项目编号：R2017060004

上海市计算机软件评测重点实验室

Shanghai Key Laboratory of Computer Software Testing and Evaluating

信息系统安全等级能力认定报告

系统名称：马上贷平台

委托单位：资鼎（上海）互联网金融信息服务有限公司

测评单位：上海计算机软件技术开发中心

报告时间：二〇一七年九月五日

上海市计算机软件评测重点实验室

（上海计算机软件技术开发中心）

声明

本报告是资鼎（上海）互联网金融信息服务有限公司的马上贷平台的安全等级能力认定报告。

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。

本机构根据特定标准出具的系统安全测评基本符合的结论，仅表明该系统基本达到了标准所规定的要求，并不保证该系统是绝对安全的。

本报告根据测评依据进行测评，对于报告中出现未在认定范围中的参数，不适用于检验检测资质认定。

本报告记录号：R201706004-FB01

上海计算机软件技术开发中心

2017 年 09 月 05 日

安全等级能力认定结论

认定结论与综合得分			
系统名称	马上贷平台	**保护等级**	第三级
系统简介	马上贷平台系统是资鼎（上海）互联网金融信息服务有限公司研发部门自主研发的面向社会公众提供借贷服务的中介平台。马上贷平台系统的安全保障由资鼎（上海）互联网金融信息服务有限公司承担，其中研发部门负责系统的日常运维工作。 马上贷平台系统依托阿里云平台，通过租赁云主机的方式为用户提供借贷服务，系统的功能主要包括：用户前段系统、中间层系统、业务管理平台等。在网络安全边界上通过阿里云的态势感知和防 D 进行安全防护，内部用户通过 windows 堡垒机进行安全管理。马上贷平台系统数据库采用 MonGoDB、Mysql，用户敏感数据加密传输和存储。		
测评过程简介	受资鼎（上海）互联网金融信息服务有限公司委托，上海计算机软件技术开发中心 于 2017 年 7 月 11 日至 2017 年 8 月 21 日对马上贷平台进行了系统安全等级测评工作。本次安全测评的范围主要包括马上贷平台的主机、业务应用系统、安全管理制度和人员等。安全测评通过静态评估、现场测试、综合评估等相关环节和阶段，从主机安全、应用安全、数据安全与备份恢复、安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理八个方面，对马上贷平台进行信息系统安全等级能力认定测评。		
测评结论	基本符合	**综合得分**	80.40 分

总体评价

马上贷平台系统依托阿里云平台，通过租赁云主机的方式为用户提供借贷服务，系统的功能主要包括：用户前段系统、中间层系统、业务管理平台等。

上海计算机软件技术开发中心受的资鼎（上海）互联网金融信息服务有限公司委托，对马上贷平台系统进行信息系统安全等级保护（三级）能力认定测评。本次主要从主机安全、应用安全、数据安全及备份恢复、安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理 8 个方面进行测评。资鼎（上海）互联网金融信息服务有限公司的马上贷平台应测 389 项，不适用 111 项，实测 278 项，实测项中符合 196 项。

通过对信息系统基本安全保护状态的分析，资鼎（上海）互联网金融信息服务有限公司针对马上贷平台面临的主要安全威胁采取了相应的安全机制，基本达到保护信息系统重要资产的作用。

马上贷平台部署了阿里云盾 WEB 防火墙对常见攻击行为进行安全监测和报警，通过阿里云盾的抗 DDOS 模块进行流量攻击防护，目前防护阈值为 22GB，通过阿里云数据库审计系统对数据库的访问和操作系统进行日志审计。

主机操作系统和数据库系统均采用跳板机通过内网方式进行远程管理。操作系统和数据库启用了身份鉴别、口令复杂度设置、访问控制、安全审计等功能。主机操作系统遵循最小安装原则，仅安装需要的组件和应用程序，并开启了所需的端口，且没有多余和过期的账户。采用 SSH 加密的方式进行远程管理，且部署了数据库审计系统对数据库操作日志进行审计和分析。为用户提供了统一登录模块，通过用户名和静态口令的方式进行身份标识和鉴别。

应用系统前后台均提供了身份鉴别、口令复杂度要求、安全审计、数据有效性检验、闲置超时断开连接等功能。应用系统后台提供了访问控制功能，根据用户部门配置用户角色，授予不同账户业务所需的最小权限，配置了管理角色、业务角色，在账户间形成了相互制约的关系。

在数据保护方面，的应用系统采用 HTTPS 协议对数据传输过程进行加密，并采用 AES 对鉴别信息和重要业务数据存储过程进行加密，保证了敏感数据和重要数据在传输和存储过程中的完整性和保密性。数据库每天快照进行完全备份。

安全管理方面建立了由安全策略、管理制度、操作规程等组成的信息安全管理体系及《信息系统安全管理制度》等一系列制度，内容覆盖安全管理活动中的组织安全、人员安全、物理和环境安全、访问控制安全、开发和维护、信息安全事故管理以及运维等方面。公司信息化工作委员会负责起草信息安全政策，确定信息安全管理标准，督促各信息安全执行部门实施信息安全政策、措施。

设立安全主管、信息安全管理员岗位，明确安全主管和信息安全管理员的岗位职责，并设立系统管理员、数据库管理员等岗位。公司信息安全工作小组负责定期召开信息安全工作会议，定期总结信息安全事件记录报告。加强与同业机构、通讯服务商及监管部门的合作与沟通。在人员管理方面规范了录用、离岗流程，要求对被录用人员的身份、背景、专业资格和资质等进行审查和核实，并与员工签署保密协议。

制定了运维管理制度对资产、介质、设备的使用、传输、存储、销毁等进行了规范。对系统安全配置、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进行了规范。对突发的信息网络安全事件进行及时发现、及时报告。对应急预案框架进行了说明，包括日常准备工作、应急处理流程、事件分类、全局事件处理和区域事件处理等方面。

通过对信息系统基本安全保护状态的分析，马上贷平台安全等级能力认定结论为基本符合。测评项符合率为 70.50%，部分符合率为 7.60%，不符合率为 21.90%。问题数总计 109 个，其中高风险问题 0 个，中风险问题数 18 个，低风险问题 91 个。

主要安全问题

1、主机安全

1） 中风险 **操作系统未采用两种或两种以上组合的鉴别技术。**用户登录服务器仅采用用户名+密码方式进行身份鉴别，未采用两种或两种以上的鉴别技术。口令可能被恶意用户猜测获得，合法用户身份被仿冒，导致系统被非授权访问。

2） 中风险 **未限制终端接入地址。**Windows 服务器操作系统未限制终端远程接入地址 IP 或网段。恶意用户可使用任意终端，尝试非授权访问服务器。

3） 中风险 **未对系统资源使用进行限制。**操作系统未限制单个用户对系统资源的最大或最小使用限度。若单个用户过度占用系统资源，可能导致网络瘫痪、服务器宕机等安全事故。

4） 低风险 **未安装防病毒软件。**Centos 服务器操作系统未安装防病毒软件。缺乏统一的病毒监控机制将不利于管理员掌握系统内各主机操作系统的病毒防护现状，无法在病毒暴发时采取及时的应对措施。

5） 低风险 **操作系统未采取完整性保护措施。**操作系统未采取措施对系统内重要程序的完整性进行保护。无法及时发现系统内重要程序被恶意篡改，可能造成业务中断。

6） 低风险 **未提供设置敏感标记功能。**系统未提供设置敏感标记的功能，无法对敏感信息资源进行保护。存在恶意用户通过修改用户权限等方法，非授权访问重要信息资源的可能。

7） 低风险 **未提供专用日志查询分析工具。**系统未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。不利于管理员定期分析系统日志信息，从而无法及时发现系统可能存在的侵害。

8） 低风险 **防病毒软件不支持统一管理。**Windows 服务器操作系统安装的防恶意代码软件为单机版，不支持统一管理。存在发生恶意代码在系统内部网络传播的可能性。

9） 低风险 **未采取措施清除剩余信息。**数据库系统本身具备一定的剩余信息保护机制，同时服务器在物理访问控制、用户授权等方面均采取了较严格的控制管理和操作流程，但是信息删除后无法保证完全清除。可能导致信息泄漏，重要信息资源被非授权的访问。

10） 低风险 **剩余信息保护不完善。**剩余信息保护不完善，无法确保信息删除后完全清除。操作系统和数据库系统均无法确保信息删除后完全清除。

2、应用安全

1） 中风险 **未设置资源分配限额。**系统未对一个访问帐户或一个请求进程占用的资源的最大/最小值进行限制。可能导致系统资源或网络带宽占用率过高，影响业务稳定运行。

2） 中风险 **未提供服务优先级设定功能。**系统未提供服务优先级设定功能，无法根据优先级进行资源分配。存在优先级较低的服务占用过多资源，造成优先级较高的服务资源紧张，无法正常提供服务的可能性，不利于信息系统的正常运行。

3） 中风险 **未限制一个时间段内的并发会话连接数。**系统未对一个时间段内的并发会话连接数进行限制。可能导致业务高峰期系统资源或网络带宽占用率过高，影响业务稳定运行。

4） 低风险 **未采用两种或两种以上的鉴别技术进行身份鉴别。**未采用两种以上组合鉴别技术进行用户身份鉴别。可能导致用户身份信息被冒用，用户口令信息被暴力破解。

5） 低风险 **未提供设置敏感标记功能。**系统未提供设置敏感标记的功能，无法对敏感信息资源进行保护。存在恶意用户通过修改用户权限等方法，非授权访问重要信息资源的可能。

6） 低风险 **剩余信息保护机制不完善。**用户鉴别信息直接记录在 URL 地址中，用户注销后，通过浏览器的历史记录，可以直接访问系统。由于上述问题，恶意人员可能获取到合法用户的鉴别信息，并利用这些鉴别信息仿冒他人身份访问目标系统，侵害了其他合法用户的利益，影响了信息系统的正常运行。

7） 低风险 **未提供空闲会话超时机制。**系统未对用户会话空闲超时时间进行设置，长时间不操作系统不会要求重新鉴别用户身份。存在恶意用户非授权访问系统，造成系统业务信息被非法获取的可能性。

8） 低风险 **未采用数字签名等方式进行接收抗抵赖。**系统目前未采取数字签名等密码技术实现接收抗抵赖功能。仅通过 CA 证书登录时可以实现接收抗抵赖功能。存在操作抵赖事件发生的可能性。

9） 低风险 **未限制最大并发会话连接数。**系统未对最大并发会话连接数进行限制。可能导致业务高峰期系统资源或网络带宽占用率过高，影响业务稳定运行。

10） 低风险 **剩余信息保护机制不完善。**用户退出后未及时清除，其他用户可以获取上次登录用户访问的文件信息。由于上述问题，恶意人员可能获取到合法用户的敏感数据，造成敏感数据的泄露，从而侵害了其他合法用户的利益，影响了信息系统的正常运行。

3、安全管理

1） 中风险 **各个部门和岗位的职责、分工和技能要求不完善。**未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。可能存在部分安全管理职责没有得到有效落实，对组织的信息系统造成风险。

2） 中风险 **未建立安全管理中心。**未建立安全管理中心，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。无法对保护对象进行统一监视和控制，当安全事件发生时无法及时对威胁源进行阻断和干预。

3） 中风险 **未对应急预案进行定期更新和审查。**未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。未及时更新应急预案，导致使用时出现错误或导致无法在规定时间内完成应急工作。

4） 中风险 **岗位设置不完善。**除信息科技部和运行保障部外，其他部门未设立部门信息安全人员负责本部门的信息安全管理工作，协同科技部门开展信息安全管理工作。如可能因缺乏足够的人员配备，导致对信息安全的管理工作不到位。

5） 中风险 **安全方案设计不完善。**尚未提供近期和远期的信息安全建设工作计划。可能导致安全投入缺乏计划性，信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。

6） 中风险 **未制定相关策略对安全措施有效性进行持续监控。**未制定相关策略对安全措施有效性进行持续监控，应指定相关策略对系统安全措施有效性进行监控。无法对保护对象安全措施的有效性进行监控，当安全措施失效时，无法及时对对威胁源进行阻断和干预。

7） 中风险 **安全服务商选择管理不完善。**选定的安全服务商未提供技术培训和服务承诺。可能存在由于相关运维人员技能不足、操作不规范或安全服务商提供的服务水平不到位对系统安全稳定运行带来的风险。

8） 中风险 **介质管理不完善。**未提供重要纸质文档的借阅登记表或申请表。可能导致由于未对技术文档资料进行有效的借阅管理而造成重要信息的泄露，对组织的信息资产及声誉造成风险。

9） 中风险 **未建立详细的设备维护手册。**未建立系统设备的详细操作维护手册，并严格按照系统操作维护手册进行操作维护管理。可能存在系统进行维护过程中出现误操作或违规操作的风险。

10） 中风险 **消防演练频率不满足要求。**每年组织消防演练，但尚未达到每半年一次。消防演练频率过低，无法保证人员对突发事件处理流程的熟悉度，可能存在事件发生时无法正确有效处理的风险。

11） 低风险 **测试验收不完善。**系统上线前，未对系统进行安全性测试验收。安全隐患可能在系统上线运行前未被发现并作出相应处理。

12） 低风险 **安全方案设计不完善。**无安全设计规划文档，安全管理策略大面积缺失。可能导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。

14） 低风险 **外部人员访问受控区域管理不规范。**未要求外部人员访问受控区域前先提出书面申请，访问过程中缺乏专人全程陪同或监督，未进行有效登记。可能导致外部人员非授权访问受控区域，缺乏监督，造成泄密。

15） 低风险 **信息安全管理制度体系不完善。**未形成全面的信息安全管理制度体系，缺失安全策略、管理制度、操作规程中的部分内容。可能导致信息安全管理制度体系存在疏漏，部分管理内容无法有效实施。

16） 低风险 **未聘请信息安全专家作为常年的安全顾问。**未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。可能存在信息系统安全需求设计、安全规划等过程中，缺乏专业性指导。

17） 低风险 **定期审查审批事项制度不完善。**未定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。如可能导致审批项目、审批部门以及审批人等发生变化未及时更新从而给组织内的信息系统带来风险。

18） 低风险 **自行软件开发不完善。**未对程序资源库的修改、更新、发布进行授权和批准管理。可能存在程序资源管理不到位，程序资源遭到非授权访问或覆盖的风险。

19） 低风险 **自行软件开发不完善。**未制定代码编写安全规范。可能存在应用系统软件代码编写不规范，不利于应用系统的升级扩展或不利于应用系统的稳定运行等。

20）低风险 **产品采购管理不完善。**未对产品进行选型测试，确定产品的候选范围，且未定期审定和更新候选产品名单。可能存在采购的产品的安全性和性能不能满足业务需要。

问题处置建议

1、主机安全

1） 中风险 **操作系统未采用两种或两种以上组合的鉴别技术。**建议使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，如动态口令，USB key 等方式，有效保证身份鉴别的可靠性。

2） 中风险 **未限制终端接入地址。**建议限制可登录服务器的管理终端地址，仅允许特定的地址登录。

3） 中风险 **未对系统资源使用进行限制。**建议限制单个用户对系统资源的最大或最小使用限度。

4） 低风险 **未安装防病毒软件。**建议部署网络恶意代码防护产品和主机防病毒软件，并通过病毒监控中心对服务器病毒感染情况进行监控。定期更新防病毒软件特征库降低主机感染病毒、木马的风险。

5） 低风险 **操作系统未采取完整性保护措施。**建议安装第三方的完整性保护软件。

6） 低风险 **未提供设置敏感标记功能。**建议对系统重要资源增加敏感标记的功能，并控制用户对已标记的敏感信息的操作。

7） 低风险 **未提供专用日志查询分析工具。**建议为系统增加对审计日志统计、查询、分析及生成审计报表的功能。

8） 低风险 **防病毒软件不支持统一管理。**建议安装并使用支持统一管理的防恶意代码软件。

9） 低风险 **未采取措施清除剩余信息。**建议采取措施清除剩余信息。

10） 低风险 **剩余信息保护不完善。**建议在存储空间被释放或重新分配前完全清除系统内的文件、目录和数据库记录。

2、应用安全

1） 中风险 **未设置资源分配限额。**建议根据需要对一个帐户或进程占用的资源进行最大/最小额度限制。

2） 中风险 **未提供服务优先级设定功能。**建议对访问用户或请求进行的优先级进行划分，并根据优先级合理分配系统资源。

3） 中风险 **未限制一个时间段内的并发会话连接数。**建议根据需要对系统允许的一个时间段内（如：业务高峰期）系统最大并发会话数以及一个帐户或进程占用的资源分配阈值进行限制。

4） 低风险 **未采用两种或两种以上的鉴别技术进行身份鉴别。**建议采用两种或两种以上的组合鉴别技术进行身份鉴别。

5） 低风险 **未提供设置敏感标记功能。**建议对系统重要资源增加敏感标记的功能，并控制用户对已标记的敏感信息的操作。

6） 低风险 **剩余信息保护机制不完善。**采取技术措施保证系统重要信息资源存储空间在释放或再分配前完全清除，避免鉴别相关信息直接反映到 URL 地址中。

7） 低风险 **未提供空闲会话超时机制。**建议根据业务需要对系统空闲回话超时时间进行设置。

8） 低风险 **未采用数字签名等方式进行接收抗抵赖。**采用数字签名等方式对用户的重要业务操作进行抗抵赖验证。

9） 低风险 **未限制最大并发会话连接数。**建议根据需要对系统允许统最大并发会话数以及一个帐户或进程占用的资源分配阈值进行限制。

10） 低风险 **剩余信息保护机制不完善。**建议用户退出后及时清除用户产生的文件。

3、安全管理

1） 中风险 **各个部门和岗位的职责、分工和技能要求不完善。**建议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。

2） 中风险 **未建立安全管理中心。**建议建立安全管理中心，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。

3） 中风险 **未对应急预案进行定期更新和审查。**建议定期对应急预案进行审查和根据实际情况更新的内容，并按照执行。

4） 中风险 **岗位设置不完善。**建议除信息科技部外，其他部门均设立至少一名部门计算机安全员负责本部门的信息安全管理工作，协同科技部门开展信息安全管理工作。

5） 中风险 **安全方案设计不完善。**建议授权专门的部门对信息系统的安全建设进行总体规划，并制定近远期的安全建设工作计划指导信息系统的安全建设工作。

6） 中风险 **未制定相关策略对安全措施有效性进行持续监控。**制定相关策略对系统安全措施有效性进行持续监控。

7） 中风险 **安全服务商选择管理不完善。**建议与安全服务商签订的协议中明确包含技术培训和服务承诺的相关条款，对安全服务商的提供服务水平和技术培训进行约束。

8） 中风险 **介质管理不完善。**完善文档管理制度，对于重要文档的电子文档采用OA 等电子化办公审批平台进行管理，重要纸质文档采用借阅制度。

9） 中风险 **未建立设备维护手册。**建议建立并完善系统设备操作维护手册，系统运行维护人员严格按照系统操作维护手册进行操作，规范系统操作管理。

10） 中风险 **消防演练频率不满足要求。**建立增加定期消防演练的频率，达到每半年一次。

11） 低风险 **测试验收不完善。**补充在系统验收阶段需委托第三方测试单位对系统进行安全性测试的相关规定，保证今后在系统建设验收阶段委托第三方进行安全测试。

12） 低风险 **安全方案设计不完善。**建议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。

13） 低风险 **安全方案设计不完善。**建议授权专门的部门对信息系统的安全建设进行总体规划，有计划地开展安全建设工作。

14） 低风险 **外部人员访问受控区域管理不规范。**建议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。

15） 低风险 **信息安全管理制度体系不完善。**建议形成由安全策略、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。

16） 低风险 **未聘请信息安全专家作为常年的安全顾问。**建议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。

17） 低风险 **定期审查审批事项制度不完善。**建议定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。

18） 低风险 **自行软件开发不完善。**建议对程序资源库的修改、更新、发布建立授权审批机制，控制程序资源的访问，并尽量采用相关的程序资源管理工具实施权限管理和程序资源的使用。

19） 低风险 **自行软件开发不完善。**建议补充完善代码编写安全相关规范，并要求开发人员参照规范编写代码，提高软件产品的质量和安全性。

20） 低风险 **产品采购管理不完善。**建议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。

目录

安全等级能力认定结论 III

总体评价 IV

主要安全问题 VI

问题处置建议 XI

1 测评项目概述 1

1.1 测评目的 1

1.2 测评依据 1

1.3 测评过程 1

1.4 报告分发范围 3

2 被测信息系统情况 3

2.1 承载的业务情况 3

2.2 网络结构 3

2.3 系统资产 4

2.3.1 机房 5

2.3.2 网络设备 5

2.3.3 安全设备 5

2.3.4 服务器/存储设备 5

2.3.5 终端 5

2.3.6 业务应用软件 6

2.3.7 关键数据类别 6

2.3.8 安全相关人员 6

2.3.9 安全管理文档 7

2.4 安全服务 7

2.5 安全环境威胁评估 7

3 等级测评范围与方法.....8
3.1 测评指标.....8
3.1.1 基本指标.....9
3.1.2 不适用指标.....13
3.1.3 特殊指标.....20
3.2 测评对象.....20
3.2.1 测评对象选择方法.....20
3.2.2 测评对象选择结果.....21
3.3 测评方法.....22
3.3.1 测评方式.....22
3.3.2 测评工具.....23
3.3.3 测评工具接入点说明.....23
4 单元测评.....23
4.1 物理安全.....23
4.1.1 结果汇总.....24
4.2 网络安全.....24
4.2.1 结果汇总.....24
4.3 主机安全.....24
4.3.1 结果汇总.....24
4.3.2 结果分析.....25
4.4 应用安全.....25
4.4.1 结果汇总.....25
4.4.2 结果分析.....26
4.5 数据安全及备份恢复.....27
4.5.1 结果汇总.....27

4.5.2 结果分析 *27*

4.6 安全管理制度 27

4.6.1 结果汇总 *27*

4.6.2 结果分析 *28*

4.7 安全管理机构 28

4.7.1 结果汇总 *28*

4.7.2 结果分析 *29*

4.8 人员安全管理 29

4.8.1 结果汇总 *29*

4.8.2 结果分析 *30*

4.9 系统建设管理 30

4.9.1 结果汇总 *30*

4.9.2 结果分析 *30*

4.10 系统运维管理 32

4.10.1 结果汇总 *32*

4.10.2 结果分析 *32*

4.11 特殊指标 35

4.12 单元测评小结 35

4.12.1 控制点符合情况汇总 *35*

4.12.2 安全问题汇总 *38*

5 整体测评 71

5.1 安全控制间安全测评 71

5.2 层面间安全测评 71

5.3 区域间安全测评 71

5.4 验证测试 71

5.5 整体测评结果汇总 72
6 总体安全状况分析 73
6.1 系统安全防护评估 73
6.2 安全问题风险评估 75
6.3 等级能力认定结论 96
7 问题处置建议 97
附录 A 等级测评结果记录 106
A.1 物理安全 106
A.2 网络安全 106
A.3 主机安全 106
A.4 应用安全 122
A.5 数据安全及备份恢复 135
A.6 安全管理制度 138
A.7 安全管理机构 140
A.8 人员安全管理 146
A.9 系统建设管理 149
A.10 系统运维管理 160
A.11 验证测试 185

1 测评项目概述

1.1 测评目的

对资鼎（上海）互联网金融信息服务有限公司的马上贷平台系统进行测评，验证其是否满足GB/T 22239-2008《信息安全技术 信息系统安全等级保护基本要求》三级（S3A3G3）和JR/T 0071-2012《金融行业信息系统信息安全等级保护实施指引》三级的要求。

1.2 测评依据

- GB/T 22239-2008：《信息安全技术 信息系统安全等级保护基本要求》
- JR/T 0071-2012：《金融行业信息系统信息安全等级保护实施指引》
- JR/T 0072-2012：《金融行业信息系统信息安全等级保护测评指南》

以下为本次测评的相关参考标准和文档：

- GB/T28448-2012：《信息安全技术 信息系统安全等级保护测评要求》
- GB/T28449-2012：《信息系统安全等级保护测评过程指南》
- GB/T20984-2007：《信息安全技术 信息安全风险评估规范》

1.3 测评过程

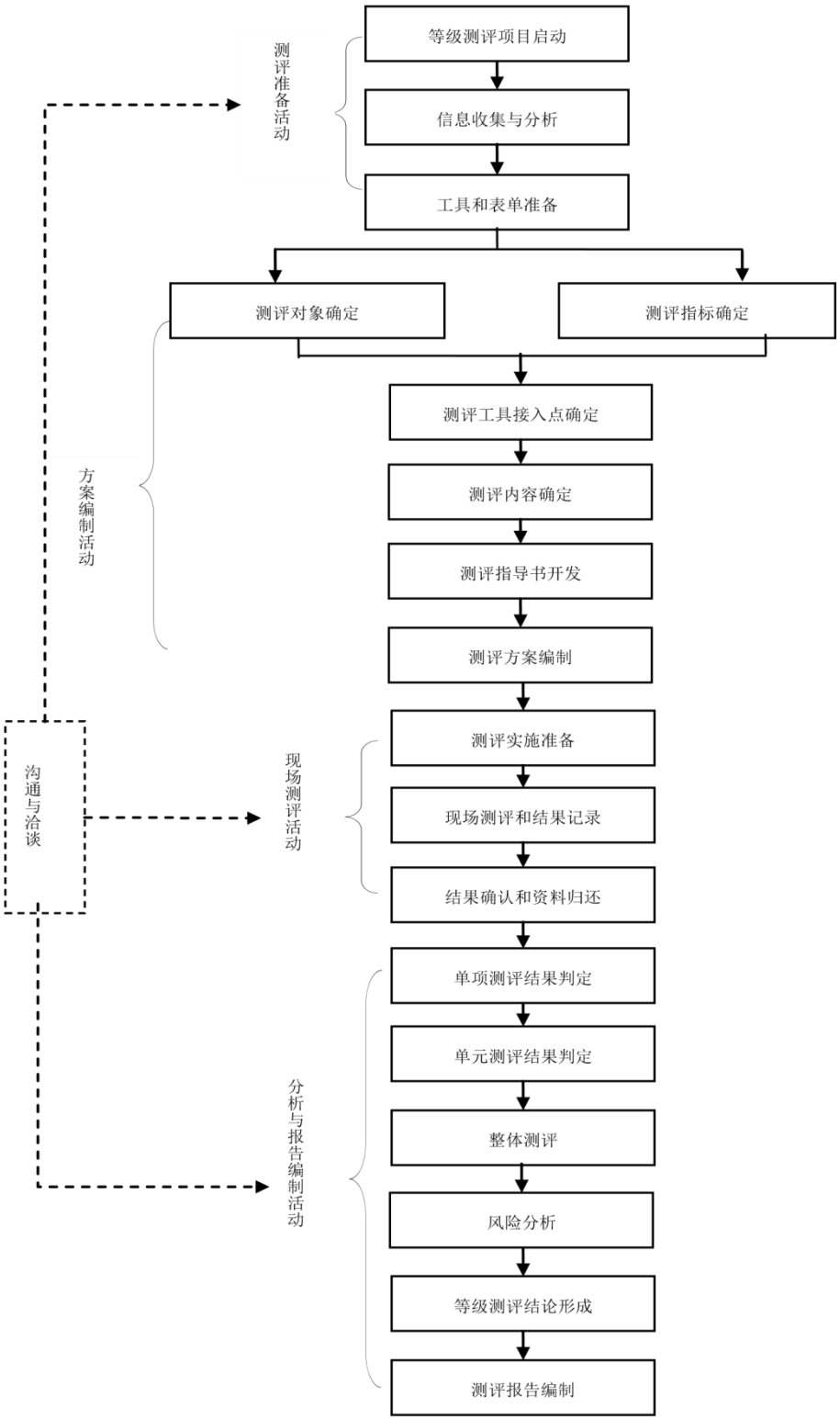


图 1.1 等级保护测评工作流程图

本次等级测评分为四个过程：测评准备过程、方案编制过程、测评实施过程、分析与报告编制过程。具体如图 1.1 所示。其中，各阶段的时间安排如下：

1、2017 年 7 月 11 日～7 月 13 日，测评准备过程。

2、2017 年 7 月 14 日～7 月 15 日，方案编制过程。

3、2017 年 7 月 17 日～8 月 21 日，现场实施过程。

4、2017 年 8 月 22 日～9 月 5 日，分析与报告编制过程。

其中，2017 年 7 月 11 日召开了项目启动会议，确定了工作方案及项目人员名单；2017 年 8 月 16 日召开了项目末次会议，确认了测评发现的问题；2017 年 8 月 21 日对系统的整改情况进行了复核确认。

1.4 报告分发范围

等级测评报告正本一式两份，其中资鼎（上海）互联网金融信息服务有限公司一份，上海计算机软件技术开发中心一份。

2 被测信息系统情况

资鼎（上海）互联网金融信息服务有限公司建立了一套具有较强的业务处理能力的马上贷平台，并对该系统进行信息安全保护。

2.1 承载的业务情况

马上贷平台，是由资鼎（上海）互联网金融信息服务有限公司推出的一个固定周期小额微贷 P2P 项目：为借款人提供一站式风险评估，以及网贷信息中介服务；为出借人提供平台筛选的的优质小额资产，通过小额分散的投资方式来降低风险。

2.2 网络结构

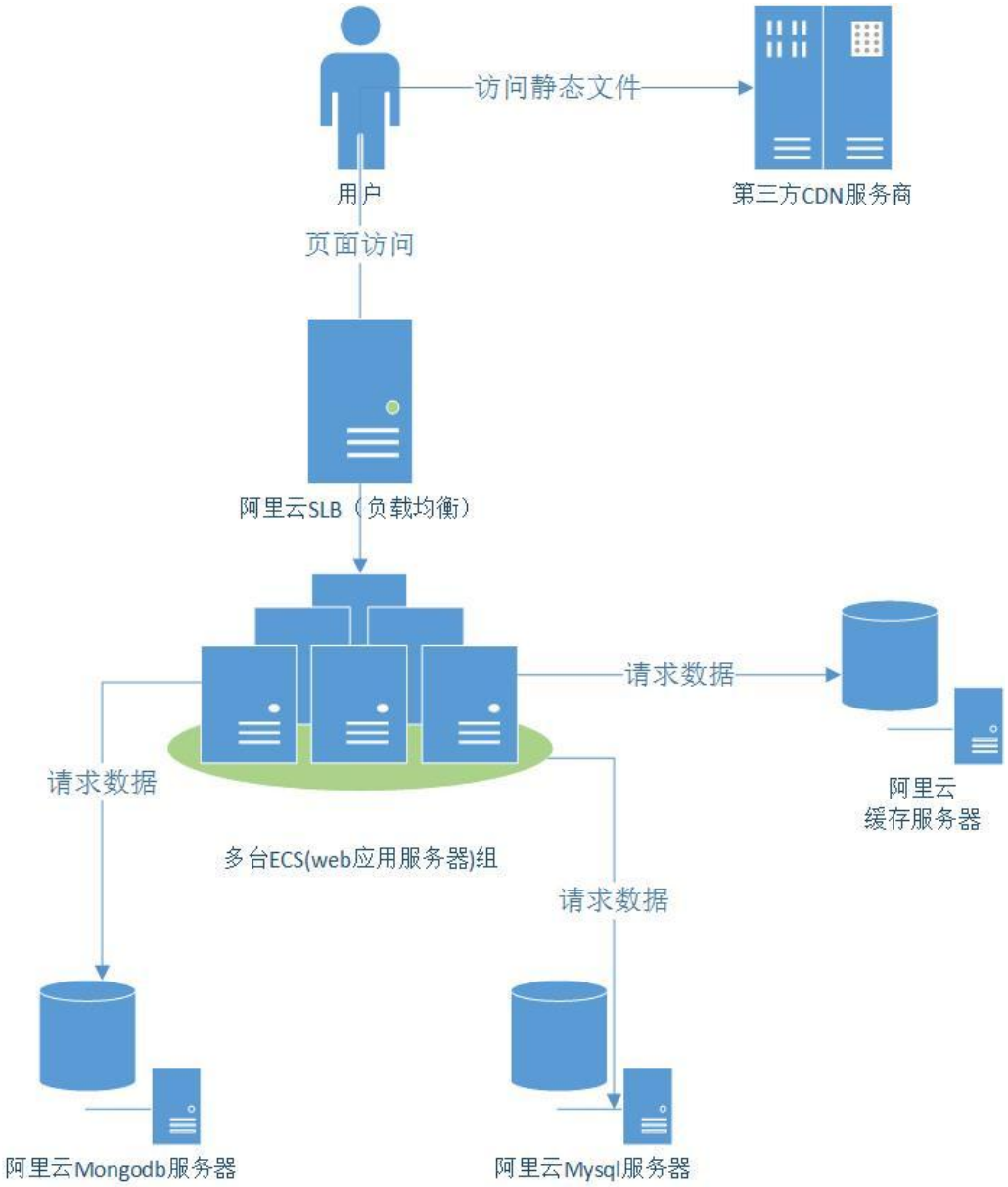


图 2.1 网络拓扑图

如图 2.1 马上贷平台网络拓扑图所示，马上贷平台系统依托阿里云平台，通过租赁云主机的方式为用户提供服务，在网络安全边界上通过阿里云的态势感知和防D 进行安全防护，内部用户通过 windows 堡垒机进行安全管理。马上贷平台系统数据库采用 MonGoDB、Mysql，数据库的维护和管理由阿里云负责。

2.3 系统资产

系统资产包括被测信息系统相关的所有软硬件、人员、数据及文档等。

2.3.1 机房

被测信息系统部署在阿里云平台。

2.3.2 网络设备

被测信息系统部署在阿里云平台。

2.3.3 安全设备

以列表形式给出被测信息系统中的安全设备。

序号	设备名称	操作系统	品牌	型号	用途	数量（台/套）	重要程度
1	WEB 防火墙	--	阿里云	--	应用层防护	1	重要
2	数据库审计	--	阿里云	--	数据库日志审计	1	重要

2.3.4 服务器/存储设备

以列表形式给出被测信息系统中的服务器和存储设备，描述服务器和存储设备的项目包括设备名称、操作系统、数据库管理系统以及承载的业务应用软件系统。

序号	设备名称[1]	操作系统/数据库管理系统	版本/IP	业务应用软件	数量（台/套）	重要程度
1	centos	centos	6.5	马上贷平台	1	非常重要
2	windows	windows	2008	马上贷平台	1	非常重要
3	mysql	阿里云	5.6	马上贷平台	1	非常重要
4	MongoDB	--	3.2	马上贷平台	1	非常重要

2.3.5 终端

以列表形式给出被测信息系统中的终端，包括业务管理终端、业务终端和运维终端等。

序号	设备名称	操作系统	用途	数量（台/套）	重要程度
1	DELL 台式电脑	Windows 10	运维终端	1	一般

[1]设备名称在本报告中应唯一，如 xx 业务主数据库服务器或 xx-svr-db-1。

序号	设备名称	操作系统	用途	数量（台/套）	重要程度
2	华硕笔记本电脑	Win10	日常工作	1	一般

2.3.6 业务应用软件

以列表的形式给出被测信息系统中的业务应用软件（包括含中间件等应用平台软件），描述项目包括软件名称、主要功能简介。

序号	软件名称	主要功能	开发厂商	重要程度
1	马上贷微信端	用户端，前台展示	自主开发	非常重要
2	马上贷后台	管理端，后台管理	自主开发	非常重要

2.3.7 关键数据类别

以列表形式描述具有相近业务属性和安全需求的数据集合。

序号	数据类别[1]	所属业务应用	安全防护需求[2]	重要程度
1	系统管理数据	马上贷平台	保密性	非常重要
2	业务数据	马上贷平台	保密性	非常重要
3	鉴别信息	马上贷平台	保密性	非常重要

2.3.8 安全相关人员

以列表形式给出与被测信息系统安全相关的人员情况。相关人员包括（但不限于）安全主管、系统建设负责人、系统运维负责人、网络（安全）管理员、主机（安全）管理员、数据库（安全）管理员、应用（安全）管理员、机房管理人员、资产管理员、业务操作员、安全审计人员等。

序号	姓名	岗位/角色	联系方式
1	姚力	安全主管	13916347636
2	温健根	系统建设负责人	15921587198
3	徐垚鑫	系统运维负责人	13262509737
4	吴姜为	网络管理员	17612124551

[1]如鉴别数据、管理信息和业务数据等，而业务数据可从安全防护需求（保密、完整等）的角度进一步细分。

[2]保密性，完整性等。

2.3.9 安全管理文档

以列表形式给出与信息系统安全相关的文档，包括管理类文档、记录类文档和其他文档。

序号	文档名称	主要内容
1	资鼎安全管理制度汇编	信息安全组织机构、人员信息安全管理、系统建设安全管理、机房安全管理、信息资产安全管理、截止管理、设备安全管理、网络安全管理、系统安全管理、恶意代码防范管理、变更控制管理、设备恢复管理、安全事件管理等

2.4 安全服务

无安全服务。

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	威胁分(子)类	描述
1	软硬件故障	对业务实施或系统运行产生影响的设备硬件故障、通讯链路中断、系统本身或软件缺陷等问题
2	物理环境影响	对信息系统正常运行造成影响的物理环境问题和自然灾害
3	无作为或操作失误	应该执行而没有执行相应的操作，或无意执行了错误的操作
4	管理不到位	安全管理无法落实或不到位，从而破坏信息系统正常有序运行
5	恶意代码	故意在计算机系统上执行恶意任务的程序代码
6	越权或滥用	通过采用一些措施，超越自己的权限访问了本来无权访问的资源，或者滥用自己的

序号	威胁分(子)类	描述
		权限，做出破坏信息系统的行为
7	网络攻击	利用工具和技术通过网络对信息系统进行攻击和入侵
8	物理攻击	通过物理的接触造成对软件、硬件、数据的破坏
9	泄密	信息泄露给不应了解的他人
10	篡改	非法修改信息，破坏信息的完整性使系统的安全性降低或信息不可用
11	抵赖	不承认收到的信息和所作的操作和交易
12	资源不足	系统重要设备负载较高，不满足业务需求，一旦设备因负载较高而出现故障将影响业务连续性
13	敏感信息泄漏	敏感信息包括用户信息、 公民信息、地理信息，数量级 0~1 万、1~10 万、10~100 万、100 万以上
14	网页篡改	针对连接互联网的网站面临被篡改的可能性较大

3 等级测评范围与方法

3.1 测评指标

《基本要求》中对不同等级信息系统的安全功能和措施提出了具体要求，等级测评应根据信息系统的安全保护等级从中选取相应等级的安全测评指标，并依据《测评要求》和《测评过程指南》对信息系统实施安全测评。

本次安全等级测评范围内的测试系统的安全保护等级为第三级，其中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(S3A3G3)。

表 3-1 测评指标统计列表（S3A3G3）

测评指标					
技术/管理	安全分类	安全子类数量			
		S3	A3	G3	小计
安全技术	物理安全	1	1	8	10
	网络安全	1	0	6	7
	主机安全	3	1	3	7
	应用安全	5	2	2	9
	数据安全及备份恢复	2	1	0	3
安全管理	安全管理制度	0	0	3	3
	安全管理机构	0	0	5	5
	人员安全管理	0	0	5	5
	系统建设管理	0	0	11	11
	系统运维管理	0	0	13	13
合　　计					73

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 3-2 中列出。鉴于信息系统的复杂性和特殊性，《基本要求》的个别要求项可能不适用，对于这些不适用项应在表后给出不适用原因。

表 3-2 基本指标

安全层面[1]	安全控制点[2]	测评项数
物理安全	物理位置的选择	3

[1] 安全层面对应基本要求中的物理安全、网络安全、主机安全、应用安全、数据安全与备份恢复、安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理等 10 个安全要求类别。

[2]安全控制点是对安全层面的进一步细化，在《基本要求》目录级别中对应安全层面的下一级目录。

安全层面[1]	安全控制点[2]	测评项数
	物理访问控制	4
	防盗窃和防破坏	6
	防雷击	3
	防火	8
	防水和防潮	4
	防静电	3
	温湿度控制	5
	电力供应	7
	电磁防护	4
网络安全	结构安全	7
	访问控制	9
	边界完整性检查	2
	入侵防范	2
	恶意代码防护	2
	安全审计	4
	网络设备防护	14
主机安全	身份鉴别	6
	剩余信息保护	2
	入侵防范	3
	恶意代码防范	4
	资源控制	6
	访问控制	7
	安全审计	6
应用安全	身份鉴别	8

安全层面[1]	安全控制点[2]	测评项数
	访问控制	7
	安全审计	5
	剩余信息保护	2
	通信完整性	1
	通信保密性	2
	抗抵赖	2
	软件容错	3
	资源控制	7
数据安全及备份恢复	数据完整性	1
	数据保密性	1
	备份和恢复	6
安全管理制度	管理制度	4
	制定和发布	5
	评审和修订	3
安全管理机构	岗位设置	8
	人员配备	3
	授权和审批	6
	沟通和合作	5
	审核和检查	5
人员安全管理	人员录用	6
	人员离岗	3
	人员考核	3
	安全意识教育和培训	5
	外部人员访问管理	3

安全层面[1]	安全控制点[2]	测评项数
系统建设管理	系统定级	4
	安全方案设计	5
	产品采购和使用	9
	自行软件开发	5
	外包软件开发	8
	工程实施	5
	测试验收	6
	系统交付	6
	系统备案	3
	等级测评	4
	安全服务商选择	4
系统运维管理	环境管理	10
	资产管理	4
	介质管理	15
	设备管理	10
	监控管理和安全管理中心	4
	网络安全管理	8
	系统安全管理	8
	恶意代码防范管理	5
	密码管理	6
	变更管理	8
	备份与恢复管理	11
	安全事件处置	7
	应急预案管理	9

安全层面[1]	安全控制点[2]	测评项数
	总计	389

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 3-3 不适用指标

安全层面	安全控制点	不适用项	原因说明
物理安全	--	--	被测系统部署在阿里云，物理安全由阿里云维护
网络安全	--	--	被测系统部署在阿里云，网络安全由阿里云维护
主机安全	访问控制	c)应实现操作系统和数据库系统特权用户的权限分离；	操作系统未安装数据库，该项不适用
	剩余信息保护	a)应保证操作系统和数据库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使用人员前得到完全清除，无论这些信息是存放在硬盘上 还是在内存中；	被测对象为操作系统，此项不适用
		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	被测对象为操作系统，此项不适用

安全层面	安全控制点	不适用项	原因说明
		他使用人员前得到完全清除。	
	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；	被测对象为操作系统，此项不适用
		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或在检测到完整性即将受到破坏时进行事前阻断；	被测对象为操作系统，此项不适用
		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、系统软件预防性维护服务等方式保持系统补丁及时得到更新。	被测对象为操作系统，此项不适用
	资源控制	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；	被测对象为操作系统，此项不适用

安全层面	安全控制点	不适用项	原因说明
		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；	被测对象为操作系统，此项不适用
		f)所有的服务器应全部专用化，不使用服务器进行收取邮件、浏览互联网操作。	被测对象为操作系统，此项不适用
应用安全	身份鉴别	g)对于系统自动分配或者预设的强度较弱的初始密码，系统应强制用户首次登录时修改初始密码；	应用系统前台通过手机号和短信验证码对登录用户进行身份，无初始口令
数据安全及备份恢复	备份和恢复	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；	备份数据保存在阿里云，该项不适用
		c)对于同城数据备份中心，应与生产中心直线距离至少达到 30 公里，可以接管所有核心业务的运行；对于异地数据备份中心，应与生产中心直线距离至少达到 100 公里；	备份数据保存在阿里云，该项不适用
		f)异地备份中心应配备恢复所需的运行环境，并处于就	备份数据保存在阿里云，该项不适用

安全层面	安全控制点	不适用项	原因说明
		绪状态或运行状态，"就绪状态"指备份中心的所需资源(相关软硬件以及数据等资源)已完全满足但设备cpu还没有运行；"运行状态"指备份中心除所需资源完全满足要求外，cpu也在运行状态。	
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、安全性需求分析、详细设计方案等相关配套文件。	被测系统首次进行等级保护测评
	产品采购和使用	d)各机构购置扫描、检测类信息安全产品应报本机构科技主管部门批准、备案；	未购置扫描、检测类信息安全产品
		f)扫描、检测类信息安全产品仅限于本机构信息安全管理人员或经主管领导授权的网络管理员使用；	未购置扫描、检测类信息安全产品
	外包软件开发	a)应根据开发需求	被测系统采用自行

安全层面	安全控制点	不适用项	原因说明
		检测软件质量；	软件开发，该项不适用
		b)应在软件安装之前检测软件包中可能存在的恶意代码；	被测系统采用自行软件开发，该项不适用
		c)应要求开发单位提供软件设计的相关文档和使用指南；	被测系统采用自行软件开发，该项不适用
		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和隐蔽信道；	被测系统采用自行软件开发，该项不适用
	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；	此次测评为首次等保测评，该项不适用
		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；	此次测评为首次等保测评，该项不适用
系统运维管理	环境管理	a)应建立集中的机房，统一为各信息	被测系统部署于阿里云，有阿里云负

安全层面	安全控制点	不适用项	原因说明
		系统提供运行环境。机房设施配备应符合国家计算机机房有关标准要求；	责机房的运行维护
		b)机房应采用结构化布线系统，配线机柜内如果配备理线架，应做到跳线整齐，跳线与配线架统一编号，标记清晰；	被测系统部署于阿里云
		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的管理作出规定；	被测系统部署于阿里云
		d)应指定部门负责机房安全，指派专人担任机房管理员，对机房的出入进行管理，定期巡查机房运行状况，对机房供配电、空调、温湿度控制等设施进行维护管理，填写机房值班记录、巡视记录；	被测系统部署于阿里云
		e)机房管理员应经过相关培训，掌握机房各类设备的操	被测系统部署于阿里云

安全层面	安全控制点	不适用项	原因说明
		作要领；	
		f)应定期对机房设施进行维修保养，加强对易损、易失效设备或部件的维护保养；	被测系统部署于阿里云
		g)机房人员进出机房必须使用主管部门制发的证件；	被测系统部署于阿里云
		h)应单独设置弱电井，并留有足够的可扩展空间；	被测系统部署于阿里云
		i)机房所在区域应安装 24 小时视频监控录像装置，重要机房区域实行 24 小时警卫值班，机房实行封闭式管理，设置一个主出入口和一个或多个备用出入口，出入口控制、入侵报警和电视监控设备运行资料应妥善保管，保存期限不少于 3 个月，销毁录像等资料应经机构主管领导批准后实施；	被测系统部署于阿里云
	密码管理	e)密钥注入、密钥管理功能调试和密钥档案的保管应由专人负责。密钥资	不使用密钥

安全层面	安全控制点	不适用项	原因说明
		料须保存在保险柜内。保险柜钥匙由专人负责。使用密钥和销毁密钥要在监督下进行并应有使用、销毁记录；	
	备份与恢复管理	f)恢复及使用备份数据时需要提供相关口令密码的，应把口令密码密封后与数据备份介质一并妥善保管；	备份数据不需要提供口令密码

3.1.3 特殊指标

本次测评未采用特殊指标。

3.2 测评对象

3.2.1 测评对象选择方法

测评对象是等级测评的直接工作对象，也是在被测系统中实现特定测评指标所对应的安全功能的具体系统组件。因此，选择测评对象是编制测评方案的必要步骤，也是整个测评工作的重要环节。恰当选择测评对象的种类和数量是整个等级测评工作能够获取足够证据、了解到被测系统的真实安全保护状况的重要保证。

依据 GB/T 28449-2012《信息系统安全等级保护测评过程指南》确定本次测评对象。本次测评对象采用抽查的方法，即抽查信息系统中具有代表性的组件作为测评对象，并且在测评对象确定任务中应兼顾工作投入与结果产出两者的平衡关系。在确定测评对象时，除了考虑资产的重要程度以外，还应遵循以下原则：

1. 恰当性：选择的设备、软件系统等满足相应等级的测评强度要求；
2. 重要性：抽查对被测系统来说重要的服务器、数据库和网络设备等；
3. 安全性：抽查对外暴露的网络边界；

4. 共享性：抽查共享设备和数据交换平台/设备；

5. 代表性：抽查尽量覆盖系统各种设备类型、操作系统类型、数据库系统类型和应用系统类型。

3.2.2 测评对象选择结果

1） 机房

被测系统部署于阿里云平台。

2） 网络设备

被测系统部署于阿里云平台。

3） 安全设备

被测系统部署于阿里云平台。

4） 服务器/存储设备

序号	设备名称[1]	操作系统 /数据库管理系统	业务应用软件	重要程度
1	centos	centos	马上贷平台	非常重要
2	windows	windows	马上贷平台	非常重要
3	mysql	阿里云	马上贷平台	非常重要
4	MongoDB	--	马上贷平台	非常重要

5） 终端

序号	设备名称	操作系统	用途	重要程度
1	DELL 台式电脑	Windows 10	运维终端	一般
2	华硕笔记本电脑	Win10	日常工作	一般

6） 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	所在设备名称	重要程度
1	mysql	数据库	阿里云	非常重要

[1]设备名称在本报告中应唯一，如 xx 业务主数据库服务器或 xx-svr-db-1。

序号	数据库系统名称	数据库管理系统类型	所在设备名称	重要程度
2	MongoDB	数据库	阿里云	非常重要

7） 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	马上贷微信端	用户端，前台展示	自主开发	非常重要
2	马上贷后台	管理端，后台管理	自主开发	非常重要

8） 访谈人员

序号	姓名	岗位/职责
1	姚力	安全主管
2	温健根	系统建设负责人
3	徐垚鑫	系统运维负责人
4	吴姜为	网络管理员

9） 安全管理文档

序号	文档名称	主要内容
1	资鼎安全管理制度汇编	信息安全组织机构、人员信息安全管理、系统建设安全管理、机房安全管理、信息资产安全管理、截止管理、设备安全管理、网络安全管理、系统安全管理、恶意代码防范管理、变更控制管理、设备恢复管理、安全事件管理等

3.3 测评方法

3.3.1 测评方式

根据信息系统安全等级保护测评准则，现场测评的方法包括检查、访谈和测试等三类，在此基础上进行综合风险分析。

访谈是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，获取证据以证明信息系统安全等级保护措施是否有效的一种方法。访谈对象涉及物理安全、网络安全、系统安全、应用安全、数据安全和安全管理等方面的内容。其中物理安全、安全管理重点采取访谈方式。

检查不同于行政执法意义上的监督检查，是指测评人员通过对测评对象进行观察、查验、分析等活动，获取证据以证明信息系统安全等级保护措施是否有效的一种方法。检查包括文档核查和配置核查两种，涉及物理安全、网络安全、系统安全、应用安全、数据安全和安全管理等方面的内容。

测试是测评人员通过对测评对象按照预定的方法/工具使其产生特定的行为等活动，查看、分析输出结果，获取证据以证明信息系统安全等级保护措施是否有效的一种方法。测试对象主要涉及网络安全、主机安全、应用安全和数据安全方面的内容。

通过访谈相关安全管理人员、检查配置、规章制度、日常记录、漏洞扫描等手段，结合文件检查和现场核查进行测评。

风险评估过程包含资产识别与赋值、脆弱性评估、威胁评估、现有的安全控制措施评估、风险评价等过程。

3.3.2 测评工具

本次测评采用的工具有：

序号	工具名称	厂商	版本	漏洞库版本
1.	明鉴 Web 应用弱点扫描器	杭州安恒信息技术有限公司	V6.0.1.7	V6.1.82

3.3.3 测评工具接入点说明

马上贷平台应用系统部署于阿里云平台，本次测评主要通过互联网接入的方式进行安全扫描，直接将测评工具接入到互联网进行安全扫描。

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

马上贷平台系统部署于阿里云平台。

4.2 网络安全

4.2.1 结果汇总

马上贷平台系统部署于阿里云平台。

4.3 主机安全

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-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	centos	符合	5	4	6	0	2	0	5
		部分符合	0	0	0	0	0	0	0
		不符合	1	2	0	2	1	3	1
		不适用	0	1	0	0	0	1	0
2	mysql	符合	5	5	6	0	0	-	2
		部分符合	0	0	0	0	0	-	0
		不符合	1	2	0	0	0	-	1
		不适用	0	0	0	2	3	-	3
3	windows	符合	5	4	5	0	3	2	4
		部分符合	0	0	0	0	0	0	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
		不符合	1	2	1	2	0	2	1
		不适用	0	1	0	0	0	0	0

4.3.2 结果分析

部分符合或不符合情况统计如下：

1、用户登录服务器仅采用用户名+密码方式进行身份鉴别，未采用两种或两种以上的鉴别技术。

2、系统未提供设置敏感标记的功能，无法对敏感信息资源进行保护。

3、系统未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。

4、数据库系统本身具备一定的剩余信息保护机制，同时服务器在物理访问控制、用户授权等方面均采取了较严格的控制管理和操作流程，但是信息删除后无法保证完全清除。

5、剩余信息保护不完善，无法确保信息删除后完全清除。

6、操作系统未采取措施对系统内重要程序的完整性进行保护。

7、操作系统未安装防病毒软件。

8、操作系统安装的防恶意代码软件为单机版，不支持统一管理。

9、操作系统未限制终端远程接入地址 IP 或网段。

10、操作系统未限制单个用户对系统资源的最大或最小使用限度。

4.4 应用安全

4.4.1 结果汇总

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

表 4-4 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	马上贷微信端	符合	4	2	5	0	1	2	0	3	2
		部分符合	0	0	0	0	0	0	0	0	0
		不符合	2	2	0	2	0	0	2	0	5
		不适用	2	3	0	0	0	0	0	0	0
2	马上贷管理后台	符合	6	5	4	0	1	2	0	3	4
		部分符合	0	0	0	0	0	0	0	0	0
		不符合	1	2	1	2	0	0	2	0	3
		不适用	1	0	0	0	0	0	0	0	0

4.4.2 结果分析

部分符合或不符合情况统计如下：

1、未采用两种以上组合鉴别技术进行用户身份鉴别

2、系统目前未提供超时自动断开功能

3、系统未提供设置敏感标记的功能，无法对敏感信息资源进行保护。

4、未提供显示上一次成功登录的相关信息的功能。

5、用户鉴别信息直接记录在 URL 地址中，用户注销后，通过浏览器的历史记录，可以直接访问系统。

6、下载文件地址按顺序增长，或者易被猜测到，且用户退出后未及时清除，其他用户可以下载这些文件。

7、系统目前未采取数字签名等密码技术实现接收抗抵赖功能。仅通过 CA 证书登录时可以实现接收抗抵赖功能。

8、系统未对用户会话空闲超时时间进行设置，长时间不操作系统不会要求重新鉴别用户身份。

9、系统未对最大并发会话连接数进行限制。

10、系统未对一个时间段内的并发会话连接数进行限制。

11、系统未对一个访问帐户或一个请求进程占用的资源的最大/最小值进行限制。

12、系统未提供服务优先级设定功能，无法根据优先级进行资源分配。

4.5 数据安全及备份恢复

4.5.1 结果汇总

针对不同安全控制点对单个测评对象在数据安全及备份恢复层面的单项测评结果进行汇总和统计。

表 4-5 数据安全及备份恢复-单元测评结果汇总表

序号	测评对象	符合情况	安全控制点		
			数据完整性	数据保密性	备份和恢复
1	数据安全及备份恢复	符合	1	1	3
		部分符合	0	0	0
		不符合	0	0	0
		不适用	0	0	3

4.5.2 结果分析

数据安全及备份恢复方面，未发现部分符合或不符合的情况。

4.6 安全管理制度

4.6.1 结果汇总

针对不同安全控制点对单个测评对象在安全管理制度层面的单项测评结果进行汇总和统计。

表 4-6 安全管理制度-单元测评结果汇总表

序号	测评对象	符合情况	安全控制点		
			管理制度	制度和发布	评审和修订
1	安全管理制度	符合	3	5	2
		部分符合	1	0	0
		不符合	0	0	1
		不适用	0	0	0

4.6.2 结果分析

部分符合或不符合情况统计如下：

1、未形成全面的信息安全管理制度体系，缺失安全策略、管理制度、操作规程中的部分内容。

2、安全管理制度格式不统一，缺乏版本控制。

4.7 安全管理机构

4.7.1 结果汇总

针对不同安全控制点对单个测评对象在安全管理机构层面的单项测评结果进行汇总和统计。

表 4-7 安全管理机构-单元测评结果汇总表

序号	测评对象	符合情况	安全控制点				
			岗位设置	人员配置	授权和审批	沟通和合作	审核和检查
1	安全管理机构	符合	6	2	4	4	4
		部分符合	0	1	0	0	0
		不符合	2	0	2	1	1
		不适用	0	0	0	0	0

4.7.2 结果分析

部分符合或不符合情况统计如下：

1、未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。

2、未设立系统管理员、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。

3、除信息科技部和运行保障部外，其他部门未设立部门信息安全人员负责本部门的信息安全管理工作，协同科技部门开展信息安全管理工作。

4、未定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。

5、未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。

6、未制定相关策略对安全措施有效性进行持续监控，应指定相关策略对系统安全措施有效性进行监控。

4.8 人员安全管理

4.8.1 结果汇总

针对不同安全控制点对单个测评对象在人员安全管理层面的单项测评结果进行汇总和统计。

表 4-8 人员安全管理-单元测评结果汇总表

序号	测评对象	符合情况	安全控制点				
			人员录用	人员离岗	人员考核	安全意识教育和培训	外部人员访问管理
1	人员安全管理	符合	5	3	3	5	2
		部分符合	0	0	0	0	0
		不符合	1	0	0	0	1

序号	测评对象	符合情况	安全控制点				
			人员录用	人员离岗	人员考核	安全意识教育和培训	外部人员访问管理
		不适用	0	0	0	0	0

4.8.2 结果分析

部分符合或不符合情况统计如下：

1、未定义关键岗位；存在外部人员承担关键岗位的情况；关键岗位人员未签署岗位安全协议。

2、未要求外部人员访问受控区域前先提出书面申请，访问过程中缺乏专人全程陪同或监督，未进行有效登记。

4.9 系统建设管理

4.9.1 结果汇总

针对不同安全控制点对单个测评对象在系统建设管理层面的单项测评结果进行汇总和统计。

表 4-9 系统建设管理-单元测评结果汇总表

序号	测评对象	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	系统建设管理	符合	4	2	6	4	2	3	2	2	3	2	4
		部分符合	0	1	0	0	0	0	0	1	0	0	0
		不符合	0	1	1	1	2	2	4	3	0	0	0
		不适用	0	1	2	0	4	0	0	0	0	2	0

4.9.2 结果分析

部分符合或不符合情况统计如下：

1、尚未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。

2、尚未提供近期和远期的信息安全建设工作计划。

3、无安全设计规划文档，安全管理策略大面积缺失。

4、未对产品进行选型测试，确定产品的候选范围，且未定期审定和更新候选产品名单。

5、系统中使用的安全产品存在国外产品，不完全符合《信息安全等级保护管理办法》（公通字[2007]43 号）中关于第三级以上信息系统信息安全产品选择的相关规定。

6、未制定代码编写安全规范。

7、未对程序资源库的修改、更新、发布进行授权和批准管理。

8、未制定制度要求外包的服务商定期开展安全风险评估。

9、目前未要求外包服务商提供信息安全风险评估报告。

10、未提供详细的工程实施方案，来明确项目实施过程、方法、项目进度及项目质量管理等内容。

11、未指定或授权专门的部门或人员负责工程实施过程的管理。

12、系统上线前，未对系统进行安全性测试验收。

13、未对测试验收报告进行审定并签字。

14、系统测试验收前未制定测试验收方案进行系统的测试验收。

15、已制定制度规定，在系统正式上线运行前进行试运行，但未明确试运行时间；已制定制度规定测试阶段应包含模拟运行，但未明确模拟运行时间。

16、现有的制度中缺少系统交付的控制方法和人员行为准则进行规定。

17、选定的安全服务商未提供技术培训和服务承诺。

4.10 系统运维管理

4.10.1 结果汇总

针对不同安全控制点对单个测评对象在系统运维管理层面的单项测评结果进行汇总和统计。

表 4-10 系统运维管理-单元测评结果汇总表

序号	测评对象	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	系统运维管理	符合	1	4	13	7	2	7	5	4	5	5	3	6	3
		部分符合	0	0	0	0	0	0	2	1	0	2	1	0	3
		不符合	0	0	2	3	2	1	1	0	0	1	6	1	3
		不适用	9	0	0	0	0	0	0	0	1	0	1	0	0

4.10.2 结果分析

部分符合或不符合情况统计如下：

1、未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。

2、未建立系统备份与恢复策略。

3、未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。

4、未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。

5、未提供重要纸质文档的借阅登记表或申请表。

6、未对需要维修或报废的介质采取敏感信息清除措施，防止敏感信息泄露。

7、目前系统未进行灾备切换演练或无法提供切换演练操作记录。

8、未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。

9、未建立基于申报、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。

10、未建立配套设施、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。

11、未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。

12、经现场查看本系统备份数据未按照规定的周期进行恢复性验证。

13、未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。

14、未建立相关的安全管理规范，对信息处理设备带入机房或办公区域进行严格的审批管理等。

15、未组织相关人员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。

16、未建立安全管理中心，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。

17、未对系统外部连接进行有效管理，存在未经授权和批准的连接。

18、未定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补。

19、仅当软件出现 BUG 时，评估是否对生产运行造成影响，根据需求进行升级，未定期检验网络设备的软件版本。

20、未建立系统设备操作维护手册，并严格按照系统操作维护手册进行操作维护管理。

21、未对通信线路、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。

22、未及时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。

23、未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。

24、未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。

25、未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。

26、系统重大变更前未建立系统变更方案。

27、未提供相应的灾难恢复工作的审计报告。

28、未建立健全的灾难恢复计划。

29、已确定由 XXX 部门负责信息系统的灾难恢复工作，但现场未提供对于灾难恢复工作的审计报告。

30、在安全事件报告和响应处理过程中，未分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训等。

31、未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。

32、未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。

33、未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。

34、每年组织消防演练，但尚未达到每半年一次。

4.11 特殊指标

本次测评未涉及特殊指标。

4.12 单元测评小结

4.12.1 控制点符合情况汇总

根据附录 A 中测评项的符合程度得分，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（参见附件《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。

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 4-11 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	N/A				√
2		物理访问控制	N/A				√
3		防盗窃和防破坏	N/A				√
4		防雷击	N/A				√
5		防火	N/A				√
6		防水和防潮	N/A				√

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
7		防静电	N/A				√
8		温湿度控制	N/A				√
9		电力供应	N/A				√
10		电磁防护	N/A				√
11	网络安全	结构安全	N/A				√
12		访问控制	N/A				√
13		安全审计	N/A				√
14		边界完整性检查	N/A				√
15		入侵防范	N/A				√
16		恶意代码防护	N/A				√
17		网络设备防护	N/A				√
18	主机安全	身份鉴别	3.9		√		
19		访问控制	3.0		√		
20		安全审计	4.8		√		
21		剩余信息保护	0.0			√	
22		入侵防范	3.8		√		
23		恶意代码防范	2.5		√		
24		资源控制	4.3		√		
25	应用安全	身份鉴别	3.6		√		
26		访问控制	3.2		√		
27		安全审计	5.0	√			
28		剩余信息保护	0.0			√	
29		通信完整性	5.0	√			
30		通信保密性	5.0	√			
31		抗抵赖	0.0			√	
32		软件容错	5.0	√			
33		资源控制	1.6		√		
34	数据安全及备份恢复	数据完整性	5.0	√			
35		数据保密性	5.0	√			
36		备份和恢复	5.0	√			
37	安全管理制度	管理制度	4.6		√		
38		制定和发布	5.0	√			
39		评审和修订	5.0	√			
40	安全管理	岗位设置	3.3		√		

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
41	机构	人员配备	4.5		√		
42		授权和审批	4.1		√		
43		沟通和合作	4.2		√		
44		审核和检查	4.2		√		
45	人员安全管理	人员录用	5.0	√			
46		人员离岗	5.0	√			
47		人员考核	5.0	√			
48		安全意识教育和培训	5.0	√			
49		外部人员访问管理	3.6		√		
50	系统建设管理	系统定级	5.0	√			
51		安全方案设计	3.5		√		
52		产品采购和使用	5.0	√			
53		自行软件开发	5.0	√			
54		外包软件开发	-		√		
55		工程实施	4.1		√		
56		测试验收	1.5		√		
57		系统交付	1.5		√		
58		系统备案	5.0	√			
59		等级测评	5.0	√			
60		安全服务商选择	5.0	√			
61	系统运维管理	环境管理	5.0	√			
62		资产管理	5.0	√			
63		介质管理	5.0	√			
64		设备管理	5.0	√			
65		监控管理和安全管理中心	2.5		√		
66		网络安全管理	5.0	√			
67		系统安全管理	4.6		√		
68		恶意代码防范管理	4.8		√		
69		密码管理	5.0	√			
70		变更管理	4.6		√		

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
71		备份与恢复管理	5.0	√			
72		安全事件处置	5.0	√			
73		应急预案管理	2.6		√		

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 4-12 安全问题汇总表

问题编号	安全问题	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
W001	操作系统未采用两种或两种以上组合的鉴别技术。	centos,windows,mysql	主机安全	身份鉴别	f) 宜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，例如以密钥证书、动态口令卡、生物特征等作为身份鉴别信息。	1	5.0
W002	未提供设置敏感标记功能。			访问控制	f) 应对重要信息资源设置敏感标记；	1	5.0

问题编号	安全问题	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
W003	未提供设置敏感标记功能。				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	5.0
W004	未提供专用日志查询分析工具。	windows		安全审计	f)应保护审计记录，避免受到未预期的删除、修改或覆盖等。	0.5	2.5
W005	未采取措施清除剩余信息。	centos,windows		剩余信息保护	a)应保证操作系统和数据库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使用人员前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；	0.5	2.5
W006	剩余信息保护不完				b)应确保系统内的	0.2	1.0

问题编号	安全问题	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
	善。				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使用人员前得到完全清除。		
W007	操作系统未采取完整性保护措施。	centos		入侵防范	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或在检测到完整性即将受到破坏时进行事前阻断；	1	5.0
W008	未安装防病毒软件			恶意代码防范	a)应安装国家安全部门认证的正版防恶意代码软件，对于依附于病毒库进行恶意代	1	5.0

问题编号	安全问题	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
					码查杀的软件应及时更新防恶意代码软件版本和恶意代码库，对于非依赖于病毒库进行恶意代码防御的软件，如主动防御类软件，应保证软件所采用的特征库有效性与实时性，对于某些不能安装相应软件的系统可以采取其他安全防护措施来保证系统不被恶意代码攻击；		
W009	防病毒软件不支持统一管理。	centos,windows			c)应支持防恶意代码的统一管理；	0.5	2.5
W010	未安装防病毒软件				d)应建立病毒监控	-	-

问题编号	安全问题	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
					中心，对网络内计算机感染病毒的情况进行监控。		
W011	未限制终端接入地址。	windows		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；	0.5	1.0
W012	未对系统资源使用进行限制。	centos,windows,mysql			d)应限制单个用户对系统资源的最大或最小使用限度；	0.2	1.0
W013	未采用两种或两种以上的鉴别技术进行身份鉴别	马上贷平台,马上贷平台-2	应用安全	身份鉴别	b)应对同一用户的关键操作采用两种或两种以上组合的鉴别技术实现用户身份鉴别；如使用磁卡、IC 卡、动态密码卡、动态口令设备、手机	1	5.0

问题编号	安全问题	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
					短信动态密码、指纹识别等方式加强鉴别；		
W014	未设置登录超时	马上贷平台			f)应用软件应能在指定的闲置时间间隔到期后，自动锁定客户端的使用；	-	-
W015	未提供设置敏感标记功能。	马上贷平台,马上贷平台-2		访问控制	f)宜具有对重要信息资源设置敏感标记的功能；	1	5.0
W016	未提供设置敏感标记功能。				g)宜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	5.0
W017	未提供用户上次成功登录的信息	马上贷平台-2		安全审计	e)对于从互联网客户端登陆的应用系统，应在每次用户登录时提供用户上	-	-

问题编号	安全问题	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
					一次成功登录的日期、时间、方法、位置等信息，以便用户及时发现可能的问题。		
W018	剩余信息保护机制不完善。	马上贷平台,马上贷平台-2		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；	0.5	2.5
W019	剩余信息保护机制不完善。				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	0.2	1.0

问题编号	安全问题	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
					除。		
W020	未采用数字签名等方式进行接收抗抵赖			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，原发证据包括应用系统操作与管理记录，至少应包括操作时间、操作人员及操作类型、操作内容等记录，交易系统还应能够详细记录用户合规交易数据，如业务流水号、账户名、IP 地址、交易指令等信息以供审计，并能够追溯到用户；	0.5	2.5

问题编号	安全问题	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
W021	未采用数字签名等方式进行接收抗抵赖				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，接受证据应用系统操作与管理记录至少应包括应用系统操作与管理记录，至少应包括操作时间、操作人员及操作类型、操作内容等记录，交易系统还应能够详细记录用户合规交易数据，如业务流水号、账户名、IP 地址、交易指令等信息以供审计，并能	0.5	2.5

问题编号	安全问题	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
					够追溯到用户。		
W022	未提供空闲会话超时机制。	马上贷平台		资源控制	a)对于有会话或短连接的应用系统，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；	0.5	2.5
W023	未限制最大并发会话连接数。				b)应能够对系统的最大并发会话连接数进行限制；	0.2	1.0
W024	未限制一个时间段内的并发会话连接数。	马上贷平台,马上贷平台-2			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；	0.2	1.0
W025	未设置资源分配限额。				e)宜能够对系统占用的资源设定限额，超出限额时给出提示信	0.5	2.5

问题编号	安全问题	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；		
W026	未提供服务优先级设定功能。				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
W027	信息安全管理制度体系不完善。	安全管理制度	安全管理制度	管理制度	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	1.0
W028	安全管理制度格式不规范。			评审和修订	b)应该建立对门户网站内容发布的审核、管理和监控机制；	-	-
W029	各个部门和岗位的职责、分工和技能	安全管理机构	安全管理机构	岗位设置	a)金融机构信息安全管理工作实行统	1	5.0

问题编号	安全问题	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
	要求不完善。				一领导、分级管理，总部统一领导分支机构的信息安全管理，各机构负责本单位和辖内的信息安全管理；		
W030	系统管理员、网络管理员、安全管理员等岗位设置不完善。				h)除科技部门外，其他部门均应指定至少一名部门计算机安全员，具体负责本部门的信息安全管理工作，协同科技部门开展信息安全管理工作。	-	-
W031	岗位设置不完善。			人员配备	c)关键事务岗位应配备多人共同管理。	0.5	1.0
W032	定期审查审批事项制度不完			授权和审批	c)应定期审查审批事项，及	0.2	1.0

问题编号	安全问题	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
	善。				时更新需授权和审批的项目、审批部门和审批人等信息；		
W033	定期审查审批事项制度不完善。				f)应建立系统用户及权限清单，定期对员工权限进行检查核对，发现越权用户要查明原因并及时调整，同时清理过期用户权限，做好记录归档。	-	-
W034	未聘请信息安全专家作为常年的安全顾问。			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
W035	未制定相			审核和检	e)应制定	0.5	2.5

问题编号	安全问题	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
	关策略对安全措施有效性进行持续监控。			查	违反和拒不执行安全管理措施规定的处罚细则。		
W036	关键岗位人员的选拔制度不完善。	人员安全管理	人员安全管理	人员录用	e)对信息安全管理人员应实行备案管理，信息安全管理人员的配备和变更情况，应及时报上一级科技部门备案，金融机构总部信息管理人员在总部科技部门备案；	-	-
W037	外部人员访问受控区域管理不规范。			外部人员访问管理	b)应对允许被外部人员访问的金融机构计算机系统和网络资源建立存取控制机制、认证机制，列明所有用户	0.2	1.0

问题编号	安全问题	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
					名单及其权限，其活动应受到监控；		
W038	安全方案设计不完善。	系统建设管理	系统建设管理	安全方案设计	a)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	2.0
W041	安全方案设计不完善。				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、安全性需求分析、详细设计方案等相关配套文件的合理性和正确性进	0.5	2.5

问题编号	安全问题	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
					行论证和审定，并且经过批准后，才能正式实施；		
W043	产品采购管理不完善。			产品采购和使用	h)应定期对各类信息安全产品产生的日志和报表进行备份存，至少保存 3 个月；	-	-
W046	自行软件开发不完善。			自行软件开发	e)在软件开发过程中，应同步完成相关文档手册的编写工作，保证相关资料的完整性和准确性。	-	-
W048	未要求对外包服务商开展信息安全风险评估。			外包软件开发	f)应要求外包服务商每年至少开展一次信息安全风险评估并提交评估报告，应要求外包服	-	-

问题编号	安全问题	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
					务商聘请外部机构定期对其进行安全审计并提交审计报告，督促其及时整改发现的问题；		
W049	未要求外包服务商提供信息安全风险评估报告。				h)应制定数据中心外包服务应急计划，制订供应商替换方案，以应对外包服务商破产、不可抗力或其它潜在问题导致服务中断或服务水平下降的情形，支持数据中心连续、可靠运行。	-	-
W051	工程实施管理不完善。			工程实施	d)应制定灾难备份系统集成与测试计划并组织	0.2	1.0

问题编号	安全问题	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
					实施。通过技术和业务测试，确认灾难备份系统的功能与性能达到设计指标要求；		
W052	工程实施管理不完善。				e)网络系统的建设、升级、扩充等工程应经过科学的规划、充分的论证和严格的技术审查，有关材料应妥善保存并接受主管部门的检查。	-	-
W053	测试验收不完善。			测试验收	b)应由项目承担单位（部门)或公正的第三方制定安全测试方案，对系统进行安全性测试，出具安全性	0.5	2.5

问题编号	安全问题	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
					测试报告，测试报告报科技部门审查；		
W054	测试验收不完善。				c)在测试验收前应根据设计方案或合同要求等制订测试验收方案，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；	0.2	1.0
W055	测试验收不完善。				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；	0.2	1.0
W056	模拟运行、试运行时间周期不明确。				f)新建应用系统投入生产运行前应进行不少于1个月的模拟运行	-	-

问题编号	安全问题	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
					和不少于3个月的试运行。		
W057	系统交付不完善。			系统交付	b)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；	0.2	1.0
W058	系统交付不完善。				c)系统建设单位应在完成建设任务后将系统建设过程文档和系统运维文档全部移交科技部门；	0.2	1.0
W059	安全服务商选择管理不完善。				d)系统建设单位应对负责系统运行维护的技术人员进行相应的技能培训；	0.5	2.5
W060	安全服务商选择管理不完				f)外部建设单位应与金融机	-	-

问题编号	安全问题	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
	善。				构签署相关知识产权保护协议和保密协议，不得将系统采用的关键安全技术措施和核心安全功能设计对外公开。		
W070	备份恢复手册管理不完善。	系统运维管理	系统运维管理	介质管理	n)应对技术文档实行有效期管理，对于超过有效期的技术文档降低保密级别，对已经失效的技术文档定期清理，并严格执行技术文档管理制度中的销毁和监销规定；	-	-
W071	未建立备份与恢复管理制度。				o)应定期对主要备份业务数据进行恢	-	-

问题编号	安全问题	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
					复验证，根据介质使用期限及时转储数据。		
W074	未对系统运行日志等进行分析。			设备管理	d)制定规范化的故障处理流程，建立详细的故障日志(包括故障发生的时间、范围、现象、处理结果和处理人员等内容)；	-	-
W076	未按照规定的周期进行恢复性验证。				g)新购置的设备应经过测试，测试合格后方能投入使用；	-	-
W077	设备维护管理不完善。				i)需要废止的设备，应由科技部门使用专用工具进行数据信息消除处理，如废止设备不	-	-

问题编号	安全问题	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
					再使用或调配到金融机构以外的单位，应由科技部门对其数据信息存储设备进行消磁或物理粉碎等不可恢复性销毁处理，同时备案；		
W079	未对监控记录进行分析。				b)应建立计算机系统运行监测周报、月报或季报制度，统计分析运行状况；	-	-
W080	未建立安全管理中心。			监控管理和安全管理中心	d)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	5.0

问题编号	安全问题	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
W081	未对系统外部连接进行有效管理。			网络安全管理	h)所有网间互联应用系统和外联网络区应定期进行威胁评估和脆弱性评估并提供威胁和脆弱性评估报告。	-	-
W082	未对系统进行漏洞扫描。			系统安全管理	d)应每半年至少进行一次漏洞扫描，对发现的系统安全漏洞及时进行修补，扫描结果应及时上报；	0.5	0.5
W083	未定期评估网络设备软件版本				e)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	1	1.0

问题编号	安全问题	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
					系统补丁程序的安装，并对系统变更进行记录；		
W086	未对系统进行监控管理。				h)系统用户权限变更应以书面记录，并经相关管理层批准。	-	-
W087	用户防病毒意识不足。			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；	0.2	0.2
W090	变更申报和审批管理不完			变更管理	d)应建立变更控制的申报和	0.2	0.2

问题编号	安全问题	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
	善。				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；		
W091	变更申报和审批管理不完善。				e)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	0.5
W092	变更管理不完善。				h)当生产中心发生变更时，应同步分析灾备系统变更需求并进行相应的变更，评估灾备恢复的有效性；应尽	-	-

问题编号	安全问题	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
					量减少紧急变更。		
W096	灾难恢复计划管理不完善。			备份与恢复管理	d)应每年至少进行一次重要信息系统专项灾备切换演练，每三年至少进行一次重要信息系统全面灾备切换演练，根据不同的应急恢复内容，确定演练的周期，并指定专人管理和维护应急预案，根据人员、信息资源等变动情况以及演练情况适时予以更新和完善，确保应急预案的有效性和灾难发生时的可获取	-	-

问题编号	安全问题	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
					性；		
W097	未按照规定的周期进行恢复性验证。				e)应定期对备份数据的有效性进行检查，每次抽检数据量不低于5%。备份数据要实行异地保存；	-	-
W098	灾难恢复计划管理不完善。				g)灾难恢复的需求应定期进行再分析，再分析周期最长为三年，当生产中心环境、生产系统或业务流程发生重大变更时，单位应立即启动灾难恢复需求再分析工作，依据需求分析制定灾难恢复策略；	-	-
W099	备份恢复				h)应建立	-	-

问题编号	安全问题	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
	手册管理不完善。				健全灾难恢复计划，恢复计划至少要包括灾难恢复范围和目标、灾难切换规程、灾后重续运行操作指引、各系统灾难切换操作手册；		
W100	缺少灾难恢复工作审计。				i) 金融机构应根据信息系统的灾难恢复工作情况，确定审计频率。单位应每年至少组织一次内部灾难恢复工作审计；	-	-
W101	灾难恢复计划管理不完善。				j) 应定期开展灾难恢复培训，并根据实际情况进行灾难恢复演	-	-

问题编号	安全问题	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
					练；		
W102	未建立备份与恢复管理制度。				k)应建立灾难备份系统，主备系统实际切换时间应少于60分钟，灾备系统处理能力应不低于主用系统处理能力的50%，通信线路应分别接入主备系统，有条件时可采用主、备系统处理能力相同、轮换交替使用的双系统模式。	-	-
W103	安全事件报告和响应处理不完善。			安全事件处置	g)应建立有效的技术保障机制，确保在安全事件处置过程中不会因技术能力缺乏而导致处置	-	-

问题编号	安全问题	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
					中断或延长应急处置时间。		
W104	应急预案管理不完善。			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应急组织机构、启动应急预案的条件、应急处理流程、系统恢复流程、事件信息收集、分析、报告制度、事后教育和培训等内容，业务处理系统应急预案的编制工作应由相关业务部门和科技部门共同完成，并由预案涉	1	1.0

问题编号	安全问题	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
					及的相关机构签字盖章；		
W105	未对应急预案进行培训。				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	1.0
W106	未对应急预案进行定期更新和审查。				d)在与第三方合作的业务中，应建立并完善内部责任机制和与相关机构之间的协调机制，制定完整的应急预案及应急协调预案，并定期参加联合演练；	1	5.0
W107	未对应急预案进行定期更新和审查。				e)突发事件应急处置领导小组应统一领导计算机系统的应急管理	-	-

问题编号	安全问题	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
					工作，指挥、决策重大应急处置事宜，并协调应急资源，明确具体应急处置联络人，并将具体联系方式上报本行业信息安全监管部门；		
W108	消防演练频率不满足要求。				h)应定期对原有的应急预案重新评估，并根据安全评估结果，定期修订、演练，并进行专项内部审计；	0.5	2.5
W109	未对应急预案进行培训。				i)应急演练结束后，金融机构应撰写应急演练情况总结报告，总结报告包括但不	-	-

问题编号	安全问题	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
					限于：内容和目的、总体方案、参与人员、准备工作、主要过程和关键时间点记录、存在的问题、后续改进措施及实施计划、演练结论。		

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。

5.1 安全控制间安全测评

主机操作系统存在未安装防恶意代码软件的情况，但主机均采用 Linux 操作系统，一定程度上降低了受到恶意代码攻击的风险，但不能使该控制点完全符合要求。

5.2 层面间安全测评

经分析未发现层面间安全功能的相互补充现象。

5.3 区域间安全测评

经分析未发现区域间安全功能的相互补充现象。

5.4 验证测试

2017 年 8 月 17 日，上海计算机软件技术开发中心的测评人员使用明鉴 Web 应用弱点扫描器在互联网对马上贷平台应用系统进行了安全扫描。应用系统扫描共发现中风险漏洞 2 类 90 个，低风险漏洞 2 类 2 个，未发现高漏洞。扫描报告见附录 A。

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[2]

序号	问题编号[3]	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
1	W008	未安装防病毒软件	1	主机操作系统存在未安装防恶意代码软件的情况，但主机均采用 Linux 操作系统，一定程度上降低了受到恶意代码攻击的风险	0.6	3	2
2	W009	防病毒软件不支持统一管理。	0.5	主机操作系统存在未安装防恶意代码软件的情况，但主机均采用 Linux 操作系统，一定程度上降低了受到恶意代码攻击的风险	0.5	1.25	2.5

[1]问题严重程度值最高为 5。

[2]该处仅列出问题严重程度有所修正的安全问题。

[3]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。

6 总体安全状况分析

6.1 系统安全防护评估

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，并根据 4.12.1 的安全控制点得分，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。

层面得分=$\frac{\sum_{k=1}^{p} \text{测评项 k 的多对象平均分×测评项权重}}{\sum_{k=1}^{p} \text{测评项 k 权重}} \times 20$，p 为该层面下的总测评项数，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。

表 6-1 系统安全防护情况得分表

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	N/A	N/A
2		物理访问控制	N/A	
3		防盗窃和防破坏	N/A	
4		防雷击	N/A	
5		防火	N/A	
6		防水和防潮	N/A	
7		防静电	N/A	
8		温湿度控制	N/A	
9		电力供应	N/A	
10		电磁防护	N/A	
11	网络安全	结构安全	N/A	
12		访问控制	N/A	
13		安全审计	N/A	
14		边界完整性检查	N/A	
15		入侵防范	N/A	
16		恶意代码防护	N/A	
17		网络设备防护	N/A	
18	主机安全	身份鉴别	3.9	71.97
19		访问控制	3.0	

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	4.8	
21		剩余信息保护	0.0	
22		入侵防范	3.8	
23		恶意代码防范	2.5	
24		资源控制	4.3	
25	应用安全	身份鉴别	3.6	67.45
26		访问控制	3.2	
27		安全审计	5.0	
28		剩余信息保护	0.0	
29		通信完整性	5.0	
30		通信保密性	5.0	
31		抗抵赖	0.0	
32		软件容错	5.0	
33		资源控制	1.6	
34	数据安全及备份恢复	数据完整性	5.0	100.00
35		数据保密性	5.0	
36		备份和恢复	5.0	
37	安全管理制度	管理制度	4.6	95.24
38		制定和发布	5.0	
39		评审和修订	5.0	
40	安全管理机构	岗位设置	3.3	79.81
41		人员配备	4.5	
42		授权和审批	4.1	
43		沟通和合作	4.2	
44		审核和检查	4.2	
45	人员安全管理	人员录用	5.0	97.98
46		人员离岗	5.0	
47		人员考核	5.0	
48		安全意识教育和培训	5.0	
49		外部人员访问管理	3.6	
50	系统建设管理	系统定级	5.0	80.27
51		安全方案设计	3.5	
52		产品采购和使用	5.0	
53		自行软件开发	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
54		外包软件开发	-	
55		工程实施	4.1	
56		测试验收	1.5	
57		系统交付	1.5	
58		系统备案	5.0	
59		等级测评	5.0	
60		安全服务商选择	5.0	
61	系统运维管理	环境管理	5.0	86.75
62		资产管理	5.0	
63		介质管理	5.0	
64		设备管理	5.0	
65		监控管理和安全管理中心	2.5	
66		网络安全管理	5.0	
67		系统安全管理	4.6	
68		恶意代码防范管理	4.8	
69		密码管理	5.0	
70		变更管理	4.6	
71		备份与恢复管理	5.0	
72		安全事件处置	5.0	
73		应急预案管理	2.6	

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
W001	主机安全	操作系统未采用两种或两种以上组合的鉴别技术。	centos,windows,mysql	网络攻击、越权或滥用	口令可能被恶意用户猜测获得，合法用户身份被仿冒，导致系统被非授权访问。	中
W002		未提供设置敏感标记功能。		越权或滥用	存在恶意用户通过修改用户权限等方法，非授权访问重要信息资源的可能。	低
W003		未提供设置敏感标记功能。		越权或滥用	存在恶意用户通过修改用户权限等方法，非授权访问重要信息资源的可能。	低
W004		未提供专用日志查询分析工具。	windows	管理不到位	不利于管理员定期分析系统日志信息，从而无法及时发现系统可能	低

[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。

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
					存在的侵害。	
W005		未采取措施清除剩余信息。	centos,windows	泄密	可能导致信息泄漏，重要信息资源被非授权的访问。	低
W006		剩余信息保护不完善。		泄密	操作系统和数据库系统均无法确保信息删除后完全清除。	低
W007		操作系统未采取完整性保护措施。	centos	篡改	无法及时发现系统内重要程序被恶意篡改，可能造成业务中断。	低
W008		未安装防病毒软件		恶意代码	缺乏统一的病毒监控机制将不利于管理员掌握系统内各主机操作系统的病毒防护现状，无法在病毒暴发时采取及时的应对措施。	低

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
W009		防病毒软件不支持统一管理。	centos,windows	恶意代码	存在发生恶意代码在系统内部网络传播的可能性。	低
W010		未安装防病毒软件		恶意代码	缺乏统一的病毒监控机制将不利于管理员掌握系统内各主机操作系统的病毒防护现状，无法在病毒暴发时采取及时的应对措施。	低
W011		未限制终端接入地址。	windows	越权或滥用	恶意用户可使用任意终端，尝试非授权访问服务器。	中
W012		未对系统资源使用进行限制。	centos,windows,mysql	网络攻击、越权或滥用	若单个用户过度占用系统资源，可能导致网络瘫痪、服务器宕机等安全事故。	中
W013	应用安全	未采用两种或两种	马上贷微信端,马上	越权或滥用	可能导致用户身份	低

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
		以上的鉴别技术进行身份鉴别	贷管理后台		信息被冒用，用户口令信息被暴力破解	
W014		未设置登录超时	马上贷微信端	网络攻击	未设置登录超时，可能导致数据信息泄露	低
W015		未提供设置敏感标记功能。	马上贷微信端,马上贷管理后台	越权或滥用	存在恶意用户通过修改用户权限等方法，非授权访问重要信息资源的可能。	低
W016		未提供设置敏感标记功能。		越权或滥用	存在恶意用户通过修改用户权限等方法，非授权访问重要信息资源的可能。	低
W017		未提供用户上次成功登录的信息	马上贷管理后台	泄密,抵赖	合法用户身份被仿冒，导致系统被非授权访问后，用户可能无法及时发现。	低
W018		剩余信息保护机制	马上贷微信端,马上	越权或滥用	由于上述问题，恶意	低

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
		不完善。	贷管理后台		人员可能获取到合法用户的鉴别信息，并利用这些鉴别信息仿冒他人身份访问目标系统，侵害了其他合法用户的利益，影响了信息系统的正常运行。	
W019		剩余信息保护机制不完善。		越权或滥用	由于上述问题，恶意人员可能获取到合法用户的敏感/重要数据，造成敏感/重要数据的泄露，从而侵害了其他合法用户的利益，影响了信息系统的正常运行。	低
W020		未采用数字签名等方式进行接收抗抵		抵赖	存在操作抵赖事件发生的可能性。	低

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
		赖				
W021		未采用数字签名等方式进行接收抗抵赖		抵赖	存在操作抵赖事件发生的可能性。	低
W022		未提供空闲会话超时机制。	马上贷微信端	越权或滥用	存在恶意用户非授权访问系统，造成系统业务信息被非法获取的可能性。	低
W023		未限制最大并发会话连接数。		软硬件故障	可能导致业务高峰期系统资源或网络带宽占用率过高，影响业务稳定运行。	低
W024		未限制一个时间段内的并发会话连接数。	马上贷微信端,马上贷管理后台	软硬件故障	可能导致业务高峰期系统资源或网络带宽占用率过高，影响业务稳定运行。	中
W025		未设置资源分配限额。		软硬件故障	可能导致系统资源或网络带宽占用率过高，影响	中

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
					业务稳定运行。	
W026		未提供服务优先级设定功能。		软硬件故障	存在优先级较低的服务占用过多资源，造成优先级较高的服务资源紧张，无法正常提供服务的可能性，不利于信息系统的正常运行。	中
W027	安全管理制度	信息安全管理制度体系不完善。	安全管理制度	管理不到位	可能导致信息安全管理制度体系存在疏漏，部分管理内容无法有效实施。	低
W028		安全管理制度格式不规范。		管理不到位	可能导致安全管理制度格式不统一，版本混乱，不利于执行落实。	低
W029	安全管理机构	各个部门和岗位的职责、分工和技能要求不完善。	安全管理机构	管理不到位	可能存在部分安全管理职责没有得到有效落实，	中

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
					对组织的信息系统造成风险。	
W030		系统管理员、网络管理员、安全管理员等岗位设置不完善。		管理不到位	专门的岗位、职责未明确，使信息安全管理工作无法正常有序的开展，可能对信息系统的正常运行产生影响。	低
W031		岗位设置不完善。		管理不到位	如可能因缺乏足够的人员配备，导致对信息安全的管理工作不到位。	中
W032		定期审查审批事项制度不完善。		管理不到位	如可能导致审批项目、审批部门以及审批人等发生变化未及时更新从而给组织内的信息系统带来风险。	低
W033		定期审查审批事项制度不完善。		管理不到位	如可能导致审批项目、审批部门以及审	低

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
					批人等发生变化未及时更新从而给组织内的信息系统带来风险。	
W034		未聘请信息安全专家作为常年的安全顾问。		管理不到位	可能存在信息系统安全需求设计、安全规划等过程中，缺乏专业性指导。	低
W035		未制定相关策略对安全措施有效性进行持续监控。		抵赖	无法对保护对象安全措施的有效性进行监控，当安全措施失效时，无法及时对对威胁源进行阻断和干预。	中
W036	人员安全管理	关键岗位人员的选拔制度不完善。	人员安全管理	管理不到位	可能导致关键岗位人员不可靠，安全责任意识不强，未有效履行岗位职责。	低
W037		外部人员访问受控		管理不到位、泄密	可能导致外部人员	低

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
		区域管理不规范。			非授权访问受控区域，缺乏监督，造成泄密。	
W038	系统建设管理	安全方案设计不完善。	系统建设管理	管理不到位	可能导致安全投入缺乏计划性，信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。	低
W041		安全方案设计不完善。		管理不到位	可能导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。	中
W043		产品采购管理不完善。		恶意代码、网络攻击、管理不到位	产品安全性不可控，产品可能存在的安全漏洞被攻击者利用实施攻击行为，影响信息系统正常运行。	低

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
W046		自行软件开发不完善。		管理不到位、无作为或操作失误、越权	可能存在程序资源管理不到位，程序资源遭到非授权访问或覆盖的风险。	低
W048		未要求对外包服务商开展信息安全风险评估。		管理不到位,恶意代码,网络攻击	由于外包服务商提供的服务或其自身存在安全风险，导致该风险被引入到信息系统。	低
W049		未要求外包服务商提供信息安全风险评估报告。		管理不到位	外包商未提供安全风险评估报告，无法保证相关业务的安全性。	低
W051		工程实施管理不完善。		管理不到位、无作为或操作失误	可能由于工程实施方案制定不详细或缺乏工程实施方案造成工程实施过程缺乏计划性或不可控。	低
W052		工程实施		管理不到	可能导致	低

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
		管理不完善。		位、无作为或操作失误	工程实施缺少组织性，工程实施管理不到位。	
W053		测试验收不完善。		管理不到位、无作为或操作失误	安全隐患可能在系统上线运行前未被发现并作出相应处理。	低
W054		测试验收不完善。		管理不到位、无作为或操作失误	未对验收报告信息审定并签字，系统的测试验收管理不到位。	低
W055		测试验收不完善。		管理不到位、无作为或操作失误	可能由于未制定测试验收方案造成测试过程缺乏计划性及操作性，无法保证经过测试验收的系统达到既定的安全性等目标。	低
W056		模拟运行、试运行时间周期不明确。		管理不到位	未明确模拟运行、试运行时间周期，易导	低

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
					致各系统预留时间不足，隐藏问题尚未及时暴露。	
W057		系统交付不完善。		管理不到位	存在交付过程不规范、交付管理不够完善。	低
W058		系统交付不完善。		管理不到位	存在交付过程不规范、交付管理不够完善。	低
W059		安全服务商选择管理不完善。		管理不到位	可能存在由于相关运维人员技能不足、操作不规范或安全服务商提供的服务水平不到位对系统安全稳定运行带来的风险。	中
W060		安全服务商选择管理不完善。		管理不到位	可能存在由于相关运维人员技能不足、操作不规范或安全服务商提供的服务	低

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
					水平不到位对系统安全稳定运行带来的风险。	
W070	系统运维管理	备份恢复手册管理不完善。	系统运维管理	管理不到位、无作为或操作失误	可能导致备份及恢复策略未被有效实施，一旦发生应急情况无法找到或实施数据恢复操作。	低
W071		未建立备份与恢复管理制度。		管理不到位	可能存在重要数据未实施备份或备份不合理的情况。	低
W074		未对系统运行日志等进行分析。		管理不到位	可能存在无法及早发现并处置安全隐患的风险。	低
W076		未按照规定的周期进行恢复性验证。		管理不到位	一旦发生安全事件，无法对备份数据的有效性进行保障，可能造成备份数据恢复失败，影响正常业	低

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
					务运行。	
W077		设备维护管理不完善。		管理不到位、软硬件故障	可能存在信息系统部分设备、线路不可用等风险。	低
W079		未对监控记录进行分析。		管理不到位	可能存在无法及早发现并处置安全隐患的风险。	低
W080		未建立安全管理中心。		管理不到位	无法对保护对象进行统一监视和控制，当安全事件发生时无法及时对威胁源进行阻断和干预。	中
W081		未对系统外部连接进行有效管理。		管理不到位、越权或滥用、泄密	可能存在未经授权的外部连接，直接导致信息系统被非授权访问，甚至发生敏感信息泄露的风险。	低
W082		未对系统进行漏洞扫描。		管理不到位、网络攻击	可能存在未授权人员利用漏洞攻击信	低

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
					息系统的风险。	
W083		未定期评估网络设备软件版本		管理不到位	由于未定期检验、评估设备的软件版本信息，无法及时发现设备软件漏洞，影响系统服务。	低
W086		未对系统进行监控管理。		管理不到位	可能导致无法及时判定事件类型及事件原因，系统应急处理不及时。	低
W087		用户防病毒意识不足。		管理不到位、恶意代码	可能导致信息系统被恶意代码感染，存在信息系统敏感信息泄露的风险。	低
W090		变更申报和审批管理不完善。		管理不到位	可能在变更过程中或变更后出现问题的情况下，存在无法回退的风险。	低
W091		变更申报		管理不到	可能在变	低

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
		和审批管理不完善。		位	更过程中或变更后出现问题的情况下，存在无法回退的风险。	
W092		变更管理不完善。		管理不到位	可能出现变更失败，并且在变更过程中对系统造成软硬件故障或数据丢失等风险。	低
W096		灾难恢复计划管理不完善。		管理不到位	可能发生在不同的灾难场景下，现有的灾难恢复计划无法有效应对的情况，从而发生业务数据丢失等状况，影响系统正常运行，造成损失。	低
W097		未按照规定的周期进行恢复性验证。		管理不到位	一旦发生安全事件，无法对备份数据的有效性进行保障，可	低

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
					能造成备份数据恢复失败，影响正常业务运行。	
W098		灾难恢复计划管理不完善。		管理不到位	可能发生在不同的灾难场景下，现有的灾难恢复计划无法有效应对的情况，从而发生业务数据丢失等状况，影响系统正常运行，造成损失。	低
W099		备份恢复手册管理不完善。		管理不到位、无作为或操作失误	可能导致备份及恢复策略未被有效实施，一旦发生应急情况无法找到或实施数据恢复操作。	低
W100		缺少灾难恢复工作审计。		管理不到位、越权或滥用	未及时进行灾难恢复工作并对其进行审计，可能造成无法了解系统	低

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
					的灾备需求，无法保证系统发生故障时能及时采取有效机制保证业务的正常运行。	
W101		灾难恢复计划管理不完善。		管理不到位	可能发生在不同的灾难场景下，现有的灾难恢复计划无法有效应对的情况，从而发生业务数据丢失等状况，影响系统正常运行，造成损失。	低
W102		未建立备份与恢复管理制度。		管理不到位	可能存在重要数据未实施备份或备份不合理的情况。	低
W103		安全事件报告和响应处理不完善。		管理不到位	存在类似安全事件再次发生的可能性。	低
W104		应急预案管理不完善。		管理不到位	可能导致应急预案设计不完	低

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
					整，执行及管理过程不到位。	
W105		未对应急预案进行培训。		管理不到位	一旦发生安全事件，可能存在系统相关人员尚未了解及掌握适当的应急措施，损失补救时间。	低
W106		未对应急预案进行定期更新和审查。		管理不到位	未及时更新应急预案，导致使用时出现错误或导致无法在规定时间内完成应急工作。	中
W107		未对应急预案进行定期更新和审查。		管理不到位	原先制定的应急预案可能已不符合当前实际情况，导致使用时出现错误或无法在规定时间内完成应急工作。	低
W108		消防演练频率不满		网络攻击、物理攻击	消防演练频率过低，	中

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
		足要求。			无法保证人员对火灾等突发事件处理流程的熟悉度，可能存在发生火情时无法正确有效处理的风险。	
W109		未对应急预案进行培训。		管理不到位	一旦发生安全事件，可能存在系统相关人员尚未了解及掌握适当的应急措施，损失补救时间。	低

6.3 等级能力认定结论

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。

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。	$\frac{\sum_{k=1}^{p} 测评项的多对象平均分 \times 测评项权重}{\sum_{k=1}^{p} 测评项权重} \times 20$，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。	$\left(60 - \frac{\sum_{j=1}^{l} 修正后问题严重程度值}{\sum_{k=1}^{p} 测评项权重} \times 12\right)$，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。

测评结论	判别依据	综合得分
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	80.40 分

7 问题处置建议

1、主机安全

1） 中风险 **操作系统未采用两种或两种以上组合的鉴别技术。**建议使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，如动态口令，USB key 等方式，有效保证身份鉴别的可靠性。

2） 中风险 **未限制终端接入地址。**建议限制可登录服务器的管理终端地址，仅允许特定的地址登录。

3） 中风险 **未对系统资源使用进行限制。**建议限制单个用户对系统资源的最大或最小使用限度。

4） 低风险 **未提供设置敏感标记功能。**建议对系统重要资源增加敏感标记的功能，并控制用户对已标记的敏感信息的操作。

5） 低风险 **操作系统未采取完整性保护措施。**建议安装第三方的完整性保护软件。

6） 低风险 **未安装防病毒软件。**建议部署网络恶意代码防护产品和主机防病毒软件，并通过病毒监控中心对服务器病毒感染情况进行监控。定期更新防病毒软件特征库降低主机感染病毒、木马的风险。

7） 低风险 **防病毒软件不支持统一管理。**建议安装并使用支持统一管理的防恶意代码软件。

8） 低风险 **未采取措施清除剩余信息。**建议采取措施清除剩余信息。

9） 低风险 **未提供专用日志查询分析工具。**建议为系统增加对审计日志统计、查询、分析及生成审计报表的功能。

10） 低风险 **剩余信息保护不完善。**建议在存储空间被释放或重新分配前完全清除系统内的文件、目录和数据库记录。

2、应用安全

1） 中风险 **未设置资源分配限额。**建议根据需要对一个帐户或进程占用的资源进行最大/最小额度限制。

2） 中风险 **未提供服务优先级设定功能。**建议对访问用户或请求进行的优先级进行划分，并根据优先级合理分配系统资源。

3） 中风险 **未限制一个时间段内的并发会话连接数。**建议根据需要对系统允许的一个时间段内（如：业务高峰期）系统最大并发会话数以及一个帐户或进程占用的资源分配阈值进行限制。

4） 低风险 **未采用两种或两种以上的鉴别技术进行身份鉴别。**建议采用两种或两种以上的组合鉴别技术进行身份鉴别。

5） 低风险 **未提供设置敏感标记功能。**建议对系统重要资源增加敏感标记的功能，并控制用户对已标记的敏感信息的操作。

6） 低风险 **剩余信息保护机制不完善。**采取技术措施保证系统重要信息资源存储空间在释放或再分配前完全清除，避免鉴别相关信息直接反映到 URL 地址中。

7） 低风险 **未采用数字签名等方式进行接收抗抵赖。**采用数字签名等方式对用户的重要业务操作进行抗抵赖验证。

8） 低风险 **未提供空闲会话超时机制。**建议根据业务需要对系统空闲回话超时时间进行设置。

9） 低风险 **未限制最大并发会话连接数。**建议根据需要对系统允许统最大并发会话数以及一个帐户或进程占用的资源分配阈值进行限制。

10） 低风险 **剩余信息保护机制不完善。**建议用户退出后及时清除用户产生的文件，或者避免下载地址按顺序增长，或者避免被猜测到。

11） 低风险 **未提供用户上次成功登录的信息。**建议对通过互联网登录的系统，增加上一次用户登录的日志记录，日志记录内容包括登录时间、方法、位置等信息，以便用户查看，并能够及时发现可能存在的安全问题。

12） 低风险 **未设置登录超时。**建议对登录超时进行限制。

3、安全管理

1） 中风险 **各个部门和岗位的职责、分工和技能要求不完善。**建议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。

2） 中风险 **未建立安全管理中心。**建议建立安全管理中心，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。

3） 中风险 **未对应急预案进行定期更新和审查。**建议定期对应急预案进行审查和根据实际情况更新的内容，并按照执行。

4） 中风险 **消防演练频率不满足要求。**建立增加定期消防演练的频率，达到每半年一次。

5） 中风险 **未建立设备维护手册。**建议建立并完善系统设备操作维护手册，系统运行维护人员严格按照系统操作维护手册进行操作，规范系统操作管理。

6） 中风险 **岗位设置不完善。**建议除信息科技部外，其他部门均设立至少一名部门计算机安全员负责本部门的信息安全管理工作，协同科技部门开展信息安全管理工作。

7） 中风险 **未制定相关策略对安全措施有效性进行持续监控。**制定相关策略对系统安全措施有效性进行持续监控。

8） 中风险 **安全方案设计不完善。**建议授权专门的部门对信息系统的安全建设进行总体规划，并制定近远期的安全建设工作计划指导信息系统的安全建设工作。

9） 中风险 **安全服务商选择管理不完善。**建议与安全服务商签订的协议中明确包含技术培训和服务承诺的相关条款，对安全服务商的提供服务水平和技术培训进行约束。

10） 中风险 **介质管理不完善。**完善文档管理制度，对于重要文档的电子文档采用OA 等电子化办公审批平台进行管理，重要纸质文档采用借阅制度。

11） 低风险 **测试验收不完善。**补充在系统验收阶段需委托第三方测试单位对系统进行安全性测试的相关规定，保证今后在系统建设验收阶段委托第三方进行安全测试。

12） 低风险 **安全方案设计不完善。**建议授权专门的部门对信息系统的安全建设进行总体规划，有计划地开展安全建设工作。

13） 低风险 **安全方案设计不完善。**建议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。

14） 低风险 **产品采购管理不完善。**建议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。

15） 低风险 **自行软件开发不完善。**建议补充完善代码编写安全相关规范，并要求开发人员参照规范编写代码，提高软件产品的质量和安全性。

16） 低风险 **自行软件开发不完善。**建议对程序资源库的修改、更新、发布建立授权审批机制，控制程序资源的访问，并尽量采用相关的程序资源管理工具实施权限管理和程序资源的使用。

17） 低风险 **定期审查审批事项制度不完善。**建议定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。

18） 低风险 **未聘请信息安全专家作为常年的安全顾问。**建议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。

19） 低风险 **信息安全管理制度体系不完善。**建议形成由安全策略、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。

20） 低风险 **外部人员访问受控区域管理不规范。**建议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。

21） 低风险 **测试验收不完善。**建议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。

22） 低风险 **测试验收不完善。**建议制定详细的测试验收方案，并对测试结果进行详细的记录，形成测试验收报告。

23） 低风险 **未对资产进行标示管理。**建议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。

24） 低风险 **系统交付不完善。**建议补充完善系统交付相关制度，规范系统交付的控制方法和人员行为准则，并定期对制度的执行情况进行检查，保证制度的有效执行。

25） 低风险 **设备安全管理制度不完善。**建议建立基于申报、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。

26） 低风险 **设备维护管理制度不完善。**建议建立配套设施、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。

27） 低风险 **未定期评估网络设备软件版本。**建议定期对网络设备软件的版本进行检验，并评估其升级的必要性。

28） 低风险 **应急预案管理不完善。**建议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，并对培训结果进行记录。

29） 低风险 **未对应急预案进行培训。**建议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。

30） 低风险 **灾难恢复工作的审计管理不完善。**建议根据信息系统的灾难恢复工作情况，确定审计频率，每年至少应组织一次内部灾难恢复工作审计。

31） 低风险 **未对系统进行漏洞扫描。**建议定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补。

32）低风险 **工程实施管理不完善。**建议补充提供工程实施方案，对项目实施过程、方法、项目进度及项目质量管理等内容进行明确，并根据实际情况对实施过程进行记录，达到控制的目的。

33） 低风险 **未对信息处理设备带入机房或办公区域进行严格的审批管理。**建议建立相关的安全管理规范，对信息处理设备带入机房或办公区域进行严格的审批管理等。

34） 低风险 **用户防病毒意识不足。**建议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。

35） 低风险 **未对恶意代码防护记录进行定期分析处理。**建议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。

36） 低风险 **变更申报和审批管理不完善。**建议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。

37） 低风险 **未对应急预案进行定期更新和审查。**建议定期对应急预案进行审查，根据实际情况更新应急预案内容，并按照执行。

38） 低风险 **未要求对外包服务商开展信息安全风险评估。**建议通过制度，要求外包服务商聘请外部机构定期对其进行风险评估或安全审计并提交报告，督促其及时整改发现的安全问题。

39） 低风险 **未要求外包服务商提供信息安全风险评估报告。**建议要求外包服务商定期提供信息安全风险评估报告。

40） 低风险 **产品采购管理不完善。**建议根据《信息安全等级保护管理办法》（公通字[2007]43 号）中第三级信息系统安全产品选择的相关要求，在对设备性能等进行充分测试后，选择满足业务需要的设备。

41） 低风险 **安全管理制度格式不规范。**建议安全管理制度使用统一的格式，并进行版本控制。

42） 低风险 **系统管理员、网络管理员、安全管理员等岗位设置不完善。**建议设立系统管理员、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。

43） 低风险 **关键岗位人员的选拔制度不完善。**建议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。

44） 低风险 **工程实施管理不完善。**建议指定或授权专门的部门或人员负责工程实施过程的管理。

45） 低风险 **模拟运行、试运行时间周期不明确。**建议完善有关管理制度，新系统投入生产运行前应进行不少于 1 个月的模拟运行和不少于 3 个月的试运行。

46） 低风险 **备份恢复策略管理不完善。**建议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。

47） 低风险 **未建立介质安全管理制度。**建议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。

48） 低风险 **未建立备份与恢复管理制度。**建议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。

49） 低风险 **介质维修和报废管理不完善。**建议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。

50） 低风险 **系统未进行灾备切换演练。**建议定期对系统进行灾备切换演练，保留演练记录。

51） 低风险 **备份恢复手册管理不完善。**建议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。

52） 低风险 **灾难恢复计划管理不完善。**建议建立完善健全的灾难恢复计划，包括灾难恢复范围和目标、灾难切换规程、灾后重续运行操作指引、各系统灾难切换操作手册等。

53） 低风险 **缺少灾难恢复工作审计。**建议完善灾难恢复审计工作，详细记录灾难恢复操作日志，包括重要的灾难恢复操作记录、参数的设置和修改等内容。同时，系统应每年至少组织一次内部灾难恢复工作审计。

54） 低风险 **安全事件报告和响应处理不完善。**建议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。

55） 低风险 **变更管理不完善。**建议系统重大变更前建立变更方案，规范系统重大变更行为。

56） 低风险 **密码使用管理制度不完善。**建议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。

57） 低风险 **未对系统进行监控管理。**建议建立监控管理系统，对系统通信线路、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（可通过短信或邮件形式），形成记录并妥善保存。

58） 低风险 **未对监控记录进行分析。**建议组织相关人员定期（每周、每月等，可根据系统重要程度等确定分析周期）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。

59） 低风险 **未对系统外部连接进行有效管理。**建议完善系统外部连接管理，保证所有与外部系统的连接均得到授权和批准，并对授权和批准过程进行记录和保存。

60） 低风险 **未对系统运行日志等进行分析。**建议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。

61） 低风险 **未按照规定的周期进行恢复性验证。**建议按规定周期对备份数据进行恢复性验证。

62） 低风险 **设备维护管理不完善。**建议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。

附录 A 等级测评结果记录

A.1 物理安全

马上贷平台系统部署于阿里云平台。

A.2 网络安全

马上贷平台系统部署于阿里云平台。

A.3 主机安全

以表格形式给出主机安全的现场测评结果。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）。

测评对象	安全控制点	测评指标	结果记录	符合程度
centos	身份鉴别	a)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；	查看用户列表,用户名具有唯一性	5
		b)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；	通过用户名、口令对登录用户进行身份鉴别	5
		c)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，系统的静态口令应在7位以上并由字母、数字、符号等混合组成并每三个月更换口令；	启用了口令复杂度要求,至少 10 位，包含数字、大小写字母、特殊符号	5
		d)应启用登录失败处理功能，可采	启用登录失败处理功能,失败三次自动断开	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		取结束会话、限制登录间隔、限制非法登录次数和自动退出等措施；		
		e)主机系统应对与之相连的服务器或终端设备进行身份标识和鉴别，当对服务器进行远程管理时，应采取加密措施，防止鉴别信息在网络传输过程中被窃听；	通过 SSH 对服务器进行远程管理,采用加密防止鉴别信息在网络传输的过程中被窃听	5
		f)宜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，例如以密钥证书、动态口令卡、生物特征等作为身份鉴别信息。	未采用组合鉴别方式对登录用户进行身份鉴别	0
	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；	操作系统启用了访问控制功能,依据策略控制用户对系统资源的访问	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；	修改了 root 用户的名称为马上贷平台、新建用户 xyx 用于 app 管理	5
		c)应实现操作系统和数据库系统特权用户的权限分离；	操作系统未安装数据库,该项不适用	不适用
		d)应严格限制默	操作系统修改了 root 账户	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		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；	的默认口令，重命名默认账户 root 为马上贷平台	
		e)应及时删除多余的、过期的帐户，避免共享帐户的存在；	操作系统未见多余、过期的、共享的账户	5
		f)应对重要信息资源设置敏感标记；	操作系统未对重要信息资源设置敏感标记	0
		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。	操作系统未对重要信息资源设置敏感标记	0
	安全审计	a)审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户；	操作系统启用了安全审计功能，审计范围覆盖操作系统上的每个用户	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、账号的分配、创建与变更、审计策略的调整、审计系统功能的关闭与启动等系统内重要的安全相关事件；	审计记录内容仅包括系统事件、用户操作等重要事件进行安全审计	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，并定期备份审计记录，涉及敏感数据的记录保	审计记录的内容包括事件的日期、事件、等级、具体内容等	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		存时间不少于半年；		
		d)应能够根据记录数据进行分析，并生成审计报表；	日志自动汇总到日志服务器 10.252.80.196，通过人工的方式每季度进行日志审计分析，并生成审计记录报表	5
		e)应保护审计进程，避免受到未预期的中断；	审计进程受到保护，避免受到未预期的中断	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。	审计记录保存在服务器本地和日志服务器上，避免受到未预期的删除、修改或覆盖	5
	剩余信息保护	a)应保证操作系统和数据库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使用人员前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；	操作系统未启用剩余信息保护功能	0
		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使用人员前得到完全清除。	操作系统未启用剩余信息保护功能	0
	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	通过阿里云云盾对入侵事件进行检测，记录内容包括事件的类型、攻击者 IP、攻击次数、发现时间、危险等级等内容	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		的目的、攻击的时间，并在发生严重入侵事件时提供报警；		
		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或在检测到完整性即将受到破坏时进行事前阻断；	未对重要程度的完整性进行检测	0
		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、系统软件预防性维护服务等方式保持系统补丁及时得到更新。	操作系统遵循最小安装原则，仅安装业务所需的程序,定期手动方式对操作系统补丁进行更新	5
	恶意代码防范	a)应安装国家安全部门认证的正版防恶意代码软件，对于依附于病毒库进行恶意代码查杀的软件应及时更新防恶意代码软件版本和恶意代码库，对于非依赖于病毒库进行恶意代码防御的软件，如主动防御类软件，应保证软件所采用的特征库有效性与实	操作系统未安装杀毒软件	0

测评对象	安全控制点	测评指标	结果记录	符合程度
		时性，对于某些不能安装相应软件的系统可以采取其他安全防护措施来保证系统不被恶意代码攻击；		
		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；	操作系统未安装杀毒软件	不适用
		c)应支持防恶意代码的统一管理；	操作系统未安装杀毒软件	0
		d)应建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。	未建立病毒监控中心	0
	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；	只允许堡垒机服务器通过内网方式进行远程登录	5
		b)应根据安全策略设置登录终端的操作超时锁定；	堡垒机超时时间为 10 分钟，服务器超时时间为 10 分钟	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；	通过阿里云对服务的运行状态进行监控，监控内容包括服务器的 CPU、内存、磁盘、读写和重要进程等	5
		d)应限制单个用户对系统资源的最大或最小使用限度；	未限制单个用户对系统资源的使用进行限制	0
		e)应能够对系统的服务水平降低到预先规定的最	通过阿里云对服务的运行状态进行监控，当检测到系统的服务水平低于阈值时	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		小值进行检测和报警；	通过短信、邮件进行报警	
		f)所有的服务器应全部专用化，不使用服务器进行收取邮件、浏览互联网操作。	服务器应用专用化	5
windows	身份鉴别	a)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；	查看用户列表,用户名具有唯一性	5
		b)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；	通过用户名、口令对登录用户进行身份鉴别	5
		c)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，系统的静态口令应在7位以上并由字母、数字、符号等混合组成并每三个月更换口令；	通过用户名对用户身份进行标识,开启用户口令复杂度要求，长度至少10位，每90天强制更换口令	5
		d)应启用登录失败处理功能，可采取结束会话、限制登录间隔、限制非法登录次数和自动退出等措施；	启用登录失败处理功能,连续登录失败三次,自动锁定30分钟	5
		e)主机系统应对与之相连的服务器或终端设备进行身份标识和鉴别，当对服务器进	通过 Windows 远程桌面对服务器进行远程管理,采用SSL加密防止鉴别信息在网络传输的过程中被窃听	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		行远程管理时，应采取加密措施，防止鉴别信息在网络传输过程中被窃听；		
		f)宜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，例如以密钥证书、动态口令卡、生物特征等作为身份鉴别信息。	未采用组合鉴别方式对登录用户进行身份鉴别	0
	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；	操作系统启用了访问控制功能，依据策略控制用户对系统资源的访问	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；	操作系统仅启用了管理员马上贷平台账户和 xyx 普通账户，实现管理用户的权限分离	5
		c)应实现操作系统和数据库系统特权用户的权限分离；	操作系统未安装数据库，该项不适用	不适用
		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；	操作系统修改了管理员账户的默认口令，重命名默认账户 administrator 为马上贷平台	5
		e)应及时删除多余的、过期的帐户，避免共享帐户的存在；	操作系统未见多余、过去的账户、共享账户	5
		f)应对重要信息资	操作系统未对重要信息资	0

测评对象	安全控制点	测评指标	结果记录	符合程度
		源设置敏感标记；	源设置敏感标记	
		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。	操作系统未对重要信息资源设置敏感标记	0
	安全审计	a)审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户；	操作系统启用了安全审计功能，审计范围覆盖操作系统上的每个用户	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、账号的分配、创建与变更、审计策略的调整、审计系统功能的关闭与启动等系统内重要的安全相关事件；	审计记录内容开启了审核策略，所有审核内容均为成功、失败	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，并定期备份审计记录，涉及敏感数据的记录保存时间不少于半年；	审计记录的内容包括事件的日期、事件、等级、具体内容等	5
		d)应能够根据记录数据进行分析，并生成审计报表；	采用人工方式对日志进行安全分析，分析结果记录在月报中	5
		e)应保护审计进程，避免受到未预期的中断；	审计进程受到保护，避免受到未预期的中断	5
		f)应保护审计记	审计记录保存在服务器本	0

测评对象	安全控制点	测评指标	结果记录	符合程度
		录，避免受到未预期的删除、修改或覆盖等。	地，无法避免受到未预期的删除、修改或覆盖	
	剩余信息保护	a)应保证操作系统和数据库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使用人员前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；	操作系统未启用剩余信息保护功能	0
		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使用人员前得到完全清除。	操作系统未启用剩余信息保护功能	0
	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；	通过阿里云云盾对入侵事件进行检测，记录内容包括事件的类型、攻击者 IP、攻击次数、发现时间、危险等级等内容	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或在检测到完整性即将受到	操作系统对重要程序的完整性进行检测，检测到破坏后自动恢复	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		破坏时进行事前阻断；		
		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、系统软件预防性维护服务等方式保持系统补丁及时得到更新。	操作系统未遵循最小安装原则，定期通过阿里云监控对操作系统补丁进行更新	5
	恶意代码防范	a)应安装国家安全部门认证的正版防恶意代码软件，对于依附于病毒库进行恶意代码查杀的软件应及时更新防恶意代码软件版本和恶意代码库，对于非依赖于病毒库进行恶意代码防御的软件，如主动防御类软件，应保证软件所采用的特征库有效性与实时性，对于某些不能安装相应软件的系统可以采取其他安全防护措施来保证系统不被恶意代码攻击；	操作系统安装了免费的360防病毒软件	5
		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；	网络层面部署了阿里云盾应用层防火墙，操作系统部署了360防病毒	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		c)应支持防恶意代码的统一管理；	操作系统未安装杀毒软件	0
		d)应建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。	未建立病毒监控中心	0
	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；	通过远程桌面进行远程管理，未限制远程终端接入的网络地址范围	3
		b)应根据安全策略设置登录终端的操作超时锁定；	启用了超时锁定功能，超时10分钟，自动断开	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；	通过阿里云对服务的运行状态进行监控，监控内容包括服务器的CPU、内存、磁盘、读写和重要进程等	5
		d)应限制单个用户对系统资源的最大或最小使用限度；	未限制单个用户对系统资源的使用进行限制	0
		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；	通过阿里云对服务的运行状态进行监控，当检测到系统的服务水平低于阈值时通过短信、邮件进行报警	5
		f)所有的服务器应全部专用化，不使用服务器进行收取邮件、浏览互联网操作。	服务器应用专用化	5
mysql	身份鉴别	a)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	查看数据库用户列表，用户名具有唯一性	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		户名具有唯一性；		
		b)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；	通过用户名、口令对登录用户进行身份鉴别	5
		c)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，系统的静态口令应在7位以上并由字母、数字、符号等混合组成并每三个月更换口令；	数据库启用了口令复杂度要求，要求口令长度至少8位，至少包含大小写字母、数字和特殊符号中的三种	5
		d)应启用登录失败处理功能，可采取结束会话、限制登录间隔、限制非法登录次数和自动退出等措施；	数据库启用登录失败处理功能	5
		e)主机系统应对与之相连的服务器或终端设备进行身份标识和鉴别，当对服务器进行远程管理时，应采取加密措施，防止鉴别信息在网络传输过程中被窃听；	通过阿里云管理平台对数据库进行远程管理，采用HTTPS，通过加密防止鉴别信息在网络传输的过程中被窃听	5
		f)宜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，例如以密钥证书、动态口令卡、生物	未采用组合鉴别方式对登录用户进行身份鉴别	0

测评对象	安全控制点	测评指标	结果记录	符合程度
		特征等作为身份鉴别信息。		
	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；	数据库启用了访问控制功能，依据策略控制用户对数据库资源的访问	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；	依据管理用户的业务需要分配了账户的读写权限，仅授予用户业务所需的最小权限	5
		c)应实现操作系统和数据库系统特权用户的权限分离；	数据库采用阿里 RDS 数据库，采用单独的用户权限进行管理，数据库设置了业务账号和管理账户两类	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；	限制了数据库默认账户的反外挂权限	5
		e)应及时删除多余的、过期的帐户，避免共享帐户的存在；	数据库存在业务类、管理类两个账户，目前只有一个数据库管理员	5
		f)应对重要信息资源设置敏感标记；	数据库未对重要信息资源设置敏感标记	0
		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。	数据库未对重要信息资源设置敏感标记	0
	安全审计	a)审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户；	数据库启用了安全审计功能，审计范围覆盖到数据库上的每个用户	5
		b)审计内容应包	数据库启用了安全审计功	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		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、账号的分配、创建与变更、审计策略的调整、审计系统功能的关闭与启动等系统内重要的安全相关事件；	能，对数据库系统事件、用户登录、用户操作命令进行安全审计	
		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，并定期备份审计记录，涉及敏感数据的记录保存时间不少于半年；	错误日志审计记录内容包括事件的采集时间、日志内容、事件的执行时间、SQL语句、客户端 IP、数据库名等内容	5
		d)应能够根据记录数据进行分析，并生成审计报表；	部署了阿里云数据库审计系统，通过数据库审计系统对记录数据进行分析和生成审计报表	5
		e)应保护审计进程，避免受到未预期的中断；	审计进程受到保护，避免受到未预期的中断	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。	审计记录保存在阿里云平台和数据库审计系统内，避免审计记录受到未预期的删除、修改或覆盖	5
	剩余信息保护	a)应保证操作系统和数据库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使用人员前得到完全清除，	被测对象为操作系统，此项不适用	不适用

测评对象	安全控制点	测评指标	结果记录	符合程度
		无论这些信息是存放在硬盘上还是在内存中；		
		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使用人员前得到完全清除。	被测对象为操作系统，此项不适用	不适用
	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；	被测对象为操作系统，此项不适用	不适用
		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或在检测到完整性即将受到破坏时进行事前阻断；	被测对象为操作系统，此项不适用	不适用
		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、系统软件预防性维护服务等方式保持系统补	被测对象为操作系统，此项不适用	不适用

测评对象	安全控制点	测评指标	结果记录	符合程度
		丁及时得到更新。		
	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；	数据库对终端接入的网络地址范围进行了限制，通过阿里管理平台设置了访问 IP 列表	5
		b)应根据安全策略设置登录终端的操作超时锁定；	数据库启用了终端接入的超时锁定，超时时间为 5 分钟	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；	被测对象为操作系统，此项不适用	不适用
		d)应限制单个用户对系统资源的最大或最小使用限度；	未限制单个用户对系统资源的使用限度	0
		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；	被测对象为操作系统，此项不适用	不适用
		f)所有的服务器应全部专用化，不使用服务器进行收取邮件、浏览互联网操作。	被测对象为操作系统，此项不适用	不适用

A.4 应用安全

以表格形式给出应用安全的现场测评结果。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）。

测评对象	安全控制点	测评指标	结果记录	符合程度

测评对象	安全控制点	测评指标	结果记录	符合程度
马上贷微信端	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；	应用系统前台为手机 APP，通过用户手机号和短信验证码对登录用户进行身份鉴别	5
		b)应对同一用户的关键操作采用两种或两种以上组合的鉴别技术实现用户身份鉴别；如使用磁卡、IC 卡、动态密码卡、动态口令设备、手机短信动态密码、指纹识别等方式加强鉴别；	应用系统前台 APP 未采用组合鉴别技术对用户进行身份鉴别	0
		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；	应用系统前台 APP 通过用户手机号和短信验证码对登录用户进行身份鉴别，用户手机号具有唯一性，手机号码不能更改	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；	应用系统前台 APP 动态验证码连续输入错误十次，锁定账户一天，当天无法再次登录	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；	应用系统启用了身份鉴别、用户身份标识唯一性检查功能，口令采用 6 位数字动态验证码	5
		f)应用软件应能在	系统前台 APP 未设置超时	0

测评对象	安全控制点	测评指标	结果记录	符合程度
		指定的闲置时间间隔到期后，自动锁定客户端的使用；		
		g)对于系统自动分配或者预设的强度较弱的初始密码，系统应强制用户首次登录时修改初始密码；	应用系统前台通过手机号和短信验证码对登录用户进行身份，无初始口令	不适用
		h)修改密码时，不允许新设定的密码与旧密码相同。	通过手机动态验证码进行身份识别,用户名无法修改	不适用
	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；	应用系统前台 APP 仅对注册用户提供服务,无具体权限的划分	不适用
		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；	应用系统前台 APP 针对普通用户开放,无访问控制需求	不适用
		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；	应用系统前台 APP 针对普通用户开放,未设置默认账户	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；	应用系统前台 APP 针对普通用户开放,所有用户均属于用户组,无权限的划分需求	不适用
		e)应有生产系统关键账户与权限的关系表；	所有用户账号统一存在数据库 user 表中	5
		f)宜具有对重要信	应用系统无对重要信息资	0

测评对象	安全控制点	测评指标	结果记录	符合程度
		息资源设置敏感标记的功能；	源设置敏感标记的功能	
		g)宜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。	应用系统无对重要信息资源设置敏感标记的功能	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；	应用系统前台 APP 提供了覆盖到每个用户的安全审计功能，对用户登录事件、对用户操作行为等进行安全审计	5
		b)应保证无法单独中断审计进程，不提供删除、修改或覆盖审计记录的功能；	审计进程无法单独终端，未提供删除、修改或覆盖审计记录的功能	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，并定期备份审计记录，保存时间不少于半年；	审计记录内容包括登录事件的账户、操作人员 IP、浏览器、操作时间等	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；	APP 本身可查询业务操作记录、上次登录日期。其余日志均保存在后台数据库中，通过数据库审计系统进行安全审计，并生成审计报表	5
		e)对于从互联网客户端登陆的应用系统，应在每次用户登录时提供用户上一次成功登录的日期、时间、方法、位置等	每次用户登录时，可查询上一次成功登录的日期、时间、方法、位置等信息的功能	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		信息，以便用户及时发现可能的问题。		
	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；	应用系统未提供剩余信息保护功能	0
		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。	应用系统未提供剩余信息保护功能	0
	通信完整性	a)应采用密码技术保证通信过程中关键数据的完整性。	APP 端数据通过 https 加密后传输到后台服务器	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；	应用系统 APP 通过用户和口令进行会话初始化验证	5
		b)对于通过互联网对外提供服务的系统，在通信过程中的整个报文或会话过程，应通过专用的通信协议或加密的方式保证通信过程的机密性进行加密。	APP 通过 https 方式进行加密传输，通过排序、加签后进行数据传输	5
	抗抵赖	a)应具有在请求的	应用系统未提供抗抵赖功	0

测评对象	安全控制点	测评指标	结果记录	符合程度
		情况下为数据原发者或接收者提供数据原发证据的功能，原发证据包括应用系统操作与管理记录，至少应包括操作时间、操作人员及操作类型、操作内容等记录，交易系统还应能够详细记录用户合规交易数据，如业务流水号、账户名、IP 地址、交易指令等信息以供审计，并能够追溯到用户；	能	
		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，接受证据应用系统操作与管理记录至少应包括应用系统操作与管理记录，至少应包括操作时间、操作人员及操作类型、操作内容等记录，交易系统还应能够详细记录用户合规交易数据，如业务流水号、账户名、IP 地址、交易指令等信息以供审计，并能够追溯到用户。	应用系统未提供抗抵赖功能	0

测评对象	安全控制点	测评指标	结果记录	符合程度
	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；	应用系统提供了数据有效性校验功能，对用户输入数据的格式、长度进行校验	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；	通过自动轮循机制进行检查，故障发生时，对于未生成记录的操作，会自动回滚到初始状态，对于已生成记录的操作，会通过轮循机制自动补单	5
		c)应能够有效屏蔽系统技术错误信息，不将系统产生的错误信息直接反馈给客户。	应用系统前台 APP 定制专门的报错页面，将系统产生的错误信息直接反馈给客户	5
	资源控制	a)对于有会话或短连接的应用系统，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；	应用系统前台 APP 未提供会话限制超时	0
		b)应能够对系统的最大并发会话连接数进行限制；	应用系统未对系统的最大并发会话数进行限制	0
		c)对于有会话的应用系统，应能够对单个帐户的多重并发会话进行限制；	应用系统前台 APP 对单个账号的多重并发会话进行了限制	5
		d)应能够对一个时间段内可能的并发会话连接数	应用系统未对一个时间段内可能的并发会话连接数进行限制	0

测评对象	安全控制点	测评指标	结果记录	符合程度
		进行限制；		
		e)宜能够对系统占用的资源设定限额，超出限额时给出提示信息；	应用系统未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进行限制	0
		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；	应用系统通过阿里云监控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的功能	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。	应用系统未提供服务优先级设定功能	0
马上贷管理后台	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；	应用系统管理后台通过用户名、口令和验证码对登录用户进行身份鉴别	5
		b)应对同一用户的关键操作采用两种或两种以上组合的鉴别技术实现用户身份鉴别；如使用磁卡、IC 卡、动态密码卡、动态口令设备、手机短信动态密码、指纹识别等方式加强鉴别；	后台未采用组合鉴别技术对用户进行身份鉴别	0
		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	应用系统后台启用了口令复杂度要求，要求口令长度至少为 8 位，至少包括字母和数字两种，不满足要求会进行弱口令提示	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		份鉴别信息不易被冒用；		
		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；	系统后台开启登录失败处理功能，连续登录失败十次，当天无法登录	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；	应用系统启用了身份鉴别、用户身份标识唯一性检查、口令复杂度、登录失败等功能	5
		f)应用软件应能在指定的闲置时间间隔到期后，自动锁定客户端的使用；	应用系统后台开启了超时锁定，超过 15 分钟自动锁定	5
		g)对于系统自动分配或者预设的强度较弱的初始密码，系统应强制用户首次登录时修改初始密码；	应用系统管理后台无自动分配或预设的用户口令，该项不适用	不适用
		h)修改密码时，不允许新设定的密码与旧密码相同。	修改密码时要求不允许新设定的密码与旧密码相同	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；	应用系统管理后台分为业务权限、管理权限等，分别提供了访问控制功能，依据策略控制用户对系统模块的访问	5
		b)访问控制的覆盖范围应包括与资源访问相关的	访问控制的覆盖范围包括系统用户角色和系统模块间的操作	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		主体、客体及它们之间的操作；		
		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；	应用系统后台由应用管理员配置访问控制策略，应用管理员账户名为姓名的全拼	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；	应用系统授予各个业务相关部门人员业务所需的最小权限，设立了管理员、业务人员等不同角色	5
		e)应有生产系统关键账户与权限的关系表；	形成了生产系统关键账户与权限的关系表	5
		f)宜具有对重要信息资源设置敏感标记的功能；	应用系统无对重要信息资源设置敏感标记的功能	0
		g)宜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。	应用系统无对重要信息资源设置敏感标记的功能	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；	应用系统提供了覆盖到每个用户的安全审计功能，对用户登录事件、用户操作、权限配置等重要事件进行审计	5
		b)应保证无法单独中断审计进程，不提供删除、修改或覆盖审计记录的功能；	审计进程无法单独终端，未提供删除、修改或覆盖审计记录的功能	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，并	审计记录内容包括登录事件的账户、操作人员 IP、浏览器、操作时间等	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		定期备份审计记录，保存时间不少于半年；		
		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；	提供了审计记录查询功能，审计记录保存在数据库中，通过数据库审计系统进行日志的统计、查询、分析及生成审计报表	5
		e)对于从互联网客户端登陆的应用系统，应在每次用户登录时提供用户上一次成功登录的日期、时间、方法、位置等信息，以便用户及时发现可能的问题。	未提供在每次用户登录时提供用户上一次成功登录的日期、时间、方法、位置等信息的功能	0
	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；	应用系统未提供剩余信息保护功能	0
		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。	应用系统未提供剩余信息保护功能	0
	通信完整性	a)应采用密码技术保证通信过程中关键数据的完整性。	应用系统后台通过 https 方式进行数据传输	5

测评对象	安全控制点	测评指标	结果记录	符合程度
	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；	应用系统利用 HTTPS 方式进行数据传输，通过密码技术进行会话初始化验证	5
		b)对于通过互联网对外提供服务的系统，在通信过程中的整个报文或会话过程，应通过专用的通信协议或加密的方式保证通信过程的机密性进行加密。	应用系统后台通过 https 方式进行数据传输	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，原发证据包括应用系统操作与管理记录，至少应包括操作时间、操作人员及操作类型、操作内容等记录，交易系统还应能够详细记录用户合规交易数据，如业务流水号、账户名、IP 地址、交易指令等信息以供审计，并能够追溯到用户；	应用系统未提供抗抵赖功能	0
		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，接受证	应用系统未提供抗抵赖功能	0

测评对象	安全控制点	测评指标	结果记录	符合程度
		据应用系统操作与管理记录至少应包括应用系统操作与管理记录，至少应包括操作时间、操作人员及操作类型、操作内容等记录，交易系统还应能够详细记录用户合规交易数据，如业务流水号、账户名、IP地址、交易指令等信息以供审计，并能够追溯到用户。		
	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；	应用系统提供了数据有效性校验功能，对用户输入数据的格式、长度进行校验	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；	应用系统部署了冗余的应用服务器进行负载均衡，每周 3 次对业务数据进行备份，确保在系统部分故障时能够进行恢复	5
		c)应能够有效屏蔽系统技术错误信息，不将系统产生的错误信息直接反馈给客户。	定制专门的报错页面，将系统产生的错误信息直接反馈给客户	5
	资源控制	a)对于有会话或短连接的应用系统，当应用系统的通信双方中的一方	应用系统管理后台超时 15 分钟，自动断开	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		在一段时间内未作任何响应，另一方应能够自动结束会话；		
		b)应能够对系统的最大并发会话连接数进行限制；	应用系统管理后台限制最大并发连接数未为300	5
		c)对于有会话的应用系统，应能够对单个帐户的多重并发会话进行限制；	应用系统管理后台限制单个账户的多重并发	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；	应用系统未对一个时间段内可能的并发会话连接数进行限制	0
		e)宜能够对系统占用的资源设定限额，超出限额时给出提示信息；	应用系统未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进行限制	0
		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；	应用系统通过阿里云负载均衡监听的方式应用系统的端口开放情况、服务响应情况进行监控，并通过手机短信的方式进行报警	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。	应用系统未提供服务优先级设定功能	0

A.5 数据安全及备份恢复

以表格形式给出数据安全及备份恢复的现场测评结果。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）。

测评对象	安全控制点	测评指标	结果记录	符合程度
数据安全及备份恢复	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采集、传输、使用和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。	"通过 AES 加密算法对用户身份证号、银行卡号、手机号等重要数据的存储完整性进行校验，通过 MD5 加盐对后台管理用户鉴别信息的存储完整性进行校验，但未对其他用户业务数据和管理数据进行校验	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采集、传输、使用和存储过程的保密性。	通过 AES 加密算法实现用户身份证号、银行卡号等重要数据的存储加密，通过 MD5 加盐实现后台管理用户鉴别信息的存储加密；应用系统前台和后台均通过 https 方式进行数据传输	5
	备份和恢复	a)应提供本地数据备份与恢复功能，采取实时备份与异步备份或增量备份与完全备份的方式，增量数据备份每天一次，完全数据备份每周一次，备份介质场外存放，数据保存期限依照国家相关规定；	通过阿里云实现数据备份和恢复功能，每天进行一次完全备份，备份数据保存一周	5
		b)应提供异地数据备份功能，利用通信网络将关键	备份数据保存在阿里云，该项不适用	不适用

测评对象	安全控制点	测评指标	结果记录	符合程度
		数据定时批量传送至备用场地；		
		c)对于同城数据备份中心，应与生产中心直线距离至少达到 30 公里，可以接管所有核心业务的运行；对于异地数据备份中心，应与生产中心直线距离至少达到 100 公里；	备份数据保存在阿里云，该项不适用	不适用
		d)为满足灾难恢复策略的要求，应对技术方案中关键技术应用的可行性进行验证测试，并记录和保存验证测试的结果；	每天进行全量备份，并不定期开展恢复测试	5
		e)数据备份存放方式应以多冗余方式，完全数据备份至少保证以一个星期为周期的数据冗余；	通过阿里云实现数据备份和恢复功能，每天对业务数据进行全量备份，备份数据保存一周	5
		f)异地备份中心应配备恢复所需的运行环境，并处于就绪状态或运行状态，"就绪状态"指备份中心的所需资源(相关软硬件以及数据等资源)已完全满足但设备 cpu 还没有运行；"运行状态"指备份中心除所需	备份数据保存在阿里云，该项不适用	不适用

测评对象	安全控制点	测评指标	结果记录	符合程度
		资源完全满足要求外，cpu 也在运行状态。		

A.6 安全管理制度

以表格形式给出安全管理制度的现场测评结果。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）。

测评对象	安全控制点	测评指标	结果记录	符合程度
安全管理制度	管理制度	a)应制定信息安全工作的总体方针和安全策略，说明安全工作的总体目标、范围、原则和安全框架等，并编制形成信息安全方针制度文件；	已建立了《信息安全管理制度 V1.0》，明确了信息安全工作的总体方针和策略，内容包括了信息安全的目标、范围、原则、框架等	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；	已建立了《信息安全管理制度 V1.0》，内容覆盖了制度管理、机构管理、人员管理、系统建设管理和运维管理等方面的各类安全管理活动	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；	已建立了《信息安全管理制度 V1.0》，对重要管理操作建立规程	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。	已建立了《信息安全管理制度 V1.0》，制度体系包括了安全政策、管理制度、部分文档记录模板等，未提供部分操作规程和记录文档，信息安全管理体系未达到全面的程度	4
	制定和发布	a)由金融机构总部	明确要求由研发部负责制	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		科技部门负责制定适用全机构范围的安全管理制度，各分支机构的科技部门负责制定适用辖内的安全管理制度；	定适用全机构范围的安全管理制度	
		b)安全管理制度应具有统一的格式，并进行版本控制；	《信息安全管理制度V1.0》中对文档发布规范制度作出了规定：统一文档版本、格式等，并定期按照制度对文档进行更新，以保证所有文档的时效性	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；	《信息安全管理制度V1.0》中明确了信息安全工作小组对体系文件每年进行一次评审，有具体评审流程	5
		d)安全管理制度应通过正式、有效的方式发布；	已建立了《信息安全管理制度V1.0》，明确了文件审批与发布管理制度的流程，规定了安全管理制度的制定、发布程序和发布范围等各项要求	5
		e)安全管理制度应注明发布范围，并对收发文进行登记。	已建立了《信息安全管理制度V1.0》，明确了文件审批与发布管理制度的流程，规定了安全管理制度的制定、发布程序和发布范围等各项要求	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；	《信息安全管理制度V1.0》中明确每年检查一次文件的适用情况，并对现有文件的有效性进行评审。对不合适的地方进行修订，必要时更换新版	5
		b)应该建立对门	未建立对门户网站内容发	0

测评对象	安全控制点	测评指标	结果记录	符合程度
		户网站内容发布的审核、管理和监控机制；	布的审核、管理和监控机制	
		c)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。	《信息安全管理制度 V1.0》中明确了信息安全工作小组对体系文件每年进行一次评审，对不合适的地方进行修订，必要时更换新版	5

A.7 安全管理机构

以表格形式给出安全管理机构的现场测评结果。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）。

测评对象	安全控制点	测评指标	结果记录	符合程度
安全管理机构	岗位设置	a)金融机构信息安全管理工作实行统一领导、分级管理，总部统一领导分支机构的信息安全管理，各机构负责本单位和辖内的信息安全管理；	未要求信息安全管理工作实行统一领导、分级管理的工作机制	0
		b)应设立由本机构领导、业务与技术相关部门主要负责人组成的信息安全领导小组，负责协调本机构及辖内信息安全管理工作，决策本机构及辖内信息安全重大事宜；	建立了信息安全领导小组，信息安全领导小组是信息安全的领导部门，全面负责本单位的信息安全的领导和决策工作，信息安全领导小组由最高管理者负责	5
		c)应设立专门的信	已设立了安全审计员岗位，	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		息科技风险审计岗位，负责信息科技审计制度和流程的实施，制订和执行信息科技审计计划，对信息科技整个生命周期和重大事件等进行审计；	负责审计计划的制定和审计的执行等工作	
		d)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；	已成立了信息安全管理小组，在《信息安全组织机构制度》中明确了信息安管理小组的职责，设立了机房管理员、主机管理员、网络管理员、应用系统管理员、安全管理员等岗位，在《信息安全组织机构制度》中明确了各个工作岗位的职责和分工	5
		e)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；	已设立了机房管理员、主机管理员、网络管理员、应用系统管理员、安全管理员等岗位，并在《信息安全组织机构制度》中明确了各岗位的职责、分工	5
		f)金融机构的主要负责人为本单位计算机信息系统安全保护工作的第一责任人。金融机构的计算机信息系统安全保护领导小组、专职部门和专(兼)职安全管理人员以及其他有关人员应当协助第一责任人	建立了信息安全领导小组，信息安全领导小组是信息安全的领导部门，全面负责本单位的信息安全的领导和决策工作，信息安全领导小组由最高管理者负责	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		组织落实有关规定;		
		g)应坚持三分离原则，实现前后台分离、开发与操作分离、技术与业务分离，信息技术人员任职要专岗专责，不得由业务人员兼任，也不得兼任业务职务；	《信息安全组织机构》中明确了信息科技岗位的设立应坚持三分离原则，实现前后台分离、开发与操作分离、技术与业务分离，信息技术人员任职要专岗专责，不得由业务人员兼任，也不得兼任业务职务	5
		h)除科技部门外，其他部门均应指定至少一名部门计算机安全员，具体负责本部门的信息安全管理工作，协同科技部门开展信息安全管理工作。	未要求除科技部门外，其他部门均应指定至少一名部门计算机安全员	0
	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；	在《信息安全组织机构制度》中明确需配备了一定数量的机房管理员、主机管理员、网络管理员、应用管理员、安全管理员等	5
		b)应配备专职安全管理人员，实行A、B 岗制度，不可兼任；	在《信息安全组织机构制度》要求安全管理员不可兼任其他岗位	5
		c)关键事务岗位应配备多人共同管理。	已设立了机房管理员、主机管理员、网络管理员、应用系统管理员、安全管理员等岗位，并在《信息安全组织机构制度》中明确了机构内各部门和各负责人的职责，但未配备多人共同管理	3
	授权和审批	a)应根据各个部门	《信息安全组织机构制度》	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		和岗位的职责明确授权审批事项、审批部门和批准人等；	的“(三) 关键活动的授权和审批”中明确了各项审批事项的审批部门和审批人等	
		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；	《信息安全组织机构制度》中明确了在机房基础设施变更、重要操作、物理访问等的进行逐级审批	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；	未定期审查审批事项	0
		d)应记录审批过程并保存审批文档；	提供《系统配置变更审批单》包含申请人、日期、部门、变更描述、变更类型、维护单位意见和签字、公司意见和签字等	5
		e)用户应被授予完成所承担任务所需的最小权限，重要岗位的员工之间应形成相互制约的关系。权限变更应执行相关审批流程，并有完整的变更记录；	《信息安全组织机构制度》中规定了用户应被授予完成所承担任务所需的最小权限，重要岗位的员工之间应形成相互制约的关系	5
		f)应建立系统用户及权限清单，定期对员工权限进行检查核对，发现越权用户要查明原因并及时调整，同	未提供系统用户权限清单，未定期对员工权限进行检查核对	0

测评对象	安全控制点	测评指标	结果记录	符合程度
		时清理过期用户权限，做好记录归档。		
	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，并形成会议纪要；	已建立了《沟通与合作管理制度》，规定了中各类管理人员之间、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	5
		b)应加强与兄弟单位、公安机关、电信公司的合作与沟通；	已建立了《沟通与合作管理制度》，规定了加强与兄弟单位、公安机关、电信公司的合作与沟通	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；	已建立了《沟通与合作管理制度》，规定了加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通	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；	提供了外联单位联系列表，包括外链为名称、内容和联系方式等	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。	未聘请信息安全专家作为常年的安全顾问	0
	审核和检查	a)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，按	《信息安全组织机构制度》(四) “审核和检查”中明确要求组织专门人员(或委托外部公司)每季度进行安	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		要求定期开展安全审核和安全检查活动；	全检查，包括网络、安全设备、系统等各方面的安全检查。记录检查结果。规范安全检查的内容并统一分析检查结果	
		b)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；	安全管理员负责日常的安全检查，检查内容包括系统日常运行情况、数据备份情况等内容	5
		c)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；	《信息安全组织机构制度》(四) “审核和检查”中明确要求组织专门人员（或委托外部公司）每季度进行安全检查，包括网络、安全设备、系统等各方面的安全检查。记录检查结果。规范安全检查的内容并统一分析检查结果	5
		d)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，要求限期整改的需要对相关整改情况进行后续跟踪，并将每次安全检查报告和整改落实情况整理汇总后，报上一级机构科技部门备案；	《信息安全组织机构制度》(四) “审核和检查”中明确要求组织专门人员（或委托外部公司）每季度进行安全检查，包括网络、安全设备、系统等各方面的安全检查。记录检查结果。规范安全检查的内容并统一分析检查结果	5
		e)应制定违反和拒不执行安全管理措施规定的处	未制定违反和拒不执行安全管理措施规定的处罚细则	0

测评对象	安全控制点	测评指标	结果记录	符合程度
		罚细则。		

A.8 人员安全管理

以表格形式给出人员安全管理的现场测评结果。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）。

测评对象	安全控制点	测评指标	结果记录	符合程度
人员安全管理	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；	已授权人力资源部负责人员录用工作	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；	已建立了《人员信息安全管理制度》，要求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	5
		c)应与员工签署保密协议；	员工入职需要签订《保密协议》，协议中有保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等内容	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；	《人员信息安全管理制度》中规定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	5
		e)对信息安全管理人员应实行备案管理，信息安全管理人员的配备和变更情况，应及时报上一级科技部门备案，金融机构总部信息管理人员在总部科技	未要求信息安全管理人员应实行备案管理，信息安全管理人员的配备和变更情况，应及时报上一级科技部门备案，金融机构总部信息管理人员在总部科技部门备案，未提供备案记录	0

测评对象	安全控制点	测评指标	结果记录	符合程度
		部门备案；		
		f)凡是因违反国家法律法规和金融机构有关规定受到过处罚或处分的人员，不得从事信息安全管理工作。	《人员信息安全管理制度》规定: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;凡是因违反国家法律法规和金融机构有关规定受到过处罚或处分的人员,不得从事信息安全管理工作	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；	《人员离职和转岗的安全管理规定》中规定：各部门在人员任用终止时,应按照离岗手续,通知相关部门对该人员使用信息和信息系统的权限进行调整	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；	《人员离职和转岗的安全管理规定》中规定? 离岗人员在离岗时归还其使用的组织资产,包括所有先前发放的软件、访问卡、文件和设备等。相关部门应与离岗人员进行离岗交接,并做好记录	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，并保证离岗人员负责的信息技术系统的口令必须立即更换。	所有人员离岗时,均须承诺调离后的保密义务后方可离开	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	《人员信息安全管理制度》中对人员考核做出了规定，要求定期对各个岗位的人	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		知的考核；	员进行安全技能及安全认知的考核	
		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；	《人员信息安全管理制度》中对人员考核做出了规定，对关键岗位的人员进行全面、严格的安全审查和技能考核	5
		c)应对考核结果进行记录并保存。	《人员信息安全管理制度》要求对考核结果进行记录并保存	5
	安全意识教育和培训	a)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；	《人员信息安全管理制度》要求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	5
		b)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，普及信息安全基础知识、规范岗位操作、提高安全技能；	《人员信息安全管理制度》中明确要求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	5
		c)每年至少对信息安全管理人员进行一次信息安全培训；	《人员信息安全管理制度》中明确要求：每年至少对信息安全管理人员进行一次信息安全培训，对安全教育和培训的情况和结果进行记录并归档保存	5
		d)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；	在管理制度中对安全责任和惩戒措施进行书面规定	5
		e)应对安全教育	《人员信息安全管理制度》	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		和培训的情况和结果进行记录并归档保存。	要求对对安全教育和培训的情况和结果进行记录并归档保存	
	外部人员访问管理	a)各机构指定责任部门负责非涉密计算机系统和网络相关的外部人员访问授权审批，批准后由专人全程陪同或监督，并登记备案；	《机房安全管理制度》规定:研发部负责非涉密计算机系统和网络相关的外部人员访问授权审批	5
		b)应对允许被外部人员访问的金融机构计算机系统和网络资源建立存取控制机制、认证机制，列明所有用户名单及其权限，其活动应受到监控；	未对允许被外部人员访问的金融机构计算机系统和网络资源建立存取控制机制、认证机制，未列明所有用户名单及其权限,未进行监控	0
		c)获得外部人员访问授权的所有单位和个人应与金融机构签订安全保密协议，不得进行未授权的增加、删除、修改、查询数据操作，不得复制和泄漏金融机构的任何信息。	《机房安全管理制度》规定:获得外部人员访问授权的所有单位和个人应与金融机构签订安全保密协议，不得进行未授权的增加、删除、修改、查询数据操作，不得复制和泄漏金融机构的任何信息	5

A.9 系统建设管理

以表格形式给出系统建设管理的现场测评结果。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）。

测评对象	安全控制点	测评指标	结果记录	符合程度
系统建设管理	系统定级	a)应明确信息系统的边界和安全保护等级；	《信息系统安全等级保护定级报告》明确了信息系统安全保护等级为 S3A3G3，并对系统边界进行了描述	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；	《信息系统安全等级保护定级报告》明确了信息系统的安全保护等级确定的方法和理由	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；	被测系统的定级结果经过了主管部门的合理性和正确性的论证和审定	5
		d)应确保信息系统的定级结果经过相关部门的批准。	信息系统的定级结果经过主管部门的批准	5
	安全方案设计	a)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；	已建立了《信息系统建设安全管理制度》，文档中对系统总体规划设计作出了规定，但未提供具体的系统建设和整改方案	3
		b)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；	提供近期和远期的安全建设工作计划	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	《系统建设安全管理制度》中规定根据信息系统的等级划分情况，建立总体安全策略、安全技术框架、安全管理策略、总体建设规划和	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		框架、安全管理策略、总体建设规划、安全性需求分析、和详细设计方案，并形成配套文件；	详细设计方案等配套系列文件	
		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、安全性需求分析、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；	未提供对配套文件的合理性和正确性进行论证和审定的记录	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、安全性需求分析、详细设计方案等相关配套文件。	被测系统首次进行等级保护测评	不适用
	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。	《系统建设安全管理制度》中对设备选型进行了规定：应确保产品采购和使用符合国家信息安全的有关规定	5
		b)应确保密码产品采购和使用符	《系统建设安全管理制度》中对设备选型进行了规定：	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		合国家密码主管部门的要求。	严禁使用未经国家密码管理部门批准和未通过国家信息安全质量认证的密码设备	
		c)应指定或授权专门的部门负责产品的采购，设备采购应坚持公开、公平、公正的原则，宜采用招标、邀标等形式完成；	《系统建设安全管理制度》，授权研发部按照单位的预算制度和审批流程购买及管理	5
		d)各机构购置扫描、检测类信息安全产品应报本机构科技主管部门批准、备案；	未购置购置扫描、检测类信息安全产品	不适用
		e)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。	《系统建设安全管理制度》中规定：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；设备符合系统选型要求并获得批准后，方可购置	5
		f)扫描、检测类信息安全产品仅限于本机构信息安全管理人员或经主管领导授权的网络管理员使用；	未购置购置扫描、检测类信息安全产品	不适用
		g)应定期查看各类信息安全产品相关日志和报表信息并汇总分析，若发现重大问题，立即采取控制措施并按规定程序报告；	由信息技术部负责定期查看各类信息安全产品相关日志和报表信息	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		h)应定期对各类信息安全产品产生的日志和报表进行备份存，至少保存 3 个月；	未定期对各类信息安全产品产生的日志和报表进行备份存档	0
		i)应及时升级维护信息安全产品，凡超过使用期限的或不能继续使用的信息安全产品，要按照固定资产报废审批程序处理。	使用防病毒软件等安全产品，升级病毒库，未有超过使用期限的或不能继续使用的信息安全产品	5
	自行软件开发	a)应制定软件开发管理制度和代码编写安全规范，明确说明开发过程的控制方法和人员行为准则，要求开发人员参照规范编写代码，不得在程序中设置后门或恶意代码程序；	《系统建设安全管理制度》中明确说明开发过程的控制方法和人员行为准则	5
		b)应确保开发环境与实际运行环境物理分开，应确保开发人员和测试人员分离，开发人员不能兼任系统管理员或业务操作人员，确保测试数据和测试结果受到控制；	《系统建设安全管理制度》其中要求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	5
		c)应确保提供软件设计的相关文档和使用指南，并由	《系统建设安全管理制度》中规定：确保提供软件设计的相关文档和使用指南，并	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		专人负责保管。	妥善保管	
		d)应确保对程序资源库的修改、更新、发布进行授权和批准。	《系统建设安全管理制度》中规定:确保对程序资源库的修改、更新、发布进行授权和批准	5
		e)在软件开发过程中，应同步完成相关文档手册的编写工作，保证相关资料的完整性和准确性。	未在软件开发过程中形成相关的手册文档	0
	外包软件开发	a)应根据开发需求检测软件质量；	被测系统采用自行软件开发，该项不适用	不适用
		b)应在软件安装之前检测软件包中可能存在的恶意代码；	被测系统采用自行软件开发，该项不适用	不适用
		c)应要求开发单位提供软件设计的相关文档和使用指南；	被测系统采用自行软件开发，该项不适用	不适用
		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和隐蔽信道；	被测系统采用自行软件开发，该项不适用	不适用
		e)应要求外包服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要；	《外包软件开发管理》规定：项目实施过程中，应要求外包服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要	5
		f)应要求外包服务商每年至少开展一次信息安全风	未要求外包服务商每年至少开展一次信息安全风险评估并提交评估报告，未要	0

测评对象	安全控制点	测评指标	结果记录	符合程度
		险评估并提交评估报告，应要求外包服务商聘请外部机构定期对其进行安全审计并提交审计报告，督促其及时整改发现的问题；	求外包服务商聘请外部机构定期对其进行安全审计并提交审计报告	
		g)应禁止外包服务商转包并严格控制分包，保证外包服务水平；	《外包软件开发管理》规定：签订开发合同时，应明确禁止外包服务商转包并严格控制分包，保证外包服务水平	5
		h)应制定数据中心外包服务应急计划，制订供应商替换方案，以应对外包服务商破产、不可抗力或其它潜在问题导致服务中断或服务水平下降的情形，支持数据中心连续、可靠运行。	未制定数据中心外包服务应急计划，未制订供应商替换方案	0
	工程实施	a)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；	《系统建设安全管理制度》(四) “工程实施”中规定：由实施方制定工程实施方面的管理规范，明确说明实施过程的控制方法和人员行为准则，及时向公司提交相关表单文档	5
		b)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；	《系统建设安全管理制度》(四) “工程实施”中规定：指定或授权研发部负责工程实施过程的管理，必要时可引入外部信息工程监理机构进行工程实施的监理	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		c)应制定详细的工程实施方案控制实施过程，并制定相关过程控制文档，并要求工程实施单位能正式地执行安全工程过程；	《系统建设安全管理制度》(四) “工程实施”中规定：由实施方制定详细的工程实施方案控制实施过程，由公司认可并要求工程实施单位能按计划执行工程实施	5
		d)应制定灾难备份系统集成与测试计划并组织实施。通过技术和业务测试，确认灾难备份系统的功能与性能达到设计指标要求；	未制定灾难备份系统集成与测试计划并组织实施	0
		e)网络系统的建设、升级、扩充等工程应经过科学的规划、充分的论证和严格的技术审查，有关材料应妥善保存并接受主管部门的检查。	未提供对 网络系统的建设、升级、扩充等工程的科学规划、论证和严格技术审查的记录	0
	测试验收	a)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；	《系统建设安全管理制度》(五) “测试验收”中对系统测试验收的控制方法和人员行为准则作出了规定	5
		b)应由项目承担单位（部门)或公正的第三方制定安全测试方案，对系统进行安全性测试，出具安全性测试报告，测试报告报科技部门审查；	未提供测试验收方案和测试验收报告	0

测评对象	安全控制点	测评指标	结果记录	符合程度
		c)在测试验收前应根据设计方案或合同要求等制订测试验收方案，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；	未提供第三方测试单位出具的安全性测试报告	0
		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；	《系统建设安全管理制度》(五) “测试验收”中规定：指定研发部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	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；	未提供系统测试验收报告	0
		f)新建应用系统投入生产运行前应进行不少于1个月的模拟运行和不少于3个月的试运行。	未要求新建应用系统投入生产运行前应进行不少于 1 个月的模拟运行和不少于 3 个月的试运行，没有试运行记录	0
	系统交付	a)应对系统交付的控制方法和人员行为准则进行书面规定；	《系统建设安全管理制度》(六) “系统交付”对系统交付的控制方法和人员行为准则进行了规定	5
		b)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；	未提供系统交付的设备、软件和文档清单	0
		c)系统建设单位应	未提供相关文档,未提供移	0

测评对象	安全控制点	测评指标	结果记录	符合程度
		在完成建设任务后将系统建设过程文档和系统运维文档全部移交科技部门；	交记录	
		d)系统建设单位应对负责系统运行维护的技术人员进行相应的技能培训；	未对负责系统运行维护的技术人员进行相应的技能培训	0
		e)应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作；	《系统建设安全管理制度》(六) “系统交付”中规定：指定或授权研发部负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作	5
		f)外部建设单位应与金融机构签署相关知识产权保护协议和保密协议，不得将系统采用的关键安全技术措施和核心安全功能设计对外公开。	与建设单位签订了合同，但合同中没有知识产权相关内容	4
	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；	指定研发部负责系统定级的管理工作	5
		b)应将系统等级及相关材料报系统主管部门备案；	系统等级和系统属性等资料报系统主管部门备案，并形成《信息系统安全等级保护备案表》	5
		c)应将系统等级及其他要求的备案材料报相应公安	被测系统的系统等级及其他要求的备案资料已报公安机关备案	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		机关备案。		
	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；	此次测评为首次等保测评，该项不适用	不适用
		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；	此次测评为首次等保测评，该项不适用	不适用
		c)应选择具有公安部认可的《全国等级保护测评机构推荐目录》中的测评单位进行等级测评，并与测评单位签订安全保密协议；	上海计算机软件技术开发中心是公安部认可的信息安全等级保护测评单位	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。	指定研发部负责等级测评的管理工作	5
	安全服务商选择	a)选择信息安全服务提供商时应评估其资质、经营行为、业绩、服务体系和服务品质等要素；	选择上海计算机软件技术开发中心进行等保测试，评估资质、经营行为、业绩、服务体系和服务品质等要素	5
		b)应确保安全服务商的选择符合	上海计算机软件技术开发中心是公安部认可的信息	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		国家的有关规定；	安全等级保护测评单位	
		c)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；	与上海计算机软件技术开发中心签订合同,其中包括与安全相关的协议,明确约定相关责任	5
		d)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。	与上海计算机软件技术开发中心签订服务合同,包括后期的技术服务和技术支持	5

A.10 系统运维管理

以表格形式给出系统运维管理的现场测评结果。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）。

测评对象	安全控制点	测评指标	结果记录	符合程度
系统运维管理	环境管理	a)应建立集中的机房，统一为各信息系统提供运行环境。机房设施配备应符合国家计算机机房有关标准要求；	被测系统部署于阿里云,有阿里云负责机房的运行维护	不适用
		b)机房应采用结构化布线系统，配线机柜内如果配备理线架，应做到跳线整齐，跳线与配线架统一编号，标记清晰；	被测系统部署于阿里云	不适用
		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	被测系统部署于阿里云	不适用

测评对象	安全控制点	测评指标	结果记录	符合程度
		等方面的管理作出规定；		
		d)应指定部门负责机房安全，指派专人担任机房管理员，对机房的出入进行管理，定期巡查机房运行状况，对机房供配电、空调、温湿度控制等设施进行维护管理，填写机房值班记录、巡视记录；	被测系统部署于阿里云	不适用
		e)机房管理员应经过相关培训，掌握机房各类设备的操作要领；	被测系统部署于阿里云	不适用
		f)应定期对机房设施进行维修保养，加强对易损、易失效设备或部件的维护保养；	被测系统部署于阿里云	不适用
		g)机房人员进出机房必须使用主管部门制发的证件；	被测系统部署于阿里云	不适用
		h)应单独设置弱电井，并留有足够的可扩展空间；	被测系统部署于阿里云	不适用
		i)机房所在区域应安装 24 小时视频监控录像装置，重要机房区域实行 24 小时警卫值班，机房实行封闭式管理，设置一个主出入口和一个或	被测系统部署于阿里云	不适用

测评对象	安全控制点	测评指标	结果记录	符合程度
		多个备用出入口，出入口控制、入侵报警和电视监控设备运行资料应妥善保管，保存期限不少于3个月，销毁录像等资料应经机构主管领导批准后实施；		
		j)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。	《人员信息安全管理制度》中规定：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	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；	制定了《资产清单》，对资产的重要程度、责任部门进行规定	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；	《信息资产管理制度》中对资产安全管理作出了规定，内容覆盖资产使用、维护等方面	5
		c)应根据资产的重	在资产记录表中，根据资产	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		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；	的重要程度对资产进行标识管理	
		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。	《资产安全管理制度》中对信息分类与标识方法作出了规定，并对信息的使用、传输和存储等进行规范化管理	5
	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；	《介质管理规定》中对介质安全管理作出了规定，内容包括介质的使用、维修、销毁等过程的操作	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；	《介质管理规定》中规定：介质在长期保管时，其保管的地点必须满足防火、防水、防震、防潮、防霉、防鼠害、防虫蛀、防静电、防磁等方面的安全要求，介质的保管要符合介质生产商对介质保管的要求	5
		c)所有数据备份介质应防磁、防潮、防尘、防高温、防挤压存放；	通过阿里云进行数据备份，备份数据存储在阿里云上，无备份截止存储的要求	5
		d)应对介质在物理传输过程中的人员选择、打包、交付等情况进行安全控制，应选择安全可靠的传递、交接方式，做好防信息泄露控制措施；	《介质管理规定》中对介质在物理传输过程中的人员选择、打包、交付等情况进行要求	5
		e)应对介质归档	《介质管理规定》中对介质	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		和查询等进行登记记录，管理员应根据存档介质的目录清单定期盘点；	的归档和查询进行规定，目前系统内未使用介质设备	
		f)对于重要文档，如是纸质文档则应实行借阅登记制度，未经相关部门领导批准，任何人不得将文档转借、复制或对外公开，如是电子文档则应采用 OA 等电子化办公审批平台进行管理；	《介质管理规定》中对重要纸质文档的借阅登记进行规定，目前系统内均采用电子化存储管理，无纸质介质	5
		g)应按照统一格式对技术文档进行编写并及时更新，达到能够依靠技术文档恢复系统正常运行 的要求；	技术文档格式统一，存档的技术文档完备	5
		h)应对带出工作环境的存储介质进行内容加密和监控管理；	《介质管理规定》中要求对带出工作环境的存储介质进行内容加密和监控，目前系统内未使用到存储介质	5
		i)应对送出维修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；	《介质安全管理制度》对介质的使用过程、送出维修及销毁等作出了规定，信息安全介质因故障需送外修理，必须经领导批准，由安全管理员负责送修。申请维修的人员陪同，并在修理现场进行监督，当场取回，并填写维修记录表。安全管理员定期（每半年一次）将损坏的	5

测评对象	安全控制点	测评指标	结果记录	符合程度
			介质集中，填写《介质销毁审批表》，经信息安全领导小组批准后，交研发部进行统一销毁	
		j)对载有敏感信息存储介质的销毁，应报有关部门备案，由科技部门进行信息消除、消磁或物理粉碎等销毁处理，并做好相应的销毁记录，信息消除处理仅限于存储介质仍将在金融机构内部使用的情况，否则应进行信息的不可恢复性销毁；	《介质管理规定》中规定对载有敏感信息存储介质的销毁，并进行登记	5
		k)应制定移动存储介质使用规范，并定期核查移动存储介质的使用情况；	制定了《介质管理规定》移动存储介质使用进行规范，要求定期核查移动存储介质使用情况	5
		l)应建立重要数据多重备份机制，其中至少1份备份介质应存放于科技部门指定的同城或异地安全区域；	数据备份通过阿里云进行，阿里云提供异地数据灾备服务	5
		m)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。	《介质管理规定》中规定重要介质中的数据和软件采取加密存储，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	5
		n)应对技术文档	未对技术文档实行有效期	0

测评对象	安全控制点	测评指标	结果记录	符合程度
		实行有效期管理，对于超过有效期的技术文档降低保密级别，对已经失效的技术文档定期清理，并严格执行技术文档管理制度中的销毁和监销规定；	管理	
		o)应定期对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。	未定期对主要备份业务数据进行恢复验证	0
	设备管理	a)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；	《设备管理制度》中明确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	5
		b)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；	《设备管理制度》包括了维护人员的责任、涉外维修和服务的审批	5
		c)设备确需送外单位维修时，应彻底清除所存的工作相关信息，并与设备维修厂商签订	《设备安全管理制度》规定：对送修设备是否存有内部敏感信息进行检查。如有，应先对磁盘信息进行彻底清除后，方能送修	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		保密协议，与密码设备配套使用的设备送修前必须请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息，并派专人在场监督；		
		d)制定规范化的故障处理流程，建立详细的故障日志(包括故障发生的时间、范围、现象、处理结果和处理人员等内容)；	未建立规范化的故障处理流程,未建立详细的故障日志	0
		e)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；	提供了对终端计算机、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的操作规程	5
		f)各机构科技部门负责对信息系统相关的各种设备（包括备份和冗余设备)、线路等进行维护管理；	研发部负责对信息系统相关的各种设备(包括备份和冗余设备)、线路等进行维护管理	5
		g)新购置的设备应经过测试，测试合格后方能投入使用；	未要求新购置的设备应经过测试,测试合格后方能投入使用，未提供测试记录	0

测评对象	安全控制点	测评指标	结果记录	符合程度
		h)应做好设备登记工作，制定设备管理规范，落实设备使用者的安全保护责任；	对设备进行了登记，具有设备登记表	5
		i)需要废止的设备，应由科技部门使用专用工具进行数据信息消除处理，如废止设备不再使用或调配到金融机构以外的单位，应由科技部门对其数据信息存储设备进行消磁或物理粉碎等不可恢复性销毁处理，同时备案；	对废止的设备，没有专用工具进行数据信息消除处理	0
		j)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。	程序文件要求带离设备需填写《机房设备出门单》，经过审批，才可执行	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；	采购了阿里云监控系统，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，并形成审计记录	5
		b)应建立计算机系统运行监测周报、月报或季报制度，统计分析运行状况；	未建立计算机系统运行监测周报、月报或季报制度，未统计分析运行状况	0
		c)应定期对监测和报警记录进行分	组织了运维人员定期对监测和报警记录进行分析，并	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		析、评审，发现可疑行为，形成分析报告，发现重大隐患和运行事故应及时协调解决，并报上一级单位相关部门；	对可疑行为形成分析报告，立即上报	
		d)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。	未建立安全管理中心	0
	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，并有操作和复核人员的签名，维护记录应至少妥善保存 3 个月；	《网络安全管理制度》规定由网终管理员负责对网络进行维护管理，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	5
		b)应建立网络安全运行管理制度，对网络安全配置(最小服务配置)、日志保存时间、安全策略、升级与打补丁、口令更新周期、重要文件备份等方面作出规定；	《网络安全管理制度》对对网络安全配置、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	5
		c)应制定网络接入管理规范，任何设备接入网络前，接入方案应经过科技部门的审核，审	《网络安全管理制度》中规定：任何设备接入网络前，接入方案应经过信息安全主管领导的审核，审核批准后方可接入网络并分配相	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		核批准后方可接入网络并分配相应的网络资源；	应的网络资源	
		d)应制定远程访问控制规范，确因工作需要进行远程访问的，应由访问发起机构科技部门核准，提请被访问机构科技部门（岗)开启远程访问服务，并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施；	《网络安全管理制度》规定:一般情况下应禁止远程访问内部系统,确因工作需要进行远程访问的,应由访问发起机构科技部门核准,提请被访问机构科技部门（岗）开启远程访问服务,并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施	5
		e)各机构以不影响正常网络传输为原则，合理控制多媒体网络应用规模和范围，未经科技主管部门批准，不得在内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用；	《网络安全管理制度》规定:未经信息安全主管领导批准,不得在内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用	5
		f)信息安全管理人员经本部门主管领导批准后，有权对本机构或辖内网络进行安全检测、扫描，检测、扫描结果属敏感信息，未经授权不得对外公开，未经科技主管部门授	《网络安全管理制度》规定:信息安全管理人员经本部门主管领导批准后,有权对本机构或辖内网络进行安全检测、扫描，检测、扫描结果属敏感信息,未经授权不得对外公开,未经信息安全主管领导授权,任何外部机构与人员不得检测或扫描机构内部网络	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		权，任何外部机构与人员不得检测或扫描机构内部网络；		
		g)金融业网间互联安全实行统一规范、分级管理、各负其责的安全管理模式，未经金融机构科技主管部门核准，任何机构不得自行与外部机构实施网间互联；	《网络安全管理制度》规定:所有与外部系统的连接均应得到信息安全主管领导的授权和批准	5
		h)所有网间互联应用系统和外联网络区应定期进行威胁评估和脆弱性评估并提供威胁和脆弱性评估报告。	未定期进行网间互联应用系统和外联网络区威胁评估和脆弱性评估,未提供威胁和脆弱性评估报告	0
	系统安全管理	a)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；	《系统安全管理制度》中对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定	5
		b)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；	《信息安全组织机构》中对主机管理员、数据库管理员、安全管理员的职责和义务作出了规定	5
		c)系统管理员不得兼任业务操作人	《信息安全组织机构》中规定： 系统管理员不得兼任	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		员，系统管理员不得对业务数据进行任何增加、删除、修改等操作，系统管理员确需对数据库系统进行业务数据维护操作的，应征得业务部门书面同意，并详细记录维护内容、人员、时间等信息；	业务操作人员，系统管理员不得对业务数据进行任何增加、删除、修改等操作，系统管理员确需对数据库系统进行业务数据维护操作的，应征得业务部门书面同意，并详细记录维护内容、人员、时间等信息	
		d)应每半年至少进行一次漏洞扫描，对发现的系统安全漏洞及时进行修补，扫描结果应及时上报；	《系统安全管理制度》中规定需定期（每年一次）对系统进行漏洞扫描，对发现的系统安全漏洞及时进行修补，但未提供漏洞扫描报告	4
		e)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，并对系统变更进行记录；	《系统安全管理制度》中规定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。系统日志中有补丁安装升级记录，但未提供测试记录	4
		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，重要计算机系统的系统设置要求至	提供了系统操作手册、运维手册，对重要计算机系统的系统设置要求至少两人在场	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		少两人在场；		
		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；	每季度对系统运行日志和审计数据进行分析，并生成审计报表	5
		h)系统用户权限变更应以书面记录，并经相关管理层批准。	未提供用户权限变更的审批记录	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；	《恶意代码防范管理制度》中规定：定期进行培训，提高所有用户的防恶意代码意识和安全技能，但未提供培训记录	4
		b)金融机构客户端应统一安装病毒防治软件，设置用户密码和屏幕保护口令等安全防护措施，确保及时更新病毒特征码并安装必要的补丁程序；	客户端已经统一安装病毒防治软件，设置用户密码和屏幕保护口令等安全防护措施，及时更新病毒库	5
		c)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；	由安全管理员负责恶意代码的检测，使用 360 防病毒软件，防病毒软件系统日志保留病毒检测记录	5
		d)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	《恶意代码防范管理制度》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	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		出明确规定；		
		e)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，对防病毒系统不能自动清除的计算机病毒，提出解决办法，并形成书面的报表和总结汇报。	《恶意代码防范管理制度》中规定:安全管理员负责本机构病毒库的版本更新工作,终端用户要及时进行补丁升级,避免因操作系统漏洞而造成的恶意代码入侵,并做好本机重要数据的备份	5
	密码管理	a)选用的密码产品和加密算法应符合国家相关密码管理政策规定；	《密码使用管理制度》中对密码使用管理作出了规定，由安全管理员负责码的保管、分配、修改、授权	5
		b)应建立对所有密钥的产生、分发和接收、使用、存储、更新、销毁等方面进行管理的制度，密钥管理人员必须是本机构在编的正式员工，并逐级进行备案，规范密钥管理；	《密码使用管理制度》中对密码使用管理作出了规定，由安全管理员负责码的保管、分配、修改、授权	5
		c)主机管理员、数据库管理员、网络管理员、业务操作人员均须设置口令密码，至少每3个月更换一次，口	要求 3 个月更新口令，口令开启了强度要求	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		令密码的强度应满足不同安全性要求；		
		d)敏感计算机系统和设备的口令密码设置应在安全的环境下进行，必要时应将口令密码纸质密封交相关部门保管，未经科技部门主管领导许可，任何人不得擅自拆阅密封的口令密码，拆阅后的口令密码使用后应立即更改并再次密封存放；	敏感计算机系统和设备的口令密码设置在内部安全的环境下进行	5
		e)密钥注入、密钥管理功能调试和密钥档案的保管应由专人负责。密钥资料须保存在保险柜内。保险柜钥匙由专人负责。使用密钥和销毁密钥要在监督下进行并应有使用、销毁记录；	不使用密钥	不适用
		f)确因工作需要经授权可远程接入内部网络的用户，应妥善保管其身份认证介质及口令密码，不得转借他人使用。	《网络安全管理制度》规定:经授权可远程接入内部网络的用户,应妥善保管其身份认证介质及口令密码，不得转借他人使用	5
	变更管理	a)变更管理应流程	《变更控制管理制度》要	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		化、文档化和制度化，变更流程中应明确变更发起方、实施方的职责，应明确变更方案的测试、审批流程及实施策略，对有可能影响客户利益的变更应事先通知客户并得到客户的确认；	求：明确变更发起方、实施方的职责，应明确变更方案的测试、审批流程及实施策略	
		b)应确认系统中要发生的变更，并制定变更方案，包括变更的组织结构与实施计划、操作步骤、应急及回退方案等，变更方案应经过测试，对于无法测试或不具备测试条件的变更，应得到充分论证和审批；	《变更控制管理制度》中规定变更申请人识别具体的变更需求（如范围、可交付成果、时限、组织等），填写《变更申请表》，制定变更方案，交给变更审批人进行审批	5
		c)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；	《变更控制管理制度》对变更管理制度做出了规定，要求变更提出申请并得到批准，并要求变更完成后由变更实施人员向相关人员通告	5
		d)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	《变更控制管理制度》中对变更管理控制作出了规定，要求制定变更方案，方案中对变更影响进行分析，交给变更审批人进行审批，但未	4

测评对象	安全控制点	测评指标	结果记录	符合程度
		更实施过程，并妥善保存所有文档和记录；	提供变更分析记录	
		e)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；	《变更控制管理制度》中对变更不成功的恢复措施作出了规定，取消所做变更，从备份资料中获得原始软件资料，重新运行，恢复原始状态；根据变更操作记录，查找变更失败原因，以便再次做变更操作时避免同样的错误发生。未提供变更失败后恢复过程的演练记录	4
		f)变更前做好系统和数据的备份。风险较大的变更，应在变更后对系统的运行情况进行跟踪；	《变更控制管理制度》规定:变更前做好系统和数据的备份。风险较大的变更，应在变更后对系统的运行情况进行跟踪	5
		g)如果需要使用生产环境进行测试，应纳入变更管理，并制定详细的系统及数据备份、测试环境搭建、测试后系统及数据恢复、生产系统审核等计划，确保生产系统的安全；	《变更控制管理制度》规定:变如果需要使用生产环境进行测试,应纳入变更管理,并制定详细的系统及数据备份、测试环境搭建、测试后系统及数据恢复、生产系统审核等计划,确保生产系统的安全	5
		h)当生产中心发生变更时，应同步分析灾备系统变更需求并进行相应的变更，评估灾备恢复的有效性；应尽量减少紧急	在变更管理方案中未明确灾备系统的变更要求	0

测评对象	安全控制点	测评指标	结果记录	符合程度
		变更。		
	备份与恢复管理	a)应制定数据备份与恢复相关安全管理制度，对备份信息的备份方式、备份频度、存储介质、保存期等进行规范；	《备份与恢复管理制度》中要求制定《信息备份计划》，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定	5
		b)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；	《备份与恢复管理制度》中要求制定《信息备份计划》，对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等进行规定	5
		c)应建立控制数据备份和恢复过程的程序，记录备份过程，对需要采取加密或数据隐藏处理的备份数据，进行备份和加密操作时要求两名工作人员在场，所有文件和记录应妥善保存；	制定了《备份与恢复管理制度》，对备份和恢复的过程进行了明确的要求	5
		d)应每年至少进行一次重要信息系统专项灾备切换演练，每三年至少进行一次重要信息系统全面灾备切换演练，根据	未进行灾备切换演练，未对应急预案进行完善	0

测评对象	安全控制点	测评指标	结果记录	符合程度
		不同的应急恢复内容，确定演练的周期，并指定专人管理和维护应急预案，根据人员、信息资源等变动情况以及演练情况适时予以更新和完善，确保应急预案的有效性和灾难发生时的可获取性；		
		e)应定期对备份数据的有效性进行检查，每次抽检数据量不低于5%。备份数据要实行异地保存；	未定期对备份数据的有效性进行检查	0
		f)恢复及使用备份数据时需要提供相关口令密码的，应把口令密码密封后与数据备份介质一并妥善保管；	备份数据不需要提供口令密码	不适用
		g)灾难恢复的需求应定期进行再分析，再分析周期最长为三年，当生产中心环境、生产系统或业务流程发生重大变更时，单位应立即启动灾难恢复需求再分析工作，依据需求分析制定灾难恢复策略；	未定期对灾难恢复的需求进行再分析	0

测评对象	安全控制点	测评指标	结果记录	符合程度
		h)应建立健全灾难恢复计划，恢复计划至少要包括灾难恢复范围和目标、灾难切换规程、灾后重续运行操作指引、各系统灾难切换操作手册；	提供健全的灾难恢复计划、灾难切换规程、灾后重续运行操作指引、各系统灾难切换操作手册等，但未开展恢复测试	4
		i)金融机构应根据信息系统的灾难恢复工作情况，确定审计频率。单位应每年至少组织一次内部灾难恢复工作审计；	未提供审计记录	0
		j)应定期开展灾难恢复培训，并根据实际情况进行灾难恢复演练；	未提供灾难恢复培训记录	0
		k)应建立灾难备份系统，主备系统实际切换时间应少于 60 分钟，灾备系统处理能力应不低于主用系统处理能力的 50%，通信线路应分别接入主备系统，有条件时可采用主、备系统处理能力相同、轮换交替使用的双系统模式。	未建立灾难备份系统	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	《安全事件管理制度》中规定信息安全事件的报告过程包括：事件通知、事件调查报告等，并规定了安全时	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		试验证弱点；	间响应流程，规定所有员工对于发现的系统漏洞或弱点，应立即报告，不允许对弱点进行任何尝试和验证	
		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；	《安全事件管理制度》中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	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；	制度中将信息安全事件划分为四个级别：特别重大事件、重大事件、较大事件和一般事件，对事件划分方法进行了规定	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；	《安全事件管理制度》中对安全事件处理流程作出了规定，出现事件后当信息系统发生事件时，信息系统使用或维护部门应立即在第一时间向安全主管部门通知事件情况，说明事件发生的时间、部位、表象、程度和影响，相关责任部门组织抢修工作	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	制定了《安全事件记录报告》，包括了发生时间、事件发生单位、安全事件现象描述、已经造成的损失和预计损失、已经采取的措施、报告人、报告时间等	5

测评对象	安全控制点	测评指标	结果记录	符合程度
		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；		
		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；	当发生安全事件时，信息系统管理员或维护人应立即在第一时间向技术部口头通知事件情况，说明事件发生的时间、部位、表象、程度和影响；发现安全事件时应立即组织人员开展抢修工作对安全泄密时间，规定了在发现数据泄露后立即调查数据泄露的原因，影响范围，制定不要的纠正措施，并在必要时向公安机关报案	5
		g)应建立有效的技术保障机制，确保在安全事件处置过程中不会因技术能力缺乏而导致处置中断或延长应急处置时间。	未利用灾备机房等技术保障措施，保证处置中断的及时可靠	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应急组织机构、启动应急预案的条件、应急处理流程、系统恢复流程、事件信息收集、分析、报告制度、事后教育和培训等内容,业务处理系统应急预	《安全事件管理制度》中对信息系统应急预案的制定，演练等做出了规定，但是未提供由预案涉及的相关机构签字盖章的应急预案	4

测评对象	安全控制点	测评指标	结果记录	符合程度
		案的编制工作应由相关业务部门和科技部门共同完成，并由预案涉及的相关机构签字盖章；		
		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；	《安全事件管理制度》中规定：应制定各系统的应急预案，应急预案应从人力、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	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；	《安全事件管理制度》规定每年举行一次对系统内管理运维人员进行教育培训、安全培训、应急响应培训、技能培训等，但未提供应急预案的培训记录	4
		d)在与第三方合作的业务中，应建立并完善内部责任机制和与相关机构之间的协调机制，制定完整的应急预案及应急协调预案，并定期参加联合演练；	未提供演练报告，未提供第三方参与演练的相关信息	0
		e)突发事件应急处置领导小组应统一领导计算机系统的应急管理工作，指挥、决策重大应急处置事宜，并协调应急资源，明确具体应急处置联络人，并将具体联系方式上	《信息事件管理制度》中规定：当安全事件发生时，信息技术部应当立即启动应急预案或采取有效措施，全力而有序地组织抢救抢修，防止事件扩大，消除各种危险，尽快恢复系统，将各种损失减到最低程度，但未明确具体应急处置联络人	4

测评对象	安全控制点	测评指标	结果记录	符合程度
		报本行业信息安全监管部门；		
		f)金融机构应急领导小组应及时向新闻媒体发布相关信息，严格按照行业、机构的相关规定和要求对外发布信息，机构内其它部门或者个人不得随意接受新闻媒体采访或对外发表个人看法；	《信息事件管理制度》中规定:研发部应及时向新闻媒体发布相关信息,严格按照行业、机构的相关规定和要求对外发布信息,机构内其它部门或者个人不得随意接受新闻媒体采访或对外发表个人看法	5
		g)实施报告制度和启动应急预案的单位应当实行重大突发事件 24 小时值班制度；	《信息事件管理制度》中规定：应建立 24 小时值班制度	5
		h)应定期对原有的应急预案重新评估，并根据安全评估结果，定期修订、演练，并进行专项内部审计；	未提供对应急预案重新评估，定期修订、演练，内部审计的记录	0
		i)应急演练结束后，金融机构应撰写应急演练情况总结报告，总结报告包括但不限于：内容和目的、总体方案、参与人员、准备工作、主要过程和关键时间点记录、存在的问题、后续改进措施及实施计划、演练	未提供应急演练情况总结报告	0

测评对象	安全控制点	测评指标	结果记录	符合程度
		结论。		

A.11 验证测试

2017 年 8 月 17 日，上海计算机软件技术开发中心的测评人员使用明鉴 Web 应用弱点扫描器在互联网对马上贷平台应用系统进行了安全扫描。应用系统扫描共发现中风险漏洞 2 类 90 个、2 类 2 个低风险，未发现高风险漏洞。具体扫描结果如下：

2．网站漏洞详细报告

2.1．weixin.17msd.com:80详细报告

2.1.1．扫描信息列表

名称	内容
项目名称	9.4网站扫描
扫描对象	weixin.17msd.com
主机端口	80
开始时间	2017-08-17 15:24:44
结束时间	2017-08-17 15:31:27
扫描用时(时:分:秒)	0:06:43
服务器信息	Tengine
服务器时间	2017-08-17 15:25:11
协　议	http
域　名	weixin.17msd.com
已访问URL	677
URL总数	677
网站安全值	85
漏洞个数	97

图 A11-1 应用系统扫描结果

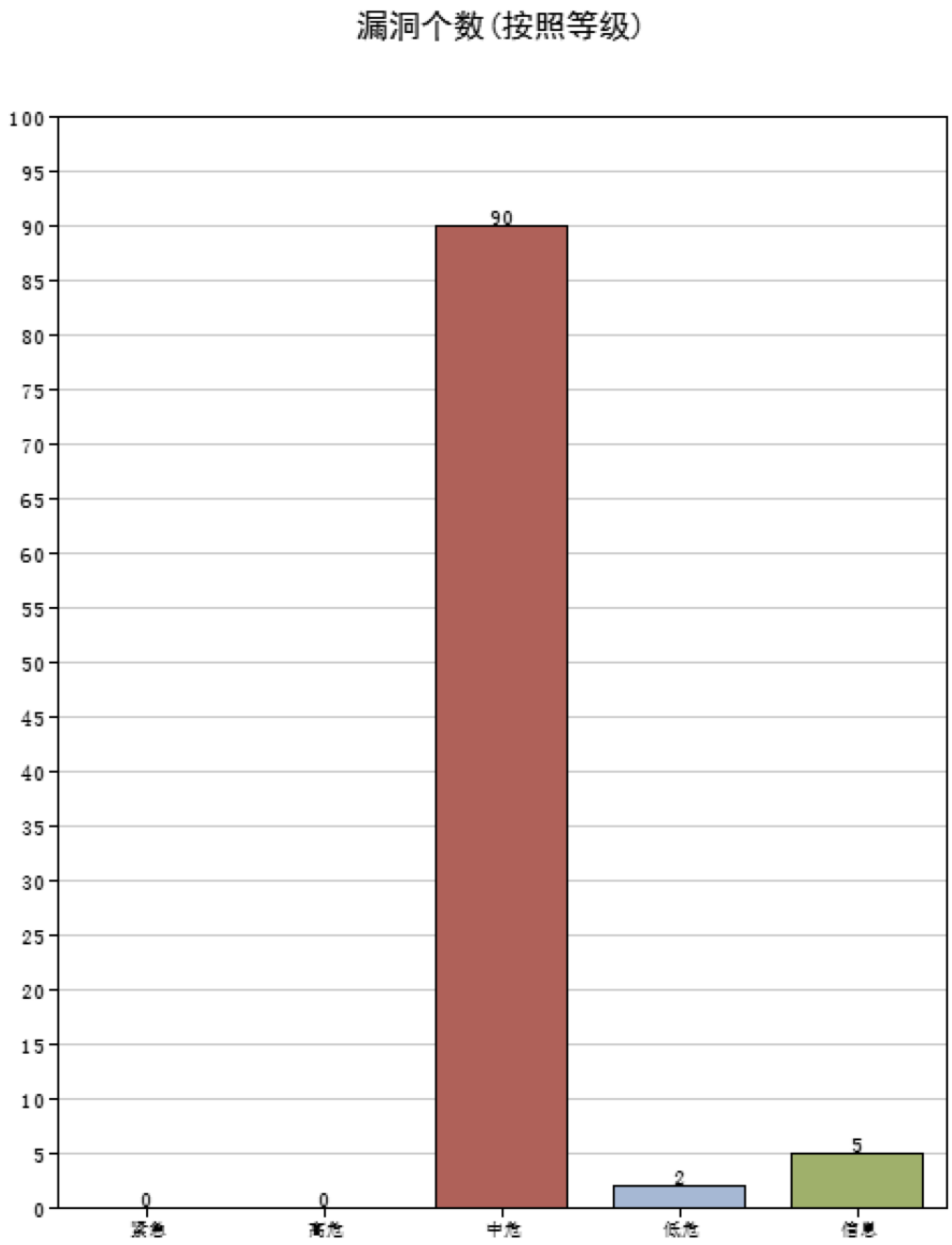
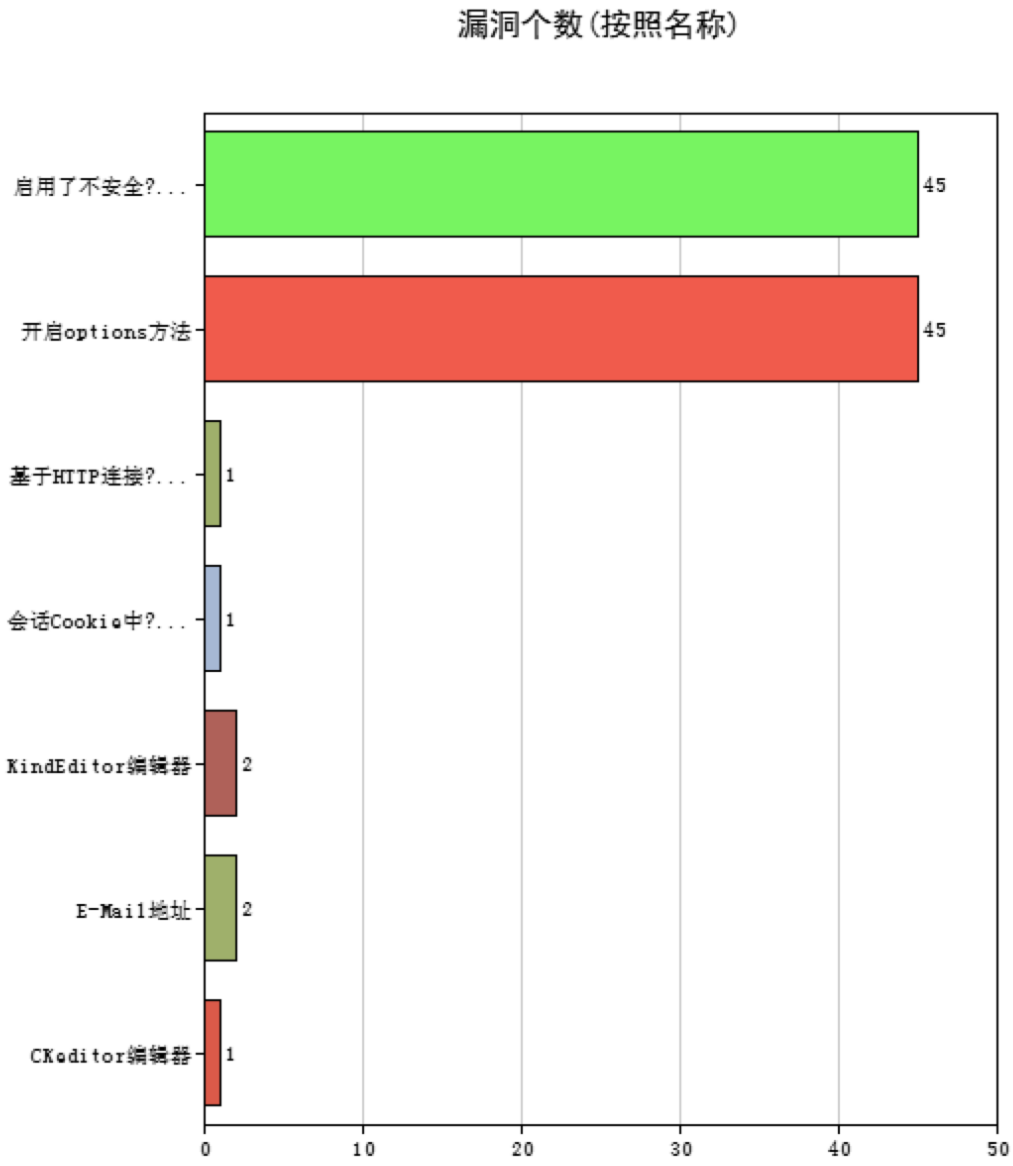


图 A11-2 漏洞数量统计图

2.1.3．按照名称统计



A11-3 漏洞类型统计图