信息系统安全防护测评报告

系统名称：互联网金融资产交易系统

被测单位：深圳市时间价值信息技术股份公司

测评单位： 广州市安鸿网络科技有限公司

报告时间：2016 年 5 月 13 日

信息系统安全测评基本信息表

信息系统					
系统名称	互联网金融资产交易系统			**安全保护等级**	3.2 级
被测单位					
单位名称	深圳市时间价值信息技术股份公司				
单位地址	深圳市南山区科技园科技路 9 号桑达科技工业大厦二层			**邮政编码**	528400
联 系 人	姓　　名	黎元春	职务/职称	技术总监	
	所属部门	技术部	办公电话	0755-26037885	
	移动电话	18611694803	电子邮件	Liyc@sjjz.com	
测评单位					
单位名称	广州市安鸿网络科技有限公司				
通信地址	广州市越秀区环市东路 416 号-3 高迅大厦 1701 室			**邮政编码**	510000
联 系 人	姓　　名	罗斌	职务/职称	销售总监	
	所属部门	销售部	办公电话		
	移动电话	13609060580	电子邮件		
审核批准	编 制 人	钟英南	编制日期	2016 年 4 月 16 日	
	审 核 人	罗斌	审核日期	2016 年 4 月 19 日	
	批 准 人		批准日期		

声明

本报告是深圳市时间价值信息技术股份公司的互联网金融资产交易系统安全测评报告。

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。

本报告一式三份，二份交委托单位，一份留存本单位。

深圳市时间价值信息技术股份公司

广州市安鸿网络科技有限公司

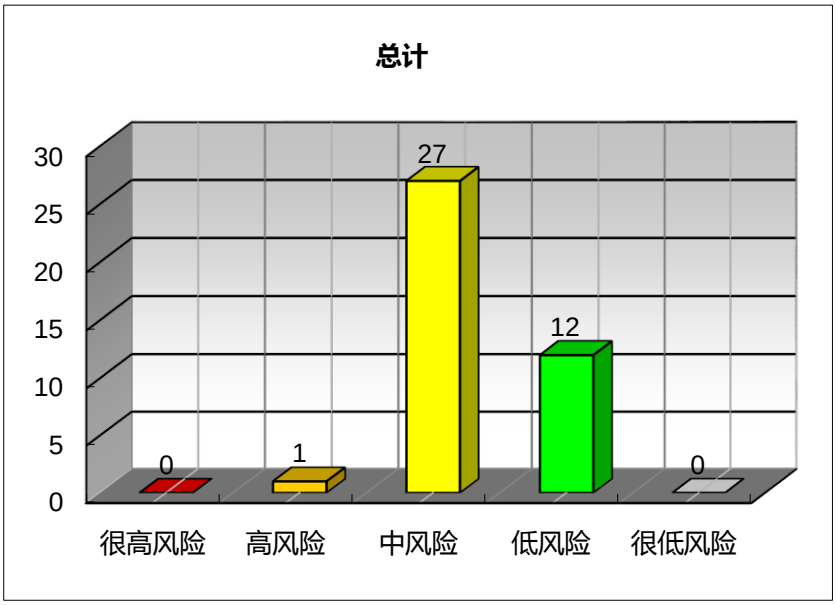
2016 年 5 月 13 日

目 录

报告摘要

受深圳市时间价值信息技术股份公司（以下简称“深圳时间价值”）委托，广州市安鸿网络科技有限公司（以下简称“广州安鸿”）于 2016 年 3 月 1 日-2016 年 3 月 5 日对深圳时间价值的互联网金融资产交易系统进行安全测评工作。

广州安鸿项目实施小组使用访谈、符合性检查、渗透测试等手段对该系统进行安全测评，总计识别出 40 项风险，其中 1 项高风险、27 项中风险，12 项低风险。如下图所示：



风险分布图

综上，按照信息资产的类型，各类资产的风险级别汇总表如下：

风险级别		数组分割值	系统资产	总计
很高风险	5 级	25	0	0
高风险	4 级	20	1	1
中风险	3 级	15	27	27
低风险	2 级	10	12	12
很低风险	1 级	5	0	0
合计			**40**	**40**

各类资产风险级别汇总表

整改完成后，广州安鸿于 2016 年 4 月 8 日对该系统发现的问题进行复测，本次复测仅发

现 1 低风险未整改，如未使用源代码审计工具对应用程序的代码进行审计。

以上存在的安全问题及已整改过的问题，详见第9章。

1 测评项目概述

1.1 测评目的

对互联网金融资产交易系统的信息安全测评工作，通过测试手段对安全技术和安全管理上各个层面的安全控制进行整体性验证，确保该系统满足信息安全防护的基本要求，减少信息安全事件发生的可能，同时协助用户完成系统的安全测评工作。

1.2 测评原则

测评工作实施过程将遵循以下原则：

- **规范性原则**

根据项目管理方法，在人员、质量和时间进度等方面进行严格管控。

- **标准化原则**

严格遵守国家和行业的相关法规、标准，并参考国家的标准来实施。

- **保密性原则**

在进行信息安全评估的过程中，将严格遵守保密原则，评估过程中将采取严格的管理措施，确保所涉及到的任何用户保密信息，不会泄露给第三方单位或个人，不利用这些信息损害用户利益。

- **互动性原则**

在进行信息安全评估过程中，将强调受评估方的互动参与，从而保证评估的效果并提高受评估方的安全技能和安全意识。

- **最小影响原则**

应从项目管理和技术应用的层面，考虑评估对目标系统的正常运行可能产生的不利影响，将风险降到最低，保证目标系统业务正常运行。

1.3 测评依据

本次对系统的安全测评主要参考标准如下：

- ✧ YD/B 108—2012《增值电信业务系统安全防护定级和评测实施规范 网络交易系统》
- ✧ GB/T 20984-2007《信息安全技术 信息安全风险评估规范》
- ✧ YD/T 1729-2008《电信网和互联网安全等级保护实施指南》

2 被测信息系统情况

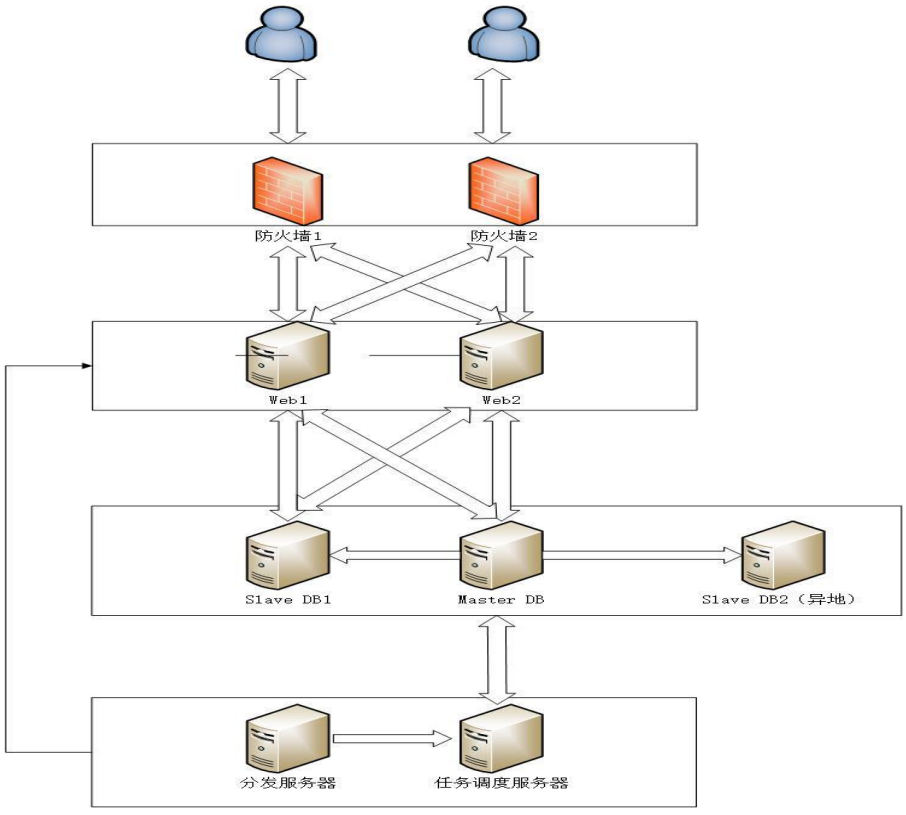
深圳时间价值互联网金融资产交易系统通过逻辑隔离措施进行了安全控制规划，形成了一个或多个物理网段或逻辑网段的集合，已经形成了区域边界安全防护、横向逻辑隔离、纵向的访问控制实体。系统的分域防护不仅实现了边界防护，而且体现了一组在网络、主机、应用等多个层次上深层防护措施。

2.1 承载的业务情况

时间价值金融资产交易平台将致力于为金融机构资产流动提供具有公信力的承载平台，为金融市场体系中相关内容产品和权益交易流转提供灵活快捷的中间市场支持。通过规范开展各类金融资产交易业务，自觉接受行业主管部门的监督指导，与各类产权交易机构一起，共同推动资本市场的发展。

2.2 系统与网络结构

本系统为托管在阿里云的主机服务器上运行的系统，在出口购买了阿里云的防火墙服务，在防火墙上设置了相关的访问控制策略，应用前端使用了双机热备、后端数据库也使用了双机热备，因此该系统可高可用地运行，具体网络拓扑图如下：



2.3 系统构成

2.3.1 业务应用软件

序号	软件名称	主要功能	重要程度
1	互联网金融资产交易系统	主要包括后台模块和前台模块，后台模块基于分布式的 Mysql 数据库，扩展开发出中间逻辑处理层，完成对各种金融资产的交易处理。前台模块完成云接入功能，负责使用者的多终端接入，主要是由 Html、CSS、Javascript 及 Html5 相关应用接口组成。	重要

2.3.2 关键数据类别

序号	数据类别	所属业务应用	主机/存储设备	重要程度
1	互联网金融资产交易系统	互联网用户交易数据	托管阿里云主机	重要

2.3.3 主机/存储设备

目前该系统托管到阿里云的主机服务器上进行业务运营，涉及的资产如下：

序号	设备名称	IP 地址	操作系统类型	数据库软件	重要程度
1	Web1	182.92.175.206/255.255.255.252.0/ 182.92.175.247	Centos 6.5 X64		重要
2	Web2	123.57.9.11/255.255.255.252/ 123.57.11.247	Centos 6.5 X64		重要
3	Databse Master	101.201.146.76/ 255.255.252.0/ 101.201.147.247	Centos 6.5 X64	Mysql 5.7	重要
4	Database Slave	123.56.192.64/255.255.255.252/ 123.56.195.247	Centos 6.5 X64	Mysql 5.7	重要
5	Distribute	101.201.220.148/255.255.255.252/ 101.201.223.247	Centos 6.5 X64		重要
6	Beta	47.88.15.255/255.255.255.252/ 47.88.15.247	Centos 6.5 X64		重要

2.3.4 安全相关人员

序号	姓名	岗位/角色	联系方式
1	黎元春	技术总监	
2			

2.3.5 安全管理文档

序号	文档名称	用途	重要程度
1	信息安全管理办法	信息安全工作的总体方针政策文件，保证单位的信息系统的安全，结合公司信息系统建设的实际情况，制订的有关计算机、网络和信息安全的相关法规和安全制度	重要
2	信息化工作管理办法	信息化工作的具体管理办法	重要
3	信息化规划管理办法	信息化规划管理办法	重要
4	数据处理与存储中心运行管理规定	机房安全管理制度，	重要
5	网络安全系统运行管理规定	网络运行的管理制度	重要
6	第三方安全管理规范 V	对第三方人员访问的管理规范	重要
7	介质安全管理规定	保密移动存储介质的管理，确保档案信息的安全	重要
8	数据加密保护管理规定	对于数据加密保护等的详细规定	重要
9	无线网络信息安全防护技术参考规范	对无线网络的使用的详细规定	重要
10	信息安全管理体系手册	对信息安全工作各个方面实际情况，制定的关于各个方面的管理规定，包括系统、网络、设备、介质、人员等等	重要
11	信息安全漏洞扫描及加固参考规范	对系统漏洞的管理及发现漏洞后的加固参考规范	重要
12	运维管理设备部署参考规范	对设备部署的规定	重要
13	运维管理设备管理策略要求	对设备安全管理的策略	重要
14	信息资产管理制度	规范资产的管理	重要
17	终端安全系统应急预案	终端安全系统应急预案	重要
18	防病毒系统应急预案	防病毒系统应急预案	重要

3 安全测评指标与方法

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《增值电信业务系统安全防护定级和评测实施规范 网络交易系统》中对应级别的安全要求作为等级测评的基本指标。

鉴于信息系统的复杂性和特殊性（如某些信息系统未部署数据库服务器），基本指标中可能存在部分不适用项，可以在测评时进行识别。

3.1.2 特殊指标

根据系统相关等级保护定级情况及办公业务平台环境，此次测评主要依据相关的要求进行，不再增加特殊指标。

技术/管理	层面	测评项数量	备注
安全技术	物理安全	32	托管在阿里云上
	网络安全	33	托管在阿里云上
	主机安全	21	
	应用安全	68	
安全管理	安全管理机构	23	
	安全管理制度	14	
	人员安全管理	25	
	系统建设管理	50	
	系统运维管理	63	

3.2 测评方法

现场测评过程中将主要采用访谈、检查、测试等方法进行等级测评。

- **访谈**

现场测评时，通过与各相关部门人员进行交谈，主要是管理访谈，以收集测评证据。

- **检查**

现场测评时，检查工作主要包括：

- 配置检查：通过对信息系统各平台的安全配置情况进行人工审计，以收集测评证据。
- 文档审阅：通过查阅文件及记录，以收集测评证据。
- 实地查看：通过实地观察基础设施及物理环境的现状，以收集测评证据。

- **测试**

现场测评时，测试工作主要包括：

- 漏洞扫描：通过在网络环境中的不同节点中部署漏洞扫描工具，对信息系统进行全面的脆弱性扫描和测试，以收集测评证据。

- 技术性测试及验证：通过对信息系统进行针对性的技术性测试和验证，以收集测评证据。

另外，在现场测评时，对于有疑义的问题，可采取跟踪验证的方式，以收集客观、真实的测评证据。

4 符合性测评结果记录

4.1 物理安全

该系统是托管在阿里云上运行的业务系统，且阿里云满足物理安全的相关安全防护要求，如下所示：

环境控制:

（1）电力

为保障阿里云业务 7*24 持续运行，阿里云数据中心采用冗余的电力系统（交流和高压直流），主电源和备用电源具备相同的供电能力，且主电源发生故障后（如：电压不足、断电、过压、或电压抖动），会由柴油发电机和带有冗余机制的电池组对设备进行供电，保障数据中心在一段时间的持续运行能力，这是阿里云数据中心一个关键的组成部分。

（2）气候和温度

阿里云任意一个数据中心，均采用空调（新风系统冷却或水冷系统冷却）保障服务器或其他设备在一个恒温的环境下运行，并对数据中心的温湿度进行精密电子监控，一旦发生告警立即采取对应措施。并且，设备冷风区域进行了冷风通道密闭，充分提高制冷效率，绿色节能。空调机组均采用 N+1 的热备冗余模式（部分数据中心采用 N+2 的冷、热双重冗余模式），空调配电柜采用不同的双路电源模式，以应对其中一路市电电源发生故障后空调能正常接收供电。且在双路市电电源发生故障后，由柴油发电系统提供紧急电源，减少服务中断性的可能，以防止设备过热。

（3）火灾检测及消防

自动火灾检测和灭火设备防止破坏计算机硬件。火灾探测系统的传感器位于数据中心的天花板和底板下面，利用热、烟雾和水传感器实现。在火灾或烟雾事件触发时，在着火区提供声光报警。在整个数据中心，也安装手动灭火器。数据中心接受火灾预防及灭火演练培训，包括如何使用灭火

安全防护措施

物理安全控制:

阿里云数据中心在地理位置上呈分布式状态，涵盖中国本土内的两地三中心布局。对所有数据中心的所有资产设备，物资配件，耗材，人员，均采用了多种不同的物理安全机制。在技术和安全上对人员和设备的控制机制可能取决或遵循于实际运营商的条件，如建筑物的位置和区域风险差异，以及设备和人员进出控制流程等。但阿里云每个数据中心都包含以下标准的物理安全控制要

（1） 数据中心各线上设备区域系统、各核心骨干区域系统、各动力区域系统、各仓储系统、各报警监控系统的访问均需使用定制的电子卡，且电子卡由数据中心专门物业保管，特定授权需求方按需求领取归还，并配备紧急电子卡以备不时之需（如常规电子卡遗失），一旦发生遗失情况立即申请电子卡管理系统进行权限注销；

（2） 数据中心的物理设备（包括其对应的各种组件），配件耗材的安置或存放区域必须要与所有办公区域和公共区域隔离（如办公室或大堂）；

（3） 数据中心所有阿里云专属的所有物理设备、设备配件、网络耗材，以及设备厂商的维修设备、配件、耗材等进出数据中心，必须由阿里云内部授权人员发送盖有专人保管印章的设备进出单传真，数据中心现场核实无误后方可允许设备、配件、耗材等的进出；

（4） 仓储系统中的重要配件，如核心网络设备的网络模块，精密存储介质等，由仓储系统中的专门电子加密保险箱存放，且由专人进行保险箱的开关；

（5） 仓储系统中的任何配件，必须由授权工单和授权人员方能领取，且领取必须在仓储管理系统中进行登记记录，阿里云专人定期对所有仓储系统物资进行综合盘点追踪；

（6） 数据中心内部的每个区域，或外部走廊区域，或仓库门口区域，都使用了摄像机，物业保安 7x24 小时分段巡逻，并对所有基础设施进行 7x24 小时集中视频监控；

（7） 采用全方位电子摄像机对阿里云的基础设施内外部区域进行视频监控，对设施区域中的其他系统进行检测（如动力和制冷）和监控跟踪入侵者；

（8） 所有人员活动记录电子保存（长期），所有视频记录被保存（3 个月），以备后期审计，同时提供额外的安全控制措施，如:特定区域采用铁笼隔离，掌纹识别技术；

（9） 只允许具备长期授权名单内的内部人员（实时更新），或审批通过的其他人员，以及授权认可的第三方固定人员名单内的人员（每月更新）进入数据中心，且非长期授权人员再以核实需求工单真实性的形式进行二次审核，准确无误后方可进入；

（10）非长期授权，非固定人员授权名单内的人员访问，必须要求阿里云内部需求方在流程系统上提交需求，由各层级主管提前审批通过后，方可同意其访问想要访问的内部特殊区域，并由对应数据中心的驻场人员全程指导陪同。阿里云不定期对访问数据中心的人员登记情况进行审计，严格控制非授权人员访问数据中心；

4.2 网络安全

该系统是托管在阿里云上运行的业务系统，且阿里云满足网络安全的相关安全防护要求，如下所示：

网络安全

阿里云采用了多层防御，以帮助保护网络边界面临的外部攻击。在公司网络中，只允许被授权的服务和协议传输，未经授权的数据包将被自动丢弃，阿里云网络安全策略由以下组件组成：

（1） 控制网络流量和边界，使用行业标准的防火墙和 ACL 技术对网络进行强制隔离；

（2） 网络防火墙和 ACL 策略的管理包括变更管理、同行业审计和自动测试；

（3） 使用个人授权限制设备对网络的访问；

（4） 通过自定义的前端服务器定向所有外部流量的路由，可帮助检测和禁止恶意的请求；

（5） 建立内部流量汇聚点，帮助更好的监控；

传输层安全

阿里云提供的很多服务都采用了更安全的 HTTPS 浏览连接协议，例如用户使用阿里云账号登陆 aliyun 的默认情况为 HTTPS。通过 HTTPS 协议，信息在阿里云端到接受者计算机实现加密传输。

操作系统安全

基于特殊的设计，阿里云生产服务器都是基于一个包括运行阿里云“飞天”必要的组件而定制的 linux 系统版本。该系统专为阿里云能够保持控制在整个硬件和软件栈，并支持安全应用程序环境。阿里云生产服务器安装标准的操作系统，公司所有的基础设施均需要安装安全补丁。

4.3 主机安全

4.3.1 结果记录

序号	指标名称	测评项	现场结果记录
1	身份鉴别	应采用两种或两种以上组合的鉴别技术对相关设备的管理用户进行身份鉴别。	不符合 用户名/密码
		重要主机应使用安全性较高的身份鉴别措施（如，数字证书）对用户进行身份鉴别。	符合 非重要主机
		应为操作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。	符合 不存在 uid 相同的账户
		操作系统用户身份标识应具有不易被冒用的特点，相关用户口令长度应不小于 8 字节，口令应有复杂度要求（使用大写字母、小写字母、数字、标点及特殊字符四种字符中至少二	不符合 PASS_MAX_DAYS 99999 PASS_MIN_DAYS 0

		种的组合，且与用户名或 ID 无相关性）并定期更换（更新周期不大于 90 天）。	PASS_MIN_LEN 5 PASS_WARN_AGE 7
		应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。	不符合 未设置
		当对各类主机进行远程管理时，应采取必要措施，防止鉴别信息在传输过程中被窃听。	符合 sshd 0:off 1:off 2:on 3:on 4:on 5:on 6:off
2	访问控制	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。	不符合 UMASK 077
		应及时删除多余的、过期的账户，避免共享账户的存在。	符合 无多余的、过期的账户
		应实现操作系统和数据库系统特权用户的权限分离。	符合 非数据库服务器
		应限制默认账户的访问权限，修改这些账户的默认口令，条件允许下，应重命名默认账户。	不符合 sync、 shutdown、 halt 未禁用
		应根据最小权限分配原则，按设备相关各类管理、维护账号的角色分配权限，实现管理账号与操作、维护账号的权限分离。	符合 已进行权限分离
		应对重要信息资源设置敏感标记。	不符合 未对重要信息资源设置敏感标记
		应依据安全策略严格控制有关用户对有敏感标记重要信息资源的操作。	不符合 未对重要信息资源设置敏感标记
3	安全审计	审计范围应覆盖到主机/服务器上的每个操作系统用户和数据库用户。	符合 rsyslog 0:off 1:off 2:on 3:on 4:on 5:on 6:off
		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。	不符合 cron.* /var/log/cron authpriv.* /var/log/secure

		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。	符合 包含要求的内容
		应保护审计记录，避免其受到未预期的删除、修改或覆盖等，保留一定期限（至少 180 天）。	符合 /etc/rsyslog.conf 644 /var/log/messages 600
		应能根据记录数据进行分析，并生成审计报表。	不符合 未审计数据生成报表
		应保护审计进程，避免受到未预期的中断。	符合 rsyslog 0:off 1:off 2:on 3:on 4:on 5:on 6:off
4	入侵防范	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，并通过安全的方式（如，设置升级服务器）保持系统补丁及时得到更新。	符合 遵循最小安装的原则， 保持系统补丁及时得到更新 LSB Version: :base-4.0-amd64:base-4.0-noarch:core-4.0-amd64:core-4.0-noarch Distributor ID: CentOS Description: CentOS release 6.5 (Final) Release: 6.5 Codename: Final
		应对重要服务器进行入侵行为的监测，能够记录入侵的源 IP、攻击的类型、攻击的目的地址、攻击的时间，并在发生严重入侵事件时提供告警。	符合 部署了阿里云盾，阿里安骑士入侵防御检测设备
		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。	不符合 未部署了第三方监测软件或硬件（防篡改设备等）

			对系统重要资源进行备份，且可进行完整恢复
5	恶意代码防范	应安装防范病毒、木马等恶意代码的软件，并及时更新防恶意代码软件版本和恶意代码库。	不符合 未安装防范病毒、木马等恶意代码的软件
		应支持防恶意代码的统一管理。	不符合 未安装防范病毒、木马等恶意代码的软件
		主机防恶意代码产品应使用与网络/系统防恶意代码产品不同的恶意代码库。	不符合 网络防恶意代码产品阿里安骑士
6	资源控制	应通过设定终端接入方式、网络地址范围等条件限制管理终端登录。	不符合 未限制
		应根据安全策略设置登录终端的操作超时锁定。	不符合 未设置
		应限制单个用户对系统资源的最大或最小使用限度。	不符合 未设置
		应对重要服务器进行性能监测，包括监测服务器的 CPU、硬盘、内存、网络等资源的使用情况。	不符合 未设置
		应能够对服务器、数据库等系统的服务水平设定告警阈值，当监测到服务水平降低到阈值时应能进	不符合 未设置
7	其他	重要设备应采用热备份的保护方式进行保护。	符合 热备份
		系统应有必要的流量负荷分担设计。	符合 已部署负载均衡
		系统应具备较好的灾难备份和业务恢复的能力，提供重要服务的业务及应用系统应进行系统级备份，以保证其业务连续性。	不符合 1、未拥有灾难备份 2、未有业务恢复的措施 3、重要服务业务未进行系统级备份
		应建立对主机全部数据、信息进行备份和恢复的管理和控制机制。	不符合 未设置
		相关主机数据备份范围和时间间隔、数据恢复能力应满足行业管理、业务运营企业应急预案相关要求。	符合 热备
		重要的主机相关数据应进行异址备份。	不符合 未进行异地备份
		应提供数据自动保护功能，当发生故障后应保证系统能够恢复到故障前的业务状态。	符合 数据库事务完整性，同步备份

		加强口令复杂度要求，在原基础上还应不含有常用字符组合、数字组合、键盘顺序等可预测密码组合。	不符合 未设置
		重要服务器应使用资源强制访问控制策略。（如用户、进程、文件内核级保护）。	不符合 未开启 SELinux status: disabled

4.3.2 结果汇总

序号	测评对象	测评指标						
		身份鉴别	访问控制	安全审计	入侵防范	恶意代码防范	资源控制	其它安全
1	主机安全	符合	符合	符合	符合	符合	符合	符合
		2/6	1/7	4/6	2/3	0/3	0/5	4/10

4.4 应用安全

4.4.1 结果记录

序号	指标名称		测评项	现场结果记录
1.	业务逻辑安全		应能根据需要对业务及应用相关通信过程中的全部报文或整个会话过程提供必要的保护（如进行通信数据加密），并提供业务及应用相关访问、通信等数据的防抵赖功能。	部分符合 传输使用了 HTTPS 加密保护，但未对 cookie 保护，涉及链接如下： https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com
2.			应定义业务水平阈值，能够对业务及应用服务水平进行检测，并具备当服务水平降低到预先规定的 阈值时进行告警的功能。	不符合

3.			需要登录访问的信息服务业务平台（或模块），应对业务用户访问和操作的有关环节（如，注册、 登录、操作、管理、浏览等）提供有效的保护措施（如，用户注册口令进行强度检查、用户 ID 检测和账 号保护、以图形验证码保护各类提交信息、对用户重要操作进行确认和验证、授权访问页面使用安全连 接等）。	部分符合 无口令强度检查（但有提示），已注册 ID 不能重复注册，在重要操作需进行短信验证，传输使用了,涉及的链接如： https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com
4.			应提供有效的恶意代码检测和过滤技术手段，对业务平台向用户提供的各类信息（如：用户发布和 上传的文件、资源站点可供下载的文件）进行必要的安全检查和过滤。	不符合要求，没有相关 waf 设备
5.			业务及应用应具备必要的流量负荷分担设计。	符合 存在两台负载均衡设备，nginx，涉及链接如下： https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com
6.			业务及应用应具备较好的灾难备份和业务恢复的能力，提供重要服务的业务及应用系统应进行系统 级备份，以保证其业务连续性。	符合 https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com
7.			应建立对业务及应用全部数据、信息进行备份和恢复的管理和控制机制。	符合 灾难备份环境：在线热备份；数据库存在本地和异地备份，涉及链接如下： https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com
8.			重要的业务及应用相关数据应进行异址备份。	符合 存在异地备份环境，热备份，涉及链接如下： https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com

9.			应提供数据自动保护功能，当发生故障后应保证系统能够恢复到故障前的业务状态。	符合 存在自保护功能，涉及链接如下： https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com
10.			采用两种或两种以上组合的鉴别技术实现用户身份鉴别。	不符合 前台用户登录需要密码认证，重要操作采用短信验证，后台采用密码认证，涉及链接如下： https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com
11.			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。	部分符合 有审计功能，无生成报表功能，涉及链接如下： https://aa.sjjz.com/sys/admin/
12.			登录验证模块应能防止身份鉴别暴力攻击。（如登录模块随机验证码验证、并且保证验证码不易被 自动预测、识别）。	不符合 https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com
13.			加强口令复杂度要求，在原基础上还应不含有常用字符组合、数字组合、键盘顺序等可预测密码组 合。	符合 后台最少 8 位密码，存在字符数字字母，涉及链接如下： https://aa.sjjz.com/sys/admin/ 不符合 前台无加强口令复杂的要求，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com
14.			业务系统管理后台不应暴漏给任意用户；管理接口通信内容不应使用明文协议。	符合 后台使用单独域名 IP，https 加密，涉及链接如下： https://aa.sjjz.com/sys/admin/
15.			应保证系统中使用的第三方软件、运维软件无已知后门、漏洞。	符合 使用开源第三方软件 mysql,nginx,tomcat，涉及链

				接如下： https://www.sjjz.com/ https://aa.sjjz.com/sys/admin https://m.sjjz.com
16.	web 安全	输入控制	应对所有来源的输入进行验证，默认所有输入都可能包含恶意信息，只要其来源不在可信任的范围 之内，就应对输入进行验证并尽量使用白名单验证方法。	不符合 涉及链接如下 https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/
17.			应设计一套统一的验证接口，向整个应用系统提供一致的验证方法，并降低开发与代码维护的工作 量。	不符合 无相关统一身份验证平台，涉及链接如下： https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com
18.			应在服务器端进行输入验证，避免客户端输入验证被绕过。	符合 上传、登录、发布都不存在本地验证，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/
19.			应对输入内容进行规范化处理后再进行验证，如文件路径、URL 地址等。	符合 存在规范化处理，涉及链接如下： https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com
20.			应防止关键参数被篡改，关键参数应直接从服务器端提取，避免从客户端输入。	符合 有效，如上传路径，上传文件名等，涉及相关链接如下： https://www.sjjz.com/ https://m.sjjz.com
21.		身份认证	应禁止明文传输用户密码，建议采用 SSL 加密隧道确保用户密码的传输安全。	符合 存在 ssl 加密，涉及相关链接如下： https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com

22.			应禁止在数据库或文件系统中明文存储用户密码，建议采用单向散列值在数据库中存储用户密码，	符合 使用的加密方式(md5+key)+md5，涉及相关链接如下： https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com
23.			在生成单向散列值过程中加入随机盐值，降低存储的用户密码被字典攻击的风险。	符合 在储存中使用了 key 作为随机盐值，涉及相关链接如下： https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com
24.			应禁止在 COOKIE 中保存用户密码。	部分符合 cookie 中保存了用户名，无保存密码，涉及相关链接如下： https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/
25.			应采用图形验证码来增强身份认证安全，防止恶意脚本自动发送身份认证请求来猜测用户认证鉴权性质的信息。要求图形验证码能够抵抗工具的自动识别。	不符合 登录认证不存在验证码，注册和修改密码等重要操作存在验证码，涉及相关链接如下： https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com
26.			应对关键业务操作，例如修改用户认证鉴权信息（如密码、密码取回问题及答案、绑定手机号码等），需要经过二次鉴权，以避免因用户身份被冒用，给用户造成损失。	部分符合 存在短信验证，涉及相关链接如下： https://www.sjjz.com/ https://m.sjjz.com 不符合 不存在短信验证，涉及相关链接如下： https://aa.sjjz.com/sys/admin/
27.			应避免认证错误提示泄露信息，在认证失败时，应向用户提供通用的错误提示信息，不应区分是	符合 https://www.sjjz.com/ https://aa.sjjz.com/sys/ad

			账号错误还是密码错误，避免这些错误提示信息被攻击者利用。	min/ https://m.sjjz.com
28.			应支持密码策略设置，从业务系统层面支持强制的密码策略，包括密码长度、复杂度、更换周期等，特别是业务系统的管理员密码。	部分符合 后台存在 8 位以上强度密码，但无强制更换周期，涉及链接如下： https://aa.sjjz.com/sys/admin/ 不符合 不满足密码长度、复杂度、更换周期要求，涉及链接如下 https://www.sjjz.com/ https://m.sjjz.com
29.			应支持账号锁定功能，系统应限制连续登录失败次数，在客户端多次尝试失败后，服务器端需要对用户账号进行短时锁定，且锁定策略支持配置解锁时长。	不符合要求 无锁定机制，涉及链接如下： https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com
30.		访问控制	应确保用户不能访问到未授权的功能和数据，未经授权的用户试图访问受限资源时，系统应予以拒绝或提示用户进行身份鉴权。	部分符合要求 不存在越权问题，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com 不符合要求 存在测试功能未进行权限验证，涉及链接如下： https://aa.sjjz.com/sys/admin/
31.			应在服务器端实现对系统内受限资源的访问控制，避免客户端访问控制被绕过。	不符合要求 存在测试功能未进行权限验证，涉及链接如下： https://aa.sjjz.com/sys/admin/
32.			应采用统一的访问控制机制，保证整体访问控制策略的一致性。同时应确保访问控制策略不被非法修改。	符合要求 存在访问控制策略，分配不同权限的用户组，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/
33.		会话管理	应确保会话的安全创建，在用户认证成功后，应为用户创建新的会话并释放原有会话，创建的会	部分符合要求 会话存在随机性和长度要求，

			话标识应满足随机性和长度要求，避免被攻击者猜测。建议会话与 IP 地址绑定，降低会话被盗用的风险。	但创建新会话时候未对原会话进行释放，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin
34.			应确保会话数据的存储安全，用户登录成功后所生成的会话数据应存储在服务器端，并确保会话数据不能被非法访问，当更新会话数据时，要对数据进行严格的输入验证，以免会话数据的非法篡改。	符合要求 会话存储文件在 tomcat 分配的目录下,涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/
35.			应确保会话数据的传输安全，防止泄露会话标识。	部分符合要求，未对 cookie 进行保护 https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/
36.			应确保会话的安全终止，当用户登录成功并成功创建会话后，应在 web 应用系统的各个页面提供用户登出功能，登出时应及时删除服务器端的会话数据。当处于登录状态的用户直接关闭浏览器时，需要提示用户执行安全登出或者自动为用户完成登出过程，从而安全的终止本次会话。	部分符合要求 各页面都存在登出功能，当用户直接关闭浏览器时未提示执行登出，涉及链接如下： https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ 不符合要求 只有用户首页存在登出功能，其他页面不存在，涉及链接如下： https://m.sjjz.com
37.			应设置合理的会话超时阀值，在合理范围内尽可能减小会话超时阀值，可以降低会话被劫持和重复攻击的风险，超过会话超时阀值后立刻销毁会话，清除会话的信息。	符合要求 前台，后台超时 15 分钟，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/
38.			应限制会话并发连接数，限制同一用户的会话并发连接数，避免恶意用户创建多个并发的会话来消耗系统资源，影响业务可用性。	不符合要求 无并发连接数限制，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com

				https://aa.sjjz.com/sys/admin/
39.			在涉及到关键业务操作的 web 页面，应为当前 web 页面生成一次性随机令牌，作为主会话标识的补充。在执行关键业务前，应确保用户提交的一次性随机令牌与服务器端保存的一次性随机令牌匹配，以避免跨站请求伪造等攻击。	不符合要求 web 页面无随机令牌，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/
40.		数据存储	对于不同安全级别的数据，比如日志记录和业务数据，应采取相应的隔离措施和安全保护措施。	部分符合要求 日志和业务数据分别存储不同的服务器，存在备份，但未对日志记录主机和业务数据主机进行安全配置，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/
41.			应尽量避免存储用户敏感数据，禁止在本地存储用户敏感数据，如用户密码、身份信息等。	符合要求 未在本地存储用户数据，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/
42.			应避免在代码中硬编码密码，即在代码中直接嵌入密码，会导致密码修改困难，甚至密码的泄露，建议从配置文件载入密码。	符合要求 不存在硬编码密码问题，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/
43.			在配置文件中禁止明文存储数据库连接密码、FTP 服务密码、主机密码、外部系统接口认证密码等。	不符合要求 数据库密码明文，无配置其他密码，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/
44.		数据传输	应确保敏感信息通信信道的安全，建议在客户端与 web 服务器之间使用 SSL。并正确配置 SSL，建议 使用 SSL 3.0/ TLS 1.0 以上版本，对称加密密	符合要求 使用 3.0 版本，非对称密钥长度 1024，涉及链接如下： https://www.sjjz.com/

			钥长度不少于 128 位，非对称加密密钥长度不少于 1024 位， 单向散列值位数不小于 128 位。	https://m.sjjz.com https://aa.sjjz.com/sys/admin/
45.		日志记录	日志记录范围应覆盖到每个用户的关键操作、重要行为、业务资源使用情况等重要事件。如普通用户异常登录、发布恶意代码、异常修改账号信息等行为，以及管理员在业务功能及账号控制方面的关键操作。	部分符合要求，无异常修改或登录记录 https://www.sjjz.com/ https://m.sjjz.com 部分符合要求，对管理后台异常登录存在记录 https://aa.sjjz.com/sys/admin/
46.			应禁止在日志中记录用户密码等敏感信息，如果确实需要记录敏感信息，则应进行模糊化处理。	符合要求 日志不存在记录用户敏感信息问题，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/
47.			应防止日志欺骗，如果在生成日志时需要引入来自非受信源的数据，则需要进行严格校验，防止日志欺骗攻击。	符合要求 无第三方源导入，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/
48.			应禁止将日志保存到 web 目录下，确保日志数据的安全存储并严格限制日志数据的访问权限，建议对日志记录进行签名来实现防篡改。	部分符合要求 保存到本地系统其他目录下和远程备份，无日志防篡改，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/
49.			Web 程序上线前或升级后应进行代码审计，形成报告，并对审计出的问题进行代码升级完善；	不符合要求 不存在源代码审计，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/
50.			应避免使用含有已公开漏洞的开源第三方应用组件及代码（漏洞库可参考 CVE、CNVD 等）。	符合要求 不存在使用第三方应用组件及代码问题，涉及链接如下： https://www.sjjz.com/

				https://m.sjjz.com https://aa.sjjz.com/sys/admin/
51.	支付接口安全		应提供数据有效性检验功能，保证通过 Web 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。	符合要求 存在数据有效性校验功能，使用前后端校验，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/
52.			接口均必须分别设置专门服务器，通过服务器的接口应用实现内外系统的交互。	符合要求 支付接口调用第三方接口使用，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/
53.			接口数据传输应尽量采用加密方式，原则上要求内外系统交互时，接口报文中的敏感信息应进行加密传输，如接口认证需要的密码等敏感数据。	符合要求 传输和保温使用加密并校验，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/
54.			接口数据传输应进行校验，确保数据在传输过程中的完整性。	符合要求 存在完整性校验，使用 hash 值校验，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/
55.			接口应具有严格的认证机制（如证书认证等），保证接口通信安全。	符合要求 使用非对称加密和证书认证，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/
56.			接口认证信息必须以密文的形式单独存储在配置文件中。	符合要求 存在证书加密，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com

				https://aa.sjjz.com/sys/admin/
57.			接口应用通信应采用 10000 以上的 TCP/UDP 端口号，尤其要避免与可能造成严重影响的蠕虫、木马所利用的端口相同。	不符合要求 使用第三方接口，通过 443 端口进行通信，使用证书和 ssl 加密，未使用 10000 以上端口进行通信，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/
58.			应对接口的状态和交互过程进行监控，并支持异常恢复。	符合要求 存在监控，通过日志监控，支持异常恢复，涉及链接如下： https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/
59.	客户端安全		应确保身份认证模块不能被非法绕过。	符合要求 使用网站登录，无内置登录模块或接口，涉及链接如下： https://m.sjjz.com
60.			软件运行时应对自身进行完整性校验，及时有效的发现是否被恶意修改。	不符合要求 不存在完整性校验，涉及链接如下： https://m.sjjz.com
61.			应采取会话保护措施防止软件与服务器之间的会话不可被篡改、伪造、重放等。	符合要求 存在 https 加密传输，涉及链接如下： https://m.sjjz.com
62.			应确保软件配置信息、用户认证信息等敏感数据采用加密方式存储。	符合要求 使用网站登录，存在加密存储，无内置登录模块或接口，涉及链接如下： https://m.sjjz.com
63.			应确保软件内存管理不存在逻辑缺陷，如未释放资源、敏感信息驻留内存等。	符合要求 不存在内存管理问题，涉及链接如下： https://m.sjjz.com
64.			应确保软件的用户身份鉴别模块能有效抵抗键盘记录等攻击。	不符合要求 使用网站登录，无内置登录模块或接口，无法抵抗键盘记录等攻击，涉及链接如下： https://m.sjjz.com

65.			应确保软件不非法操作与自身功能不相关的文件。	符合要求 未对自身功能外文件进行操作，涉及链接如下： https://m.sjjz.com
66.			软件应具有异常处理功能，防止由于软件运行异常导致业务流程中断。	不符合要求 不存在异常处理，涉及链接如下： https://m.sjjz.com

4.4.2 结果汇总

序号	测评对象	测评指标			
		业务逻辑安全	Web 安全	支付接口安全	客户端安全
1	应用安全	符合 8/15	符合 16/35	符合 7/8	符合 4/8

4.5 安全管理制度

4.5.1 结果记录

序号	指标名称	测评项	现场结果记录
1	管理制度	应制定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。	符合 具有总体安全方针策略文件
		应对安全管理活动中重要的管理内容建立安全管理制度。	符合 建立了内部管理制度
		应对安全管理人员或操作人员执行的重要管理操作建立操作规程。	符合 建立了操作规程
		应对安全管理活动中的各类管理内容建立安全管理制度，以规范安全管理活动；	符合 建立了内部管理制度
		应形成由安全策略、管理制度、操作规程等构成的全面的安全管理制度体系。	
2	制定和发布	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。	符合 技术部专人负责
		应组织相关人员对制定的安全管理制度进行论证和审定。	符合 定期评审
		应将安全管理制度以某种方式发布到相关人员手中。	符合 通过 OA 或纸质版
		安全管理制度应有统一的格式，并进行版本控制；	符合 具有统一格式
		安全管理制度应通过正式、有效的方式发布；	符合 正式发送，如 OA 系统

		安全管理制度应注明发布范围，并对收发文进行登记。	符合 有适应范围
3	评审和修订	应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。	符合 定期修订
		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；	符合 定期评审
		应定期或不定期对安全管理制度进行检查和审定。	符合

4.5.2 结果汇总

序号	测评对象	测评指标		
		管理制度	制定和发布	评审和修订
1	安全管理制度	符合	符合	符合
		5/5	6/6	3/3

4.6 安全管理机构

4.6.1 结果记录

序号	指标名称	测评项	现场结果记录
1	岗位设置	应设立安全主管、安全管理各个方面的负责人岗位，定义各负责人的职责。	符合 已有安全主管
		应设立系统管理人员、网络管理人员、安全管理员岗位，定义各个工作岗位的职责。	符合 定义了系统管理人员、网络管理人员、安全管理员岗位的职责
		应设立安全管理工作的职能部门；	符合 已设定
		应成立指导和管理安全工作的委员会或领导小组，其最高领导应由单位主管领导委任或授权；	符合 有领导小组
		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。	符合 明确分工何职责
2	人员配备	应配备一定数量的系统管理人员、网络管理人员、安全管理员等。	符合
		应配备专职安全管理员，不可兼任；	符合
		关键事务岗位应配备多人共同管理。	符合
3	授权和审批	应根据各个部门和岗位的职责明确授权审批部门及批准人，对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批。	符合
		应针对关键活动建立审批流程，并由批准人签字确认。	符合
		应根据各个部门和岗位的职责明确授权审批事项；	符合

		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	符合
		批过程，对重要活动建立逐级审批制度；	符合
		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；	符合
4	沟通和合作	应加强各类管理人员之间、组织内部机构之间以及网络安全职能部门内部的合作与沟通。	符合
		应加强与相关外部单位的合作与沟通。	符合
		各类管理人员之间、组织内部机构之间以及系统安全职能部门内部定期或不定期召开协调会议，共同协作处理网络安全问题；	符合
		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；	符合
		应聘请网络安全专家作为常年的安全顾问，指导网络安全建设，参与安全规划和安全评审等	符合
	审核和检查	应由安全管理人员定期进行安全检查，检查内容包括用户账号、系统漏洞、数据备份等情况。	符合
		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；	符合
		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；	符合
		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。	符合

4.6.2 结果汇总

序号	测评对象	测评指标				
		岗位设置	人员配备	授权和审批	沟通和合作	审核和检查
1	安全管理机构	符合	符合	符合	符合	符合
		4/4	3/3	6/6	5/5	4/4

4.7 人员安全管理

4.7.1 结果记录

序号	指标名称	测评项	现场结果记录
1	人员录用	应指定或授权专门的部门或人员负责人员录用。	符合
		应规范人员录用过程，对被录用人员的身份、背景和专业资格等进行审查，对其所具有的技术技能进行考核。	符合

		应与从事关键岗位的人员签署保密协议。	符合
		应严格规范人员录用过程，对被录用人的资质等进行审查；	符合
		应签署保密协议；	符合
		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。	符合
2	人员离岗	应规范人员离岗过程，及时终止离岗员工的所有访问权限。	符合
		对于离岗人员，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。	符合
		对于离岗人员，应办理严格的调离手续。	符合
		关键岗位人员离岗须承诺调离后的保密义务后方可离开	符合
3	人员考核	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。	符合
		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；	符合
		应对考核结果进行记录并保存。	符合
4	人员和技术支持能力	业务及应用系统的运维应有专职的管理责任人。	符合
		应有系统业务管理和控制，以及设备操作、维护、管理等相关技术人员。	符合
		相关管理和技术人员应通过技术培训和考核。	符合
5	安全意识教育和培训	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。	符合
		应告知人员相关的安全责任和惩戒措施，并对违反违背安全策略和规定的人员进行惩戒。	符合
		应制定安全教育和培训计划，对网络安全基础知识、岗位操作规程等进行培训。	符合
		应对安全责任和惩戒措施进行书面规定；	符合
		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；	符合
		教育和培训的情况和结果进行记录并归档保存。	符合
6	外部人员访问管理	应确保在外部人员访问受控区域前得到授权或审批，批准后由专人全程陪同或监督，并登记备案。	符合
		应确保在外部人员访问受控区域前先提出书面申请	符合
		对外部人员允许访问的区域、网络、设备、信息等内容应进行书面的规定，并按照规定执行	符合

4.7.2 结果汇总

序号	测评对象		测评指标				
		人员录用	人员离岗	人员考核	人员和技术能力	安全意识教育和培训	外部人员访问管理
1	人员安全管理	符合	符合	符合	符合	符合	符合
		6/6	4/4	3/3	3/3	5/5	3/3

4.8 系统建设管理

4.8.1 结果记录

序号	指标名称	测评项	现场结果记录
1	定级	应明确网络的边界和安全保护等级。	不适用 首次测评
		应以书面的形式说明网络确定为某个安全等级的方法和理由。	
		应确保网络的定级结果经过相关部门的批准。	
		应组织相关部门和有关安全技术专家对系统定级结果的合理性和正确性进行论证和审定；	
		应将定级结果分级上报至全国或地区的主管部门，主管部门对定级结果审批	
2	安全方案设计	应根据网络的安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施。	符合 不符合已根据要求进行整改
		应以书面形式描述对网络的安全保护要求、策略和措施等内容，形成网络的安全方案。	符合 已正式
		应对安全方案进行细化，形成能指导安全系统建设、安全产品采购和使用的详细设计方案。	符合
		应组织相关部门和有关安全技术专家对安全设计方案的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。	符合
		应指定和授权专门的部门对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；	符合
		应根据安全等级划分情况，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；	符合
		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	符合

		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；	
		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。	符合
3	产品采购和使用	应确保安全产品采购和使用符合国家的有关规定。	符合
		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。	符合
		应指定或授权专门的部门负责产品的采购。	符合
		自行软件开发应确保开发环境与实际运行环境物理分开。	符合
		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。	符合
		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。	符合
		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。	符合
4	自行软件开发	应确保开发环境与实际运行环境物理分开。	符合
		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。	符合
		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。	符合
		应确保开发人员和测试人员分离，测试数据和测试结果受到控制；	符合
		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；	符合
		确保对程序资源库的修改、更新、发布进行授权和批准。	符合
	外包软件开发	应根据开发需求检测软件质量。	不适用 无外包软件开发
		应要求开发单位提供软件设计的相关文档和使用指南。	不适用
		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
	工程实施	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。	符合

		应制定详细的工程实施方案，控制工程实施过程。	符合
		要求工程实施单位能正确地执行安全工程过程；	符合
		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。	符合
	测试验收	应对系统进行安全性测试验收。	符合
		在测试验收前应根据设计方案或合同要求等制订覆盖网络安全要求的测试验收方案，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。	符合
		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；	符合
		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。	符合
	交付	应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点。	符合
		应对负责运行维护的技术人员进行相应的技能培训。	符合
		应对交付的控制方法和人员行为准则进行书面规定；	符合
		应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成交付工作；	符合
		在正式投入使用前，应根据实际情况进行试运行，试运行期间应提供相关应急预防措施；	符合
		在正式投入使用后，应对开发、建设过程中涉及安全要求的配置、口令等内容重新修改、设定。	符合
	安全服务商的选择	应确保安全服务商的选择符合国家的有关规定。	符合
		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。	符合
		应确保选定的安全服务商提供技术支持和服务承诺，必要时与其签订服务合同。	符合
	等级测评	在系统运行过程中，应至少每年进行一次等级测评，发现不符合相应等级保护标准要求的及时整改。	不适用 目前首次测评
		应在系统发生变更时及时对定级单元进行等级测评，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。	

		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。	
		应指定或授权专门的部门或人员负责等级测评的管理。	

4.8.2 结果汇总

序号	测评对象	测评指标									
		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	验收测试	系统交付	安全服务商选择	等级测评
	系统建设管理	N/A	符合	符合	符合	N/A	符合	符合	符合	符合	N/A
1		N/A	8/8	7/7	6/6	N/A	4/4	4/4	6/6	3/3	N/A

4.9 系统运维管理

4.9.1 结果记录

序号	指标名称	测评项	现场结果记录
1	运行维护能力	应具有完善运行维护管理制度，管理制度应涵盖业务管理和控制、系统运行、设备操作和维护等方面。	符合
		应按照统一的运行维护要求，对业务及应用系统进行规范化的维护。	符合
		应有业务及应用系统相关介质存取、验证和转储的管理制度，确保有关备份数据、信息的授权访问；	符合
		应保持与其他部门、外部单位间良好的联络和协作能力。	符合
2	环境管理	应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设备设施进行维护管理。	符合
		应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。	符合
		应建立机房安全管理制度，对有关机房物理区域访问，物品带进、带出机房和机房环境安全等方面的管理作出规定。	符合
		应加强对办公环境的保密性管理，包括工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员等内容。	符合
		应有指定的部门负责机房安全，并配置电子门禁系统，对机房来访人员实行登记记录和电子记录双重备案管理；	符合
		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。	符合

3	资产管理	应编制与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。	符合
		应建立资产安全管理制度，规定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。	符合
		应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；	符合
		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。	符合
4	介质管理	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。	符合
		应对介质归档和查询等过程进行记录，并根据存档介质的目录清单定期盘点。	符合
		应对需要送出维修或销毁的介质，首先清除其中的敏感数据，防止信息的非法泄漏。	符合
		应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。	符合
		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；	符合
		应对介质的物理传输过程中人员选择、打包、交付等情况进行控制；	符合
		应对存储介质的使用过程进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，对保密性较高的存储介质未经批准不得自行销毁；	符合
		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；	符合
		应对重要介质中的数据和软件采取加密存储。	符合
	设备管理	应对网络相关的各种设备（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。	符合
		应建立基于申报、审批和专人负责的设备安全管理制度，对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。	符合
		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，按操作规程实现关键设备（包括备份和冗余设备）的启动/停止、加电/断电等操作。	符合
		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。	符合
		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。	符合

	网络安全管理	应指定人员对网络进行管理，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。	符合
		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。	符合
		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。	符合
		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。	符合
		应对网络设备的配置文件进行定期备份。	符合
		应保证所有与外部系统的连接均得到授权和批准。	符合
	恶意代码防范管理	应提高所有用户的防病毒意识，告知及时升级防病毒软件，在读取移动存储设备上的数据以及从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。	符合
		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。	符合
		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。	符合
		应定期检查网络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。	符合
	密码管理	应使用符合国家密码管理规定的密码技术和产品。	符合
		应建立密码使用管理制度。	符合
	变更管理	应确认网络中要发生重要变更的行为，并制定相应的变更方案。	符合
		网络发生重要变更前，应向主管领导申请，审批后方可实施变更，并在实施后向相关人员通告。	符合
		应建立变更管理制度，变更和变更方案需有评审过程；	符合
		应建立变更申报和变更审批文件化程序，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；	符合
		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。	符合
	备份与恢复管理	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。	符合
		应规定备份信息的备份方式（如增量备份或全备份等）、备份频度（如每日或每周等）、存储介质、保存期等。	符合

		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，备份策略应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。	符合
		应建立备份与恢复管理相关的安全管理制度；	符合
		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；	符合
		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。	符合
	安全事件处置	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。	符合
		应制定安全事件报告和处置管理制度，明确安全事件类型，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。	符合
		应根据安全事件对本网络产生的影响，对本网络安全事件进行等级划分。	符合
		应记录并保存所有发现的安全弱点和可疑事件，分析事件原因，监督事态发展，采取措施避免安全事件发生。	符合
		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；	符合
		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；	符合
		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。	符合
	应急预案管理	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。	符合
		应对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。	符合
		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；	符合
		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；	符合
		应规定应急预案需要定期审查和根据实际情况更新等内容，并按照执行。	符合

4.9.2 结果汇总

序号	测评对象	测评指标											
		运行维护能力	环境管理	资产管理	介质管理	设备管理	网络安全管理	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	系统运维管理	符合	符合	符合	符合	符合	符合	符合	符合	符合	符合	符合	符合
		4/4	6/6	4/4	9/9	5/5	6/6	4/4	2/2	5/5	6/6	7/7	5/5

5 资产识别与评价

5.1 资产概述

根据深圳时间价值互联网金融资产交易系统资产情况，并参考结合依据 YD/T 1729-2008《电信网和互联网安全等级保护实施指南》进行资产识别与分类，具体如下表所示：

分类	一般描述
系统资产	互联网金融资产交易系统

5.2 资产识别与分析

5.3 系统资产及赋值

资产名称	IP 地址/URL 地址	资产价值要素			资产价值
		I（社会影响力）	V（业务价值）	A（可用性）	
交易系统 Web1	182.92.175.206	3	3	3	3
交易系统 Web2	123.57.9.11	3	3	3	3
交易系统 Databse Master	101.201.146.76	3	3	3	3
交易系统 Database Slave	123.56.192.64	3	3	3	3
交易系统 Distribute	101.201.220.148	3	3	3	3
交易系统 Beta	47.88.15.255	3	3	3	3

5.3.1 主机列表

资产名称	IP 地址	主机(系统平台 OS 类型)
交易系统 Web1	182.92.175.206	Centos 6.5 X64
交易系统 Web2	123.57.9.11	Centos 6.5 X64
交易系统 Databse Master	101.201.146.76	Centos 6.5 X64
交易系统 Database Slave	123.56.192.64	Centos 6.5 X64
交易系统 Distribute	101.201.220.148	Centos 6.5 X64
交易系统 Beta	47.88.15.255	Centos 6.5 X64

5.3.2 应用系统列表

资产名称	URL 地址
互联网金融资产交易系统	www.sjjz.com

6 威胁识别与分析

- **互联网金融资产交易系统**

威胁类型	威胁编号	威胁名称	威胁来源*			威胁赋值	威胁描述
			故意	意外	环境		
信息系统	1T01	窃听	✓			2	以网络嗅探、窃听或偷听形式造成的信息泄露
	1T02	远程间谍	✓			1	无意地被安装了代理程序，使得攻击者可以远程获取客户端操作信息
	1T03	蓄意泄密	✓			2	内部人员玩忽职守，蓄意泄漏机密信息
	1T04	蓄意破坏/篡改	✓			2	蓄意破坏信息资产而导致资产不可用或者不完整
	1T05	非授权访问/使用	✓	✓		3	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
	1T06	非法的软件拷贝	✓			2	以非授权形式进行的软件分发
	1T07	使用盗版软件	✓	✓		1	使用未经授权的操作系统软件、应用软件或工具软件
	1T08	数据丢失		✓		1	非故意地丢失数据或遗失信息资产
	1T09	操作失误	✓	✓		1	在正常工作或使用过程中，由于操作不当而无意中造成对资产的侵害
	1T10	恶意代码	✓	✓		1	受到病毒、蠕虫、逻辑炸弹、木马后门等恶意代码的攻击
	1T11	黑客入侵	✓			2	被黑客入侵造成系统失常或信息泄露
	1T12	拒绝服务	✓			1	系统由于受到攻击等意外原因而无法对外提供正常服务
	1T13	软件故障	✓	✓		1	软件在正常使用过程中发生的故障
	1T14	设备故障/老化		✓		1	设备或介质在正常使用中出现故障或老化而导致可用性降低或不可用
	1T15	系统/网络过载	✓	✓		1	网络流量过载或系统资源耗竭而导致可用性降低或不可用
	2T01	管理不当	✓			2	网络、软件、系统、设备管理混乱的可能性

7 脆弱性识别与评价

序号	资产名称	威胁名称	主机（ＩＰ）	弱点名称	问题描述	风险因素			风险值	风险说明
						资产价值	威胁值	弱点值		
1.	互联网金融资产	非授权访问/使用	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03LI01身份鉴别弱点	未两种或两种以上组合的鉴别技术对相关设备的管理用户进行身份鉴	3	4	4	12	中风险
2.	互联网金融资产	非授权访问/使用	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03LI01身份鉴别弱点	未对口令设置复杂度	3	4	4	12	中风险
3.	互联网金融资产	非授权访问/使用	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03LI01身份鉴别弱点	未启用登录失败处理功能	3	4	4	12	中风险
4.	互联网金融资产	非授权访问/使用	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03LI02访问控制弱点	UMASK 设置为 077	3	3	3	9	低风险

5.	互联网金融资产	非授权访问/使用	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03 LI 02 访问控制弱点	未对 sync、shutdown、 halt 账号禁用	3	4	4	12	中风险
6.	互联网金融资产	非授权访问/使用	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03 LI 02 访问控制弱点	未对重要信息资源设置敏感标记	3	3	3	9	低风险
7.	互联网金融资产	非授权访问/使用	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03 LI 04 入侵防范弱点	日志审计不全	3	4	4	12	中风险
8.	互联网金融资产	非授权访问/使用	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03 LI 04 入侵防范弱点	未定期根据审计数据生成报表	3	3	3	9	低风险
9.	互联网金融资产	非授权访问/使用	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03 LI 04 入侵防范	对重要程序的完整性进行检测	3	3	3	9	低风险

				弱点						
10.	互联网金融资产	非授权访问/使用	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03 LI 06 资源控制弱点	未通过设定终端接入方式、网络地址范围等条件限制管理终端登录。	3	3	3	9	低风险
11.	互联网金融资产	非授权访问/使用	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03 LI 06 资源控制弱点	未对登录终端的操作超时锁定	3	4	4	12	中风险
12.	互联网金融资产	非授权访问/使用	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03 LI 06 资源控制弱点	对单个用户占用系统资源进行限制功能	3	3	3	9	低风险
13.	互联网金融资产	非授权访问/使用	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03 LI 06 资源控制弱点	未对服务器的CPU、硬盘、内存、网络等资源的使用情况进行监测	3	3	3	9	低风险
14.	互联网金融资产	非授权访问/使用	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03 LI 06 资源控	未使用 IT 监控设备对服务器的服务水平进行监测	3	3	3	9	低风险

				制弱点						
15.	互联网金融资产	非授权访问/使用	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03 LI 06 资源控制弱点	未提供重要服务的业务及应用系统应进行系统级备份，以保证其业务连续性。	3	4	4	12	中风险
16.	互联网金融资产	非授权访问/使用	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03 LI 06 资源控制弱点	未建立对主机全部数据、信息进行备份和恢复的管理和控制机制	3	4	4	12	中风险
17.	互联网金融资产	非授权访问/使用	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03 LI 06 资源控制弱点	重要主机未进行异地备份	3	4	4	12	中风险
18.	互联网金融资产	非授权访问/使用	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03 LI 06 资源控制弱点	服务器未使用了资源强制访问控制策略	3	3	3	9	低风险
19.	互联网金融资产	黑客入侵	https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com	04 AP 02 访问	部分符合 传输使用了 HTTPS 加密保护，但未对 cookie 保护	3	4	4	12	中风险

				控制弱点						
20.	互联网金融资产	黑客入侵	https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com	04AP07资源控制弱点	未能够定义业务水平阈值，能够对业务及应用服务水平进行检测，并具备当服务水平降低到预先规定的 阈值时进行告警的功能	3	3	3	9	低风险
21.	互联网金融资产	黑客入侵	https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com	04AP01身份鉴别弱点	部分符合 无口令强度检查（但有提示），已注册 ID 不能重复注册，在重要操作需进行短信验证，传输使用了	3	4	4	12	中风险
22.	互联网金融资产	黑客入侵	https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com	04AP01身份鉴别弱点	不符合要求，前台用户登录需要密码认证，重要操作采用短信验证，后台采用密码认证	3	4	4	12	中风险
23.	互联网金融资产	黑客入侵	https://aa.sjjz.com/sys/admin/	04AP03安全审计弱点	部分符合 有审计功能，无生成报表功能	3	3	3	9	低风险
24.	互联网金融资产	黑客入侵	https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com	04AP02访	登录无验证模块，可进行暴力攻击	3	4	4	12	中风险

				问控制弱点						
25.	互联网金融资产	黑客入侵	https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com	04AP06软件容错弱点	存在 xss 过滤，但规则无效或过滤不完整；不存在 sql 注入过滤；不存在垃圾信息过滤。	3	4	4	12	中风险
26.	互联网金融资产	黑客入侵	https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com	04AP01身份鉴别弱点	无相关统一身份验证平台	3	4	4	12	中风险
27.	互联网金融资产	黑客入侵	https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com	04AP01身份鉴别弱点	登录认证不存在验证码，注册和修改密码等重要操作存在验证码	3	4	4	12	中风险
28.	互联网金融资产	黑客入侵	https://aa.sjjz.com/sys/admin/	04AP01身份鉴别弱点	不存在短信验	3	4	4	12	中风险
29.	互联网金融资产	黑客入侵	https://www.sjjz.com/ https://m.sjjz.com	04AP01	不满足密码长度、复杂度、更换周期要求	3	4	4	12	中风险

				身份鉴别弱点						
30.	互联网金融资产	黑客入侵	https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com	04AP01身份鉴别弱点	不符合要求 无锁定机制	3	4	4	12	中风险
31.	互联网金融资产	黑客入侵	https://aa.sjjz.com/sys/admin/	04AP02访问控制弱点	存在测试功能未进行权限验证	3	4	4	12	中风险
32.	互联网金融资产	黑客入侵	https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com	04AP01身份鉴别弱点	web 页面无随机令牌	3	4	4	12	中风险
33.	互联网金融资产	黑客入侵	https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com	04AP03安全审计弱点	部分符合要求 日志和业务数据分别存储不同的服务器，存在备份，但未对日志记录主机和业务数据主机进行安全配置	3	4	4	12	中风险

34.	互联网金融资产	黑客入侵	https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/	04 AP 02 访问控制弱点	不符合要求 数据库密码明文，无配置其他密码	3	5	5	20	高风险
35.	互联网金融资产	黑客入侵	https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/	04 AP 02 访问控制弱点	部分符合要求 保存到本地系统其他目录下和远程备份，无日志防篡改	3	4	4	12	中风险
36.	互联网金融资产	黑客入侵	https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/	04 AP 02 访问控制弱点	不存在源代码审计	3	3	3	9	低风险
37.	互联网金融资产	黑客入侵	https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/	04 AP 02 访问控制弱点	不符合要求 使用第三方接口，通过 443 端口进行通信，使用证书和 ssl 加密，未使用 10000 以上端口进行通信	3	4	4	12	中风险
38.	互联网金融资产	黑客入侵	https://m.sjjz.com	04 AP 02 访问控制	不符合要求 不存在完整性校验	3	4	4	12	中风险

				弱点						
39.	互联网金融资产	黑客入侵	https://m.sjjz.com	04AP02访问控制弱点	不符合要求 使用网站登录，无内置登录模块或接口，无法抵抗键盘记录等攻击	3	4	4	12	中风险
40.	互联网金融资产	黑客入侵	https://m.sjjz.com	04AP02访问控制弱点	不存在异常处理	3	4	4	12	中风险

8 风险影响分析

目前经过安全整改，大部分的风险已经消除，目前还存在如下安全风险

- 应用安全

序号	对象	内容
1	风险描述	未使用源代码工具对应用代码进行审计
	影响范围	访问控制安全
	影响地址	互联网金融交易系统
	后果分析	深度的安全隐患未能排查，导致应用系统存在入侵等风险。

9 安全整改建议

风险编号	资产名称	主机（ＩＰ）	弱点名称	问题描述	风险值	风险说明	安全整改建议	安全整改情况
1.	互联网金融资产	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03LI01 身份鉴别弱点	未两种或两种以上组合的鉴别技术对相关设备的管理用户进行身份鉴	12	中风险	建议增加一种用户鉴别方式（动态口令、智能卡、指纹、KEY 等）	已整改
2.	互联网金融资产	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03LI01 身份鉴别弱点	未对口令设置复杂度	12	中风险	整改建议： 在/etc/pam.d/system-auth 文件中添加如下配置: password required pam_cracklib.so dcredit=-1 ucredit=-1 ocredit=-1 lcredit=0 minlen=8 /etc/login.defs 口令生存期配置： PASS_MAX_DAYS 90 PASS_MIN_DAYS 10 PASS_WARN_AGE 7	已整改
3.	互联网金融资产	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03LI01 身份鉴别弱点	未启用登录失败处理功能	12	中风险	整改建议： 1.#cp /etc/pam.d/system-auth /etc/pam.d/system-auth.bak 2.vi /etc/pam.d/system-auth 文件中添加如下配置: auth required	已整改

							/lib/security/pam_tally.so onerr=fail no_magic_root account required /lib/security/pam_tally.so deny=3 no_magic_root reset	
4.	互联网金融资产	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03LI02 访问控制弱点	UMASK 设置为 077	9	低风险	建议设置 umask 为 022	已整改
5.	互联网金融资产	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03LI02 访问控制弱点	未对 sync、shutdown、halt 账号禁用	12	中风险	建议对 sync、 shutdown、 halt 账号禁用	已整改
6.	互联网金融资产	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03LI02 访问控制弱点	未对重要信息资源设置敏感标记	9	低风险	建议采用第三方专用敏感设备	已整改
7.	互联网金融资产	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64	03LI04 入侵防范弱点	日志审计不全	12	中风险	参考步骤: 编辑/etc/rsyslog.conf,在文件中加入如下内容: *.err;kern.debug;daemon.notice	已整改

		101.201.220.148 47.88.15.255					/var/log/messages auth.info /var/log/authlog authpriv.* /var/log/secure cron.* /var/log/cron 重启日志服务： #/etc/init.d/syslog restart	
8.	互联网金融资产	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03LI04 入侵防范弱点	未定期根据审计数据生成报表	9	低风险	整改建议：定期根据审计数据生成报表	已整改
9.	互联网金融资产	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03LI04 入侵防范弱点	对重要程序的完整性进行检测	9	低风险	建议部署了、第三方监测软件或硬件（防篡改设备）	已整改
10.	互联网金融资产	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64	03LI06 资源控制弱点	未通过设定终端接入方式、网络地址范围等条件限制管理终端登录。	9	低风险	建议修改 第一种方法： /etc/hosts.allow，/etc/hosts.deny 文件，限制可访问主机的 IP 范围	已整改

		101.201.220.148 47.88.15.255					第二种方法： 在防火墙对访问主机的 IP 地址进行限制	

11.	互联网金融资产	182.92.175.206
		123.57.9.11
		101.201.146.76
		123.56.192.64
		101.201.220.148
		47.88.15.255
			03LI06 资源控制弱点	未对登录终端的操作超时锁定	12	中风险	参考配置:
							(1).执行备份：
							#cp -p /etc/profile /etc/profile_bak
							(2).在/etc/profile 文件增加以下两行(如果存在则修改,否则手工添加)：
							#vi /etc/profile
							TMOUT=300
							#TMOUT 按秒计算
							export TMOUT
								已整改

12.	互联网金融资产	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03LI06 资源控制弱点	对单个用户占用系统资源进行限制功能	9	低风险	建议修改 /etc/security/limits.conf 文件，添加以下配置： * soft core 0 * hard core 0	已整改
13.	互联网金融资产	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03LI06 资源控制弱点	未对服务器的 CPU、硬盘、内存、网络等资源的使用情况进行监测	9	低风险	建议使用第三方监测软件或硬件监测服务器的使用情况	已整改

14.	互联网金融资产	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03LI06 资源控制弱点	未使用 IT 监控设备对服务器的服务水平进行监测	9	低风险	建议使用第三方监测软件或硬件监测服务器的使用情况	已整改
15.	互联网金融资产	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03LI06 资源控制弱点	未提供重要服务的业务及应用系统应进行系统级备份，以保证其业务连续性。	12	中风险	建议使用灾难备份措施	已整改
16.	互联网金融资产	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03LI06 资源控制弱点	未建立对主机全部数据、信息进行备份和恢复的管理和控制机制	12	中风险	建议建立对主机全部数据、信息进行备份和恢复的管理和控制机制	已整改
17.	互联网金融资产	182.92.175.206 123.57.9.11 101.201.146.76 123.56.192.64 101.201.220.148 47.88.15.255	03LI06 资源控制弱点	重要主机未进行异地备份	12	中风险	建议进行异地备份	已整改
18.	互联网金融资产	182.92.175.206 123.57.9.11 101.201.146.76	03LI06 资源控制弱点	服务器未使用了资源强制访问控制策略	9	低风险	整改建议: vi /etc/selinux/config 添加修改为:	已整改

		123.56.192.64 101.201.220.148 47.88.15.255					SELINUX=enforcing #SELINUX=disabled	
19.	互联网金融资产	https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com	04AP02 访问控制弱点	部分符合 传输使用了 HTTPS 加密保护，但未对 cookie 保护	12	中风险	传输使用 HTTPS 加密保护，并对 cookie 保护	已整改
20.	互联网金融资产	https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com	04AP07 资源控制弱点	未能够定义业务水平阈值，能够对业务及应用服务水平进行检测，并具备当服务水平降低到预先规定的 阈值时进行告警的功能	9	低风险	能够定义业务水平阈值，能够对业务及应用服务水平进行检测，并具备当服务水平降低到预先规定的 阈值时进行告警的功能	已整改
21.	互联网金融资产	https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com	04AP01 身份鉴别弱点	部分符合 无口令强度检查（但有提示），已注册 ID 不能重复注册，在重要操作需进行短信验证，传输使用了	12	中风险	建议对口令强度检查（但有提示），已注册 ID 不能重复注册，在重要操作需进行短信验证，传输使用了	已整改

22.	互联网金融资产	https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com	04AP01 身份鉴别弱点	不符合要求，前台用户登录需要密码认证，重要操作采用短信验证，后台采用密码认证	12	中风险	前台用户登录需要密码认证，重要操作采用短信验证，后台采用密码认证	已整改
23.	互联网金融资产	https://aa.sjjz.com/sys/admin/	04AP03 安全审计弱点	部分符合有审计功能，无生成报表功能	9	低风险	对应用的审计日志自动生成报表功能	已整改
24.	互联网金融资产	https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com	04AP02 访问控制弱点	登录无验证模块，可进行暴力攻击	12	中风险	需要登录验证模块，防止暴力攻击	已整改
25.	互联网金融资产	https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com	04AP06 软件容错弱点	存在 xss 过滤，但规则无效或过滤不完整；不存在 sql 注入过滤；不存在垃圾信息过滤。	12	中风险	建议对 XSS 和 SQL 过滤	已整改
26.	互联网金融资产	https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com	04AP01 身份鉴别弱点	无相关统一身份验证平台	12	中风险	建立统一身份验证平台	已整改
27.	互联网金融资产	https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com	04AP01 身份鉴别弱点	登录认证不存在验证码，注册和修改密码	12	中风险	建议登录认证需要验证码，注册和修改密码等重要操作存在验证码	已整改

				等重要操作存在验证码				
28.	互联网金融资产	https://aa.sjjz.com/sys/admin/	04AP01 身份鉴别弱点	不存在短信验	12	中风险	建议需要短信验证	已整改
29.	互联网金融资产	https://www.sjjz.com/ https://m.sjjz.com	04AP01 身份鉴别弱点	不满足密码长度、复杂度、更换周期要求	12	中风险	建议需要满足密码长度、复杂度、更换周期要求	已整改
30.	互联网金融资产	https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com	04AP01 身份鉴别弱点	不符合要求无锁定机制	12	中风险	建议需要锁定机制	已整改
31.	互联网金融资产	https://aa.sjjz.com/sys/admin/	04AP02 访问控制弱点	存在测试功能未进行权限验证	12	中风险	建议对测试功能进行权限验证	已整改
32.	互联网金融资产	https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com	04AP01 身份鉴别弱点	web 页面无随机令牌	12	中风险	建议 web 页面需要随机令牌	已整改
33.	互联网金融资产	https://www.sjjz.com/ https://aa.sjjz.com/sys/admin/ https://m.sjjz.com	04AP03 安全审计弱点	部分符合要求日志和业务数据分别存储不同的服务器，存在备份，但未对日志记录主机和业务数据主机进行安全配置	12	中风险	日志和业务数据分别存储不同的服务器，存在备份，需要对日志记录主机和业务数据主机进行安全配置	已整改

34.	互联网金融资产	https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/	04AP02 访问控制弱点	不符合要求数据库密码明文，无配置其他密码	20	高风险	数据库密码不能明文，配置其他密码	已整改
35.	互联网金融资产	https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/	04AP02 访问控制弱点	部分符合要求保存到本地系统其他目录下和远程备份，无日志防篡改	12	中风险	保存到本地系统其他目录下和远程备份，需要日志防篡改	已整改
36.	互联网金融资产	https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/	04AP02 访问控制弱点	不存在源代码审计	9	低风险	建议源代码审计工具对代码进行审计	未整改
37.	互联网金融资产	https://www.sjjz.com/ https://m.sjjz.com https://aa.sjjz.com/sys/admin/	04AP02 访问控制弱点	不符合要求使用第三方接口，通过 443 端口进行通信，使用证书和 ssl 加密，未使用 10000 以上端口进行通信	12	中风险	建议使用第三方接口，通过 443 端口进行通信，使用证书和 ssl 加密，并使用 10000 以上端口进行通信	已整改
38.	互联网金融资产	https://m.sjjz.com	04AP02 访问控制弱点	不符合要求不存在完整性校验	12	中风险	建议对其完整性校验	已整改
39.	互联网金融资产	https://m.sjjz.com	04AP02 访问控制弱点	不符合要求使用网站登录，无内置登	12	中风险	使用网站登录，需要内置登录模块或接口，抵抗键盘记录等攻击	已整改

				录模块或接口，无法抵抗键盘记录等攻击				
40.	互联网金融资产	https://m.sjjz.com	04AP02 访问控制弱点	不存在异常处理	12	中风险	建议异常进行处理	已整改

10 安全测评结论

经过前期调研的结果，互联网金融资产交易系统采用双机热备的部署方式，较好地保障了该应用系统的可用性；以及使用阿里云的网络层面的安全访问控制措施，提高系统层面的安全防护能力。

在初测安全评估中，发现该系统存在安全风险，40 项的不符合项，其中 1 项高风险、27 项中风险，12 项低风险。针对发现的安全问题，该系统相关责任部门对这些风险问题进行确认及安全整改工作，仅剩下 1 项低风险未整改。

综合第 5、6、7、8 章的测评与分析结果，等级测评结果中还存在 1 项不符合项，不会导致互联网金融资产交易系统面临高等级的安全风险，因此深圳时间价值的互联网金融资产交易系统的安全保护能力**基本符合要求** 3.2 级的防护要求。

11 附录

附件一：互联网金融资产交易系统定级情况说明

深圳市时间价值信息技术股份公司按照《电信网和互联网安全等级保护实施指南》以及有YD/B 108—2012《增值电信业务系统安全防护定级和评测实施规范 网络交易系统》规范进行互联网金融资产交易系统的定级。依照各专业网络定级指标赋值原则，确定定级对象安全等级应根据社会影响力、规模和服务范围、所提供服务的重要性三个相互独立的定级要素，结合各类业务系统特点，并通过安全等级计算方法计算得出网络单元的安全等级.

1,三个要素的赋值方法及赋值情况

（1）社会影响力-I

社会影响力指标	赋值	自赋值
定级对象受到破坏后不损害国家安全、社会秩序、经济运行和公共利益	1	3
定级对象受到破坏后不损害国家安全，对社会秩序、经济运行和公共利益造成轻微损害	2	
定级对象受到破坏后对国家安全造成较大损害，或者对社会秩序、经济运行和公共利益造成较为严重的损害	3	
定级对象受到破坏后对国家安全造成严重损害，或者对社会秩序、经济运行和公共利益造成特别严重损害	4	
定级对象受到破坏后对国家安全造成特别严重损害	5	

（2）规模和服务范围-R

规模和服务范围指标	赋值	自赋值
定级对象被破坏后对较少的用户造成影响、或者对较小的地区造成影响	1	1
定级对象被破坏后对较多的用户造成影响、或者对较大的地区造成影响	2	
定级对象被破坏后对很多的用户造成影响、或者对很大的地区造成影响	3	
定级对象被破坏后对非常多的用户造成影响、或者对非常大的地区造成影响	4	
定级对象被破坏后对特别多的用户造成影响、或者对特别大的地区造成影响	5	

（3）所提供服务重要性-V

所提供服务的重要性指标	赋值	自赋值
定级对象所提供服务的重要性较低，被破坏后对网络和业务运营商的合法权益造成轻微损害	1	3
定级对象所提供服务的重要性一般，被破坏后对网络和业务运营商的合法权益造成较大损害	2	
定级对象所提供服务的重要性很高，被破坏后对网络和业务运营商的合法权益造成很大损害	3	
定级对象所提供服务的重要性非常高，被破坏后对网络和业务运营商的合法	4	

权益造成非常大的损害		
定级对象所提供服务的重要性特别高，被破坏后对网络和业务运营商的合法权益造成特别严重的损害	5	

2，安全等级的计算方法及结果

安全等级计算方法：k = Round1{Log2{[α×2I+β×2R+γ×2V]}}

其中，k 代表安全等级值，I 代表社会影响力赋值、R 代表规模和服务范围赋值、V 代表所提供服务的重要性赋值，Round1{}表示四舍五入处理，保留 1 位小数，Log2[]表示取以 2 为底的对数，α、β、γ 分别表示定级对象的社会影响力、规模和服务范围、所提供服务的重要性赋值所占的权重，α≥0，β≥0，γ≥0，且 α+β+γ=1。建议权重值 α、β、γ 分别为：0.4、0.4、0.2，或者 1/3、1/3、1/3，各企业也可根据实际情况确定权重值 α、β、γ。计算所得定级对象的安全等级值与安全等级的映射关系如下表所示。

计算结果k值	安全等级值k	安全等级	自定义安全级别
2．6	1 ≤ k ＜ 1.5	第1级	第3.2级
	1.5 ≤ k ＜ 2.5	第2级	
	2.5 ≤ k ＜ 3.3	第3.1级（属于第3级）	
	3.3 ≤ k ≤ 4	第3.2级（属于第3级）	
	4 ＜ k ＜ 4.5	第4级	
	4.5 ≤ k ≤ 5	第5级	