： √是 □否	
	c）应设置交流电源地线。	1.机房内是否设置交流地线： √是 □否	5
防火	a）应设置火灾自动消防系统，自动检测火情、自动报警，并自动灭火；	1.是否设置了自动检测火情、自动报警、自动灭火的自动消防系统： √是，产品是：七氟丙烷自动消防系统 □否 2.气瓶气压是否正常： √是 □否 3.温/烟感探测器是否定期巡检： √是 □否 4.是否有专人负责维护该系统的运行： √是，负责人为：机房管理员 □否	5
	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；	1.建筑材料是否达到耐火等级： √是 □否	5
	C）机房采取区域隔离防火措施，将重要设备与其他设备隔离开	1.机房是否采取区域隔离防火措施，将重要设备与其他设备隔离开： √是，主机、网络设备、电源、精密空调等，都分组分区域各自放置在不同位置，中间使用钢化防火玻璃隔离。 □否	5
防水和防潮	a）水管安装，不得穿过机房屋顶和活动地板下；	1.机房内是否有穿过屋顶和活动地板下，穿过墙壁和楼板的水管： □是 √否 2.机房内穿过屋顶和活动地板下或穿过墙壁和楼板的水管是否采取了的保护措施： □是，措施有：_____ √否 3.机房是否发生过漏水/返潮事件： □是	5

安全控制点	测评指标	结果记录	符合程度
		√否	
	b）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	1.对机房窗户、屋顶、墙壁是否采取防水措施： √是 □否 2.机房窗户、屋顶、墙壁是否有渗水迹象： □是，迹象为：_____ √否	5
	c）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；	1.机房是否能够防止水蒸气结露和地下积水的转移： √是，措施为：采用精密空调控制机房内温度和湿度，防止水蒸气结露。 □否 2.机房内是否有结露现象： □是，现象为：_____ √否 3.机房内是否有积水现象： □是，现象为：_____ √否	5
	d）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。	1.是否设置水敏感的检测仪表或元件，对机房进行防水检测和报警： □是 √否，托管机房楼层无用水设施，也没有安装水管，精密空调部署在1楼。 2.该仪表或元件是否正常运行，是否有运行记录，是否有人负责其运行管理工作： √是，负责人:机房管理员 □否	5
防静电	a）主要设备应采用必要的接地防静电措施；	1.机房主要设备是否采取了必要的防静电措施（如机柜接地）： √是 □否	5
	b）机房应采用防静电地板。	1.机房是否采用了防静电地板： √是 □否	5
温湿度控制	a）机房应设置温、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。	1.机房是否配备了温湿度自动调节设施，保证温湿度能够满足计算机设备运行的要求： √是，设备为：精密空调 □否 2.温湿度阈值是否设置在标准范围内：	5

安全控制点	测评指标	结果记录	符合程度
		√是 □否 3.是否有过温湿度影响系统运行的事件： □有 √无 4.是否定期对温湿度自动调节设施进行定期检查维护： √有 □无	
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；	1.供电线路上是否设置了稳压器和过电压防护设备： √是，产品为：通过 UPS 作稳压器和过电压防护设备。 □否	5
	b）应提供短期的备用电力供应，至少满足主要设备在断电情况下的正常运行要求；	1.是否设置了短期备用电源设备，供电时间是否满足系统最低电力供应需求： √是 □否 2.是否定期对短期备用电源设备进行检查维护： √是 □否	5
	c）应设置冗余或并行的电力电缆线路为计算机系统供电；	1.是否安装了冗余或并行的电力电缆线路； √是，方式为：双路市电 □否	5
	d）应建立备用供电系统。	1.是否有建立备用供电系统： √是，备用发电机 □否 2.是否定期对备用供电系统进行检查维护： √是 □否	5
电磁防护	a）应采用接地方式防止外界电磁干扰和设备寄生耦合干扰；	1.是否有防止外界电磁干扰和设备寄生耦合干扰的措施： √是，措施为：主要设备外壳做了接地网处理 □否	5
	b）电源线和通信线缆应隔离铺设，避免互相干扰；	1.机房布线是否做到电源线和通信线缆隔离： √是 □否	5
	c）应对关键设备和磁介质实施电磁屏蔽。	1.磁介质是否存放在具有电磁屏蔽功能的容器中： √是	5

安全控制点	测评指标	结果记录	符合程度
		□否	

A.2 网络安全

网络安全全局

安全控制点	测评指标	结果记录	符合程度
结构安全	a）应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；	1.信息系统主要网络设备的CPU处理能力是否满足业务高峰需要： √是，主要网络设备近期CPU利用率维持在30%以下，内存使用率比较低，其性能可以满足业务高峰期需要。 □否	5
	b）应保证网络各个部分的带宽满足业务高峰期需要；	1.网络接入及核心网络的带宽能否满足业务高峰期需要： √是，接入网络和核心网络的带宽满足业务高峰期需要。 □否	5
	c）应在业务终端与业务服务器之间进行路由控制建立安全的访问路径；	1.采用何种路由协议建立访问路径： √静态路由 □动态路由协议，路由协议名称： 2.是否对动态路由协议进行认证加密： □是 √否	5
	d）应绘制与当前运行情况相符的网络拓扑结构图；	1.是否有网络拓扑图： √是 □否 2.网络拓扑图与当前运行情况是否一致： √是 □否	5
	e）应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；	1.是否进行了网段划分： √是，划分为业务、程序、数据库等。 □否	5

	f）应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段；	1.是否将重要网段部署在网络边界处直接连接外部信息系统： □是 √否 2.重要网段与其他网段之间是否采取可靠的技术隔离手段： √是，隔离手段是：部署防火墙 □否	5
	g）应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。	1.是否进行了带宽优先级分配： √是，采取技术是：软件负载均衡 □否	5
安全审计	a）应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；	1.是否采用监控平台对网络设备运行状态监控： √是，监控平台名称：Zabbix □否 2.是否采用监控平台对网络流量进行监控： √是，监控平台名称：Zabbix □否 3、是否采用审计工具记录用户行为： □是，审计工具名称： √否	2
	b）对于每一个事件，其审计记录应包括：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；	1.是否能够记录事件的审计信息： √是 □否 2.审计记录的主要内容包含但不限于： √事件的日期和时间 √用户 √事件类型 √事件是否成功 √其他：	5
	c）安全审计应根据记录数据进行分析，并生成审计报表；	1.是否定期对日志事件进行分析和统计并生成报表： √是月报、季度、年度报告。 □否	5
	d）应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。	1.是否对审计记录进行保护，避免受到未预期的删除、修改或覆盖等： √是，保护措施是：专人管理 □否	5

边界完整性检查	a）应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断；	1.是否对非授权设备私自联到内部网络的行为进行监控： √是，控制措施是：服务器、网络设备托管在 IDC，有严格控制，单位内部采用 IP/MAC 绑定技术可以防止非授权设备私自联到内部网络。 □否 2.是否能够及时发现并阻断非授权设备私自联到内部网络： √是上网行为管理系统能够监控、定位。 □否	5
	b）应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。	1.是否对非授权设备私自联到外部网络的行为进行监控： √是，控制措施是：服务器、网络设备托管在 IDC，有严格控制。 □否 2.是否能够及时发现或阻断非授权设备私自联到外部网络： √是单位内部终端通过上网行为管理系统进行监控、阻断私自联到外网的行为。 □否	5
入侵防范	a）应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；	1.在网络边界处是否部署了包含入侵防范功能的设备： √是，设备名称：通过防火墙、Nginx 入侵模块进行入侵检测。 □否 2.入侵防范设备可以监视以下攻击行为： √端口扫描 √强力攻击 √木马后门攻击 √拒绝服务攻击 √缓冲区溢出攻击 √IP 碎片攻击 √网络蠕虫攻击	5
	b）当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。	1.检测到攻击行为时，记录以下的信息包括： √攻击源 IP √攻击类型 √攻击目的 √攻击时间 2.发生严重入侵事件时是否提供报警信息： √是，报警方式为：邮件报警 □否	5

恶意代码防范	a）应在网络边界处对恶意代码进行检测和清除；	1.在网络边界处是否部署了防恶意代码产品： √是，产品名：卡巴斯基防病毒服务器。 □否 2.防恶意代码产品的是否有日志记录： √是 □否	5
	b）应维护恶意代码库的升级和检测系统的更新。	1.是否对防恶意代码产品的特征库进行升级： √是，升级方式：实时更新 □否 2.恶意代码库是否为最新版本： √是 □否	5
访问控制	a）应在网络边界部署访问控制设备，启用访问控制功能；	1.在网络边界处是否部署了访问控制设备： √是网络边界部署了防火墙，并启用访问控制策略。 □否 2.访问控制设备是否启用访问控制策略： √是 □否	5
	b）应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级；	1.访问控制设备的控制粒度是否达到端口级： √是根据业务性质明确的允许/拒绝访问的控制，控制粒度为端口级。 □否	5
	c）应对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制；	1.访问控制设备是否对进出网络的信息内容进行过滤： √是 □否	5
	d）应在会话处于非活跃一定时间或会话结束后终止网络连接；	1.访问控制设备是否设置会话处于非活跃的时间或会话结束后自动终止网络连接： √是 □否	5
	e）应限制网络最大流量数及网络连接数；	1.访问控制设备是否能限制网络最大流量数及网络连接数： √是 □否	5
	f）重要网段应采取技术手段防止地址欺骗；	1.重要网段是否采取技术手段防止地址欺骗： √是通过绑定 IP/MAC 地址等措施防止地址欺骗。 □否	5

	g）应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户；	1.网络系统是否有 VPN 接入用户： √是，VPN 设备名称：部署了 VPN 设备，用于运维管理，限制 IP/主机名。 □否 2.VPN 设备是否限制单个用户的访问资源： √是 □否	5
	h）应限制具有拨号访问权限的用户数量。	1.网络系统是否有拨号访问用户： □是，拨号设备名称： √否 2.拨号设备是否限制用户数量： □是，最大数量： √否 N/A 无拨号访问用户。	N/A

交换机

安全控制点	测评指标	结果记录	符合程度
网络设备防护	a）应对登录网络设备的用户进行身份鉴别；	1.是否可以对登录网络设备的用户进行身份鉴别： √是，用户名密码。 □否	5
	b）应对网络设备的管理员登录地址进行限制；	1.是否对网络设备管理员的登录地址进行限制： √是，登录地址范围：网络设备的管理必须通过 VPN，VPN 设备对连接客户端进行限制。 □否	5
	c）网络设备用户的标识应唯一；	1.是否为网络设备的管理员建立独立账户： √是网络设备用户标识唯一，不同用户不能使用同一标识 □否	5
	d）主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；	1.网络设备是否采取两种或两种以上组合鉴别技术进行身份鉴别： □是，鉴别方式： √否	0
	e）身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；	1.管理员使用的口令是否有复杂度要求： √是，口令复杂度要求：口令符合复杂度要求（12 位，2 种字符组合） □否 2.管理员使用的口令是否有强制定期更换的要求： √是，口令更换周期：半年更改一次 □否	5

	f）应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；	1.是否有登录失败处理功能： √是 □否 2.采取的措施包括： √结束会话 √限制非法登录次数，帐户锁定阈值：5 次 √设置连接超时自动退出，超时时间：10 分钟	5
	g）当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；	1.是否允许对网络设备进行远程管理： √是 □否 2.是否采用加密的网络协议进行远程管理： √是，加密协议为：HTTPS □否	5
	h）应实现设备特权用户的权限分离。	1.是否区分不同用户的操作权限，实现设备特权用户的权限分离： √是 □否 2.设备的特权用户包括： √系统管理员 √安全管理员 √安全审计员 √其他：	5

防火墙

安全控制点	测评指标	结果记录	符合程度
网络设备防护	a）应对登录网络设备的用户进行身份鉴别；	1.是否可以对登录网络设备的用户进行身份鉴别： √是，用户名密码。 □否	5
	b）应对网络设备的管理员登录地址进行限制；	1.是否对网络设备管理员的登录地址进行限制： √是，登录地址范围：网络设备的管理必须通过 VPN，VPN 设备对连接客户端进行限制。 □否	5
	c）网络设备用户的标识应唯一；	1.是否为网络设备的管理员建立独立账户： √是网络设备用户标识唯一，不同用户不能使用同一标识 □否	5
	d）主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；	1.网络设备是否采取两种或两种以上组合鉴别技术进行身份鉴别： □是，鉴别方式： √否	0

安全控制点	测评指标	结果记录	符合程度
	e）身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；	1.管理员使用的口令是否有复杂度要求： √是，口令复杂度要求：口令符合复杂度要求（12位，2种字符组合） □否 2.管理员使用的口令是否有强制定期更换的要求： √是，口令更换周期：半年更改一次 □否	5
	f）应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；	1.是否有登录失败处理功能： √是 □否 2.采取的措施包括： √结束会话 √限制非法登录次数，帐户锁定阈值：5次 √设置连接超时自动退出，超时时间：10分钟	5
	g）当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；	1.是否允许对网络设备进行远程管理： √是 □否 2.是否采用加密的网络协议进行远程管理： √是，加密协议为：HTTPS □否	5
	h）应实现设备特权用户的权限分离。	1.是否区分不同用户的操作权限，实现设备特权用户的权限分离： √是 □否 2.设备的特权用户包括： √系统管理员 √安全管理员 √安全审计员 √其他：	5

A.3 主机安全(OS)

后台管理服务器

安全控制点	测评指标	结果记录	符合程度
鉴 份	a）应对登录操作系统和数据库系统的用户	1.该系统所有用户是否已设置密码： √是	5

	进行身份标识和鉴别；	□否 2.登录过程中系统帐户是否使用了密码进行验证登录： √是管理员使用 Xshell 连接服务器，采用用户名密码进行身份鉴别。 □否	
	b）操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；	1.是否设置密码策略： √是 □否 2.管理用户身份鉴别使用的口令是否有复杂度要求： √有 口令最小长度：12 位。 口令复杂度要求：由大小写字母、特殊字符、数字排列组合而成。 □无 3.管理用户身份鉴别使用的口令是否有强制定期更换的要求： √有 口令更换周期：30 天。 □无	5
	c）启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；	1.是否有登录失败处理功能： √是 □否 2.采取的措施包括： □结束会话 √限制非法登录次数 □当网络登录连接超时自动退出， 超时锁定时间： □其他：	5
	d）当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；	1.是否允许对设备进行远程管理： √是 □否 2.是否采取了必要措施防止鉴别信息在传输过程中被窃听： √是 措施为：远程管理时使用 ssh 协议。 □否	5
	e）应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性；	1.操作系统和数据库系统的用户名是否具有唯一性： √是被测服务器包含管理员帐户、应用帐户和个人帐户，系统中不存在相同的用户名。	5

		□否	
	f）应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。	1.设备是否采取两种或两种以上组合鉴别技术进行身份鉴别： √是 □否 2.鉴别技术包括： √我知道的：静态密码。 √我持有的：动态密码。 □我拥有的：	5
访问控制	a）应启用访问控制功能，依据安全策略控制用户对资源的访问；	1.系统是否启用了访问控制功能： √是服务器的重要文件权限分配合理。摘抄重要文件的权限配置如下： #ls -l /etc/passwd 644 #ls -l /etc/shadow 000 □否 2.系统是否为不同的用户组设置了不同权限： √是 □否 3.系统是否存在默认共享： □是 默认共享： √否	5
	b）应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；	1.是否为管理用户分配了完成其任务的最小权限： √是被测服务器包含管理员帐户、应用帐户和个人帐户，除管理员帐户外，其他帐户只有普通权限，权限分配合理。 □否	5
	c）应实现操作系统和数据库系统特权用户的权限分离；	1.系统是否存在数据库： √是 □否 2.自然人与其管理员帐户是否做到一一对应： √是 □否 3.是否做到了管理员不能同时管理操作系统和数据库： √是 □否	5
	d）应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；	1.系统默认用户名是否已经重命名： □是 √否 2.默认用户名的默认口令是否已经修改： √是	5

		□否	
	e）应及时删除多余的、过期的帐户，避免共享帐户的存在；	1.系统是否存在多余的、过期的帐户： □是 √否 2.系统是否存在共享帐户： □是 √否 3.是否定期对多余的、过期的帐户进行清理： √是 清理周期：一个月清理一次。 □否	5
	f）应对重要信息资源设置敏感标记；	1.是否有重要信息资源清单： □有 □无 2.重要信息资源的存储方式是否有明确要求： □有 □无 3.对重要信息资源（文件或数据库内容）是否有安全技术措施实现敏感标记： □有 □无 N/A 操作系统不支持强制访问控制策略，故此项不适用。	N/A
	g）应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。	1.有敏感标记的重要信息资源的使用是否有相关管理文档： □有 □无 2.对标记为敏感的信息资源（文件或数据库内容）的操作（如：读取、写入、修改、覆盖、删除等）是否有安全策略控制（控制用户操作权限）： □是 □否 N/A 操作系统不支持强制访问控制策略，故此项不适用。	N/A
安全审计	a）安全审计应覆盖到服务器和客户端上的每个操作系统用户和数据库用户；	1.系统是否启用审计功能： √是被测服务器已启用主机安全审计。 □否 2.审计是否覆盖所有用户： √是 □否	5
	b）审计内容应包括重要用户行为、系统资源	1.审计内容包含以下内容： √重要用户行为	5

	的异常使用和重要系统命令的使用等系统内重要的安全相关事件；	√系统资源的异常使用 √重要系统命令的使用 □其他： □无	
	c）审计记录应包括日期和时间、类型、主体标识、客体标识、事件的结果等；	1.审计记录包括： √日期 √时间 √类型 √主客体标识 √事件结果	5
	d）应能根据记录数据进行分析，并生成审计报表；	1.是否能够生成审计报表： √是定期1个月内对重要的系统命令、服务器登录日志、负载状态及异常数据库操作等进行记录分析并生成审计报表。 □否	5
	e）应保护审计进程，避免受到未预期的中断；	1.是否对审计进程采取了相应的技术保护手段： √是 手段是：通过帐户权限分配，只有系统管理员才能够中断审计进程。 □否	5
	f）应保护审计记录，避免受到未预期的删除、修改或覆盖等。	1.是否对审计记录采取了相应的保护措施： √是将审计记录保存到EMC存储上，至少保存半年以上。 □否	5
剩余信息保护	a） 应保证操作系统和数据库管理系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；	1.操作系统和数据库管理系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前是否得到完全清除： √是 linux 操作系统默认关机的时候会清除系统缓存。 □否	5
	b） 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。	1.是否确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除： √是磁盘空间重新分配给其他用户时会进行格式化。 □否 2.存储设备损坏后的处理措施是： 损坏的设备统一仓库中留存。	5
防 侵	a）应能够检测到对重要服务器进行入侵的	1.是否能够检测到对重要服务器进行入侵的行为： √是	5

	行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；	措施为：启用了防火墙上的 IPS 模块。 □否 2.主机入侵检测软件是否可以监视记录以下入侵行为： √入侵的源 IP √攻击的类型 √攻击的目的 √攻击的时间 3.发生入侵事件时是否提供报警信息： √是 报警方式为：通过邮件报警。 □否	
	b）应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施；	1.是否使用文件完整性检查工具对重要文件的完整性进行检查： √是 措施为：被测单位部署了 Zabbix 用于重要程序的完整性检测，当检测到完整性遭到破坏时通过邮件报警。 □否 2.是否对重要文件进行备份： √是 □否	5
	c）操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新	1.操作系统安装是否遵循了最小安装的原则： √是服务器遵循最小安装原则，仅安装支持系统运行所需的组件。 □否 2.操作系统补丁是否及时更新： √是管理员会定期关注补丁动态，选择需要的更新，先在测试机上测试，在更新到生产服务器上。 □否	5
恶意代码防范	a）应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；	1.是否安装了防病毒软件： □是 软件名称： □否 2.恶意代码库是否最新： □是 最后一次升级时间： □否 N/A 操作系统为 LINUX，没有适用的防恶意代码软件。	N/A
	b）主机防恶意代码产品应具有与网络防恶	1.网络防病毒软件和主机防病毒软件是否是不同恶意代码库：	N/A

	意代码产品不同的恶意代码库；	□是 □否 N/A 操作系统为 LINUX，没有适用的防恶意代码软件。	
	c）应支持恶意代码防范的统一管理。	1.是否采用统一的病毒更新策略和查杀策略： □是 □否 N/A 操作系统为 LINUX，没有适用的防恶意代码软件。	N/A
资源控制	a）应通过设定终端接入方式、网络地址范围等条件限制终端登录；	1.是否设定终端接入方式： √是 方式为：管理员在服务器上做策略限制登录服务器的 IP 地址。 □否	5
	b）应根据安全策略设置登录终端的操作超时锁定；	1.登录终端是否开启终端的操作超时锁定： √是 超时时间设定为：1800s。 □否	5
	c）应对重要服务器进行监视，包括监视服务器的 CPU、硬盘、内存、网络等资源的使用情况；	1.是否对重要服务器资源使用情况进行监视： √是 工具为：被测单位部署了 Zabbix 监控系统的资源消耗情况。 □否 2.监视内容包括： √服务器的 CPU 使用情况 √服务器的硬盘使用情况 √服务器的内存使用情况 √服务器的网络使用情况	5
	d）应限制单个用户对系统资源的最大或最小使用限度；	1.是否有措施控制用户进程对系统资源的占用: □是 方式为： □否 N/A 被测服务器用户量少，无需限制单个用户对资源最大或最小消耗。	N/A
	e）应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。	1.是否对系统服务水平情况进行监视： √是 方式为：被测单位部署了 Zabbix 监控系统的资源消耗情况。 □否 2.服务水平降低到预先规定的最小值时是否会自动报警： √是	5

		报警方式为：通过邮件或短信进行报警。 □否	

API 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）应对登录操作系统和数据库系统的用户进行身份标识和鉴别；	1.该系统所有用户是否已设置密码： √是 □否 2.登录过程中系统帐户是否使用了密码进行验证登录： √是管理员使用 Xshell 连接服务器，采用用户名密码进行身份鉴别。 □否	5
	b）操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；	1.是否设置密码策略： √是 □否 2.管理用户身份鉴别使用的口令是否有复杂度要求： √有 口令最小长度：12 位。 口令复杂度要求：由大小写字母、特殊字符、数字排列组合而成。 □无 3.管理用户身份鉴别使用的口令是否有强制定期更换的要求： √有 口令更换周期：30 天。 □无	5
	c）启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；	1.是否有登录失败处理功能： √是 □否 2.采取的措施包括： □结束会话 √限制非法登录次数 □当网络登录连接超时自动退出， 超时锁定时间： □其他：	5
	d）当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在	1.是否允许对设备进行远程管理： √是 □否	5

安全控制点	测评指标	结果记录	符合程度
	网络传输过程中被窃听；	2.是否采取了必要措施防止鉴别信息在传输过程中被窃听： √是 措施为：远程管理时使用 ssh 协议。 □否	
	e）应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性；	1.操作系统和数据库系统的用户名是否具有唯一性： √是被测服务器包含管理员帐户、应用帐户和个人帐户，系统中不存在相同的用户名。 □否	5
	f）应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。	1.设备是否采取两种或两种以上组合鉴别技术进行身份鉴别： √是 □否 2.鉴别技术包括： √我知道的：静态密码。 √我持有的：动态密码。 □我拥有的：	5
访问控制	a）应启用访问控制功能，依据安全策略控制用户对资源的访问；	1.系统是否启用了访问控制功能： √是服务器的重要文件权限分配合理。摘抄重要文件的权限配置如下： #ls -l /etc/passwd 644 #ls -l /etc/shadow 000 □否 2.系统是否为不同的用户组设置了不同权限： √是 □否 3.系统是否存在默认共享： □是 默认共享： √否	5
	b）应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；	1.是否为管理用户分配了完成其任务的最小权限： √是被测服务器包含管理员帐户、应用帐户和个人帐户，除管理员帐户外，其他帐户只有普通权限，权限分配合理。 □否	5
	c）应实现操作系统和数据库系统特权用户的权限分离；	1.系统是否存在数据库： √是 □否	5

安全控制点	测评指标	结果记录	符合程度
		2.自然人与其管理员帐户是否做到一一对应： √是 □否 3.是否做到了管理员不能同时管理操作系统和数据库： √是 □否	
	d）应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；	1.系统默认用户名是否已经重命名： □是 √否 2.默认用户名的默认口令是否已经修改： √是 □否	5
	e）应及时删除多余的、过期的帐户，避免共享帐户的存在；	1.系统是否存在多余的、过期的帐户： □是 √否 2.系统是否存在共享帐户： □是 √否 3.是否定期对多余的、过期的帐户进行清理： √是 清理周期：一个月清理一次。 □否	5
	f）应对重要信息资源设置敏感标记；	1.是否有重要信息资源清单： □有 □无 2.重要信息资源的存储方式是否有明确要求： □有 □无 3.对重要信息资源（文件或数据库内容）是否有安全技术措施实现敏感标记： □有 □无 N/A 操作系统不支持强制访问控制策略，故此项不适用。	N/A
	g）应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。	1.有敏感标记的重要信息资源的使用是否有相关管理文档： □有 □无	N/A

安全控制点	测评指标	结果记录	符合程度
		2.对标记为敏感的信息资源（文件或数据库内容）的操作（如：读取、写入、修改、覆盖、删除等）是否有安全策略控制（控制用户操作权限）： □是 □否 N/A 操作系统不支持强制访问控制策略，故此项不适用。	
安全审计	a）安全审计应覆盖到服务器和客户端上的每个操作系统用户和数据库用户；	1.系统是否启用审计功能： √是被测服务器已启用主机安全审计。 □否 2.审计是否覆盖所有用户： √是 □否	5
	b）审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；	1.审计内容包含以下内容： √重要用户行为 √系统资源的异常使用 √重要系统命令的使用 □其他： □无	5
	c）审计记录应包括日期和时间、类型、主体标识、客体标识、事件的结果等；	1.审计记录包括： √日期 √时间 √类型 √主客体标识 √事件结果	5
	d）应能根据记录数据进行分析，并生成审计报表；	1.是否能够生成审计报表： √是定期 1 个月内对重要的系统命令、服务器登录日志、负载状态及异常数据库操作等进行记录分析并生成审计报表。 □否	5
	e）应保护审计进程，避免受到未预期的中断；	1.是否对审计进程采取了相应的技术保护手段： √是 手段是：通过帐户权限分配，只有系统管理员才能够中断审计进程。 □否	5
	f）应保护审计记录，避免受到未预期的删除、修改或覆盖等。	1.是否对审计记录采取了相应的保护措施： √是将审计记录保存到 EMC 存储上，至少保存半年以上。 □否	5

安全控制点	测评指标	结果记录	符合程度
剩余信息保护	a） 应保证操作系统和数据库管理系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；	1.操作系统和数据库管理系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前是否得到完全清除： √是 linux 操作系统默认关机的时候会清除系统缓存。 □否	5
	b） 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。	1.是否确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除： √是磁盘空间重新分配给其他用户时会进行格式化。 □否 2.存储设备损坏后的处理措施是： 损坏的设备统一仓库中留存。	5
入侵防范	a）应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；	1.是否能够检测到对重要服务器进行入侵的行为： √是 措施为：启用了防火墙上的 IPS 模块。 □否 2.主机入侵检测软件是否可以监视记录以下入侵行为： √入侵的源 IP √攻击的类型 √攻击的目的 √攻击的时间 3.发生入侵事件时是否提供报警信息： √是 报警方式为：通过邮件报警。 □否	5
	b）应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施；	1.是否使用文件完整性检查工具对重要文件的完整性进行检查： √是 措施为：被测单位部署了 Zabbix 用于重要程序的完整性检测，当检测到完整性遭到破坏时通过邮件报警。 □否 2.是否对重要文件进行备份： √是 □否	5

安全控制点	测评指标	结果记录	符合程度
	c）操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新	1.操作系统安装是否遵循了最小安装的原则： √是服务器遵循最小安装原则，仅安装支持系统运行所需的组件。 □否 2.操作系统补丁是否及时更新： √是管理员会定期关注补丁动态，选择需要的更新，先在测试机上测试，在更新到生产服务器上。 □否	5
恶意代码防范	a）应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；	1.是否安装了防病毒软件： □是 软件名称： □否 2.恶意代码库是否最新： □是 最后一次升级时间： □否 N/A 操作系统为 LINUX,没有适用的防恶意代码软件。	N/A
	b）主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；	1.网络防病毒软件和主机防病毒软件是否是不同恶意代码库： □是 □否 N/A 操作系统为 LINUX,没有适用的防恶意代码软件。	N/A
	c）应支持恶意代码防范的统一管理。	1.是否采用统一的病毒更新策略和查杀策略： □是 □否 N/A 操作系统为 LINUX,没有适用的防恶意代码软件。	N/A
资源控制	a）应通过设定终端接入方式、网络地址范围等条件限制终端登录；	1.是否设定终端接入方式： √是 方式为：管理员在服务器上做策略限制登录服务器的 IP 地址。 □否	5
	b）应根据安全策略设置登录终端的操作超时锁定；	1.登录终端是否开启终端的操作超时锁定： √是 超时时间设定为：1800s。 □否	5
	c）应对重要服务器进	1.是否对重要服务器资源使用情况进行监视：	5

安全控制点	测评指标	结果记录	符合程度
	行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况；	√是 工具为：被测单位部署了 Zabbix 监控系统的资源消耗情况。 □否 2.监视内容包括： √服务器的CPU使用情况 √服务器的硬盘使用情况 √服务器的内存使用情况 √服务器的网络使用情况	
	d）应限制单个用户对系统资源的最大或最小使用限度；	1.是否有措施控制用户进程对系统资源的占用: □是 方式为： □否 N/A 被测服务器用户量少，无需限制单个用户对资源最大或最小消耗。	N/A
	e）应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。	1.是否对系统服务水平情况进行监视： √是 方式为：被测单位部署了 Zabbix 监控系统的资源消耗情况。 □否 2.服务水平降低到预先规定的最小值时是否会自动报警： √是 报警方式为：通过邮件或短信进行报警。 □否	5

数据库服务器

安全控制点	测评指标	结果记录	符合程度
身份鉴别	a）应对登录操作系统和数据库系统的用户进行身份标识和鉴别；	1.该系统所有用户是否已设置密码： √是 □否 2.登录过程中系统帐户是否使用了密码进行验证登录： √是管理员使用 Xshell 连接服务器，采用用户名密码进行身份鉴别。 □否	5
	b）操作系统和数据库系统管理用户身份标	1.是否设置密码策略： √是	5

安全控制点	测评指标	结果记录	符合程度
	识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；	□否 2.管理用户身份鉴别使用的口令是否有复杂度要求： √有 口令最小长度：12 位。 口令复杂度要求：由大小写字母、特殊字符、数字排列组合而成。 □无 3.管理用户身份鉴别使用的口令是否有强制定期更换的要求： √有 口令更换周期：30 天。 □无	
	c）启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；	1.是否有登录失败处理功能： √是 □否 2.采取的措施包括： □结束会话 √限制非法登录次数， 策略为： □当网络登录连接超时自动退出， 超时锁定时间： □其他：	5
	d）当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；	1.是否允许对设备进行远程管理： √是 □否 2.是否采取了必要措施防止鉴别信息在传输过程中被窃听： √是 措施为：远程管理时使用 ssh 协议。 □否	5
	e）应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性；	1.操作系统和数据库系统的用户名是否具有唯一性： √是被测服务器包含管理员帐户、应用帐户和个人帐户，系统中不存在相同的用户名。 □否	5
	f）应采用两种或两种以上组合的鉴别技术对管理用户进行身份	1.设备是否采取两种或两种以上组合鉴别技术进行身份鉴别： √是	5

安全控制点	测评指标	结果记录	符合程度
	鉴别。	□否 2.鉴别技术包括： √我知道的：静态密码。 √我持有的：动态密码。 □我拥有的：	
访问控制	a）应启用访问控制功能，依据安全策略控制用户对资源的访问；	1.系统是否启用了访问控制功能： √是服务器的重要文件权限分配合理。摘抄重要文件的权限配置如下： #ls -l /etc/passwd 644 #ls -l /etc/shadow 000 □否 2.系统是否为不同的用户组设置了不同权限： √是 □否 3.系统是否存在默认共享： □是 默认共享： √否	5
	b）应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；	1.是否为管理用户分配了完成其任务的最小权限： √是被测服务器包含管理员帐户、应用帐户和个人帐户，除管理员帐户外，其他帐户只有普通权限，权限分配合理。 □否	5
	c）应实现操作系统和数据库系统特权用户的权限分离；	1.系统是否存在数据库： √是 □否 2.自然人与其管理员帐户是否做到一一对应： √是 □否 3.是否做到了管理员不能同时管理操作系统和数据库： √是 □否	5
	d）应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；	1.系统默认用户名是否已经重命名： □是 √否 2.默认用户名的默认口令是否已经修改： √是 □否	5

安全控制点	测评指标	结果记录	符合程度
	e）应及时删除多余的、过期的帐户，避免共享帐户的存在；	1.系统是否存在多余的、过期的帐户： □是 √否 2.系统是否存在共享帐户： □是 √否 3.是否定期对多余的、过期的帐户进行清理： √是 清理周期：一个月清理一次。 □否	5
	f）应对重要信息资源设置敏感标记；	1.是否有重要信息资源清单： □有 □无 2.重要信息资源的存储方式是否有明确要求： □有 □无 3.对重要信息资源（文件或数据库内容）是否有安全技术措施实现敏感标记： □有 □无 N/A 操作系统不支持强制访问控制策略，故此项不适用。	N/A
	g）应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。	1.有敏感标记的重要信息资源的使用是否有相关管理文档： □有 □无 2.对标记为敏感的信息资源（文件或数据库内容）的操作（如：读取、写入、修改、覆盖、删除等）是否有安全策略控制（控制用户操作权限）： □是 □否 N/A 操作系统不支持强制访问控制策略，故此项不适用。	N/A
安全审计	a）安全审计应覆盖到服务器和客户端上的每个操作系统用户和数据库用户；	1.系统是否启用审计功能： √是被测服务器已启用主机安全审计。 □否 2.审计是否覆盖所有用户： √是 □否	5

安全控制点	测评指标	结果记录	符合程度
	b）审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；	1.审计内容包含以下内容： √重要用户行为 √系统资源的异常使用 √重要系统命令的使用 □其他： □无	5
	c）审计记录应包括日期和时间、类型、主体标识、客体标识、事件的结果等；	1.审计记录包括： √日期 √时间 √类型 √主客体标识 √事件结果	5
	d）应能根据记录数据进行分析，并生成审计报表；	1.是否能够生成审计报表： √是定期1个月内对重要的系统命令、服务器登录日志、负载状态及异常数据库操作等进行记录分析并生成审计报表。 □否	5
	e）应保护审计进程，避免受到未预期的中断；	1.是否对审计进程采取了相应的技术保护手段： √是 手段是：通过帐户权限分配，只有系统管理员才能够中断审计进程。 □否	5
	f）应保护审计记录，避免受到未预期的删除、修改或覆盖等。	1.是否对审计记录采取了相应的保护措施： √是将审计记录保存到EMC存储上，至少保存半年以上。 □否	5
剩余信息保护	a） 应保证操作系统和数据库管理系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；	1.操作系统和数据库管理系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前是否得到完全清除： √是linux操作系统默认关机的时候会清除系统缓存。 □否	5
	b） 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完	1.是否确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除： √是磁盘空间重新分配给其他用户时会进行格式化。	5

安全控制点	测评指标	结果记录	符合程度
	全清除。	□否 2.存储设备损坏后的处理措施是： 损坏的设备统一仓库中留存。	
入侵防范	a）应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；	1.是否能够检测到对重要服务器进行入侵的行为： √是 措施为：启用了防火墙上的 IPS 模块。 □否 2.主机入侵检测软件是否可以监视记录以下入侵行为： √入侵的源 IP √攻击的类型 √攻击的目的 √攻击的时间 3.发生入侵事件时是否提供报警信息： √是 报警方式为：通过邮件报警。 □否	5
	b）应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施；	1.是否使用文件完整性检查工具对重要文件的完整性进行检查： √是 措施为：被测单位部署了 Zabbix 用于重要程序的完整性检测，当检测到完整性遭到破坏时通过邮件报警。 □否 2.是否对重要文件进行备份： √是 □否	5
	c）操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新	1.操作系统安装是否遵循了最小安装的原则： √是服务器遵循最小安装原则，仅安装支持系统运行所需的组件。 □否 2.操作系统补丁是否及时更新： √是管理员会定期关注补丁动态，选择需要的更新，先在测试机上测试，在更新到生产服务器上。 □否	5
恶意代码防范	a）应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；	1.是否安装了防病毒软件： □是 软件名称： □否	N/A

安全控制点	测评指标	结果记录	符合程度
		2.恶意代码库是否最新： □是 最后一次升级时间： □否 N/A 操作系统为 LINUX,没有适用的防恶意代码软件。	
	b）主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；	1.网络防病毒软件和主机防病毒软件是否是不同恶意代码库： □是 □否 N/A 操作系统为 LINUX,没有适用的防恶意代码软件。	N/A
	c）应支持恶意代码防范的统一管理。	1.是否采用统一的病毒更新策略和查杀策略： □是 □否 N/A 操作系统为 LINUX,没有适用的防恶意代码软件。	N/A
资源控制	a）应通过设定终端接入方式、网络地址范围等条件限制终端登录；	1.是否设定终端接入方式： √是 方式为：管理员在服务器上做策略限制登录服务器的 IP 地址。 □否	5
	b）应根据安全策略设置登录终端的操作超时锁定；	1.登录终端是否开启终端的操作超时锁定： √是 超时时间设定为：1800s。 □否	5
	c）应对重要服务器进行监视，包括监视服务器的 CPU、硬盘、内存、网络等资源的使用情况；	1.是否对重要服务器资源使用情况进行监视： √是 工具为：被测单位部署了 Zabbix 监控系统的资源消耗情况。 □否 2.监视内容包括： √服务器的 CPU 使用情况 √服务器的硬盘使用情况 √服务器的内存使用情况 √服务器的网络使用情况	5
	d）应限制单个用户对系统资源的最大或最小使用限度；	1.是否有措施控制用户进程对系统资源的占用: □是 方式为：	N/A

安全控制点	测评指标	结果记录	符合程度
		□否 N/A 被测服务器用户量少，无需限制单个用户对资源最大或最小消耗。	
	e）应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。	1.是否对系统服务水平情况进行监视： √是 方式为：被测单位部署了 Zabbix 监控系统的资源消耗情况。 □否 2.服务水平降低到预先规定的最小值时是否会自动报警： √是 报警方式为：通过邮件或短信进行报警。 □否	5

A.4 主机安全(DB)

mysql

安全控制点	测评指标	结果记录	符合程度
身份鉴别	a）应对登录操作系统和数据库系统的用户进行身份标识和鉴别；	1.数据库管理员用户是否已设置密码： √是 □否 2.登录过程中管理员帐户是否使用了密码进行验证登录： √是被测数据库使用用户名密码+动态密码进行身份鉴别。 □否 3.是否使用第三方工具登录系统： √是管理员先登录跳板机，再使用 Navicat 管理数据库。 □否 4.访谈记录：（附件）	5
	b）操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；	1.操作系统和数据库系统管理用户存储文件是否采用了加密技术： √是 □否 2.管理用户身份鉴别使用的口令是否有复杂度要	5

		求： √是 口令最小长度：至少 17 位密码。 口令复杂度要求：由大小写字母、数字和特殊字符组成。 □否 3.管理用户身份鉴别使用的口令是否有强制定期更换的要求： √是 口令更换周期：一个月更换一次。 □否 4.数据库默认帐户的密码是否已经修改： √是 □否	
	c）启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；	1.是否有登录失败处理功能： □是 □否 2.采取的措施包括： □结束会话 □限制非法登录次数， 策略为： N/A 被测数据库不支持登录失败处理功能，但跳板机上已启用登录失败处理功能。	N/A
	d）当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；	1.是否允许对设备进行远程管理： √是 □否 2.是否使用了第三方的远程管理工具： √是使用 Navicat 管理数据库。 □否 3.是否采取了必要措施防止鉴别信息在传输过程中被窃听： √是远程管理时使用 ssh 协议。 □否	5
	e）应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性；	1.数据库是否为每个用户分配了单独的用户名： √是被测服务器包含管理员帐户、应用帐户，系统中不存在相同的用户名。 □否	5
	f）应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。	1.数据库服务器是否采用双因子组合技术对管理员进行验证： √是被测数据库使用静态密码+动态密码进行身份鉴别。 □否	5

访问控制	a）应启用访问控制功能，依据安全策略控制用户对资源的访问；	1.除默认的管理员帐户外，是否还存在其它的管理员帐户： □是 √否 2.是否有 DBA 角色授权给了其它角色： □是 √否除默认管理用户 root 外，其他用户没有 DBA 权限。	5
	b）应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；	1.除了管理员用户之外的其他数据库用户权限是否限制在自身的应用范围之内： √是 □否 2.是否根据不同角色为管理用户分配了完成其任务的最小权限： √是 □否 3.是否对用户权限进行定期审查： √是 审查周期：一个月一次。 □否	5
	c）应实现操作系统和数据库系统特权用户的权限分离；	1.数据库从管理上是否有专门的系统管理员和数据库管理员： √是 □否 2.系统管理员使用的帐户和数据库管理员使用的帐户是否分开： √是 □否 3.自然人与其管理员帐户是否做到一一对应： √是 □否 4.是否做到了管理员不能同时管理操作系统和数据库： √是 □否	5
	d）应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；	1.数据库默认账户是否在用： √是 □否 2.数据库默认用户名是否已经重命名： □是 √否默认管理员帐户不支持重命名。 3.默认用户名的默认口令是否已经修改：	5

		√是 □否	
	e）应及时删除多余的、过期的帐户，避免共享帐户的存在；	1.数据库是否存在多余的、过期的帐户： □是 √否 2.数据库系统是否存在共享帐户： □是 √否 3.是否定期对多余的、过期的帐户进行清理： √是 清理周期：一个月一次。 □否 4.访谈记录：（附件）	5
	f）应对重要信息资源设置敏感标记；	1.访谈管理员数据库是否支持强制访问控制策略： □是 □否 N/A 数据库不支持强制访问控制策略，故此项不适用。	N/A
	g）应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。	1.访谈管理员数据库是否支持强制访问控制策略： □是 □否 N/A 数据库不支持强制访问控制策略，故此项不适用。	N/A
安全审计	a）安全审计应覆盖到服务器和客户端上的每个操作系统用户和数据库用户；	1.是否开启数据库审计功能： √是已启用数据库审计功能。 □否 2.是否存在第三方审计（软件或设备）： □是 第三方名称： √否 3.访谈记录：（附件）	5
	b）审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；	1.审计内容应该包含但不限于以下内容： √重要用户行为 √系统资源的异常使用 √重要系统命令的使用	5
	c）审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；	1.审计记录至少包含： √事件的日期 √事件的时间 √事件的类型 √主客体标识	5

		√事件结果	
	d）应能够根据记录数据进行分析，并生成审计报表；	1.是否安装有第三方审计软件或系统： □是 第三方名称： √否 2.是否能生成审计报表： √是定期1个月内对重要的系统命令、数据库登录日志、负载状态及异常数据库操作等进行记录分析并生成审计报表。 □否	5
	e）应保护审计进程，避免受到未预期的中断；	1.是否对审计进程采取了相应的技术保护手段： √是通过合理的权限分配，使得只有数据库管理员才能够中断审计进程。 □否	5
	f）应保护审计记录，避免受到未预期的删除、修改或覆盖等。	1.是否对审计记录采取了相应的保护措施： √是将审计记录保存到EMC存储上。 □否 2.是否包括以下方面： √审计记录的存储将审计记录保存到 EMC 存储上。 □审计记录的备份 □审计记录的保护	5
资源控制	a）应通过设定终端接入方式、网络地址范围等条件限制终端登录；	1.数据库配置文件是否设置了网络地址的范围限制： √是 □否 2.是否在网络层面进行网络地址范围条件限制终端登录： √是通过网络层面上限制登录地址。 □否	5
	b）应根据安全策略设置登录终端的操作超时锁定；	1.数据库配置文件是否设置了登录终端的操作超时锁定： √是由于数据库是在内网通过跳板机进行连接访问，已对跳板机的连接用户设置了过期自动锁定策略。 □否	5
	c）应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况；	1.是否对重要服务器资源使用情况进行监视： √是被测单位部署了 Zabbix 监控系统的资源消耗情况。 □否 2.是否有第三方工具实现上述功能： √是被测单位部署了 Zabbix 监控系统的资源消	5

		耗情况。 □否 3.监视内容是否包括： √服务器的 CPU 使用情况 √服务器的硬盘使用情况 √服务器的内存使用情况 √服务器的网络使用情况	
	d）应限制单个用户对系统资源的最大或最小使用限度；	1.是否有措施控制用户进程对系统资源的占用： □是 □否 N/A 被测数据库用户单一，无需对单个用户最大或最小资源消耗进行限制。	N/A
	e）应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。	1.服务水平降低到预先规定的最小值时是否会自动报警： √是通过邮件或短信进行报警。 □否	5

A.5 应用安全

你我金融信息服务系统

安全控制点	测评指标	结果记录	符合程度
身份鉴别	a）应提供专用的登录控制模块对登录用户进行身份标识和鉴别；	1.应用系统是否采取登录模块对用户进行身份标识和鉴别 √是 □否	5
	b）应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；	1.是否采用两种或两种以上组合的鉴别技术对用户进行身份鉴别； √是 □我知道的 √我持有的手机验证码 □我拥有的 □否	5

	c）应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；	1.应用系统是否对用户身份标识有唯一性要求 √是 □否 2.应用系统是否对用户身份鉴别使用的口令有复杂度要求 √是 □否 3.密码策略包括： √用户口令由数字、大小写字母、符号混排，无规律的方式 √用户口令的长度至少为8位 √用户口令每季度更换一次 □更新的口令至少5次内不能重复	5
	d）应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；	1.是否有登录失败处理功能 √是 □否 2.采取的措施是： □结束会话 √限制非法登录次数，策略为：3次 □当网络登录连接超时自动退出，超时时间设定为：	5
	e）应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。	1.应用系统是否启用身份鉴别功能 √是 □否 2.应用系统是否启用身份标识唯一性检查功能 √是 □否 3.应用系统是否启用技术措施对身份鉴别复杂度进行检查 √是 □否 4.应用系统是否启用登录失败处理功能 √是 □否 5.是否采用两种或两种以上组合的鉴别技术对用户进行身份鉴别 √是 □否 6.渗透测试未发现有可绕过身份鉴别进行系统访问的情况 √是 □否	5

访问控制	a）应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；	1.应用系统是否提供访问控制功能 √是 □否	5
	b）访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；	1.访问控制的覆盖范围包括 √与信息安全直接相关的主体 √与信息安全直接相关的客体 √主体与客体之间的操作 □无	5
	c）应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限；	1.应用系统是否由授权主体设置其它用户访问系统功能和用户数据的权限的功能 √是 □否 2.应用系统是否有默认用户 □是 □默认帐户只具备管理功能而不能进行业务操作 □未限制默认用户的访问权限 √否系统无默认账户	5
	d）应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；	1.系统是否授予不同帐户为完成各自承担任务所需的最小权限 √是 □否 2.权限之间是否相互制约 √是 □否	5
	e）应具有对重要信息资源设置敏感标记的功能；	1.N/A N/A 此项不适用	N/A
	f）应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。	1.N/A	0
安全审计	a）应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计；	1.应用系统是否启用审计功能 √是 □否 2.审计是否覆盖所有用户 √是 □否	5

	b）应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；	1.是否对审计进程采取了技术保护手段 √是，技术手段为： □否 2.是否对审计记录采取了相应的保护措施 √是 □否 3.审计功能是否可以被单独的关闭、停用等。 □是 √否 4.通过应用系统无法删除、修改或覆盖审计记录 √是 □否	5
	c）审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等；	1.审计记录的内容包含 √事件的日期 √事件的时间 √事件的类型 √事件描述 √事件结果 √发起者信息	5
	d）应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。	1.是否能够生成审计报表 √是 □否 2.是否定期对审计信息进行分析 √是 □否	5
剩余信息保护	a）应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；	1.应用系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前是否得到完全清除 √是用户鉴别信息不存储在客户端，验证信息通过 SESSION 对象保存，客户端关闭 SESSION 对象销毁 □否	5
	b）应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。	1.是否确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除 √是 □否	5
通信完整性	a）应采用密码技术保证通信过程中数据的完整性。	1.系统是否具有在数据传输过程中保护其完整性的措施 √是，措施为：HTTPS □否	5

通信保密性	a）在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；	1.系统是否可以在通信双方建立连接之前，利用密码技术进行会话初始化验证 √是，措施为：登录密码 MD5 □否	5
	b）应对通信过程中的整个报文或会话过程进行加密。	1.系统在通信过程中，是否对整个报文或会话过程进行加密 √是，采用加密方式是：RSA □否	5
抗抵赖	a）应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；	1.系统是否具有抗抵赖的措施 √是 □否 2.系统是否有在请求的情况下为数据原发者或接收者提供数据原发证据的功能 √是，方式为：通过系统操作日志、业务日志提供数据原发证据的功能 □否	5
	b）应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。	1.系统是否有在请求的情况下为数据原发者或接收者提供数据接收证据的功能 √是，方式为：通过系统操作日志、业务日志提供数据原发证据的功能 □否	5
软件容错	a）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数据格式或长度符合系统设定要求；	1.应用系统是否具有保证软件容错能力的措施 √是 □否 2.应用系统是否对人机接口输入或通信接口输入的数据进行有效性检验 √是 □否 3.应用系统是否可以上传附件 √是 □否 4.渗透测试是否发现存在输入数据有效性验证问题 □是 √否	5
	b）应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。	1.故障发生时是否自动保护当前所有状态，以保证系统能够进行恢复 √是 □否	5

资源控制	a）当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；	1.系统是否有超时响应检验功能，能够自动结束无响应的通信连接 √是 □否	5
	b）应能够对系统的最大并发会话连接数进行限制；	1.系统是否有最大并发会话连接数的限制 √是，最大并发会话连接数：后端支持 500 同时在线，APP 支持 2 万同时在线 □否	5
	c）应能够对单个帐户的多重并发会话进行限制；	1.系统是否限制单个帐户的多重并发会话 √是 □否	5
	d）应能够对一个时间段内可能的并发会话连接数进行限制；	1.系统是否对一个时间段内可能的并发会话连接数进行限制 √是，并发会话数：后端支持 500 同时在线，APP 支持 2 万同时在线 □否	5
	e）应能够对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额；	1.是否有措施控制用户进程对系统资源的占用 √是，方式为：系统连接数做限制 □否	5
	f）应能够对系统服务水平降低到预先规定的最小值进行检测和报警；	1.是否对应用系统服务水平情况进行监视 √是，方式为： □否 2.服务水平降低到预先规定的最小值时是否会自动报警 √是，报警方式为： □否	5
	g）应提供服务优先级设定功能，并在安装后根据安全策略设定访问帐户或请求进程的优先级，根据优先级分配系统资源。	1.主要应用系统是否能根据安全策略设定主体的服务优先级，并根据优先级分配系统资源 □是，策略为： □否 N/A 无优先级	N/A

A.6 数据安全及备份恢复

安全控制点	测评指标	结果记录	符合程度
数据完整性	a）应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；	1.是否对传输过程数据进行完整性检测： √是 √系统管理数据 √鉴别信息 √重要业务数据 □ □否 2.是否在检测到完整性错误时采取必要的恢复措施： √是 HTTPS □否	5
	b）应能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。	1.是否对存储过程中的以下类型数据进行完整性检测： √系统管理数据 √鉴别信息 √重要业务数据 2.是否在检测到完整性错误时采取必要的恢复措施： √是 HTTPS □否	5
数据保密性	a）应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性；	1.是否对传输中的数据采用有效措施以实现数据传输保密性： √是 RSA □否	5
	b）应采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。	1.是否对传输中的数据采用有效措施以实现数据存储保密性： √是 RSA、MD5 □否	5
备份和恢复	a）应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放；	1.是否提供本地数据备份与恢复功能： √是每天备份 3 次，存放在服务器，隔段时间会拷贝到本地。 □否 2.备份介质是否场外存放： √是备份数据会定期拷贝到本地保存。 □否	5

	b）应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地；	1.是否提供异地数据备份功能： √是数据库备份会每天保存到异地并定期把线上数据下载到本地。 □否	5
	c）应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障；	1.网络拓扑结构是否采用冗余技术设计： √是 □否	5
	d）应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。	1.核心网络设备、通信线路和数据处理系统等的硬件是否冗余： √核心设备有冗余，冗余方式：热备 √重要链路，冗余方式：双链路 □否	5

A.7 安全管理制度

安全控制点	测评指标	结果记录	符合程度
管理制度	a）应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；	1.是否形成全面的信息安全管理制度体系： √是，体系名称：《你我金融信息安全方针》 □否 2.目前已明确定义的内容 √信息安全总体方针 √范围 √原则 √框架	5
	b）应对安全管理活动中的各类管理内容建立安全管理制度；	1.是否覆盖物理、网络、主机系统、数据、应用、建设和管理等层面的各类管理内容： √是 □否 备注 已建立了《你我金融网络安全管理制度》、《你我金融系统安全管理制度》、《你我金融系统运行管理制度》、《你我金融应用服务日常管理制度》、《你我金融信息安全组织建设制度》等。	5
	c）应对要求管理人员或操作人员执行的日常管理操作建立操作规程；	1.是否具有日常管理操作的操作规程（如系统维护手册和用户操作规程等） √是 □否	5

	d）应形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。	1.目前信息安全管理制度体系由如下部分组成： √总体方针 √安全策略 √管理制度 √操作规程	5
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；	1.有专门的部门或人员负责制定安全管理制度： √是 √部门：技术中心运维组 □否	5
	b）安全管理制度应具有统一的格式，并进行版本控制；	1.格式是否统一： √是 □否 2.是否有版本标识： √是 □否	5
	c）应组织相关人员对制定的安全管理制度进行论证和审定；	1.制度发布前是否对安全管理制度进行论证和审定： √是 √参与论证与审定的部门：技术中心 √参与论证与审定的人员：技术中心运维组经理、技术中心总监 □否	5
	d）安全管理制度应通过正式、有效的方式发布；	1.安全管理制度通过正式、有效的方式发布： √是，发布方式为：邮件发布 □否	5
	e）安全管理制度应注明发布范围，并对收发文进行登记。	1.各项安全管理制度文档注明适用和发布范围： √是 □否 2.各项安全管理制度进行收发文登记： √是 □否	5
评审和修订	a）信息安全领导小组应负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定；	1.是否建立了信息安全领导小组或委员会： √是 □否 2.是否由信息安全领导小组负责定期对安全管理制度体系的合理性和适用性进行审定： √是 □否 3.是否定期评审 √是，评审周期为：每年一次 □否	5

	b）应定期或不定期对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订。	1.是否定期或不定期对安全管理制度进行检查、审定： √是 □否 2.是否在发生重大变更时对安全管理制度进行检查，对存在不足或需要改进的安全管理制度进行修订。 √是 □否	5

A.8 安全管理机构

安全控制点	测评指标	结果记录	符合程度
岗位设置	a）应设立信息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；	1.是否设立专职的安全管理机构： √是，安全管理机构名称：技术中心 □否 2.是否明确设置安全主管、安全管理各个方面的负责人： √是，安全主管为：技术中心运维总监 □否 3.是否通过管理制度明确定义相关人员的职责： √是，对应管理制度为:《你我金融信息安全组织建设制度》 □否	5
	b）应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责；	1.被测单位已设立如下工作岗位： □系统管理员 √网络管理员 √安全管理员 □其它： 2.是否通过管理制度明确定义上述岗位的职责： √是，对应管理制度为:《你我金融网络管理员职责》、《你我金融数据库管理员职责》、《你我金融系统管理员工作职责》、《你我金融安全管理岗位职责》 □否	5

	c）应成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；	1.是否设立了指导和管理信息安全工作的委员会或领导小组: √是，小组或委员会名称：信息安全领导小组 □否 2.其最高领导是否由单位主管领导委任或授权的人员担任: √是: □否	5
	d）应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。	1.是否通过管理制度明确定义安全管理机构的组成、职责、分工、技能要求： √是，对应文档为:《你我金融网络管理员职责》、《你我金融数据库管理员职责》、《你我金融系统管理员工作职责》、《你我金融安全管理岗位职责》 □否	5
人员配备	a）应配备一定数量的系统管理员、网络管理员、安全管理员等；	1.目前各岗位及人员数量为： □系统管理员： √网络管理员：1人 √安全管理员：1人 □其他：	5
	b）应配备专职安全管理员，不可兼任；	1.是否配备有安全管理岗 √是 □否 2.安全管理员专、兼职情况： □专职 √兼职，兼任岗位：系统管理员	0
	c）关键事务岗位应配备多人共同管理。	1.关键事务的管理人员是否配备2人或2人以上共同管理： √是 □否 备注 如数据库管理员由运维经理和刘工互为主备岗，系统管理员由梁工和黄工互为主备岗。	5
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；	1.是否规定了对信息系统中的重要活动要进行审批： √是 √审批部门是：技术中心 √批准人为：技术中心运维经理和运维总监 □否 2.该审批活动是否得到授权： √是 □否	5

	b）应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；	1.是否明确关键活动的审批： √是 □否 2.该审批活动是否得到授权： √是 □否 3.是否明确规定对重要活动建立审批程序： √是，审批程序：申请人通过邮件提出申请写清楚活动内容，并抄送给总监、本小组项目经理、运维组经理，总监审批通过后，由运维组负责实施。 □否 备注 针对系统重要活动有严格审批流程，经过技术中心运维经理、运维总监逐级审批批准后，方可实施。已制定《你我金融应用服务日常管理制度》、《你我金融安全审计制度》等制度对审批程序有要求规定。	5
	c）应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；	1.是否定期审查、更新审批项目: □是，审查周期： √否	0
	d）应记录审批过程并保存审批文档。	1.检查经逐级审批的文档，查看是否具有各级批准人的签字和审批部门的盖章： √是 √签字 □盖章 □否	5
沟通和合作	a）应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理信息安全问题；	1.组织机构内其它部门之间及内部各部门管理人员之间是否有进行沟通、合作机制，有哪些： √是 □否	5

	b）应加强与兄弟单位、公安机关、电信公司的合作与沟通；	1.是否建立与外单位（兄弟单位、公安机关、电信公司等）的合作与沟通: √是 □否 2.合作方式包括但不限于： □外聘 □外包 √研讨会 √资源共享 □其它： 备注 如与互联网金融协会（研讨会）、唯一网络（机房托管）、资产360（资源共享）等单位均保持长期合作沟通。	5
	c）应加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通；	1.是否建立与外单位（供应商、业界专家、专业的安全公司、安全组织等）的合作与沟通: √是 □否 2.合作方式包括但不限于： □外聘 □外包 □研讨会 □资源共享 √其它：各产品供应商（采购需求）	5
	d）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；	1.是否有外联单位联系列表： √是（包括但不限于以下内容） √外联单位的名称 √合作内容 √联系人 √联系方式 □否 2.外联单位是否包含但不限于以下单位： □公安机关 √电信公司 □兄弟单位 √供应商 □业界专家 □专业的安全公司和安全组织	5
	e）应聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。	1.是否聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等： □是 √否	0

审核和检查	a）安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；	1.是否组织人员定期对信息系统进行全面安全检查： √是，检查周期为：每月一次 □否 2.检查内容包括但不限于： √系统日常运行 √系统漏洞 √数据备份 □其它：	5
	b）应由内部人员或上级单位定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；	1.上级单位或内部人员是否定期对信息系统进行全面安全检查： □是，检查周期为： √否 2.检查内容包括但不限于： □现有安全技术措施的有效性 □安全配置与安全策略的一致性 □安全管理制度的执行情况 □其它：	0
	c）应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报；	1.是否有执行安全检查时的安全检查表、安全检查记录和结果通告记录： □是 □安全检查表 □安全检查记录 □结果通告记录 √否 2.检查结果是否进行通报，通报形式、范围如何： □是 □通报形式： □通报范围： √否	0
	d）应制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动。	1.是否制定安全管理制度规范安全审核和安全检查工作： □是，制度文档为： √否	0

A.9 人员安全管理

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；	1.是否有专门的部门或人员负责人员的录用工作： √是 √负责部门：人力行政中心 √负责人员：人事专员协助人事经理 □否	5
	b）应严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核；	1.在人员录用时是否对人员条件有明确的、具体的要求： √是 □否 2.是否对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核： √是 □否	5
	c）应签署保密协议；	1.是否与被录用人员都签署保密协议： √是 □否 2.检查保密协议，包括但不限于以下内容： √保密范围 √保密责任 √违约责任 √协议的有效期限 √责任人的签字	5
	d）应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。	1.从事关键岗位的人员是否从内部人员中选拔： √是 □否 2.是否要求其签署岗位安全协议： √是，协议为：《你我金融安全承诺书》 □否 3.检查岗位安全协议，是否包括但不限于以下内容： √岗位安全责任 √违约责任 √协议的有效期限 √责任人签字	5

人员离岗	a）应严格规范人员离岗过程，及时终止离岗员工的所有访问权限；	1.对即将离岗人员是否采取了有效控制方法： √是 √账户检查 √权限锁定 √文件限制 √资料请点/移交 □否 2.是否及时终止离岗人员的所有访问权限： √是 □否 3.检查人员离岗的管理文档，查看是否规定了人员调离手续和离岗要求： √是，管理文档为：《离职管理制度》 □否 备注 有离职意向的员工第一时间向其所在部门负责人和人事部反应，经面谈后确认无必要挽留后，进入离职手续，申请人提交《员工离职申请表》，经所在部门负责人、人事部审批后，通过《员工离职（调动）工作交接叫》完成离职交接工作，并签署《解除劳动合同协议书》，人事部发布《离职证明》，更新公司花名册并实时向总部报告人员异动情况。	5
	b）应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；	1.是否取回离岗人员物品包括但不限于： √是 √身份证件 √钥匙 √徽章 √软硬件设备 √其他： □否 2.是否有对离岗人员的安全处理记录： √是，处理记录为：《员工离职（调动）工作交接表》 □否	5

	c）应办理严格的调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开。	1.是否有严格的调离手续： √是，调离手续为：申请人提交《员工异动审批表》，经其所在部门负责人、人事部、意向部门负责人审批同意后，完成工作交接。 □否 2.是否要求关键岗位人员调离须承诺相关保密义务后方可离开： √是，保密协议为：《员工竞业限制协议》 □否	5
人员考核	a）应定期对各个岗位的人员进行安全技能及安全认知的考核；	1.是否有人负责定期对各个岗位人员进行安全技能及安全知识的考核： √是 √考核周期：每年一次 √安全技能考核内容： √安全认知考核内容： □否 2.人员录用负责人员是否负责定期对各个岗位人员进行考核： √是 √考核周期：每季度 √考核内容：KPI 考核、价值观考核 □否 备注　新员工入职考核内容已覆盖安全技能及安全认知的考核，此后每年对各岗位人员进行安全培训及考核。	5
	b）应对关键岗位的人员进行全面、严格的安全审查和技能考核；	1.是否对关键岗位的人员进行全面、严格的安全审查和技能考核： √是 □否	5
	c）应对考核结果进行记录并保存。	1.是否对考核记录进行保存： √是，考核记录为：《2015 年度你我金融考核结果》 □否	5

安全意识教育和培训	a）应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训；	1.是否制定信息安全教育及技能培训和考核管理文档，包括但不限于以下内容： √是，管理文档为:《你我金融培训与考核管理制度》 √培训周期：每月一次。 √培训方式：各部门内部培训。 √培训内容:岗位能力提升、安全技术培训等。 □其他： □否 2.培训内容覆盖但不限于以下内容: √安全意识教育 √岗位技能培训 √安全技术培训 □其他：	5
	b）应对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒；	1.是否对违反安全策略和规定的人员进行惩戒: √是 □否 2.安全责任和惩戒措施管理文档是否包含具体的安全责任和惩戒措施： √是，制度内容为:《员工行为规范管理制度》、《办公程序惩戒管理条例》 □否	5
	c）应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训；	1.是否建立安全教育和培训计划文档： □是，培训计划为: √否 2.查看培训计划文档，包含以下内容： □培训方式 □培训对象 □培训内容 □培训时间和地点 3.培训内容是否包含信息安全基础知识、岗位操作规程： □是 √否 备注 经访谈刘经理，公司目前的培训主要针对于岗位技能的培训，未对各岗位人员进行安全意识教育及相关安全技术的培训。人资部目前正在建立信息安全培训机制和培训计划中。	0

	d）应对安全教育和培训的情况和结果进行记录并归档保存。	1.是否有安全教育和培训记录： □是 √否 2.检查安全教育和培训记录，包括但不限于以下内容： □培训人员 □培训内容 □培训结果 □其他：	0
外部人员访问管理	a）应确保在外部人员访问受控区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案；	1.外部人员访问重要区域是否采取了安全措施，采取了哪些安全措施： √是 √经有关部门或负责人书面批准 √由专人全程陪同或监督 √进行记录并备案管理 √其它措施或要求： □否 2.检查是否具有外部人员访问管理文档，包含但不限于以下内容： √是 √明确允许外部人员访问的范围 √外部人员进入的条件 √外部人员进入的访问控制措施 √外部人员离开的条件 □其它措施或要求： □否	5
	b）对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行。	1.是否对外部人员允许访问的范围做出书面规定，并按照规定进行执行： √是，规定为：《你我金融人员安全管理规定》 □否 2.检查外部人员访问重要区域的登记记录，包含以下内容： √外部人员进入时间 √外部人员离开时间 √外部人员访问区域 √外部人员访问设备或信息 √外部人员陪同人 □其它信息：	5

A.10 系统建设管理

安全控制点	测评指标	结果记录	符合程度
系统定级	a）应明确信息系统的边界和安全保护等级；	1.系统定级文档是否有明确信息系统的边界和信息系统的安全保护等级： √是 □否	5
	b）应以书面的形式说明确定信息系统为某个安全保护等级的方法和理由；	1.确定信息系统安全保护等级的方法是否参照定级指南： √是 □否 2.定级过程是否有书面描述： √是 □否	5
	c）应组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定；	1.是否组织相关部门和有关安全技术专家对定级结果进行论证和审定： √是 □否	5
	d）应确保信息系统的定级结果经过相关部门的批准。	1.定级结果是否获得了相关部门的批准： √是 □否	5
安全方案设计	a）应根据系统的安全保护等级选择基本安全措施，并依据风险分析的结果补充和调整安全措施；	1.是否根据系统的安全保护等级选择基本安全措施： □是 □否 2.是否依据风险分析的结果补充和调整安全措施： □是 调整措施有： □否 N/A 本次测评为被测单位第一次测评，已承诺依据风险分析结果补充和调整安全措施。	N/A
	b）应指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划；	1.是否授权专门的部门对信息系统的安全建设进行总体规划： √是 负责部门为：技术中心运维组 □否	5

	c）应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件；	1.是否根据信息系统的等级划分情况统一考虑总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案等： □是 对应文件为： √否 2.以上策略、方案、规划等是否经过专家论证和审定，形成正式文件： □是 √否	0
	d）应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施；	1.以上策略、方案、规划等是否经过正式审批方可实施： □是 √否	0
	e）应根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。	1.是否根据等级测评、安全评估的结果定期调整和修订： □是 维护周期为： √否 2.以上策略、方案、规划等是否有维护记录或修订版本： □是 √否 3.以上策略、方案、规划等维护记录日期间隔与维护周期是否一致： □是 √否 备注 未形成配套文件	0
产品采购和使用	a）应确保安全产品采购和使用符合国家的有关规定；	1.系统使用的有关信息安全产品是否符合国家的有关规定： √符合 □不符合 备注 目前使用的安全产品有 Juniper 防火墙、华为防火墙等，符合国家有关规定。	5

	b）应确保密码产品采购和使用符合国家密码主管部门的要求；	1.系统是否采用了密码产品： □是 √否 2.密码产品的采购和使用是否符合国家密码主管部门的要求： □符合 □不符合 N/A 未使用密码产品	N/A
	c）应指定或授权专门的部门负责产品的采购；	1.是否有专门的部门负责产品的采购： √是 采购部门：技术中心运维组 □否	5
	d）应预先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。	1.采购产品前是否预先对产品进行选型测试确定产品的候选范围： √是 □否 2.是否有产品采购清单指导产品采购： √是 □否 3.是否定期审定和更新候选产品名单： √是 审定周期：每月一次 □否	5
自行软件开发	a）应确保开发环境与实际运行环境物理分开，开发人员和测试人员分离，测试数据和测试结果受到控制；	1.是否进行自主开发软件： √是 □否 2.开发人员和测试人员是否分离： √是 □否 3.开发环境和测试环境是否分离： √是 □否 4.测试数据和测试结果是否受到控制： √是 □否 备注 开发人员、测试人员、生产人员均实行物理隔离。	5

	b）应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；	1.是否制定软件开发管理制度： √是 相关制度文档为：《软件开发管控要求》 2.软件开发管理制度是否明确软件设计、开发、测试、验收过程的控制方法和人员行为准则： √是 □否 3.软件开发管理制度是否明确哪些开发活动应经过授权、审批： √是 □否 4.软件开发管理制度是否明确软件开发相关文档的管理： √是 □否	5
	c）应制定代码编写安全规范，要求开发人员参照规范编写代码；	1.是否制定代码编写安全规范； □是 文件为： √否 2.是否参照代码编写安全规范进行软件开发： □是 √否 备注 没有制定代码编写规范	0
	d）应确保提供软件设计的相关文档和使用指南，并由专人负责保管；	1.是否有明确的软件开发相关文档，并进行了管理： √是 □否 2.软件设计相关文档和使用指南是否由专人负责保管，负责人是何人： √是 负责人：技术中心运维经理 □否	5

	e）应确保对程序资源库的修改、更新、发布进行授权和批准。	1.是否对程序资源库的修改、更新、发布进行授权和批准： √是 授权部门：技术中心运维组 批准人：技术中心运维经理 □否 2.检查对程序资源库的修改、更新、发布进行授权和审批的文档或记录，查看是否有批准人的签字： √是 签字人： □否	5
外包软件开发	a）应根据开发需求检测软件质量；	1.软件交付前是否依据开发要求的技术指标对软件功能和性能等进行验收测试： □是 □否 N/A 无外包软件开发的情况	N/A
	b）应在软件安装之前检测软件包中可能存在的恶意代码；	1.软件安装之前是否检测软件中的恶意代码，检测工具是否是第三方的商业产品： □是 检查工具名称： 第三方公司名称： □否 N/A 无外包软件开发的情况	N/A
	c）应要求开发单位提供软件设计的相关文档和使用指南；	1.开发单位提供软件设计的相关文档和使用指南应包括但不限于： □是 □需求分析说明书 □软件设计说明书 □软件操作手册 □软件源代码文档 □使用指南 □否 N/A 无外包软件开发的情况	N/A
	d）应要求开发单位提供软件源代码，并审查软件中可能存在的后门。	1.是否要求开发单位提供确保软件中不存在后门的软件安全性检查报告或证明： □是 □否 N/A 无外包软件开发的情况	N/A

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；	1.是否有专门部门或人员负责工程实施管理工作： √是 √部门：技术中心运维组 □人员： □否 2.是否要求工程实施单位提供其能够安全实施系统建设的资质证明和能力保证： √是 □否	5
	b）应制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程；	1.是否制定详细的工程实施方案，并按照工程实施方案的要求对工程实施过程进行进度和质量控制： √是 □否	5
	c）应制定工程实施方面的管理制度，明确说明实施过程的控制方法和人员行为准则。	1.是否制定工程实施方面管理制度，规定实施过程的控制方法和人员行为准则： √是 □否	5
测试验收	a）应委托公正的第三方测试单位对系统进行安全性测试，并出具安全性测试报告；	1.是否委托第三方测试机构对信息系统进行独立的安全性测试，并出具相应测试报告： □是 第三方机构名称： √否 备注 仅有研发技术人员进行功能和性能测试，未委托第三方进行安全性测试，没有安全性测试报告。	0
	b）在测试验收前应根据设计方案或合同要求等制定测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告；	1.检查工程测试验收方案，查看其是否明确说明参与测试的部门、人员、测试验收的内容、现场操作过程等： √是 □否 备注 验收测试安排分为系统初验和系统终验，提出系统初验书面申请，验标准将按照“需求说明书”和双方认可的有关系统设计文档所提的要求进行，初验通过后，系统进入正式试运行期，试运行周期一般不超过三个月，终验以图表说明每一测试对象或过程的功能输入输出测试进度，最后通过邮件告知测试结果。	5
	c）应对系统测试验收的控制方法和人员行为准则进行书面规定；	1.测试验收管理文档是否包括系统测试验收的过程控制方法、参与人员的行为规范等内容： √是 □否	5

	d）应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作；	1.是否有专门的部门负责测试验收工作，由何部门负责： √是 负责部门为：技术中心运维组和系统使用部门 □否	5
	e）应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。	1.是否根据设计方案或合同要求组织相关部门和人员对系统测试验收报告进行审定： √是 □否	5
系统交付	a）应制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；	1.是否有交付清单： √是 □否 2.是否根据交付清单清点以下内容（包括但不限于）： □设备 √文档 √软件 备注 交付清单内容主要为系统软件和文档，系统相关硬件设备由技术中心运维组负责采购并提供给研发组进行研发和测试工作，为运维组资产，不需要列入交付清单中。	5
	b）应对负责系统运行维护的技术人员进行相应的技能培训；	1.目前的信息系统是否由内部人员独立运行维护： √是 □否 2.系统正式运行前是否对运行维护人员进行过培训： √是 □否 3.培训内容列举： 系统升级、你我金融niiwoo-rabbit系统安装及使用、open-api系统安装及使用、后台管理系统机构及其维护管理等。	5
	c）应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档；	1.检查是否具有以下文档： √是 √系统建设文档 √指导用户进行系统运维的文档 √系统培训手册 □否	5
	d）应对系统交付的控制方法和人员行为准则进行书面规定；	1.检查系统交付管理文档，查看其是否包括交付过程的控制方法和对交付参与人员的行为限制等方面内容： √包括 □不包括	5

	e）应指定或授权专门的部门负责系统交付的管理工作，并按照管理制度的要求完成系统交付工作。	1.是否有专门的部门负责系统交接工作，并按照规定完成管理系统交付工作： √是 负责部门：技术中心运维组 □否	5
系统备案	a）应指定专门的部门或人员负责管理系统定级的相关材料，并控制这些材料的使用；	1.是否有专门的部门或人员负责管理系统定级相关文档： √是 负责部门：技术中心 负责人员：技术中心运维组经理 □否	5
	b）应将系统等级及相关材料报系统主管部门备案；	1.是否有将系统等级相关材料报主管部门备案的记录或备案文档： √是 □否	5
	c）应将系统等级及其他要求的备案材料报相应公安机关备案。	1.是否有将系统等级相关备案材料报相应公安机关备案的记录或证明： √是 □否	5
等级测评	a）在系统运行过程中，应至少每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改；	1.是否根据要求至少每年对系统进行一次等级测评，并能根据测评结果对不符合项进行及时整改： √是 □否	5
	b）应在系统发生变更时及时对系统进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改；	1.是否在系统发生变更时及时对系统进行等级测评： √是 □否 2.发现级别发生变化的及时调整级别并进行安全改造： √是 □否 3.发现不符合相应等级保护标准要求时，是否及时整改： √是 □否	5
	c）应选择具有国家相关技术资质和安全资质的测评单位进行等级测评；	1.是否选择具有国家相关技术资质和安全资质的测评单位进行等级测评： √是 □否	5

	d）应指定或授权专门的部门或人员负责等级测评的管理。	1.是否指定或授权专门的部门或人员负责等级测评的管理： √是 负责部门：技术中心运维组 负责人员：技术中心运维组经理 □否	5
安全服务商选择	a）应确保安全服务商的选择符合国家的有关规定；	1.选择的信息系统安全服务商是否符合国家有关规定： □是 √否 备注 未选定安全服务商	0
	b）应与选定的安全服务商签订与安全相关的协议，明确约定相关责任；	1.是否具有与安全服务商签订的安全责任合同书或保密协议等文档： □是 √否 2.其内容是否包含但不限于以下方面： □保密范围 □安全责任 □违约责任 □协议的有效期限 □责任人的签字 备注 未选定安全服务商	0
	c）应确保选定的安全服务商提供技术培训和服务承诺，必要的与其签订服务合同。	1.是否具有与安全服务商签订的服务合同： □是 √否 2.其内容是否包含但不限于以下方面： □服务内容 □服务期限 □双方签字或盖章 备注 未选定安全服务商	0

A.11 系统运维管理

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定期对机房供配电、空调、温湿度控制等设施进行维护管理；	1.是否有专门的部门或人员对机房基础设施进行定期维护： √是 维护人员：机房管理员 维护周期：每季度一次 □否	5

	b）应指定部门负责机房安全，并配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理；	1.是否有专门的部门和人员负责机房环境安全管理工作： √是 管理部门：技术中心运维组 □否	5
	c）应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面作出规定；	1.机房安全管理制度是否覆盖但不限于以下方面： √是 √机房物理访问 √物品带进/带出机房 √机房环境安全 □否	5
	d）应加强对办公环境的保密性管理，规范办公环境人员行为，包括工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等。	1.是否建立了办公环境管理文档： √是 □否 2.其内容是否包含但不限于以下方面： √是 √工作人员离开座位时退出登陆状态 √桌面没有敏感信息文件 √人员调离办公室时立即收回钥匙 √不在办公区接待来访人员 □否 备注 对公司办公环境有保密要求，并制定《你我金融电脑设备管理制度》、《你我金融员工信息安全管理制度》等文档进行规定。	5
资产管理	a）应编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；	1.是否建立了资产清单： √是 □否 2.其内容是否包含但不限于以下方面： √资产责任部门 √责任人 √所处位置 √重要程度	5

	b）应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为；	1.是否建立资产安全管理制度： √是 □否 2.是否有资产管理的责任人员或部门： √是 □责任部门：技术中心运维组 □负责人： □否 3.资产安全管理制度是否明确包含但不限于以下方面： √资产管理责任部门 √资产管理责任人 √资产使用 √资产传输 √资产存储 √资产维护	5
	c）应根据资产的重要程度对资产进行定性赋值和标识管理，根据资产的价值选择相应的管理措施；	1.是否依据资产的重要程度对资产进行分类和标识管理： √是 □否 2.不同类别的资产是否采取不同的管理措施： √是 □否	5
	d）应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。	1.信息分类文档中是否明确了信息分类标识的原则和方法： □是 √否	0
介质管理	a）应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定；	1.是否建立了建立介质安全管理制度： √是，《你我金融存储介质管理制度》 □否 2.介质管理制度是否明确包含但不限于以下方面： √介质的存放环境 √介质的使用 √介质的维护	5

	b）应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理；	1.介质的存放环境是否采取保护措施防止介质被盗、被毁、介质内存储信息被未授权修改以及非法泄漏： √是 □否 2.存储环境是否有专人管理： √是 负责人员为：存储环境为东莞东城 IDC 托管机房，有机房管理员 □否	5
	c）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，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点；	1.是否有介质的目录清单： □是 √否 2.是否根据介质的目录清单对介质的使用现状进行定期检查： □是 √否 3.是否定期对其完整性（数据是否损坏或丢失）和可用性（介质是否受到物理破坏）进行检查： □是 √否	0
	d）应对存储介质的使用过程、送出维修以及销毁等进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，对送出维修或销毁的介质应首先清除介质中的敏感数据，对保密性较高的存储介质未经批准不得自行销毁；	1.对带出工作环境的存储介质是否进行内容加密和监控管理： √是 □否 2.保密性较高的介质销毁前是否有领导批准，送出维修或销毁的介质在送出之前是否对介质内存储数据进行净化处理： √是 □否 备注 一般情况存储介质不会带出其工作环境，损坏后一般采取物理破坏，介质中存有敏感数据，在送出维修或销毁时有进行净化处理，并在人员方面有严格控制。	5
	e）应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同；	1.是否对某些重要介质实行异地存储： √是 □否 2.异地存储环境是否与本地环境相同 √是 □否 备注 重要数据信息异地存储至湛江灾备中心，存储环境与东莞东城 IDC 机房相同。	5

	f）应对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理。	1.是否根据所承载数据和软件的重要性对介质进行分类和标识管理： √是 √否 2.带出工作环境的和重要的介质中的数据和软件是否进行保密性处理： □是 √否	0
设备管理	a）应对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	1.是否有专门的部门或人员对各种设备、线路进行定期维护，对各类测试工具进行有效性检查： √是 √责任部门：技术中心运维组 √维护周期：每季度一次 □否	5
	b）应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理；	1.是否建立了配套设施、软硬件维护方面的管理制度： √是 □否 2.是否对设备选用的各个环节（选型、采购、发放和领用、涉外维修和服务及信息处理设备带离机构等）进行审批控制： √是 □否 备注 已制定《你我金融设备管理制度》对设备的使用管理有要求，选型和采购方面遵循总部的制度《你我金融采购管理制度 v1.0》	5
	c）应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等；	1.是否建立了配套设施、软硬件维护方面的管理制度： √是 □否 2.该管理制度是否明确包含但不限于以下方面： √明确维护人员的责任 √涉外维修和服务的审批 √维修过程的监督控制	5

	d）应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；	1.是否对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理： √是 □否 2.对主要设备（包括备份和冗余设备）的操作是否按操作规程进行： √是 □否	5
	e）应确保信息处理设备必须经过审批才能带离机房或办公地点。	1.是否对带离机构的设备进行审批控制： √是 □否 备注　被测单位系统信息处理设备均放置在东莞东城 IDC 机房，设备有特殊情况要代理机房的，需知会技术中心运维经理，注明原因，经审批同意后可实施，且 IDC 机房有放行条制度。	5
监控管理和安全管理中心	a）应对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存；	1.是否形成监测记录文档： √是 □否 2.是否组织人员对监测记录进行整理并保管： √是 □否 备注　被测单位使用 Zabbix 监控系统实时全局监控，其主要功能有 CPU 负荷、内存使用、磁盘使用、网络状况、端口监视、日志监视等，发现异常行为通过邮件和短信的形式及时告知管理员。	5
	b）应组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施；	1.是否组织人员定期对监测记录进行分析、评审： √是 □否 2.是否发现可疑行为并对其采取必要的措施： √是 □否 3.是否形成分析报告： □是 √否 4.分析报告是否包括监测的异常现象、处理措施等： □是 √否 备注　出现异常行为通过短信和邮件及时告知管理人员，运维组管理人员每天登录 Zabbix 系统查看监控记录，进行分析评审，但未形成文档化分析报告。	3

	c）应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。	1.是否建立安全管理中心： √是 □否 2.是否对下列安全相关事项进行集中管理： √通信线路、主机、网络设备和应用软件的运行状况 √设备状态 √恶意代码 √网络流量 √补丁升级 □安全审计	5
网络安全管理	a）应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；	1.是否指定专人负责维护网络运行日志、监控记录和分析处理报警信息等网络安全管理工作： √是 负责人： □否 2.是否有网络审计日志： √是 √否 3.日志是否在规定的保存时间范围内： √是 □否	5
	b）应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定；	1.是否建立网络安全管理制度： √是 □否 2.网络安全管理制度是否包含但不限于以下内容： √网络安全配置 √安全策略 √升级与打补丁 □最小服务 √授权访问 √日志保存时间 √口令更新周期 √文件备份	5

	c）应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；	1.是否根据厂家提供的软件升级版本对网络设备进行过升级： √是 □否 3.升级前是否对重要文件（帐户数据、设备配置文件等）进行备份： √是 备份方式为：定期备份，变更后及时进行备份 □否	5
	d）应定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补；	1.是否定期对网络设备进行漏洞扫描： √是 扫描周期：每年一次 □否 2.发现漏洞是否及时修补： √是 □否	5
	e）应实现设备的最小服务配置，并对配置文件进行定期离线备份；	1.是否实现网络设备的最小服务配置： √是 □否 2.对配置文件是否进行定期离线备份： √是 备份方式：定期备份，变更后及时进行备份。 □否	5
	f）应保证所有与外部系统的连接均得到授权和批准；	1.是否所有与外部系统的连接均得到授权和批准： √是 审批部门：技术中心 □否	5
	g）应依据安全策略允许或者拒绝便携式和移动式设备的网络接入；	1.是否建立了安全策略： √是 □否 2.安全策略是否包括允许或者拒绝便携式和移动式设备的网络接入： √是 □否	5
	h）应定期检查违反规定拨号上网或其他违反网络安全策略的行为。	1.是否定期检查拨号上网等违反网络安全策略的行为： √是 □否	5

系统安全管理	a）应根据业务需求和系统安全分析确定系统的访问控制策略；	1.是否根据业务需求和系统安全分析制定系统的访问控制策略，控制分配信息系统、文件及服务的访问权限： √是 □否	5
	b）应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补；	1.是否定期对系统进行漏洞扫描： √是 扫描周期：每年一次 □否 2.发现漏洞是否及时修补： √是 □否	5
	c）应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；	1.询问是否定期对系统安装安全补丁程序： √是 □否 2.在安装系统补丁前是否对重要文件进行备份： √是 备份方式：在线备份 □否 3.是否先在测试环境中测试通过再安装： √是 □否 备注 系统安装补丁之前，一般进行测试1天，并加入到监控系统中实时监控，有技术人员对测试系统的稳定性进行评估，确保系统无异常后实施系统补丁安装。	5
	d）应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定；	1.是否建立系统安全管理制度： √是 □否 2.系统安全管理制度是否包含但不限于以下内容： √是 √系统安全策略 √安全配置 √日志管理 √日常操作流程 □否	5

	e）应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则；	1.是否指定专人对系统进行管理： □是 人员为： √否 2.系统管理员用户是否进行了分类，明确了各个角色的权限、责任和风险： √是 √否 3.权限设定是否遵循最小授权原则： √是 √否 备注 存在两名管理员共用同一个账号的情况。	0
	f）应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作；	1.是否有详细操作日志： √是 □否 2.操作日志是否包含但不限于以下内容： √重要的日常操作 √运行维护记录 √参数的设置和修改 备注 检查上线操作日志，内容包括有上线日期、上线类型、上线内容、项目经理、上线时间等。	5
	g）应定期对运行日志和审计数据进行分析，以便及时发现异常行为。	1.是否有定期对运行日志和审计结果进行分析的分析报告： □是 √否 2.分析报告是否包含但不限于以下内容： □能够记录帐户的连续多次登录失败 □非工作时间的登录 □访问受限系统或文件的失败尝试 □系统错误	0
恶意代码防范管理	a）应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查；	1.是否对员工进行基本恶意代码防范意识教育： √是 □否 2.意识教育是否包含但不限于以下内容： √告知应及时升级软件版本 √使用外来设备、网络上接收文件和外来计算机或存储设备接入	5

	b）应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；	1.是否指定专人对恶意代码进行检测： √是 负责人：网络管理员 □否 2.发现病毒后是否及时处理： √是 □否	5
	c）应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定；	1.是否具有恶意代码检测记录、恶意代码库升级记录和分析报告： □是 √否 2.升级记录是否记录升级时间、升级版本等内容： √是 □否	5
	d）应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。	1.是否定期检查恶意代码库的升级情况： □是 √否 2.对截获的危险病毒或恶意代码是否及时进行分析处理，并形成书面的报表和总结汇报： □是 √否	0
密码管理	a）应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。	1.是否有密码使用管理制度： □是 □否 2.密码技术和产品的使用是否遵照国家密码管理规定： □是 □否 N/A 未使用密码产品	N/A
变更管理	a）应确认系统中要发生的变更，并制定变更方案；	1.是否制定了变更方案指导系统执行变更： √是 □否 2.重要系统变更前是否制定： √变更方案 √失败恢复方案 √专项应急预案	5

	b）应建立变更管理制度，系统发生变更前，向主管领导申请，变更和变更方案经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告；	1.是否建立了变更管理制度： √是 □否 2.变更管理制度是否包含但不限于以下内容： √变更前审批 √变更过程记录 √变更后通报 备注 系统变更控制流程：由项目经理提出变更申请，通过邮件发送个技术中心总监审核，批复同意后实施变更，并在变更完成后在内部邮件通告，对用户使用短信告知。已制定《你我金融信息系统变更管理制度》。	5
	c）应建立变更控制的申报和审批文件化程序，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录；	1.重要系统变更前是否根据申报和审批程序得到有关领导的批准： √是 批准人：技术中心总监 □否 2.对发生的变更情况是否通知了所有相关人员： √是 通知方式：内部邮件 □否	5
	d）应建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。	1.变更失败后的恢复程序、工作方法和人员职责等是否文档化： □是 √否 2.恢复过程是否经过演练： □是 √否	0
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；	1.是否识别出需要定期备份的业务信息、系统数据及软件系统等： √是 □否 2.是否有相应的列表清单： √是 □否 备注 需要定期备份的主要有数据库、源代码等，备份策略分别为：数据库一天 2 全备、保存在 EMC 存储，保存 3 个月；源代码一天一全备、保存于硬盘，永久保存。	5

	b）应建立备份与恢复管理相关的安全管理制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范；	1.是否建立了备份和恢复管理制度： √是 □否 2.备份和恢复管理制度是否包含但不限于以下内容： √备份方式 √备份频度 √保存期 √存储介质 备注 已制定《你我金融数据备份管理制度》。	5
	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，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法；	1.数据备份和恢复策略文档内容是否包含但不限于以下内容： √是 √数据的存放场所 √文件命名规则 √介质替换频率 √数据离站传输方法 □否	5
	d）应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存；	1.是否建立了控制数据备份和恢复过程的程序： √是 □否 1.备份和恢复记录是否包含但不限于以下内容： √备份内容 √备份操作 √备份介质存放 3.记录内容与备份和恢复策略是否一致： √是 □否	5
	e）应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。	1.是否定期执行恢复程序： □是 恢复周期： √否 2.系统是否按照恢复程序完成恢复，如有问题，是否针对问题改进恢复程序或调整其他因素： □是 √否	0
安全事件处置	a）应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；	1.是否告知用户在发现安全弱点和可疑事件时应及时报告： √是 □否	5

	b）应制定安全事件报告和处置管理制度，明确安全事件的类型，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；	1.是否建立了安全事件报告和处置管理制度： √是 □否 2.安全事件报告和处置管理制度是否包含但不限于以下内容： √本系统已发生的和需要防止发生的安全事件类型 √安全事件的现场处理 √事件报告和后期恢复的管理职责	5
	c）应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分；	1.是否根据本系统已发生的和需要防止发生的安全事件对系统的影响程度划分不同等级： √是 等级划分级数为：四级 □否 2.划分方法是否参照了国家相关管理部门的技术资料： √是 □否	5
	d）应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等；	1.是否建立了安全事件报告和响应处理程序： √是 □否 2.安全事件报告和响应处理程序是否包含但不限于以下内容： √响应和处置的范围、程度、处理方法 √具体报告方式、报告内容、报告人	5
	e）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，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存；	1.安全事件记录分析文档是否记录引发安全事件的原因： √是 □否 2.安全事件记录分析文档是否记录事件处理过程： √是 □否 3.不同安全事件是否采取不同措施避免其再次发生： √是 □否 备注 已制定系统安全事件响应程序，发生安全事件，第一时间向相关负责人员和技术中心总监报告。目前未发生过安全事件。	5

	f）对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。	1.是否针对不同安全事件采取不同的处理和报告程序： □是 √否	0
应急预案管理	a）应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；	1.是否在统一的应急预案框架下制定不同事件的应急预案： √是 □否 2.应急预案框架是否包含但不限于以下内容： √启动应急预案的条件 √应急处理流程 √系统恢复流程 √事后教育和培训 备注 已制定《你我金融系统运行整体应急框架》，管理规定内容包括应急资源、应急预案体系和组织框架、预防和预警、应急响应等。	5
	b）应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；	1.是否具有应急预案小组： √是 □否 2.应急预案执行所需资金是否做过预算并能够落实： √是 □否	5
	c）应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次；	1.是否对系统相关人员进行应急预案培训： □是 培训周期： √否	0
	d）应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期；	1.是否定期对应急预案进行演练： □是 演练周期： √否	0
	e）应规定应急预案需要定期审查和根据实际情况更新的内容，并按照执行。	1.是否对应急预案定期进行审查，并根据实际情况进行更新内容： □是 √否	0

[附录 A 完]

附录 B 验证测试（已修复）

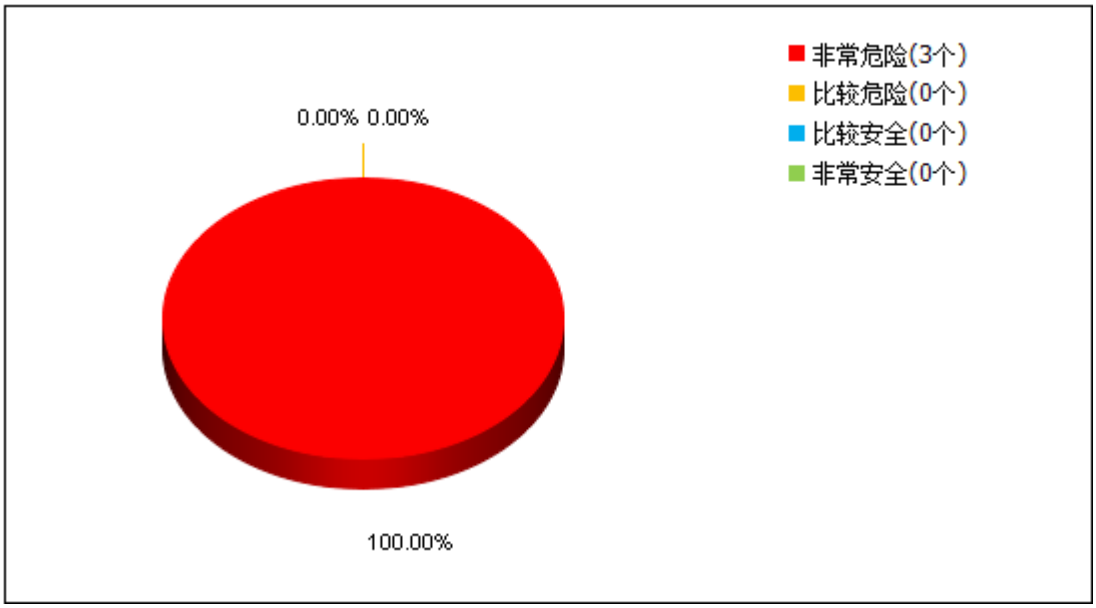
1 概述

1.1 检测结果

本次安全漏洞扫描对象为 192.168.10.14、192.168.10.15、192.168.10.34 三台主机系统。扫描结果：发现高危漏洞 4 个，中危漏洞 13 个。通过统计分析，此网段的主机存在安全隐患，建议系统管理人员及时修复。

1.1.1 主机情况统计

本次扫描共检测主机数 3 台，不同安全级别的主机数量及分布如下图：

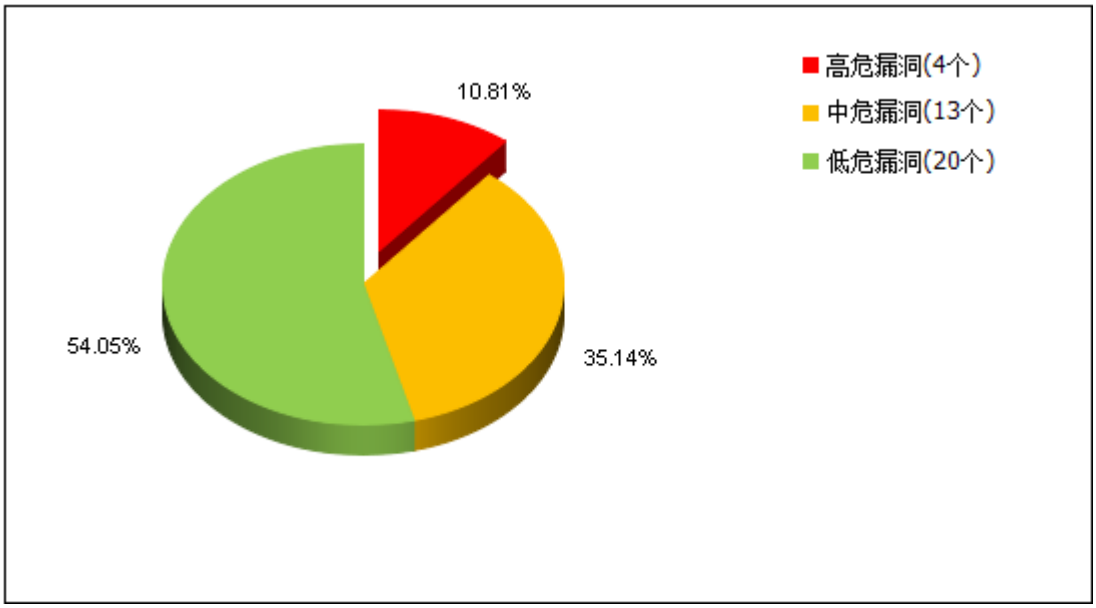


1.1.2 漏洞情况统计

高、中危漏洞数量和漏洞总数列表如下：

漏洞总数	高危漏洞	中危漏洞	低危漏洞
37	4	13	20

高、中、低危漏洞数量及饼图分布如下：



1.2 检测工具

为保证检测结果的真实性和有效性，避免遗漏，此次检测采用了专业远程安全评估系统进行安全扫描。

工具系统版本号及升级日期：

工具版本号	V6.0R02F00.0143			
已安装升级包：				
名称	**文件大小**	**发布日期**	**安装日期**	**描述**
rsas-vulsys-V6.0R02F00.0143.dat	8.0K	2016-3-11	2016-3-22	增加了系统插件。
rsas-vulsys-V6.0R02F00.0142.dat	11.8M	2016-3-11	2016-3-22	增加了系统插件。
rsas-vulsys-V6.0R02F00.0141.dat	9.7M	2016-3-07	2016-3-22	增加了系统插件。

2 检测内容

本次远程安全检测服务的检测内容包括：

1) 操作系统漏洞检测；
2) 应用服务漏洞检测；
3) 网络设备和防火墙策略检测；
4) 敏感信息泄露检测。

检测策略数量如下：

总共检测策略数量	
Windows 系列	[2282]
Unix/Linux 系列	[2218]
网络设备和防火墙	[1449]
网络信息收集	[1717]
高危漏洞扫描	[1407]
全部漏洞扫描	[3100]
DNS 检测	[47]

根据不同分类方法具体数量如下：

各分类检测策略数量			
服务 **（共 35 类）**	AntiVirus [15] BT [8] CGI [276] CVS [14] DCE/RPC [3] DNS [39] FTP [122] Finger [16] Firewall [8] IMAP [24] Kerberos [3]	Kernel [31] LDAP [4] NNTP [6] ONC/RPC [56] POP3 [19] RTSP [9] R 系列服务 [9] SMB [193] SMTP [74] SNMP [38] SSH [35]	TFTP [5] Telnet [43] WWW [547] X Window [4] 其他 [503] 打印服务 [9] 数据库 [239] 木马和后门 [37] 系统补丁 [564] 远程管理 [18]
应用 **（共 69 类）**	AnalogX [7] Apache [206] ArGoSoft [3] BIND [35] CVS [15] CheckPoint [6] Cisco [46] Cyrus [5] DB2 [30] Exchange [6]	Netscape Server [12] Nortel [6] Novell [6] OpenLDAP [3] OpenSSH [20] Oracle [95] PHP [89] Proftpd [17] Qpopper [4] RPC [21]	Sybase [14] Symantec [8] Terminal Server [4] Thttpd [5] Tomcat [18] Trend Micro [4] UW-imap [4] VNC [2] WU-FTPD [10] WarFTPd [5]

各分类检测策略数量			
	HP LaserJet [4] IIS [106] Informix [2] Ipswitch [11] JRun [5] Lotus Domino [14] MDaemon [8] MS SQL Server [43] McAfee [3] Mercur [5] MySQL [59]	Radmin [3] RealServer [6] Resin [6] SSH [13] Samba [32] Sambar [9] Sendmail [22] Serv-U [15] Snmpd [18] Squid [5]	WebLogic [12] WebSphere [9] Windows SMB [70] Windows 补丁 [651] Zope [5] cfingerd [7] iPlanet [6] pcAnywhere [3] snmpXdmid [1] 其他 [1113]
系统 **（共 14 类）**	AIX [3] BSD [3] HP-UX [3] IRIX [5] Linux [36]	MacOS [2] NetWare [7] Solaris [21] UNIX 通用 [431]	Windows [1373] 其他 [1] 系统无关 [985] 网络设备/防火墙 [102]
威胁 **（共 7 类）**	不必要的服务 [162] 其他 [343] 本地权限提升 [129]	远程信息泄露 [822] 远程执行命令 [900]	远程拒绝服务 [442] 远程数据修改 [171]

3 检测对象列表

本次远程安全检测的对象为甲方提供的 3 台主机系统：

IP 地址	主机名	操作系统	风险程度
192.168.10.34		Linux	高
192.168.10.15		Linux	高
192.168.10.14		Linux	高

4 详细检测结果

4. 1 主机详细信息

此部分列出的漏洞信息是经过分析后，把同一安全问题产生的多个漏洞进行合

并，以方便管理人员进行安全修复，所以数量上与统计报表有差异。

1）192.168.10.34

漏洞	漏洞风险
H1）OpenSSH roaming_common.c 堆缓冲区溢出漏洞(CVE-2016-0778）	高
H2）Openssh MaxAuthTries 限制绕过漏洞(CVE-2015-5600）	高
H4）OpenSSH J-PAKE 授权问题漏洞(CVE-2010-4478）	高
M1 ） OpenSSH sshd mm_answer_pam_free_ctx 释放后重利用漏洞(CVE-2015-6564）	中
M5）OpenSSH 默认服务器配置拒绝服务漏洞(CVE-2010-5107）	中
M11）OpenSSH glob 表达式拒绝服务漏洞(CVE-2010-4755）	中
M12）Portable OpenSSH 'ssh-keysign'本地未授权访问漏洞	中
M13）OpenSSH 'x11_open_helper() '函数安全限制绕过漏洞(CVE-2015-5352）	中

2）192.168.10.15

漏洞	漏洞风险
H1）OpenSSH roaming_common.c 堆缓冲区溢出漏洞(CVE-2016-0778）	高
H2）Openssh MaxAuthTries 限制绕过漏洞(CVE-2015-5600）	高
H4）OpenSSH J-PAKE 授权问题漏洞(CVE-2010-4478）	高
M1 ） OpenSSH sshd mm_answer_pam_free_ctx 释放后重利用漏洞(CVE-2015-6564）	中
M5）OpenSSH 默认服务器配置拒绝服务漏洞(CVE-2010-5107）	中
M6）Apache Tomcat Security Manager 绕过漏洞(CVE-2014-7810）	中
M11）OpenSSH glob 表达式拒绝服务漏洞(CVE-2010-4755）	中
M12）Portable OpenSSH 'ssh-keysign'本地未授权访问漏洞	中
M13）OpenSSH 'x11_open_helper() '函数安全限制绕过漏洞(CVE-2015-5352）	中

3）192.168.10.14

漏洞	漏洞风险
H3）Apache Tomcat 拒绝服务漏洞(CVE-2014-0230）	高
M2）Apache Tomcat 安全漏洞(CVE-2014-0227）	中

M3）Apache Commons FileUpload 和 Tomcat 拒绝服务漏洞(CVE-2014-0050）	中
M4）Apache Tomcat 块请求远程拒绝服务漏洞（CVE-2014-0075）	中
M6）Apache Tomcat Security Manager 绕过漏洞(CVE-2014-7810）	中
M7）Apache Tomcat 权限许可和访问控制漏洞(CVE-2014-0119）	中
M8）Apache Tomcat 权限许可和访问控制漏洞(CVE-2014-0096）	中
M9）Apache Tomcat 整数溢出漏洞(CVE-2014-0099）	中
M10）Apache Tomcat XML 外部实体信息泄露漏洞(CVE-2013-4590）	中

4. 2 漏洞详细信息

4. 2. 1 高危漏洞

H1）OpenSSH roaming_common.c 堆缓冲区溢出漏洞(CVE-2016-0778）

风险等级	**高**
漏洞描述	OpenSSH 是 SSH 协议的开源实现。 OpenSSH 5.x, 6.x, 7.1p2 之前的 7.x 版本，启用了某些代理及转发选项后，roaming_common.c 内的函数 roaming_read 及 roaming_write 未正确保留连接文件描述符，这可使远程服务器造成拒绝服务（堆缓冲区溢出）。
修补方法	OpenSSH/5.3: 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://www.openssh.com/txt/release-7.1p2
CVE 编号	CVE-2016-0778
BUGTRAQ	
涉及主机	192.168.10.15; 192.168.10.34;

H2）Openssh MaxAuthTries 限制绕过漏洞(CVE-2015-5600）

风险等级	**高**
漏洞描述	OpenSSH（OpenBSD Secure Shell）是 OpenBSD 计划组所维护的一套用于安全访问远程计算机的连接工具。该工具是 SSH 协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。 OpenSSH 6.9 及之前版本的 sshd 中的 auth2-chall.c 文件中的‘kbdint_next_device’函数存在安全漏洞，该漏洞源于程序没有正确限制处理单链接中的 keyboard-interactive 设备。远程攻击者可借助 ssh -oKbdInteractiveDevices 选项中较长且重复的列表利用该漏洞实施暴力破解

	攻击，或造成拒绝服务（CPU 消耗）。
修补方法	OpenSSH/5.3: 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://www.openssh.com/ http://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/auth2-chall.c.diff?r1=1.42&r2=1.43&f=h
CVE 编号	CVE-2015-5600
BUGTRAQ	
涉及主机	192.168.10.15; 192.168.10.34;

H3）Apache Tomcat 拒绝服务漏洞(CVE-2014-0230）

风险等级	**高**
漏洞描述	Apache Tomcat 是一个流行的开源 JSP 应用服务器程序。 未读完请求体，即将对该请求的响应返回给用户代理后，Tomcat 默认会信任剩下的请求体，接着处理连接上的下一个请求。Tomcat 对信任的请求体大小没有限制。Tomcat 不会关闭连接，处理线程也会保持连接，这可导致有限的拒绝服务。
修补方法	Tomcat/7.0.47: 厂商补丁： Apache Group ---------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： [1] http://tomcat.apache.org/security-8.html [2] http://tomcat.apache.org/security-7.html [3] http://tomcat.apache.org/security-6.html [4] http://www.openwall.com/lists/oss-security/2015/04/10/1
CVE 编号	CVE-2014-0230
BUGTRAQ	74475
涉及主机	192.168.10.14;

H4）OpenSSH J-PAKE 授权问题漏洞(CVE-2010-4478）

风险等级	**高**
漏洞描述	OpenSSH 是 SSH 协议组的实现，可为各种服务提供加密的认证传输，包括远程 shell 访问。 当 J-PAKE 启用时，OpenSSH 5.6 及之前版本不能正确验证 J-PAKE 协议中的公共参数。远程攻击者可以通过发送每一轮协议中的特制值绕过共享秘密信息

	的需求，并成功获得认证。 对于以下未给出 openssh 漏洞受影响范围的情况，请联系厂商确认其当前版本是否存在此问题,suse 系统确认不受漏洞的影响。
修补方法	OpenSSH/5.3: 厂商补丁： OpenSSH ------- 目前厂商已经发布升级版本修复此安全问题，建议升级 OpenSSH 至 5.6 版本之后版本，请到厂商的官方页面下载升级版本： http://www.openssh.com/openbsd.html 对于具体 Linux 发行版中使用的版本，可以参考如下链接，确认系统是否受该漏洞影响： Debian: https://security-tracker.debian.org/tracker/CVE-2010-4478 Gentoo: http://www.gentoo.org/security/en/glsa/glsa-201405-06.xml Ubuntu: http://people.canonical.com/~ubuntu-security/cve/2010/CVE-2010-4478.html Redhat： https://access.redhat.com/security/cve/CVE-2010-4478 SUSE: http://support.novell.com/security/cve/CVE-2010-4478.html
CVE 编号	CVE-2010-4478
BUGTRAQ	
涉及主机	192.168.10.15; 192.168.10.34;

4.2.2 中危漏洞

M1） OpenSSH sshd mm_answer_pam_free_ctx 释放后重利用漏洞(CVE-2015-6564）

风险等级	中
漏洞描述	OpenSSH 是 SSH 协议的开源实现。 非 OpenBSD 平台上 OpenSSH 7.0 之前版本，sshd 内 monitor.c 的 mm_answer_pam_free_ctx 函数存在释放后重利用漏洞，这可使本地用户利用 sshd uid 控制，发送构造的 MONITOR_REQ_PAM_FREE_CTX 请求，获取提升的权限。
修补方法	OpenSSH/5.3： 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://www.openssh.com/txt/release-7.0 https://github.com/openssh/openssh-portable/commit/d4697fe9a28dab7255c

	60433e4dd23cf7fce8a8b http://seclists.org/fulldisclosure/2015/Aug/54
CVE 编号	CVE-2015-6564
BUGTRAQ	
涉及主机	192.168.10.15; 192.168.10.34;

M2） Apache Tomcat 安全漏洞(CVE-2014-0227）

风险等级	中
漏洞描述	Apache Tomcat 是美国阿帕奇（Apache）软件基金会下属的 Jakarta 项目的一款轻量级 Web 应用服务器，它主要用于开发和调试 JSP 程序，适用于中小型系统。 Apache Tomcat 中的 java/org/apache/coyote/http11/filters/ChunkedInputFilter.java 文件存在安全漏洞，该漏洞源于程序出现错误时，没有正确限制读取数据。远程攻击者可通过发送带有畸形编码块的流数据利用该漏洞实施 HTTP 请求走私攻击，或造成拒绝服务（资源耗尽）。以下版本受到影响：Apache Tomcat 6.0.42 之前的 6.x 版本，7.0.55 之前的 7.x 版本，8.0.9 之前的 8.x 版本。
修补方法	Tomcat/7.0.47： 厂商补丁： Apache Group ---------- Apache Group 已经为此发布了一个安全公告（CVE-2014-0227）以及相应补丁: CVE-2014-0227： Fixed in Apache Tomcat 6.0.43 链接： http://tomcat.apache.org/security-6.html 补丁下载： http://svn.apache.org/viewvc?view=rev&rev=1603628
CVE 编号	CVE-2014-0227
BUGTRAQ	
涉及主机	192.168.10.14;

M3） Apache Commons FileUpload 和 Tomcat 拒绝服务漏洞(CVE-2014-0050）

风险等级	中
漏洞描述	Apache Commons FileUpload 软件包可以向小服务程序和 Web 应用添加高性能的文件上传功能。 Apache Commons FileUpload 1.0-1.3、Apache Tomcat 8.0.0-RC1 - 8.0.1、Apache Tomcat 7.0.0 - 7.0.50 在解析多部分请求的畸形内容类型报文头时，可触发安全漏洞，造成无限循环，导致程序崩溃。
修补方法	Tomcat/7.0.47： 厂商补丁：

	Apache Group ---------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://commons.apache.org/proper/commons-fileupload// http://svn.apache.org/viewvc?view=revision&revision=1565169
CVE 编号	CVE-2014-0050
BUGTRAQ	65400
涉及主机	192.168.10.14;

M4） Apache Tomcat 块请求远程拒绝服务漏洞（CVE-2014-0075）

风险等级	中
漏洞描述	Apache Tomcat 是一个流行的开源 JSP 应用服务器程序。 Apache Tomcat 8.0.0-RC1-8.0.3、7.0.0 - 7.0.52、6.0.0 - 6.0.39 版本对畸形块尺寸的请求存在安全漏洞，这可使大量的数据发送到服务器，绕过对请求的各种尺寸限制，导致拒绝服务。
修补方法	Tomcat/7.0.47： 厂商补丁： Apache Group ---------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： [1] http://tomcat.apache.org/security-8.html [2] http://tomcat.apache.org/security-7.html [3] http://tomcat.apache.org/security-6.html
CVE 编号	CVE-2014-0075
BUGTRAQ	67671
涉及主机	192.168.10.14;

M5） OpenSSH 默认服务器配置拒绝服务漏洞(CVE-2010-5107）

风险等级	中
漏洞描述	OpenSSH 是 SSH 协议的开源实现。 OpenSSH 的默认服务器配置在管理连接槽的实现上存在拒绝服务漏洞，远程攻击者可利用此漏洞耗尽服务器上连接槽，触发拒绝服务。
修补方法	OpenSSH/5.3： 厂商补丁： The openssh Project --------- 目前厂商已经发布升级版本修复此安全问题，建议升级 openssh 至 6.1 版本或之后版本，请到厂商的官方页面下载升级版本： 链接：http://www.openssh.com/portable.html

	此漏洞扫描采用的是版本扫描，不同发行版本系统的 OpenSSH 版本存在差异，可能存在误报。 对于具体 Linux 发行版本中使用的版本，可以参考如下链接，确认是否受该漏洞影响： Debian: https://security-tracker.debian.org/tracker/CVE-2010-5107 Ubuntu: http://people.canonical.com/~ubuntu-security/cve/2014/CVE-2010-5107.html Redhat： https://access.redhat.com/security/cve/CVE-2010-5107 SUSE: http://support.novell.com/security/cve/CVE-2010-5107.html Gentoo: http://www.gentoo.org/security/en/glsa/glsa-201405-06.xml Aix: http://aix.software.ibm.com/aix/efixes/security/openssh_advisory2.asc Fedora: https://lists.fedoraproject.org/pipermail/package-announce/2013-February/099281.html
CVE 编号	CVE-2010-5107
BUGTRAQ	58162
涉及主机	192.168.10.15; 192.168.10.34;

M6） Apache Tomcat Security Manager 绕过漏洞(CVE-2014-7810）

风险等级	中
漏洞描述	Apache Tomcat 是一个流行的开源 JSP 应用服务器程序。 Apache Tomcat 8.0.0-RC1 至 8.0.15、7.0.0 至 7.0.57、6.0.0 至 6.0.43 版本，在特权代码区评估表达式的实现上存在安全限制绕过漏洞，攻击者利用此漏洞可绕过 Security Manager 保护机制。
修补方法	Tomcat/7.0.56： ， Tomcat/7.0.47： 厂商补丁： Apache Group ---------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： [1] http://tomcat.apache.org/security-8.html [2] http://tomcat.apache.org/security-7.html [3] http://tomcat.apache.org/security-6.html
CVE 编号	CVE-2014-7810
BUGTRAQ	

涉及主机	192.168.10.14; 192.168.10.15;

M7） Apache Tomcat 权限许可和访问控制漏洞(CVE-2014-0119）

风险等级	中
漏洞描述	Apache Tomcat 是美国阿帕奇（Apache）软件基金会下属的 Jakarta 项目的一款轻量级 Web 应用服务器，它主要用于开发和调试 JSP 程序，适用于中小型系统。 Apache Tomcat 中存在安全漏洞，该漏洞源于程序没有正确限制类加载器访问使用 XSLT 样式表的 XML 解析器。远程攻击者可借助特制的 Web 应用程序利用该漏洞读取任意文件，或读取不同 Web 应用程序相关的文件。以下版本受到影响：Apache Tomcat 6.0.39 及之前的版本，7.0.54 之前的 7.x 版本，8.0.6 之前的 8.x 版本。
修补方法	Tomcat/7.0.47： 目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.54
CVE 编号	CVE-2014-0119
BUGTRAQ	
涉及主机	192.168.10.14;

M8） Apache Tomcat 权限许可和访问控制漏洞(CVE-2014-0096）

风险等级	中
漏洞描述	Apache Tomcat 是美国阿帕奇（Apache）软件基金会下属的 Jakarta 项目的一款轻量级 Web 应用服务器，它主要用于开发和调试 JSP 程序，适用于中小型系统。 Apache Tomcat 的默认 servlet 中的 java/org/apache/catalina/servlets/DefaultServlet.java 文件存在安全漏洞，该漏洞源于程序没有正确限制 XSLT 样式表。远程攻击者可借助特制的应用程序利用该漏洞绕过安全限制，读取任意文件。以下版本受到影响：Apache Tomcat 6.0.39 及之前的版本，7.0.53 之前的 7.x 版本，8.0.4 之前的 8.x 版本。
修补方法	Tomcat/7.0.47： 目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.53
CVE 编号	CVE-2014-0096
BUGTRAQ	
涉及主机	192.168.10.14;

M9） Apache Tomcat 整数溢出漏洞(CVE-2014-0099）

风险等级	中
漏洞描述	Apache Tomcat 是美国阿帕奇（Apache）软件基金会下属的 Jakarta 项目的一

	款轻量级 Web 应用服务器，它主要用于开发和调试 JSP 程序，适用于中小型系统。 Apache Tomcat 中的 java/org/apache/tomcat/util/buf/Ascii.java 文件存在整数溢出漏洞。远程攻击者可借助特制的 Content-Length HTTP 头利用该漏洞实施 HTTP 请求走私攻击。以下版本受到影响：Apache Tomcat 6.0.39 及之前的版本，7.0.53 之前的 7.x 版本，8.0.4 之前的 8.x 版本。
修补方法	Tomcat/7.0.47： 目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.53
CVE 编号	CVE-2014-0099
BUGTRAQ	
涉及主机	192.168.10.14;

M10） Apache Tomcat XML 外部实体信息泄露漏洞(CVE-2013-4590）

风险等级	中
漏洞描述	Apache Tomcat 是一个流行的开源 JSP 应用服务器程序。 Tomcat 8.0.0-RC1 - 8.0.0-RC5、7.0.0 - 7.0.47、6.0.0 - 6.0.37 版本的 XML(例如：web.xml, context.xml, *.tld, *.tagx, *.jspx）文件允许 XXE，这可使攻击者获取 Tomcat 内部敏感信息。
修补方法	Tomcat/7.0.47： 厂商补丁： Apache Group ---------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://jakarta.apache.org/tomcat/index.html [1] http://tomcat.apache.org/security-8.html [2] http://tomcat.apache.org/security-7.html [3] http://tomcat.apache.org/security-6.html
CVE 编号	CVE-2013-4590
BUGTRAQ	65768
涉及主机	192.168.10.14;

M11） OpenSSH glob 表达式拒绝服务漏洞(CVE-2010-4755）

风险等级	中
漏洞描述	OpenSSH 是 SSH 协议组的实现，可为各种服务提供加密的认证传输，包括远程 shell 访问。 在 FreeBSD 7.3 和 8.1 版本，NetBSD 5.0.2 版本，和 OpenBSD 4.7 版本，及其他产品中使用的 OpenSSH 5.8 及之前版本的（1）sftp-glob.c 中的 remote_glob 函数和（2）sftp.c 中的 process_put 函数中存在漏洞。远程认证用户可以借

	助不匹配任何路径名称的特制 glob 表达式导致拒绝服务（CPU 和内存消耗）。
修补方法	OpenSSH/5.3： 厂商补丁： OpenSSH ------- 目前厂商已经发布升级版本修复此安全问题，建议升级 OpenSSH 至 5.8 之后版本，请到厂商的官方页面下载升级版本： http://www.openssh.com/openbsd.html 对于具体 Linux 发行版中使用的版本，可以参考如下链接，确认系统是否受该漏洞影响： NetBSD: http://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2010-008.txt.asc Gentoo: http://www.gentoo.org/security/en/glsa/glsa-201405-06.xml Redhat： https://access.redhat.com/security/cve/CVE-2010-4755
CVE 编号	CVE-2010-4755
BUGTRAQ	
涉及主机	192.168.10.15; 192.168.10.34;

M12） Portable OpenSSH 'ssh-keysign'本地未授权访问漏洞

风险等级	中
漏洞描述	OpenSSH 是一款 SSH 协议开放源代码实现。如果使用了 ssh-rand-helper，Portable OpenSSH 的 ssh-keysign 工具允许未授权本地访问平台上的主机密钥。ssh-keysign 是一款 setuid 帮助程序用于在基于宿主机验证过程中间接访问宿主的主机私钥。其会使用提升特权来打开密钥，然后立即丢弃特权完成它的加密签名操作。在丢弃特权后，ssh-keysign 会依赖 OpenSSl 的随机生成器。在 OpenSSL 中缺少内置熵来源的配置中，ssh-keysign 会执行 ssh-rand-helper 程序尝试从系统环境中获取随机数。但是，宿主私钥文件的文件描述符在执行 ssh-rand-helper 之前没有正确关闭，由于这个进程是"born unprivileged"并继承敏感文件描述符，没有对攻击者使用 ptrace(2）挂接进行保护，可导致最后读出私钥信息。
修补方法	OpenSSH/5.3： OpenSSH 5.8 p2 已经修复此漏洞，建议用户下载使用： http://www.openssh.com/
CVE 编号	
BUGTRAQ	47691
涉及主机	192.168.10.15; 192.168.10.34;

M13） OpenSSH 'x11_open_helper()'函数安全限制绕过漏洞(CVE-2015-5352）

风险等级	中
漏洞描述	OpenSSH 是 SSH (Secure SHell）协议的免费开源实现。SSH 协议族可以用来进行远程控制，或在计算机之间传送文件。 OpenSSH 6.9 之前版本，使用非 ForwardX11Trusted 模式时，ssh channels.c 内的函数 x11_open_helper 没有检查 X 连接的拒绝截止日期，这可使远程攻击者通过允许时间窗口外的连接，利用此漏洞绕过目标访问限制。
修补方法	OpenSSH/5.3： 厂商补丁: OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://anongit.mindrot.org/openssh.git/commit/?h=V_6_9&id=1bf477d3cdf1a864646d59820878783d42357a1d http://www.openssh.com/txt/release-6.9
CVE 编号	CVE-2015-5352
BUGTRAQ	75525
涉及主机	192.168.10.15; 192.168.10.34;

4. 2. 3 主机详情

1）192.168.10.34

操作系统	Linux		风险等级	非常危险	风险值	9.9
端口	协议	服务	Banner			
58214	tcp					
58214	udp	rpc.statd				
111	udp	rpcbind				
111	tcp	rpcbind				
22	tcp	ssh				
6389	tcp	redis				
123	udp	ntp				

2）192.168.10.15

操作系统	Linux		风险等级	非常危险	风险值	9.9
端口	协议	服务	Banner			
4369	tcp					

54286	udp	rpc.mountd	
51555	udp	rpc.nlockmgr	
2049	udp	rpc.nfsd	
8080	tcp	www	
111	udp	rpcbind	
2910	tcp	tdaccess	
22	tcp	ssh	
111	tcp	rpcbind	
1099	tcp	rmiregistry	
3306	tcp	mysql	
8009	tcp	ajp13	
2049	tcp	rpcbind	
123	udp	ntp	

3）192.168.10.14

操作系统	Linux		风险等级	非常危险	风险值	7.9
端口	协议	服务	Banner			
8081	tcp	www				
8080	tcp	www				
5002	tcp	www				
5001	tcp	www				
8010	tcp	xmpp				
8009	tcp	ajp13				
22	tcp	ssh				
5004	tcp	http				
5003	tcp	http				
123	udp	ntp				

4.3 脆弱账号信息

检测未发现主机存在下列脆弱账号，暂不会对服务器造成威胁。

4.3.1Windows 系统脆弱账号

IP 地址	用户名	密码	描述
无			

4.3.2 应用程序脆弱账号

IP 地址	用户名	密码	应用程序
无			

4.3.3Unix 系统脆弱账号

IP 地址	用户名	密码	Home	Shell
无				

5 风险分析及安全建议

本次远程安全检测检测发现，该网段存在安全漏洞，漏洞主要存在于常见的应用程序。

其中，OpenSSH、Apache 等应用程序因为版本低存在安全漏洞，建议根据漏洞修补建议，尽快对这些软件进行版本升级，以免遭受不必要的损失。需要特别注意的是，安装补丁过程中会存在风险，安装前务必做好备份工作，建议联系厂商提供技术支持。

需要特别注意的是，安装升级补丁存在一定的安全风险，安装补丁前请务必做好备份工作，以便于出现问题时可以做回滚操作，建议提前在测试机上测试或者联系厂商提供技术支持。

为了保障安全状态的持续性与有效性，还建议：

•定期进行安全评估工作，避免新增漏洞和不合规配置成为网络安全短板。

•加强安全管理及规范，对各种账号，弱口令，空口令定期抽查，定期修改。

•定期更新各项操作系统及应用程序补丁，定期更新防毒软件病毒库，对重要业务系统定期进行日志备份。

•落实系统上线前安全评估与整改工作。

•对安全检测中的遗留漏洞引起重视，部分重要安全补丁的升级，如 Oracle 各项漏洞等，需要协调厂商进行业务评估及充分测试后再做升级。

•建议网络管理员、系统管理员、安全管理员关注安全信息、安全动态及最新的严重漏洞，特别是影响到生产区所使用的系统和软件的漏洞，应该在事前设计好应对规划，一旦发现系统受漏洞影响及时采取措施。

[附录 B 完]