**报告编号：43010199326-20001-21-0155-01**

**网络安全等级保护**

**SanyMall 客户云商城系统**

**等级测评报告**

|  |  |
| --- | --- |
| **被测单位：** | **三一集团有限公司** |
| **测评单位：** | **湖南省金盾信息安全等级保护评估中心有限公司** |
| **报告时间：** | **2021年12月31日** |

说明：

一、每个备案系统单独出具测评报告。

二、测评报告编号为四组数据。各组含义和编码规则如下：

第一组为系统备案表编号，由2段16位数字组成，可以从公安机关颁发的系统备案证明（或备案回执）上获得。第1段即备案证明编号的前11位（前6位为受理备案公安机关代码，后5位为受理备案的公安机关给出的备案单位的顺序编号）；第2段即备案证明编号的后5位（系统编号）。

第二组为年份，由2位数字组成。例如09代表2009年。

第三组为机构代码，由网络安全等级测评与检测评估机构服务认证证书编号最后四位数字组成。

第四组为本年度系统测评次数，由两位构成。例如02表示该系统本年度测评2次。

网络安全等级测评基本信息表

|  |  |  |  |
| --- | --- | --- | --- |
| **被测对象** | | | |
| **被测对象名称** | SanyMall 客户云商城系统 | **安全保护等级** | 第三级（S3A3） |
| **备案证明编号** | 43010199326-20001 | | |
| |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | **被测单位** | | | | | | | **单位名称** | 三一集团有限公司 | | | | | | **单位地址** | 湖南省长沙市长沙县三一路与东二路长沙三一工业城 | | | **邮政编码** | 410100 | | **联系人** | **姓名** | 刘清香 | **职务/职称** | 安全管理员 | | | **所属部门** | 流程信息化总部 | **办公电话** | -- | | | **移动电话** | 15273150727 | **电子邮件** | liuqx316@sany.com.cn | | | | | |
| |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | **测评单位** | | | | | | | **单位名称** | 湖南省金盾信息安全等级保护评估中心有限公司 | | | **机构代码** | SC20210155 | | **单位地址** | 湖南省长沙市岳麓区麓云路 100 号兴工国际产业园 10 栋502 室 | | | **邮政编码** | 410221 | | **联系人** | **姓名** | 罗晓燕 | **职务/职称** | 总经理 | | | **所属部门** | 总经办 | **办公电话** | 0731-83758161 | | | **移动电话** | 13808482451 | **电子邮件** | lxy@jdicsp.org | | | **审核批准** | **编制人** |  | **编制日期** |  | | | **审核人** |  | **审核日期** |  | | | **批准人** |  | **批准日期** |  | | | | | |

声明

本报告是三一集团有限公司SanyMall客户云商城系统的等级测评报告。

本报告测评结论的有效性建立在被测评单位提供相关证据的真实性基础之上。

本报告中给出的测评结论仅对被测对象当时的安全状态有效。当测评工作完成后，由于被测对象发生变更而涉及到的系统构成组件（或子系统）本报告不再适用。

本报告中给出的测评结论不能作为对被测对象内部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。

湖南省金盾信息安全等级保护评估中心有限公司

2021年12月31日

等级测评结论

|  |  |  |  |
| --- | --- | --- | --- |
| **测评结论和综合得分** | | | |
| **被测对象名称** | SanyMall 客户云商城系统 | **安全保护等级** | 第三级（S3A3） |
| **扩展要求 应用情况** | |  |  |  | | --- | --- | --- | | ☑云计算 | ☐移动互联 | ☐物联网 | | ☐工业控制系统 | ☐大数据 |  | | | |
| **被测对象描述** | SanyMall 客户云商城系统是三一集团商城系统，主要提供商城在线展示和交易功能，以最终用户为主要对象，提供三一整机、三一机械配件等系列终端产品和服务；致力于为客户提供方便快捷的产品选购渠道，完善智慧管理云平台生态圈。  三一集团有限公司SanyMall 客户云商城系统部署于腾讯公有云IaaS服务平台，为云服务客户业务应用系统，云服务提供商为腾讯云，业务系统部署使用的云服务模式为基础设施即服务(IaaS)。SanyMall 客户云商城系统使用腾讯云服务器作为应用服务器，腾讯云数据库作为业务系统数据处理、存储等，其基础设施与网络架构及网络设备均采用腾讯公有云IaaS服务平台服务。 | | |
| **安全状况描述** | 本次测评共发现安全问题23个，其中高风险问题0个，中风险问题21个，低风险问题2个；选取的测评指标总数为257个，不适用指标为60个，测评指标符合率为88.33%，测评指标部分符合率为7.61%，测评指标不符合率为4.06%。  本次等级测评的综合得分为86.41分，且系统不存在高等级安全风险，等级测评结论为良。 | | |
| **等级测评结论** | 良 | **综合得分** | 86.41分 |

等级测评结论扩展表（云计算安全）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **等级测评结论扩展表（云计算安全）** | | | | | |
| **被测对象**  **云计算形态** | □云计算平台  ☑云服务客户业务应用系统（平台报告编号：440320-50052-00011-21-000008-01） | | | | |
| **云计算平台**  **名称** | 腾讯公有云IaaS服务平台 | | **被测对象采用的**  **云计算服务模式** | ☑ IaaS  □ PaaS  □ SaaS | |
| **云计算平台服务能力描述** | | | | | |
| **云计算安全扩展主要要求** | | | | | **符合情况** |
| **网络架构** | b)应实现不同云服务客户虚拟网络之间的隔离； | | | | 符合 |
| c)应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力； | | | | 符合 |
| e)应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务； | | | | 符合 |
| **入侵防范** | a)应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； | | | | 符合 |
| **数据完整性和保密性** | c)应使用校验技术或密码技术保证虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施； | | | | 符合 |
| d)应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。 | | | | 符合 |
| **数据备份恢复** | a) 云服务客户应在本地保存其业务数据的备份； | | | | 符合 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | | | | 符合 |
| **剩余信息保护** | b)云服务客户删除业务应用数据时，云计算平台应将云存储在所有副本删除。 | | | | 符合 |
| **云服务商选择** | b)应在服务水平协议中规定云服务的各项服务内容和具体技术指标； | | | | 符合 |
| **供应链管理** | b)应将供应链安全事件信息或安全威胁信息及时传达到云服务客户； | | | | 符合 |
| **云计算平台等级测评结论** | | 优 | **云计算平台综合得分** | | 96.30分 |

总体评价

三一集团有限公司SanyMall 客户云商城系统定级为第三级（S3A3），此次等级测评，测评指标一共为257项，其中不适用项数为60项，通过对信息系统基本安全保护状态的分析，指标符合率为88.33%，指标部分符合率为7.61%，不符合率为4.06%，问题数总计23个，其中高风险问题0个，中风险问题数21个，低风险问题2个。测评报告得分为86.41分，其中各层面得分情况如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 层面 | 安全物理环境 | 安全通信网络 | 安全区域边界 | 安全计算环境 | 安全管理中心 |
| 得分 | -- | 94.20 | 90.91 | 89.34 | 97.96 |
| 层面 | 安全管理制度 | 安全管理机构 | 安全管理人员 | 安全建设管理 | 安全运维管理 |
| 得分 | 100.00 | 86.96 | 93.33 | 92.59 | 100.00 |

通过对信息系统基本安全保护状态的分析，三一集团有限公司针对SanyMall 客户云商城系统面临的主要安全威胁采取了相应的安全机制，基本达到保护信息系统重要资产的作用。其中：

在安全物理环境方面，三一集团有限公司SanyMall 客户云商城系统的物理环境、网络架构采用腾讯公有云IaaS服务平台服务，其已通过信息产业信息安全测评中心的三级等级测评，等级测评结论为优，综合得分为96.30分，具体信息请参阅附录J。

在安全通信网络方面，网络架构、通信传输等安全控制点基本满足《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）三级的相应要求。其中，在网络架构方面，被测系统部署于腾讯云上，在腾讯云上分配有专门的VPC，未出现由于设备性能存在瓶颈，而导致网络拥堵、阻断等情况；同时，腾讯云关键网络设备和线路已实现硬件冗余和线路冗余及云计算平台承载的业务系统等级不高于云计算平台自身的安全保护等级等；在通信传输方面，在管理网络系统云服务器及云安全产品均通过腾讯云企业子账号控制台进行管理访问，采用HTTPS协议登录腾讯云控制台，能够保证通信过程中数据的完整性及保密性等。但还存在不足，如通信设备不具有可信根芯片或硬件，未基于可信根对通信设备的系统引导程序、系统程序、重要配置参数等进行可信验证。

在安全区域边界方面，边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计等安全控制点基本满足《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）三级的相应要求。其中，在边界防护方面，被测系统部署在腾讯公有云IaaS服务平台，为云租户分配有专门的VPC网络区域，在VPC网络边界部署了高级版云防火墙访问控制设备，并配置了相应访问控制策略，对VPC边界的流量进行控制，实现VPC之间的隔离；云租户具有云防火墙管理权限，可根据业务需要或所发生的安全事件及时调整访问控制策略等；

在访问控制方面，被测系统部署在腾讯公有云IaaS服务平台，为云租户分配有专门的VPC网络区域，在VPC网络边界通过腾讯云安全组件云服务进行访问控制，有根据被测系统实际业务配置了相应出、入站规则。如：针对ping服务、系统业务访问端口、SSH(22)远程访问服务等通信设置了相应访问控制规则，默认情况下除允许通信外拒绝所有通信；同时，为被测系统提供部署了Web应用防火墙云产品，且根据企业的需求已配置了安全策略；如已设置Web应用攻击防护、CC防护及腾讯公有云IaaS服务平台在每个租户网络区域边界设置了访问控制，且该租户在边界处统一部署腾讯云安全组件云服务，设置访问控制规则，网络不存在其他非三级以外的网络区域边界等；在入侵防范方面，腾讯公有云IaaS服务平台为被测系统提供部署了主机安全云产品、Web应用防火墙云产品，主机安全云产品实现对云上虚拟服务器主机全量日志分析，对进程异常行为、异常账户、敏感文件篡改、异常网络连接等入侵行为进行检测及分析；同时，检测云上虚拟服务器主机恶意攻击行为，对进程、网络异常等行为进行预警。Web应用防火墙实现对Web应用进防护，防御各类OWASP常见Web攻击并过滤海量恶意CC攻击，保障网站业务安全性与可用性；在恶意代码及邮件防范方面，腾讯公有云IaaS服务平台为被测系统提供部署了主机安全云产品，通过主机安全云产品实现蠕虫病毒、勒索病毒、木马、网站后门等恶意代码的检测和隔离清除等；在安全审计方面，系统部署于腾讯云，被测系统相关云产品（Web应用防火墙云产品、主机安全云产品、云服务器等）所有操作行为通过云审计云产品进行审计；同时，通过主机安全云产品、Web应用防火墙云产品实现对网络中发生的各类安全事件进行审计等。但还存在不足，如未购买部署抗APT、态势感知等可检测新型网络攻击行为的安全服务等。

在安全计算环境方面，身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、数据完整性、数据备份恢复等安全控制点基本满足《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）三级的相应要求。其中，在身份鉴别方面，被测系统相关云安全服务产品、云服务器及重要终端均有设置提供身份标识和鉴别功能，用户口令均符合复杂性要求及被测系统相关云安全服务产品、云服务器远程管理需要登录腾讯云的企业账号，在控制端中对其进行安全管理。腾讯云使用的是https协议来进行远程通信，可防止鉴别数据在网络传输的过程中被窃听；在访问控制方面，被测系统相关云安全服务产品、云服务器及重要终端已修改默认账户口令为强口令，禁用或删除了多余不需要账户；在安全审计方面，被测系统相关云安全服务产品、云服务器及重要终端均设置开启了日志审计功能，能对重要用户行为和重要安全事件进行审计；且对日志记录进行了保护等；在入侵防范方面，被测系统相关云安全服务产品、云服务器关闭了不需要的系统服务和高危端口及云服务器操作系统均安装部署了已安装部署腾讯云主机安全云产品专业版，具备入侵防御功能，能够检测到对重要节点进行入侵的行为等；在恶意代码防范方面，被测系统相关云服务器操作系统均部署了腾讯云主机安全云产品专业版，具备防恶意代码功能，能够及时识别入侵和病毒行为，并将其有效阻断；在数据完整性及数据保密性方面，被测系统相关云安全服务产品远程管理需要登录腾讯云的企业账号，在控制端中对其进行安全管理；腾讯云使用的是https协议来进行远程通信，传输过程加密，可保证重要数据在传输过程中的完整性及保密性；在数据备份恢复方面，被测系统业务数据库采用的是腾讯云数据库，系统业务数据库采用实时备份，备份位置：北京腾讯云备份中心；同时，已建立恢复测试机制，定期每半年对备份数据进行恢复测试验证等；在个人信息保护方面，SanyMall 客户云商城系统只收集了业务必需的用户个人信息，如：用户名、手机号、邮箱、密码等及SanyMall 客户云商城系统个人用户详细信息只有管理人员及相关权限人员才能查询到，如：用户名、手机号、邮箱、密码等，信息均通过相关审核等。但还存在不足，如被测系统腾讯云数据库及SanyMall 客户云商城系统对账户口令未强制要求进行定期更换；被测系统相关安全产品及数据库未设置允许登录尝试次数、未设置锁定时间等策略；SanyMall 客户云商城系统及相关重要终端（办公运维管理终端）操作系统采用用户名+口令一种鉴别技术对用户进行身份鉴别，未采用两种或以上组合进行鉴别；SanyMall客户云商城系统前台用户端未限制终端访问网络地址范围及未提供异地备份措施，通过网络将系统网络内的服务器上的重要数据及系统业务数据定期备份至备份场地等。

在安全管理中心方面，系统管理、审计管理、集中管控等安全控制点基本满足《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）三级的相应要求。其中，在系统管理方面，通过腾讯云控制台对系统管理员进行身份鉴别，只允许管理员通过腾讯云控制台对系统进行管理操作，腾讯云控制台云审计云产品对这些操作进行审计；在审计管理方面，通过腾讯云控制台中的云审计云产品存储记录腾讯云账号内的所有操作行为；审计管理员通过登录到腾讯云控制台中的云审计云产品对日志进行管理，并对审计管理员的操作进行审计记录；在安全管理方面，被测系统相关相关云产品（Web应用防火墙、主机安全等）统一通过登录腾讯云企业子账号控制台进行管理访问，对云产品进行管理操作，且对操作进行审计记录；在集中管控方面，被测系统部署在腾讯云平台，通过腾讯云控制台云监控服务，可以对云安全产品、云服务器等运行状态进行集中监测并能依据设定的阀值实时报警；被测系统相关云产品（Web应用防火墙云产品、主机安全云产品等）通过腾讯云云审计云产品进行集中统一收集保存与审计分析等管理，日志留存时长可达到6个月，专职人员定期分析结合腾讯云平台为被测系统已提供部署的Web应用防火墙云产品、主机安全云产品等相关安全产品，对网络中发生的各类安全事件进行识别、报警和分析等。但还存在不足，如安全管理员对安全策略进行配置和管理中未不包括对可信验证策略和安全标记策略的配置。

在安全管理制度方面，安全策略、管理制度、制定和发布、评审和修订等安全控制点基本满足《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）三级的相应要求。管理制度体系较为健全，已建立物理环境、网络安全、数据安全、数据备份、系统建设管理等方面管理制度，制度内容明确等。

在安全管理机构方面，岗位设置、人员配备、授权和审批、沟通和合作等安全控制点基本满足《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）三级的相应要求。单位已成立三一集团有限公司信息安全工作领导委员会为网络安全管理工作的职能部门，已设立系统管理员、审计管理员、安全管理员等岗位；在制度中，已明确系统变更、重要操作、物理访问和系统接入等事项需要进行审批；有定期召开网络协调会议，有效的加强了各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通；同时，运维人员已落实安全巡检制度，每天巡检一次，巡检内容包含机房环境、设备状态、系统运行情况、数据备份等。但还存在不足，如未配备一定数量的系统网络管理员、审计管理员、安全管理员等。

在安全管理人员方面，人员录用、人员离岗、安全意识教育和培训、外部人员访问管理等安全控制点基本满足《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）三级的相应要求，建立了人员录用、人员离岗流程，针对新入职的员工会进行安全意识教育和岗位技能培训，并被告知相关的安全责任；同时，外部人员访问受控区域需向单位分管人事领导审批，方能进入，由专人全程陪同；外部人员接入受控网络访问系统需签署《商业秘密保密协议承诺函》《安全协议》并走流程审批，审批登记完成后方可接入等。但还存在不足，如未与关键岗位签署岗位责任协议。

在安全建设管理方面，定级和备案、安全方案设计、产品采购和使用、自行软件开发、工程实施、系统交付、等级测评、服务供应商选择等安全控制点基本满足《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）三级的相应要求，被测系统的定级结果已经过主管部门审批通过，已完成定级备案工作，已取得系统备案号；在安全方案设计阶段，有组织集团相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，有提供相关会议纪要；针对软件开发，已制定代码安全编写规范，要求开发人员参照规范编写代码；在验收阶段，有制定相关测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；在交付阶段，已制订项目交付清单，并对系统、设备和文档等进行了明确规定及软件开发单位提供了系统相关操作手册、培训资料等文档。在与安全服务商签订的安全服务合同中已明确双方应当履行的责任及安全服务内容等。但还存在不足，如系统未进行上线前安全性测试，未出具相关安全测试报告等。

在安全运维管理方面，环境管理、资产管理、介质管理、设备维护管理、网络和系统安全管理、恶意代码防范管理、变更管理、应急预案管理方面、外包运维管理等安全控制点基本满足《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）三级的相应要求。在环境管理方面，公司建立了办公环境安全相关的管理制度，明确了来访人员接待区域，工作人员离开座位应确保终端计算机退出登录状态及桌面上不准放置包含敏感信息的文件文档等；在资产管理方面，对信息系统相关资产进行标识管理，贴了资产标签，标明重要程度；同时，已建立《资产清单》，内容包括：资产名称、功能描述、数量、责任部门、责任人、使用人等；在介质管理方面，公司已建立《三一集团有限公司存储介质管理办法》明确了将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；在设备维护管理方面，公司明确相关维护人员的职责分工，包括日常维护管理、计算机维修及服务审批等过程的管理；在漏洞和风险管理方面，公司对该系统定期每月进行安全漏洞扫描，且测评过程中涉及渗透测试和漏洞扫描，可以有效的发现安全漏洞和隐患及时进行修补或评估可能的影响后进行修补等；在网络和系统安全管理方面，公司划分不同的管理员角色进行网络和系统的运维管理；由董办授权专干负责进行账户管理，对申请账户、建立账户、删除账户等进行控制；同时，每天一次对机房进行安全巡检，巡检内容主要是针对机房基础设施的环境、设备状态及公司建立了《三一集团有限公司网络管理办法》网络接入管理远程访问账号的申请必须获得相关部门审批，且符合远程访问控制满足一定安全的要求，如需对远程操作或使用的设备以及操作权限、允许访问的内部服务、允许访问时间、会话超时等进行严格控制；在恶意代码防范管理方面，单位会不定期宣传防恶意代码知识，服务器及终端PC均安装了防恶意代码等安全防护软件，可以对外来存储设备进行恶意代码检查等；同时，公司建立的《三一集团有限公司计算机病毒防治管理办法》中明确规定各部门在从信息网络上下载软件、程序、数据和购置、维修、借入计算机设备时，必须先对其进行计算机病毒检测，经确认无毒后方可使用，所有设备接入系统前均需查杀病毒等；在配置管理方面，如需改变服务器或软件系统相关配置参数，需经过部门相关领导的批准，及时更新基本配置信息库；在密码管理方面，购买的密码产品（如：门禁系统）已提供相关证明材料证明符合相关国家标准和行业标准；在变更管理方面，公司在OA 系统中明确了变更流程，包括变更发起方、实施方的工作内容，变更发起方需提交变更方案，变更方案需经过相关领导的审批，对有可能影响客户利益的变更事先通知客户并得到客户的确认之后再进行变更操作等；同时，公司已建立《三一集团有限公司变更管理流程》，对变更过程进行控制规定；在备份与恢复管理方面，公司已识别需要定期备份的重要业务信息（系统业务数据等），公司发布的《三一集团有限公司数据备份管理实施细则》中明确了备份方式、备份频度、存储介质、保存期等；同时，针对被测系统SanyMall 客户云商城系统相关业务等重要数据，制定了备份策略，对系统业务数据库采用实时备份等；在安全事件方面，单位各部门或员工发现的安全弱点和可疑事件会及时向宣传信息科进行报告；同时，公司制定了《三一集团有限公司信息安全事件处理与应急预案管理制度》，明确了不同安全事件的报告、处置和响应流程等；在应急预案管理方面，有制定《三一集团有限公司信息安全事件处理与应急管理制度》，包括应急处理流程、系统恢复流程等内容；同时，公司每年会组织一次应急演练，有形成相关演练记录；在外包运维管理方面，与外包运维服务商有签订相关协议，协议中有明确约定外包运维的范围和工作内容等。

依据GB/T22239—2019《信息安全技术 网络安全等级保护基本要求》和GB/T28448—2019《信息安全技术 网络安全等级保护测评要求》，经对三一集团有限公司SanyMall 客户云商城系统的安全保护状况进行综合分析评价，最终结论如下：

本次等级测评三一集团有限公司SanyMall 客户云商城系统的综合得分为86.41分，系统中不存在高等级风险，测评结论为良。

主要安全问题及整改建议

经过单项测评结果判定和整体测评发现，SanyMall 客户云商城系统存在的主要问题及整改建议如下：

**一、安全通信网络**

**（1）中风险 未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。**

建议通信设备采用可信根芯片或硬件，基于可信根对通信设备的系统引导程序、系统程序、重要配置参数等进行可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

**二、安全区域边界**

**（1）中风险 未采取技术措施对新型网络攻击行为进行分析；**

建议购买配置APT、态势感知等安全服务，实现对新型网络攻击行为的分析。

**（2）中风险 网络边界设备不具有可信根芯片或硬件，未基于可信根对通信设备的系统引导程序、系统程序、重要配置参数等进行可信验证。**

建议网络边界设备采用可信根芯片或硬件，基于可信根对网络边界设备的系统引导程序、系统程序、重要配置参数等进行可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

**三、安全计算环境**

**（1）中风险 未采用两种或两种以上组合的鉴别技术；**

建议SanyMall 客户云商城系统及相关重要终端（办公运维管理终端）操作系统采用两种或两种以上组合的鉴别技术实现用户身份鉴别，其中一种使用密码技术，如数字证书、数字令牌等，或部署堡垒机实施双因子登录。

**（2）中风险 针对重要业务数据及重要个人信息未采用校验技术或密码技术保证存储过程中的完整性；**

建议采用校验技术或密码技术保证SanyMall客户云商城系统重要业务数据及重要个人信息在存储过程中的完整性。

**（3）中风险 SanyMall客户云商城系统针对重要业务数据及重要个人信息未采用密码技术保证存储过程中的保密性；**

建议采用密码技术保证SanyMall客户云商城系统重要业务数据及重要个人信息在存储过程中的保密性。

**（4）中风险 未启用登录失败处理功能；**

建议配置并启用被测系统相关安全产品(Web应用防火墙、主机安全云产品、云审计云产品)及腾讯云数据库登录失败处理功能，如限制非法登录次数5次、锁定10分钟，配置登录连接超时时间10分钟，登录连接超时后需重新登录。

**（5）中风险 未提供异地数据备份功能；**

建议利用通信网络将系统网络内的服务器配置数据及系统业务数据等重要数据定时批量传送至备用场地，实现异地数据异地备份。

**（6）中风险 未关闭危险端口；**

建议关闭被测系统相关重要终端（办公运维管理终端）操作系统TCP 135、139、445、593、1025端口和UDP 135、137、138、445端口等危险端口。

**（7）中风险 仅收集和保存了业务必需用户个人信息，但未制定有关用户个人信息保护管理制度和流程；**

建议制定有关用户个人信息保护管理制度和流程，且需与系统实际情况一致。

**（8）中风险 对用户个人信息访问进行了限制，但未制定有关用户个人信息保护管理制度和流程；**

建议制定有关用户个人信息保护管理制度和流程，且需与系统实际情况一致。

**（9）中风险 未授予不同账户为完成各自承担任务所需的最小权限；**

建议腾讯云数据库按最小权限原则，实现管理用户权限分离，区分设立管理员、审计员、安全员角色。

**（10）中风险 未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证；**

建议系统网络中的主要计算设备(如：Web应用防火墙云产品、主机安全云产品、云审计云产品、应用服务器等)采用可信根芯片或硬件，基于可信根对计算设备的系统引导程序、系统程序、重要配置参数等进行可信验证，及对SanyMall 客户云商城系统应用程序等关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

**（11）中风险 身份鉴别模块功能不完善（账户口令未定期更换）；**

建议被测系统腾讯云数据库及SanyMall 客户云商城系统对登录账户口令进行定期修改更换。

**（12）中风险 未限制默认账户访问权限；**

建议限制系统网络内的服务器操作系统默认账户访问权限。

**（13）中风险 日志存储时间可达到6个月，但未对日志进行定期备份；**

建议采取相关技术措施，定期对被测系统重要终端（办公运维管理终端）日志进行定期备份。

**（14）低风险 未提供实现安全标记功能。**

建议对系统网络内的主要网络安全设备（Web应用防火墙云产品、主机安全云产品、云审计云产品等）及应用服务器、重要终端（办公运维管理终端）、腾讯云数据库、SanyMall 客户云商城系统内的重要信息设置安全标记，并控制对有安全标记信息资源的访问。

**四、安全管理中心**

**（1）中风险 未创未通过安全管理员对可信验证策略和安全标记策略进行配置和管理。**

建议对所有主要网络设备及安全设备创建专门的安全管理员，设置仅有安全管理员对设备安全策略进行配置，包括对可信验证策略和安全标记策略配置和管理。

**五、安全管理机构**

**（1）中风险 未明确安全主管、安全管理各方面负责人；**

建议设立网络安全管理工作职能部门，设立安全主管、安全管理各方面负责人，并定义各负责人的职责。

**（2）低风险 未配备一定数量系统管理员、审计管理员和安全管理员。**

建议配备一定数量的系统管理员、网络管理员、安全管理员等，形成AB岗。

**六、安全管理人员**

**（1）中风险 未与关键岗位（安全管理员等）签署岗位责任协议。**

建议与关键岗位（安全管理员等）签署岗位责任协议，明确岗位安全责任定义、协议的有效期限和责任人签字等内容。

**七、安全建设管理**

**（1）中风险 经核查，自行软件开发过程中未对恶意代码进行检测，无法保证软件安全性；**

建议软件开发过程中进行安全性测试，在软件安装前对恶意代码进行检测等。

**（2）中风险 系统未进行上线前的安全性测试，未出具相关安全测试报告。**

建议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，要求在系统建设验收阶段委托第三方进行安全测试，安全测试应包括密码应用安全性测试等。

目录

[网络安全等级测评基本信息表 I](#_Toc99883977)

[声明 II](#_Toc99883978)

[等级测评结论 III](#_Toc99883979)

[等级测评结论扩展表（云计算安全） IV](#_Toc99883980)

[总体评价 VI](#_Toc99883981)

[主要安全问题及整改建议 XV](#_Toc99883982)

[目录 XX](#_Toc99883983)

[1 测评项目概述 1](#_Toc99883984)

[1.1 测评目的 1](#_Toc99883985)

[1.2 测评依据 1](#_Toc99883986)

[1.3 测评过程 2](#_Toc99883987)

[1.4 报告分发范围 4](#_Toc99883988)

[2 被测对象描述 5](#_Toc99883989)

[2.1 被测对象概述 5](#_Toc99883990)

[2.1.1 定级结果 5](#_Toc99883991)

[2.1.2 业务和采用的技术 5](#_Toc99883992)

[2.1.3 网络结构 6](#_Toc99883993)

[2.2 测评指标 8](#_Toc99883994)

[2.2.1 安全通用要求指标 8](#_Toc99883995)

[2.2.2 安全扩展要求指标 11](#_Toc99883996)

[2.2.3 其他安全要求指标 11](#_Toc99883997)

[2.2.4 不适用安全要求指标 12](#_Toc99883998)

[2.3 测评对象 19](#_Toc99883999)

[2.3.1 测评对象选择方法 19](#_Toc99884000)

[2.3.2 测评对象选择结果 20](#_Toc99884001)

[3 单项测评结果分析 25](#_Toc99884002)

[3.1 安全物理环境 25](#_Toc99884003)

[3.1.1 已有安全控制措施汇总分析 25](#_Toc99884004)

[3.1.2 主要安全问题汇总分析 25](#_Toc99884005)

[3.2 安全通信网络 25](#_Toc99884006)

[3.2.1 已有安全控制措施汇总分析 25](#_Toc99884007)

[3.2.2 主要安全问题汇总分析 26](#_Toc99884008)

[3.3 安全区域边界 26](#_Toc99884009)

[3.3.1 已有安全控制措施汇总分析 26](#_Toc99884010)

[3.3.2 主要安全问题汇总分析 28](#_Toc99884011)

[3.4 安全计算环境 29](#_Toc99884012)

[3.4.1 网络设备 29](#_Toc99884013)

[3.4.2 安全设备 29](#_Toc99884014)

[3.4.3 服务器和终端 31](#_Toc99884015)

[3.4.4 系统管理软件/平台 34](#_Toc99884016)

[3.4.5 业务应用系统/平台 36](#_Toc99884017)

[3.4.6 数据资源 39](#_Toc99884018)

[3.4.7 其他系统或设备 41](#_Toc99884019)

[3.5 安全管理中心 41](#_Toc99884020)

[3.5.1 已有安全控制措施汇总分析 41](#_Toc99884021)

[3.5.2 主要安全问题汇总分析 42](#_Toc99884022)

[3.6 安全管理制度 43](#_Toc99884023)

[3.6.1 已有安全控制措施汇总分析 43](#_Toc99884024)

[3.6.2 主要安全问题汇总分析 44](#_Toc99884025)

[3.7 安全管理机构 44](#_Toc99884026)

[3.7.1 已有安全控制措施汇总分析 44](#_Toc99884027)

[3.7.2 主要安全问题汇总分析 45](#_Toc99884028)

[3.8 安全管理人员 45](#_Toc99884029)

[3.8.1 已有安全控制措施汇总分析 45](#_Toc99884030)

[3.8.2 主要安全问题汇总分析 46](#_Toc99884031)

[3.9 安全建设管理 47](#_Toc99884032)

[3.9.1 已有安全控制措施汇总分析 47](#_Toc99884033)

[3.9.2 主要安全问题汇总分析 48](#_Toc99884034)

[3.10 安全运维管理 48](#_Toc99884035)

[3.10.1 已有安全控制措施汇总分析 48](#_Toc99884036)

[3.10.2 主要安全问题汇总分析 51](#_Toc99884037)

[3.11 其他安全要求指标 51](#_Toc99884038)

[3.11.1 已有安全控制措施汇总分析 51](#_Toc99884039)

[3.11.2 主要安全问题汇总分析 51](#_Toc99884040)

[3.12 验证测试 51](#_Toc99884041)

[3.12.1 漏洞扫描 51](#_Toc99884042)

[3.12.2 渗透测试 55](#_Toc99884043)

[3.13 单项测评小结 57](#_Toc99884044)

[3.13.1 控制点符合情况汇总 57](#_Toc99884045)

[3.13.2 安全问题汇总 60](#_Toc99884046)

[4 整体测评 66](#_Toc99884047)

[4.1 安全控制点间安全测评 66](#_Toc99884048)

[4.2 区域间安全测评 66](#_Toc99884049)

[4.3 整体测评结果汇总 68](#_Toc99884050)

[5 安全问题风险分析 71](#_Toc99884051)

[6 等级测评结论 79](#_Toc99884052)

[7 安全问题整改建议 81](#_Toc99884053)

[附录A 被测对象资产 86](#_Toc99884054)

[A.1 物理机房 86](#_Toc99884055)

[A.2 网络设备 86](#_Toc99884056)

[A.3 安全设备 86](#_Toc99884057)

[A.4 服务器/存储设备 87](#_Toc99884058)

[A.5 终端设备 88](#_Toc99884059)

[A.6 其他系统或设备 88](#_Toc99884060)

[A.7 系统管理软件/平台 88](#_Toc99884061)

[A.8 业务应用系统/平台 88](#_Toc99884062)

[A.9 数据资源 89](#_Toc99884063)

[A.10 密码产品 89](#_Toc99884064)

[A.11 安全相关人员 90](#_Toc99884065)

[A.12 安全管理文档 90](#_Toc99884066)

[附录B 上次测评问题整改情况说明 92](#_Toc99884067)

[附录C 单项测评结果汇总 94](#_Toc99884068)

[C.1 安全通信网络 94](#_Toc99884069)

[C.2 安全区域边界 94](#_Toc99884070)

[C.3 安全计算环境 95](#_Toc99884071)

[C.3.1 安全设备 95](#_Toc99884072)

[C.3.2 服务器和终端 97](#_Toc99884073)

[C.3.3 系统管理软件/平台 99](#_Toc99884074)

[C.3.4 业务应用系统/平台 100](#_Toc99884075)

[C.3.5 数据资源 102](#_Toc99884076)

[C.4 安全管理中心 103](#_Toc99884077)

[C.5 安全管理制度 104](#_Toc99884078)

[C.6 安全管理机构 104](#_Toc99884079)

[C.7 安全管理人员 104](#_Toc99884080)

[C.8 安全建设管理 105](#_Toc99884081)

[C.9 安全运维管理 105](#_Toc99884082)

[附录D 单项测评结果记录 107](#_Toc99884083)

[D.1 安全通信网络 107](#_Toc99884084)

[D.1.1 安全通用要求部分 107](#_Toc99884085)

[D.1.2 云计算安全扩展要求部分 109](#_Toc99884086)

[D.2 安全区域边界 110](#_Toc99884087)

[D.2.1 安全通用要求部分 110](#_Toc99884088)

[D.2.2 云计算安全扩展要求部分 116](#_Toc99884089)

[D.3 安全计算环境 119](#_Toc99884090)

[D.3.1 安全通用要求部分 119](#_Toc99884091)

[D.3.2 云计算安全扩展要求部分 192](#_Toc99884092)

[D.4 安全管理中心 195](#_Toc99884093)

[D.4.1 安全通用要求部分 195](#_Toc99884094)

[D.4.2 云计算安全扩展要求部分 198](#_Toc99884095)

[D.5 安全管理制度 199](#_Toc99884096)

[D.5.1 安全通用要求部分 199](#_Toc99884097)

[D.6 安全管理机构 201](#_Toc99884098)

[D.6.1 安全通用要求部分 201](#_Toc99884099)

[D.7 安全管理人员 204](#_Toc99884100)

[D.7.1 安全通用要求部分 204](#_Toc99884101)

[D.8 安全建设管理 207](#_Toc99884102)

[D.8.1 安全通用要求部分 207](#_Toc99884103)

[D.8.2 云计算安全扩展要求部分 213](#_Toc99884104)

[D.9 安全运维管理 215](#_Toc99884105)

[D.9.1 安全通用要求部分 215](#_Toc99884106)

[D.9.2 云计算安全扩展要求部分 226](#_Toc99884107)

[附录E 漏洞扫描结果记录 227](#_Toc99884108)

[附录F 渗透测试结果记录 229](#_Toc99884109)

[F.1 SanyMall 客户云商城系统存在Sql注入漏洞安全问题 233](#_Toc99884110)

[F.2 SanyMall 客户云商城系统存在存储型跨站漏洞安全问题 235](#_Toc99884111)

[F.3 SanyMall 客户云商城系统存在敏感信息泄露漏洞安全问题 236](#_Toc99884112)

[附录G 回归测试 237](#_Toc99884113)

[G.1 SanyMall 客户云商城系统存在Sql注入漏洞安全问题 237](#_Toc99884114)

[G.2 SanyMall 客户云商城系统存在存储型跨站漏洞安全问题 237](#_Toc99884115)

[附录H 腾讯云采购框架协议 239](#_Toc99884116)

[附录I 威胁列表 244](#_Toc99884117)

[附录J 云计算平台测评及整改情况 245](#_Toc99884118)

# 测评项目概述

## 测评目的

安全等级测评的目的是通过对目标系统在安全技术及管理方面的测评，对目标系统的安全技术状态及安全管理状况做出初步判断，给出目标系统在安全技术及安全管理方面与其相应安全等级保护要求之间的差距。测评结论作为委托方进一步完善系统安全策略及安全技术防护措施依据。

为进一步提高信息系统的保障能力，根据《信息安全等级保护管理办法》（公通字2007【43】号）的精神，三一集团有限公司委托湖南省金盾信息安全等级保护评估中心有限公司（认证证书编号：SC202127130010155）对三一集团有限公司SanyMall 客户云商城系统实施等级测评，以期发现信息系统和等级保护标准的差距以及存在的安全隐患，为后续的安全整改工作提供参考依据。

## 测评依据

测评过程中主要依据的标准：

1. GB/T 22239—2019 《信息安全技术 网络安全等级保护基本要求》（以下简称《基本要求》）
2. GB/T 28448—2019 《信息安全技术 网络安全等级保护测评要求》

测评过程中还参考以下文件和标准：

1. GB17859—1999《计算机信息系统 安全等级保护划分准则》
2. GB/T 28449—2018《信息安全技术 网络安全等级保护测评过程指南》
3. GB/T 20984—2007《信息安全技术 信息安全风险评估规范》
4. T/ISEAA 001—2020《网络安全等级保护测评高风险判定指引》
5. 《三一集团有限公司网络安全等级测评合同》

## 测评过程

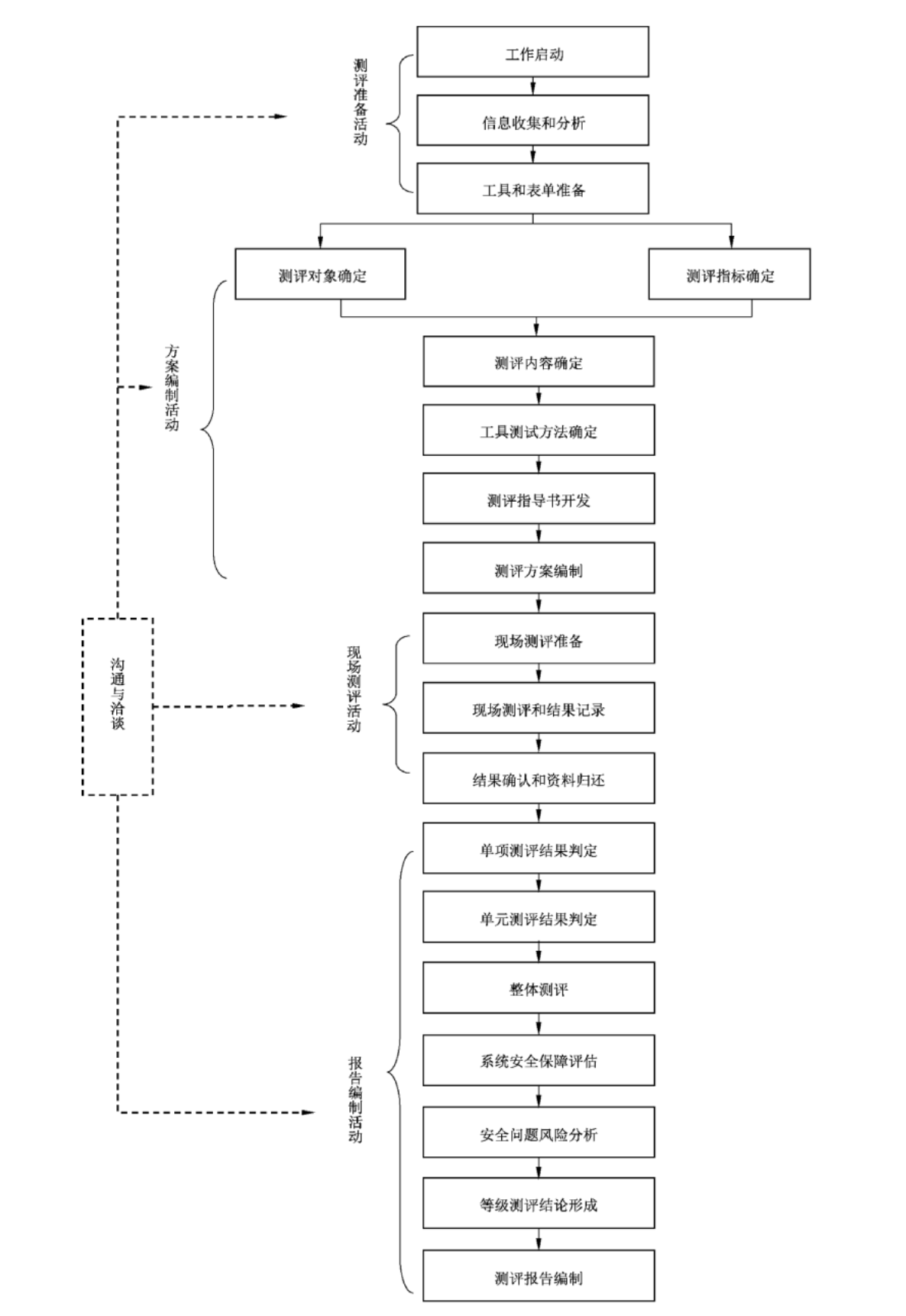


图1-1 等级保护测评工作流程图

本次等级测评分为四个过程：测评准备阶段、方案编制阶段、现场测评阶段、报告编制阶段。具体如图 1-1 所示。其中，各阶段的时间安排如下：

1. **测评准备阶段：2**021年11月29日至2021年11月30日，湖南金盾测评项目组通过电话、邮件等方式进行对项目详细调研，明确此次等级测评工作的测评对象和工作计划，并完成《信息系统基本情况调查表》。
2. **方案编制阶段：**2021年12月01日至2021年12月04日，湖南金盾测评项目组依据SanyMall 客户云商城系统的安全保护等级及调研情况，对测评对象、测评指标、测评内容、工具测试方法的确定，结合调研情况完成测评指导书开发、测评方案编制工作。
3. **现场测评阶段：**2021年12月22日至2021年12月28日开展现场测评工作，其中：

2021年12月22日，湖南金盾测评项目组与三一集团有限公司召开现场测评启动会，双方就测评方案达成一致，明确现场测评计划和配合人员，确认被测系统数据备份情况，获得三一集团有限公司的现场测评、验证测试书面授权。

2021年12月22日，湖南金盾测评项目组依据测评标准和作业指导书正式开展测评工作，通过访谈、文档审查、配置检查、工具测试、实地察看等方法获取测评结果和证据，形成结果记录，并与委托单位对结果记录进行了确认。

2021年12月28日，湖南金盾测评项目组完成了现场测评工作，向三一集团有限公司说明了系统存在的安全问题，并归还借阅的文档资料。

4、**报告编制阶段：**2021年12月29日至2021年12月30日，湖南金盾测评项目组对现场测评的单项测评结果和单元测评结果进行判定，并进行整体测评分析、风险分析，找出了SanyMall 客户云商城系统存在的主要问题和安全风险，形成等级测评结论，并针对发现的安全问题和风险提出了安全整改建议，编制完成等级测评报告。

## 报告分发范围

等级测评报告正本一式3份，其中三一集团有限公司1份，湖南省金盾信息安全等级保护评估中心有限公司1份，受理备案公安机关1份。

# 被测对象描述

## 被测对象概述

### 定级结果

**表 2**‑**1定级结果**

| **被测对象名称** | **安全保护等级** | **业务信息 安全保护等级** | **系统服务 安全保护等级** |
| --- | --- | --- | --- |
| SanyMall 客户云商城系统 | 第三级 | 第三级 | 第三级 |

### 业务和采用的技术

三一集团有限公司SanyMall 客户云商城系统是三一集团商城系统，主要提供商城在线展示和交易功能，以最终用户为主要对象，提供三一整机、三一机械配件等系列终端产品和服务；致力于为客户提供方便快捷的产品选购渠道，完善智慧管理云平台生态圈。

该系统为云计算系统，部署在腾讯公有云IaaS服务平台，涉及云计算新型技术。

### 网络结构



图 2-1 SanyMall 客户云商城系统网络拓扑图

如图2-1三一集团有限公司SanyMall客户云商城系统网络拓扑结构示意图所示，被测系统三一集团有限公司SanyMall客户云商城系统为云服务客户业务应用系统，云服务商为腾讯云，业务系统部署使用的云服务模式为基础设施即服务(IaaS)。SanyMall客户云商城系统使用腾讯云服务器作为系统应用服务器及腾讯云Mysql数据库作为系统数据库，其基础设施与网络架构及网络设备均采用腾讯公有云Iaas服务平台服务。同时，腾讯公有云Iaas服务平台为云租户分配有专门的VPC网络区域，不同VPC之间通过Vxlan协议实现的隔离及访问控制；同时，腾讯公有云Iaas服务平台为被测系统SanyMall 客户云商城系统提供了Web应用防火墙、云审计、主机安全等相关安全产品或服务，确保应用系统安全、稳定运行。SanyMall 客户云商城系统的网络结构主要包括： 办公区、互联网层、安全管理层和应用与数据层。   
 **1）办公区：**办公区主要由用户电脑和移动终端组成，为用户使用该平台提供接入服务。

**2）互联网区：**互联网层主要包括各大运营商的网络接入，建立用户和服务器之间的连接。

**3）安全管理区：**安全管理层主要包括腾讯云的安全服务和运维人员管理台， 主要由Web应用防火墙、云审计云产品、主机安全云产品和腾讯云控制台等组成，为应用系统提供安全服务和安全管理功能。

**4）应用与数据区：**由腾讯云部署的服务器和数据库组成，为该平台提供服务支撑和数据交换、数据存储服务。

## 测评指标

### 安全通用要求指标

**表 2‑2安全通用要求指标**

| **安全类** | **控制点** | **测评项数** |
| --- | --- | --- |
| 安全物理环境 | 物理位置选择 | 2 |
| 物理访问控制 | 1 |
| 防盗窃和防破坏 | 3 |
| 防雷击 | 2 |
| 防火 | 3 |
| 防水和防潮 | 3 |
| 防静电 | 2 |
| 温湿度控制 | 1 |
| 电力供应 | 3 |
| 电磁防护 | 2 |
| 安全通信网络 | 网络架构 | 5 |
| 通信传输 | 2 |
| 可信验证 | 1 |
| 安全区域边界 | 边界防护 | 4 |
| 访问控制 | 5 |
| 入侵防范 | 4 |
| 恶意代码和垃圾邮件防范 | 2 |
| 安全审计 | 4 |
| 可信验证 | 1 |
| 安全计算环境 | 身份鉴别 | 4 |
| 访问控制 | 7 |
| 安全审计 | 4 |
| 入侵防范 | 6 |
| 恶意代码防范 | 1 |
| 可信验证 | 1 |
| 数据完整性 | 2 |
| 数据保密性 | 2 |
| 数据备份恢复 | 3 |
| 剩余信息保护 | 2 |
| 个人信息保护 | 2 |
| 安全管理中心 | 系统管理 | 2 |
| 审计管理 | 2 |
| 安全管理 | 2 |
| 集中管控 | 6 |
| 安全管理制度 | 安全策略 | 1 |
| 管理制度 | 3 |
| 制定和发布 | 2 |
| 评审和修订 | 1 |
| 安全管理机构 | 岗位设置 | 3 |
| 人员配备 | 2 |
| 授权和审批 | 3 |
| 沟通和合作 | 3 |
| 审核和检查 | 3 |
| 安全管理人员 | 人员录用 | 3 |
| 人员离岗 | 2 |
| 安全意识教育和培训 | 3 |
| 外部人员访问管理 | 4 |
| 安全建设管理 | 定级和备案 | 4 |
| 安全方案设计 | 3 |
| 产品采购和使用 | 3 |
| 自行软件开发 | 7 |
| 外包软件开发 | 3 |
| 工程实施 | 3 |
| 测试验收 | 2 |
| 系统交付 | 3 |
| 等级测评 | 3 |
| 服务供应商选择 | 3 |
| 安全运维管理 | 环境管理 | 3 |
| 资产管理 | 3 |
| 介质管理 | 2 |
| 设备维护管理 | 4 |
| 漏洞和风险管理 | 2 |
| 网络和系统安全管理 | 10 |
| 恶意代码防范管理 | 2 |
| 配置管理 | 2 |
| 密码管理 | 2 |
| 变更管理 | 3 |
| 备份与恢复管理 | 3 |
| 安全事件处置 | 4 |
| 应急预案管理 | 4 |
| 外包运维管理 | 4 |
| **安全通用要求指标数量统计** | | 211 |

### 安全扩展要求指标

**表 2‑3 安全扩展要求指标**

| **扩展类型** | **安全类** | **控制点** | **测评项数** |
| --- | --- | --- | --- |
| **云计算安全扩展要求** | | | |
| 云计算安全扩展要求 | 安全物理环境 | 基础设施位置 | 1 |
| 安全通信网络 | 网络架构 | 5 |
| 安全区域边界 | 访问控制 | 2 |
| 入侵防范 | 4 |
| 安全审计 | 2 |
| 安全计算环境 | 身份鉴别 | 1 |
| 访问控制 | 2 |
| 入侵防范 | 3 |
| 镜像和快照保护 | 3 |
| 数据完整性和保密性 | 4 |
| 数据备份恢复 | 4 |
| 剩余信息保护 | 2 |
| 安全管理中心 | 集中管控 | 4 |
| 安全建设管理 | 云服务商选择 | 5 |
| 供应链管理 | 3 |
| 安全运维管理 | 云计算环境管理 | 1 |
| **安全扩展要求指标数量统计** | | | 46 |

### 其他安全要求指标

SanyMall 客户云商城系统不涉及其他安全要求指标。

### 不适用安全要求指标

**表 2‑4 不适用安全要求指标**

| **安全类** | **控制点** | **不适用项** | **不适用原因** |
| --- | --- | --- | --- |
| **安全通用要求** | | | |
| 安全物理环境 | 物理位置选择 | a）机房场地应选择在具有防震、防风和防雨等能力的建筑内； | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及安全物理环境测评对象。 |
| b）机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。 | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及安全物理环境测评对象。 |
| 物理访问控制 | a）机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。 | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及安全物理环境测评对象。 |
| 防盗窃和防破坏 | a）应将设备或主要部件进行固定，并设置明显的不易除去的标识； | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及安全物理环境测评对象。 |
| b）应将通信线缆铺设在隐蔽安全处； | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及安全物理环境测评对象。 |
| c）应设置机房防盗报警系统或设置有专人值守的视频监控系统。 | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及安全物理环境测评对象。 |
| 防雷击 | a）应将各类机柜、设施和设备等通过接地系统安全接地； | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及安全物理环境测评对象。 |
| b）应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。 | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及安全物理环境测评对象。 |
| 防火 | a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火； | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及安全物理环境测评对象。 |
| b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料； | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及安全物理环境测评对象。 |
| c）应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。 | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及安全物理环境测评对象。 |
| 防水和防潮 | a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透； | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及安全物理环境测评对象。 |
| b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透； | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及安全物理环境测评对象。 |
| c）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。 | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及安全物理环境测评对象。 |
| 防静电 | a）应采用防静电地板或地面并采用必要的接地防静电措施； | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及安全物理环境测评对象。 |
| b）应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。 | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及安全物理环境测评对象。 |
| 温湿度控制 | a）应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。 | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及安全物理环境测评对象。 |
| 电力供应 | a）应在机房供电线路上配置稳压器和过电压防护设备； | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及安全物理环境测评对象。 |
| b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求； | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及安全物理环境测评对象。 |
| c）应设置冗余或并行的电力电缆线路为计算机系统供电。 | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及安全物理环境测评对象。 |
| 电磁防护 | a）电源线和通信线缆应隔离铺设，避免互相干扰； | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及安全物理环境测评对象。 |
| b）应对关键设备实施电磁屏蔽。 | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及安全物理环境测评对象。 |
| 安全区域边界 | 边界防护 | b）应能够对非授权设备私自联到内部网络的行为进行检查或限制； | 经核查，被测系统部署在腾讯公有云IaaS服务平台，为云服务客户业务应用系统，该项不适用。 |
| c）应能够对内部用户非授权联到外部网络的行为进行检查或限制； | 经核查，被测系统部署在腾讯公有云IaaS服务平台，为云服务客户业务应用系统，该项不适用。 |
| d）应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。 | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及部署无线网络，无无线用户，该项不适用。 |
| 恶意代码和垃圾邮件防范 | b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。 | 经核查，该应用系统不涉及邮件系统，故该项不适用。 |
| 安全建设管理 | 外包软件开发 | a）应在软件交付前检测其中可能存在的恶意代码； | 经访谈，被测系统为集团自行开发，未涉及外包软件开发。 |
| b）应保证开发单位提供软件设计文档和使用指南； | 经访谈，被测系统为集团自行开发，未涉及外包软件开发。 |
| c）应保证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。 | 经访谈，被测系统为集团自行开发，未涉及外包软件开发。 |
| 安全运维管理 | 环境管理 | a）应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理； | 系统部署于腾讯公有云IaaS服务平台，机房由云平台侧负责管理。 |
| b）应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定； | 系统部署于腾讯公有云IaaS服务平台，机房由云平台侧负责管理。 |
| 设备维护管理 | a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理； | 系统部署于腾讯公有云IaaS服务平台，机房各种设备、线路等设施由云平台侧负责管理。 |
| 外包运维管理 | a）应确保外包运维服务商的选择符合国家的有关规定； | 系统部署于腾讯公有云IaaS服务平台，系统不涉及外包运维，此项不适用。 |
| b）应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容； | 系统部署于腾讯公有云IaaS服务平台，系统不涉及外包运维，此项不适用。 |
| c）应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确； | 系统部署于腾讯公有云IaaS服务平台，系统不涉及外包运维，此项不适用。 |
| d）应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对IT 基础设施中断服务的应急保障要求等。 | 系统部署于腾讯公有云IaaS服务平台，系统不涉及外包运维，此项不适用。 |
| **云计算安全扩展要求** | | | |
| 安全物理环境 | 基础设施位置 | a）应保证云计算基础设施位于中国境内。 | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及安全物理环境测评对象。 |
| 安全通信网络 | 网络架构 | b）应实现不同云服务客户虚拟网络之间的隔离； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 |
| c）应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 |
| d）应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 |
| e）应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务。 | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 |
| 安全区域边界 | 入侵防范 | a）应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 |
| 安全审计 | b）应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。 | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 |
| 安全计算环境 | 访问控制 | a）应保证当虚拟机迁移时，访问控制策略随其迁移； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 |
| b）应允许云服务客户设置不同虚拟机之间的访问控制策略。 | 被测系统部署在腾讯公有云IaaS服务平台，为云服务客户业务应用系统，该项不适用。 |
| 入侵防范 | a）应能检测虚拟机之间的资源隔离失效，并进行告警； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 |
| 镜像和快照保护 | a）应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 |
| b）应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 |
| c）应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 |
| 数据完整性和保密性 | b）应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 |
| c）应使用校验码或密码技术确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 |
| d）应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。 | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 |
| 数据备份恢复 | b）应提供查询云服务客户数据及备份存储位置的能力； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 |
| c）云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 |
| d）应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。 | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 |
| 剩余信息保护 | a）应保证虚拟机所使用的内存和存储空间回收时得到完全清除； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 |
| b）云服务客户删除业务应用数据时，云计算平台应将云存储在所有副本删除。 | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 |
| 安全管理中心 | 集中管控 | a）应能对物理资源和虚拟资源按照策略做统一管理调度与分配； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 |
| b）应保证云计算平台管理流量与云服务客户业务流量分离； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 |
| 安全运维管理 | 云计算环境管理 | a）云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。 | 经核查，被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 |
| **不适用指标数** | | | 60 |

## 测评对象

### 测评对象选择方法

SanyMall 客户云商城系统定级为三级，依据GB/T 28449-2018中测评对象的确定原则和方法，三级系统等级测评的测评对象种类上基本覆盖、数量进行抽样，重点抽查主要的设备、设施、人员和文档等。本次等级测评的测评对象在抽样时主要考虑以下几个方面：

1. 主机房（包括其环境、设备和设施等）和部分辅机房，应将放置了服务于定级对象的布局（包括整体）或对定级对象的布局（包括整体）安全性起重要作用的设备、设施的辅机房选取作为测评对象；
2. 存储被测定级对象重要数据的介质的存放环境；
3. 办公场地；
4. 整个系统的网络拓扑结构；
5. 安全设备，包括防火墙、入侵检测设备和防病毒网关等；
6. 边界网络设备（可能会包含安全设备)，包括路由器、防火墙，认证网关和边界接入设备（如楼层交换机）等；
7. 对整个定级对象或其局部的安全性起作用的网络互联设备，如核心交换机、汇聚交换机、路由器等；
8. 承载被测定级对象主要业务或数据的服务器（包括其操作系统和数据库）；
9. 管理终端和主要应用系统终端；
10. 能够完成被测定级对象不同业务使命的业务应用系统；
11. 业务备份系统；
12. 信息安全主管人员、各方面的负责人员、具体负责安全管理的当事人、业务负责人；
13. 涉及到定级对象安全的所有管理制度和记录。

抽样原则：在本级定级对象测评时，定级对象中配置相同的安全设备、边界网络设备、网络互联设备、服务器、终端以及备份设备，每类应至少抽查两台作为测评对象。

### 测评对象选择结果

#### 物理机房

被测系统三一集团有限公司SanyMall客户云商城系统为云服务客户业务应用系统，基础设施与网络环境由腾讯公有云IaaS服务平台提供，不涉及物理机房测评对象。

#### 网络设备

被测系统三一集团有限公司SanyMall客户云商城系统为云服务客户业务应用系统，基础设施与网络环境由腾讯公有云IaaS服务平台提供，不涉及网络设备测评对象。

#### 安全设备

**表 2‑5 安全设备**

| **序号** | **设备名称** | **虚拟**  **设备** | **系统及版本** | **品牌及型号** | **用途** | **重要程度** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | Web应用防火墙云产品 | 否 | 企业版 | 腾讯云 | 为云租户Web应用提供安全防护。 | 重要 |
| 2 | 主机安全云产品 | 否 | 专业版 | 腾讯云 | 为云租户主机提供入侵检测、漏洞管理、基线管理、高级防御等安全功能。 | 重要 |
| 3 | 云审计云产品 | 否 | / | 腾讯云 | 对云产品（Web应用防火墙云产品、主机安全云产品等）日志进行集中统一收集保存与审计分析等管理。 | 重要 |

#### 服务器/存储设备

**表 2‑6 服务器/存储设备**

| **序号** | **设备名称** | **所属业务应用系统/平台** | **虚拟**  **设备** | **操作系统及版本** | **数据库管理系统及版本** | **中间件及版本** | **重要**  **程度** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 应用服务器-1 | SanyMall 客户云商城系统 | 是 | CentOS Linux 7.3 | -- | Nginx 1.14.2 | 关键 |
| 2 | 应用服务器-2 | 是 | CentOS Linux 7.3 | -- | Nginx 1.14.2 | 关键 |

#### 终端设备

**表 2‑7 终端设备**

| **序号** | **设备名称** | **虚拟**  **设备** | **操作系统及版本** | **用途** | **重要程度** |
| --- | --- | --- | --- | --- | --- |
| 1 | 办公运维管理终端 | 否 | Windows10企业版 | 用于日常办公及运维管理等。 | 重要 |

#### 其他设备

SanyMall 客户云商城系统不涉及其他设备。

#### 系统管理软件/平台

**表 2‑8 系统管理软件/平台**

| **序号** | **系统管理软件/平台名称** | **主要功能** | **版本** | **所在设备名称** | **重要程度** |
| --- | --- | --- | --- | --- | --- |
| 1 | 腾讯云控制台 | 统一查看和管理腾讯云产品及服务的平台。 | -- | 腾讯云 | 重要 |
| 2 | 腾讯云数据库 | 数据存储 | MYSql 5.6 | 腾讯云 | 关键 |
| 3 | 中间件-1 | 网页发布 | Nginx 1.14.2 | 应用服务器-1 | 关键 |
| 4 | 中间件-2 | 网页发布 | Nginx 1.14.2 | 应用服务器-2 | 关键 |

#### 业务应用系统/平台

**表 2‑9 业务应用系统/平台**

| **序号** | **业务应用系统/平台名称** | **主要功能** | **业务应用软件及版本** | **开发厂商** | **重要程度** |
| --- | --- | --- | --- | --- | --- |
| 1 | SanyMall 客户云商城系统 | SanyMall 客户云商城系统是三一集团商城系统，主要提供商城在线展示和交易功能，以最终用户为主要对象，提供三一整机、三一机械配件等系列终端产品和服务；致力于为客户提供方便快捷的产品选购渠道，完善智慧管理云平台生态圈。 | Ecstore V5.0.4 | 三一集团有限公司 | 关键 |

#### 数据资源

**表 2‑10数据资源**

| **序号** | **数据类别** | **所属业务应用** | **安全防护需求** | **重要程度** |
| --- | --- | --- | --- | --- |
| 1 | 业务数据  （订单、交易明细等业务数据） | SanyMall 客户云商城系统 | 保密性：高  完整性：高 | 关键 |
| 2 | 个人信息数据  （用户名、手机号、邮箱、密码等个人信息数据） | 保密性：高  完整性：高 | 关键 |

#### 安全相关人员

**表 2‑11 安全相关人员**

| **序号** | **姓名** | **岗位/角色** | **联系方式** | **所属单位** |
| --- | --- | --- | --- | --- |
| 1 | 孟翔巍 | 安全主管 | 17770925562 | 三一集团有限公司 |
| 2 | 刘清香 | 安全管理员 | 15273150727 | 三一集团有限公司 |
| 3 | 谭智敏 | 网络管理员 | 17607310632 | 三一集团有限公司 |
| 4 | 雷杰 | 系统管理员 | 13808415415 | 三一集团有限公司 |
| 5 | 黎勃利 | 审计管理员 | 15274464567 | 三一集团有限公司 |
| 6 | 李三林 | 机房管理员 | 18073655130 | 三一集团有限公司 |

#### 安全管理文档

**表 2‑12 安全管理文档**

| **序号** | **文档名称** | **主要内容** |
| --- | --- | --- |
| 1 | 《三一重工信息安全总体方针和策略》 | 主要涉及提高集团网络信息安全管理工作的水平，切实保障信息化健康发展，建立健全安全管理组织机构而发布的信息安全总体方针和策略。 |
| 2 | 《三一重工信息系统访问控制规定》 | 主要涉及严格控制信息系统的合法访问权限，保证信息系统的安全。 |
| 3 | 《三一重工数据安全管理制度》 | 主要涉及对数据资产的管理要求，规范员工操作行为，保障公司数据在创建、采集、存储、访问、下载、分发、流转、打印等全生命周期得到合理保护和共享。 |
| 4 | 《三一重工防病毒系统管理规范》 | 主要涉及通过制订防病毒系统管理规范，完善防病毒系统架构、标准化防病毒系统的管理以达到同意策略管理、提高病毒定义更新和加强系统安全性的目的。 |
| 5 | 《三一重工数据中心管理规定》 | 主要涉及规范数据中心的管理，确保数据中心所有设备的正常运行，确保应用系统的连续性。 |
| 6 | 《三一重工员工信息安全管理制度》 | 主要明确员工在司使用公司IT资源时的信息安全行为规范，提升员工信息安全意识，合规使用公司信息系统资源，保护公司信息资产。 |
| 7 | 《三一重工信息系统业务连续性管理流程》 | 主要涉及通过制订业务连续性计划，规范业务连续性文档发布过程，规范业务连续性演练工作，检验备份恢复策略是否有效，对演练中发现的问题进行改善，从而增强在面对风险是的处置能力。 |
| 8 | 《三一重工互联网系统发布管理制度》 | 主要涉及规范集团数据中心信息系统互联网发布安全标准，提升全体IT人员互联网信息系统安全意识，引导IT人员安全合规地建设使用互联网信息系统，保护公司信息资产。 |
| 9 | 《三一重工信息系统版本准入规范》 | 主要涉及三一集团信息系统版本管理，保证基础类软件使用安全可靠的版本，信息系统软件版本的选型与维护，明确各类软件使用版本准入要求。 |
| 10 | 《三一重工IT终端安全管理制度》 | 主要涉及规范三一集团终端与服务器的安全管控，确保集团内终端安全。 |
| 11 | 《三一重工信息安全事件处理与应急管理制度》 | 主要涉及加强三一集团信息安全事件管理，提升信息安全事件预防、响应、分析、处置及反馈的效率，降低信息安全事件造成的损失。 |
| 12 | 《三一重工信息系统权限管理制度》 | 主要涉及规范信息系统各类用户的权限管理，防止信息系统被非法授权、授权不当。规范IT协助处理业务数据的操作流程，保证IT协助处理业务数据结果的准确性、安全性。 |
| 13 | 《三一重工变更管理制度》 | 主要涉及规范IT系统运营环境变更行为，降低系统故障风险，保障系统可用率。 |
| 14 | 《三一重工备份管理制度》 | 主要涉及保护公司的业务数据免受意外损坏，确保业务的连续性。 |
| 15 | 《三一重工第三方人员信息安全管理规定》 | 主要涉及确保需接入公司IT资源的第三方人员安全、有效使用公司信息系统等资源，有效保护公司机密信息。 |
| 16 | 《三一重工软件开发管理规范》 | 主要涉及规范了软件开发相关人员和流程管控等内容。 |

# 单项测评结果分析

单项测评内容包括“2.2.1安全通用要求指标”、“2.2.2安全扩展要求指标”和“2.2.3其他安全要求指标”中涉及的安全类，由已有安全控制措施汇总分析和主要安全问题汇总分析两部分构成，单项测评结果汇总、单项测评结果记录参见报告附录。

## 安全物理环境

### 已有安全控制措施汇总分析

被测系统三一集团有限公司SanyMall客户云商城系统为云服务客户业务应用系统，基础设施与网络环境采用腾讯公有云IaaS服务平台服务，本次测评工作中，被测评对象未涉及安全物理环境要求指标。

### 主要安全问题汇总分析

被测系统三一集团有限公司SanyMall客户云商城系统为云服务客户业务应用系统，基础设施与网络环境采用腾讯公有云IaaS服务平台服务，本次测评工作中，被测评对象未涉及安全物理环境要求指标。

## 安全通信网络

### 已有安全控制措施汇总分析

针对安全通信网络方面安全测评结果中存在的符合项进行汇总和分析，安全通信网络方面基本落实《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）的相关安全防护要求，总体安全保护措施相对较完善，具体措施如下：

在网络架构方面，被测系统部署于腾讯云上，在腾讯云上分配有专门的VPC，未出现由于设备性能存在瓶颈，而导致网络拥堵、阻断等情况；同时，腾讯云关键网络设备和线路已实现硬件冗余和线路冗余及云计算平台承载的业务系统等级不高于云计算平台自身的安全保护等级等。

在通信传输方面，在管理网络系统云服务器及云安全产品均通过腾讯云企业子账号控制台进行管理访问，采用HTTPS协议登录腾讯云控制台，能够保证通信过程中数据的完整性及保密性等。

### 主要安全问题汇总分析

安全通信网络存在的安全问题有:

**（1）未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证**

通信设备不具有可信根芯片或硬件，未基于可信根对通信设备的系统引导程序、系统程序、重要配置参数等进行可信验证，涉及测评对象**安全通信网络**。

## 安全区域边界

### 已有安全控制措施汇总分析

针对安全区域边界方面安全测评结果中存在的符合项进行汇总和分析，安全区域边界方面基本落实《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）的相关安全防护要求，总体安全保护措施相对较完善，具体措施如下：

在边界防护方面，被测系统部署在腾讯公有云IaaS服务平台，为云租户分配有专门的VPC网络区域，在VPC网络边界部署了高级版云防火墙访问控制设备，并配置了相应访问控制策略，对VPC边界的流量进行控制，实现VPC之间的隔离；云租户具有云防火墙管理权限，可根据业务需要或所发生的安全事件及时调整访问控制策略等。

在访问控制方面，被测系统部署在腾讯公有云IaaS服务平台，为云租户分配有专门的VPC网络区域，在VPC网络边界通过腾讯云安全组件云服务进行访问控制，有根据被测系统实际业务配置了相应出、入站规则。如：针对ping服务、系统业务访问端口、SSH(22)远程访问服务等通信设置了相应访问控制规则，默认情况下除允许通信外拒绝所有通信；同时，为被测系统提供部署了Web应用防火墙云产品，且根据企业的需求已配置了安全策略；如已设置Web应用攻击防护、CC防护及腾讯公有云IaaS服务平台在每个租户网络区域边界设置了访问控制，且该租户在边界处统一部署腾讯云安全组件云服务，设置访问控制规则，网络不存在其他非三级以外的网络区域边界等。

在入侵防范方面，腾讯公有云IaaS服务平台为被测系统提供部署了主机安全云产品、Web应用防火墙云产品，主机安全云产品实现对云上虚拟服务器主机全量日志分析，对进程异常行为、异常账户、敏感文件篡改、异常网络连接等入侵行为进行检测及分析；同时，检测云上虚拟服务器主机恶意攻击行为，对进程、网络异常等行为进行预警。Web应用防火墙实现对Web应用进防护，防御各类OWASP常见Web攻击并过滤海量恶意CC攻击，保障网站业务安全性与可用性。

在恶意代码及邮件防范方面，腾讯公有云IaaS服务平台为被测系统提供部署了主机安全云产品，通过主机安全云产品实现蠕虫病毒、勒索病毒、木马、网站后门等恶意代码的检测和隔离清除等。

在安全审计方面，系统部署于腾讯云，被测系统相关云产品（Web应用防火墙云产品、主机安全云产品、云服务器等）所有操作行为通过云审计云产品进行审计；同时，通过主机安全云产品、Web应用防火墙云产品实现对网络中发生的各类安全事件进行审计等。

### 主要安全问题汇总分析

安全区域边界存在的安全问题有:

**（1）未采取技术措施对新型网络攻击行为进行分析**

未购买部署抗APT、态势感知等可检测新型网络攻击行为的安全服务，涉及测评对象**虚拟网络边界**。

**（2）网络边界设备不具有可信根芯片或硬件，未基于可信根对通信设备的系统引导程序、系统程序、重要配置参数等进行可信验证**

1、网络边界设备不具有可信根芯片或硬件；2、未基于可信根对设备的系统引导程序、系统程序、重要配置参数等进行可信验证，涉及测评对象**虚拟网络边界**。

## 安全计算环境

### 网络设备

#### 已有安全控制措施汇总分析

被测系统三一集团有限公司SanyMall客户云商城系统为云服务客户业务应用系统，基础设施与网络环境采用腾讯公有云IaaS服务平台服务，本次测评工作中，本次测评工作中未涉及对网络设备对象测评。

#### 主要安全问题汇总分析

被测系统三一集团有限公司SanyMall客户云商城系统为云服务客户业务应用系统，基础设施与网络环境采用腾讯公有云IaaS服务平台服务，本次测评工作中，本次测评工作中未涉及对网络设备对象测评。

### 安全设备

#### 已有安全控制措施汇总分析

针对安全设备方面安全测评结果中存在的符合项进行汇总和分析，安全设备方面基本落实《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）的相关安全防护要求，总体安全保护措施相对较完善，具体措施如下：

在身份鉴别方面，被测系统相关云安全服务产品有设置提供身份标识和鉴别功能，用户口令均符合复杂性要求及被测系统相关云安全服务产品远程管理需要登录腾讯云的企业账号，在控制端中对其进行安全管理。腾讯云使用的是https协议来进行远程通信，可防止鉴别数据在网络传输的过程中被窃听等。

在访问控制方面，被测系统相关云安全服务产品已修改默认账户口令为强口令，禁用或删除了多余不需要账户等。

在安全审计方面，被测系统相关云安全服务产品设置开启了日志审计功能，能对重要用户行为和重要安全事件进行审计；且对日志记录进行了保护等。

在入侵防范方面，被测系统相关云安全服务产品关闭了不需要的系统服务和高危端口及限制了仅能通过腾讯云控制台进行访问控制等。

在数据完整性及数据保密性方面，被测系统相关云安全服务产品远程管理需要登录腾讯云的企业账号，在控制端中对其进行安全管理；腾讯云使用的是https协议来进行远程通信，传输过程加密，可保证重要数据在传输过程中的完整性及保密性等。

在数据备份恢复方面，腾讯云平台已针对云上安全产品的重要数据提供了本地备份与恢复及腾讯云的云安全产品基于分布式操作系统高可用架构集群部署，支持用于基于业务处理能力，按照需求动态调整资源，能保证系统的高可用性等。

#### 主要安全问题汇总分析

安全计算环境存在的安全问题有:

**（1）未启用登录失败处理功能**

被测系统相关安全产品未设置允许登录尝试次数、未设置锁定时间等策略，涉及测评对象**Web应用防火墙云产品，主机安全云产品，云审计云产品**。

**（3）未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证**

1、系统网络中的主要计算设备不具有可信根芯片或硬件；2、未基于可信根对设备的系统引导程序、系统程序、重要配置参数等进行可信验证，涉及测评对象**Web应用防火墙云产品，主机安全云产品，云审计云产品**。

**（3）未提供实现安全标记功能**

经核查，系统网络内的主要安全设备（Web应用防火墙云产品、主机安全云产品、云审计云产品等）未提供设置安全标记功能，涉及测评对象**Web应用防火墙云产品，主机安全云产品，云审计云产品**。

### 服务器和终端

#### 已有安全控制措施汇总分析

针对服务器和终端方面安全测评结果中存在的符合项进行汇总和分析，服务器和终端方面基本落实《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）的相关安全防护要求，总体安全保护措施相对较完善，具体措施如下：

在身份鉴别方面，被测系统相关云服务器及重要终端均有设置提供身份标识和鉴别功能，用户口令均符合复杂性要求及被测系统相关云服务器远程管理需要登录腾讯云的企业账号，在控制端中对其进行安全管理。腾讯云使用的是https协议来进行远程通信，可防止鉴别数据在网络传输的过程中被窃听等。

在访问控制方面，被测系统相关云服务器及重要终端已修改默认账户口令为强口令，禁用或删除了多余不需要账户等。

在安全审计方面，被测系统相关云服务器及重要终端均设置开启了日志审计功能，能对重要用户行为和重要安全事件进行审计；且对日志记录进行了保护等。

在入侵防范方面，被测系统相关云服务器关闭了不需要的系统服务和高危端口及云服务器操作系统均安装部署了已安装部署腾讯云主机安全云产品专业版，具备入侵防御功能，能够检测到对重要节点进行入侵的行为等。

在恶意代码防范方面，被测系统相关云服务器操作系统均部署了腾讯云主机安全云产品专业版，具备防恶意代码功能，能够及时识别入侵和病毒行为，并将其有效阻断。

在数据完整性及数据保密性方面，被测系统相关相关云服务器采用SSH加密协议连接通信，传输过程加密，可保证重要数据在传输过程中的完整性及保密性及服务器针对鉴别数据(用户口令)采用DES加密算法以密文形式保存，可保证鉴别数据存储过程中的保密性。

在数据备份恢复方面，针对被测系统云服务器操作系统重要数据(如：应用程序配置数据等)定期本地备份，一旦数据修改进行了更新，会即时备份；同时，已建立恢复测试机制，定期每半年对备份数据进行恢复测试验证及对被测系统服务器为腾讯云平台虚机，采用集群虚拟化部署，能保证系统的高可用性等。

#### 主要安全问题汇总分析

安全计算环境存在的安全问题有:

**（1）未采用两种或两种以上组合的鉴别技术**

被测系统相关重要终端（办公运维管理终端）操作系统采用用户名+口令一种鉴别技术对用户进行身份鉴别，未采用两种或以上组合进行鉴别，涉及测评对象**办公运维管理终端**。

**（2）未提供异地数据备份功能**

未提供异地备份措施，通过网络将系统网络内的服务器上的重要数据及系统业务数据定期备份至备份场地，涉及测评对象**应用服务器-1，应用服务器-2，办公运维管理终端**。

**（3）未关闭危险端口**

经核查，被测系统相关重要终端操作系统开启了TCP 135、139、445、593、1025端口和UDP 135、137、138、445 端口等危险端口，涉及测评对象**办公运维管理终端**。

**（4）未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证**

1、系统网络中的主要计算设备不具有可信根芯片或硬件；2、未基于可信根对设备的系统引导程序、系统程序、重要配置参数等进行可信验证，涉及测评对象**应用服务器-1，应用服务器-2，办公运维管理终端**。

**（5）未限制默认账户访问权限**

经核查，系统网络内的服务器已为不同管理用户分配了不同登录账户与权限；但未限制默认账户访问权限，涉及测评对象**应用服务器-1，应用服务器-2**。

**（6）日志存储时间可达到6个月，但未对日志进行定期备份**

被测系统重要终端操作系统本地日志存储时间达到了6个月，对日志记录进行了保护，普通用户无法删改日志；但未对日志进行定期备份，涉及测评对象**办公运维管理终端**。

**（7）未提供实现安全标记功能**

经核查，系统网络内的应用服务器、重要终端未提供设置安全标记功能，涉及测评对象**应用服务器-1，应用服务器-2，办公运维管理终端**。

### 系统管理软件/平台

#### 已有安全控制措施汇总分析

针对数据库、中间件及云计算安全方面安全测评结果中存在的符合项进行汇总和分析，数据库、中间件及云计算安全方面基本落实《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）的相关安全防护要求，总体安全保护措施相对较完善，具体措施如下：

在身份鉴别方面，被测系统数据库有设置提供身份标识和鉴别功能，用户口令均符合复杂性要求及被测系统相关数据库远程管理需要登录腾讯云的企业账号，在控制端中对其进行安全管理。腾讯云使用的是https协议来进行远程通信，可防止鉴别数据在网络传输的过程中被窃听等。

在访问控制方面，被测系统数据库为不同登录用户分配创建了不同账户及权限；同时，对数据库默认账户的默认登录口令进行了修改等。

在安全审计方面，被测系统数据库及应用中间件均设置并启用了安全审计功能，审计范围覆盖重要安全事件行为等。

在数据完整性及数据保密性方面，被测系统数据库远程管理需要登录腾讯云的企业账号，在控制端中对其进行安全管理；腾讯云使用的是https协议来进行远程通信，传输过程加密，可保证重要数据在传输过程中的完整性及保密性及腾讯云控制端针对用户口令采用加密算法进行加密，用户口令以密文形式保存，能保证鉴别数据存储过程中的保密性。

在数据备份恢复方面，被测系统业务数据库采用的是腾讯云数据库，系统业务数据库采用实时备份，备份位置：北京腾讯云备份中心；同时，已建立恢复测试机制，定期每半年对备份数据进行恢复测试验证等。

在个人信息保护方面，系统数据库只收集了业务必需的用户个人信息，如：用户名、手机号、邮箱、密码等及系统数据库存储的个人用户详细信息只有管理人员及相关权限人员才能查询，如：用户名、手机号、邮箱、密码等，信息均通过相关审核等。

#### 主要安全问题汇总分析

安全计算环境存在的安全问题有:

**（1）未启用登录失败处理功能**

被测系统数据库未设置允许登录尝试次数、未设置锁定时间等策略，涉及测评对象**腾讯云数据库**。

**（2）未提供异地数据备份功能**

未提供异地备份措施，通过网络将系统网络内的数据库上的重要数据及系统业务数据定期备份至备份场地，涉及测评对象**腾讯云数据库**。

**（3）仅收集和保存了业务必需用户个人信息，但未制定有关用户个人信息保护管理制度和流程**

经核查，被测系统数据库仅收集和保存了业务必需用户个人信息，但未制定有关用户个人信息保护管理制度和流程，涉及测评对象**腾讯云数据库**。

**（4）对用户个人信息访问进行了限制，但未制定有关用户个人信息保护管理制度和流程**

经核查，被测系统数据库对用户个人信息访问进行了限制，但未制定有关用户个人信息保护管理制度和流程，涉及测评对象**腾讯云数据库**。

**（5）未授予不同账户为完成各自承担任务所需的最小权限**

被测系统数据库未制定提供用户权限表，未按不同用户角色创建不同用户(管理员、审计员、操作员),目前数据库仅设置了管理用户及业务应用用户，涉及测评对象**腾讯云数据库**。

**（6）未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证**

1、系统网络中的主要计算设备不具有可信根芯片或硬件；2、未基于可信根对设备的系统引导程序、系统程序、重要配置参数等进行可信验证，涉及测评对象**腾讯云数据库**。

**（7）身份鉴别模块功能不完善（账户口令未定期更换）**

被测系统腾讯云数据库对账户口令未强制要求进行定期更换，涉及测评对象**腾讯云数据库**。

**（8）未提供实现安全标记功能**

经核查，系统腾讯云数据库未提供设置安全标记功能，涉及测评对象**腾讯云数据库**。

### 业务应用系统/平台

#### 已有安全控制措施汇总分析

针对应用方面安全测评结果中存在的符合项进行汇总和分析，应用方面基本落实《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）的相关安全防护要求，总体安全保护措施相对较完善，具体措施如下：

在身份鉴别方面，SanyMall客户云商城系统采用B/S架构，系统提供了一种登录方式。1、后台通过用户名+口令进行身份鉴别；2、商家中心通过用户名+口令+验证码进行身份鉴别；3、商城前台用户由树根系统统一身份验证；可保障鉴别及标识具有唯一性。同时，系统设置提供了身份鉴别信息复杂度校验功能，密码必须包含字母及数字，密码长度要求（不能小于8位)及系统设置了登录失败处理功能，连续登录失败达到10次，锁定10个小时，10个小时后自动解锁等。

在访问控制方面，SanyMall客户云商城系统根据不同用户工作需求给予不同权限，系统划分为：平台总运营、平台基础运营、商城报表查询、订单管理、聚合页配置等5个不同权限组。每个权限组又可以依据不同用途划分不同栏目权限等。

在安全审计方面，SanyMall客户云商城系统开启了安全审计功能，审计内容覆盖到了所有用户，对重要用户行为和重要安全事件进行了安全审计；同时，SanyMall客户云商城系统所有审计记录均保存在服务器上，以文本形式保存，前台用户无法对其进行删除、修改及覆盖等操作，日志留储时间系统上线（2019年4月上线）至今，保存时间超过6个月等。

在入侵防范方面，经渗透测试验证，发现该系统存在SQL注入高危漏洞及存储型跨站高危漏洞，但经回归测试已经修复该漏洞，应用系统对数据有效性进行了校验，对无效或非法数据进行了过滤。

在数据完整性及保密性方面，应用系统为B/S架构，采用了https数字证书进行加密传输，能保证重要数据在传输过程中的完整性及保密性；同时，应用系统对用户密码采用了Bcrypt加密工具进行加密，用户口令以密文形式保存，能保证鉴别数据存储过程中的保密性。

在数据备份恢复方面，被测系统数据库采用的是腾讯云数据库，系统业务数据采用实时备份，备份位置：北京腾讯云备份中心；同时，已建立恢复测试机制，定期每半年对备份数据进行恢复测试验证等。

在剩余信息保护方面，SanyMall客户云商城系统在注消后可释放cookie信息，可保证身份鉴别信息完全清除等。

在个人信息保护方面，SanyMall客户云商城系统采集和保存了用户名、手机号、邮箱、密码等用户个人信息，为业务必需；同时对用户个人信息访问权限进行限制，只有管理人员及相关权限人员才能查询等。

#### 主要安全问题汇总分析

安全计算环境存在的安全问题有:

**（1）未采用两种或两种以上组合的鉴别技术**

SanyMall 客户云商城系统采用一种鉴别技术对用户进行身份鉴别，未采用两种或以上组合进行鉴别，涉及测评对象**SanyMall 客户云商城系统**。

**（2）未提供异地数据备份功能**

未提供异地备份措施，通过网络将系统网络内的系统业务数据定期备份至备份场地，涉及测评对象**SanyMall 客户云商城系统**。

**（3）仅收集和保存了业务必需用户个人信息，但未制定有关用户个人信息保护管理制度和流程**

经核查，被测系统仅收集和保存了业务必需用户个人信息，但未制定有关用户个人信息保护管理制度和流程，涉及测评对象**SanyMall 客户云商城系统**。

**（4）对用户个人信息访问进行了限制，但未制定有关用户个人信息保护管理制度和流程**

经核查，被测系统对用户个人信息访问进行了限制，但未制定有关用户个人信息保护管理制度和流程，涉及测评对象**SanyMall 客户云商城系统**。

**（5）未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证**

未基于可信根对应用程序等关键执行环节进行动态可信验证，涉及测评对象**SanyMall 客户云商城系统**。

**（6）身份鉴别模块功能不完善（账户口令未定期更换）**

SanyMall 客户云商城系统对账户口令未强制要求进行定期更换，涉及测评对象**SanyMall 客户云商城系统**。

**（7）未提供实现安全标记功能**

经核查，SanyMall 客户云商城系统未提供设置安全标记功能，涉及测评对象**SanyMall 客户云商城系统**。

### 数据资源

#### 已有安全控制措施汇总分析

针对数据资源方面安全测评结果中存在的符合项进行汇总和分析，数据资源方面基本落实《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）的相关安全防护要求，总体安全保护措施相对较完善，具体措施如下：

在数据完整性及保密性方面，SanyMall客户云商城系统为B/S架构，在传输过程中采用了密码技术https加密协议，能保证重要数据在传输过程中的完整性及保密性等。

在数据备份恢复方面，被测系统数据库采用的是腾讯云数据库，系统业务数据采用实时备份，备份位置：北京腾讯云备份中心；同时，已建立恢复测试机制，定期每半年对备份数据进行恢复测试验证等。

在剩余信息保护方面，SanyMall客户云商城系统在注消后可释放cookie信息，可保证身份鉴别信息完全清除等。

在个人信息保护方面，SanyMall客户云商城系统采集和保存了用户名、手机号、邮箱、密码等用户个人信息，为业务必需；同时对用户个人信息访问权限进行限制，只有管理人员及相关权限人员才能查询等。

#### 主要安全问题汇总分析

安全计算环境存在的安全问题有:

**（1）针对重要业务数据及重要个人信息未采用校验技术或密码技术保证存储过程中的完整性**

经核查，SanyMall客户云商城系统针对重要业务数据及重要个人信息未采用校验技术或密码技术保证存储过程中的完整性，涉及测评对象**重要业务数据，重要个人信息**。

**（2）SanyMall客户云商城系统针对重要业务数据及重要个人信息未采用密码技术保证存储过程中的保密性**

经核查，SanyMall客户云商城系统针对重要业务数据及重要个人信息未采用密码技术保证存储过程中的保密性，涉及测评对象**重要业务数据，重要个人信息**。

**（3）未提供异地数据备份功能**

未提供异地备份措施，未通过网络将重要业务数据及重要个人数据定期备份至备份场地，涉及测评对象**重要业务数据，重要个人信息**。

**（4）仅收集和保存了业务必需用户个人信息，但未制定有关用户个人信息保护管理制度和流程**

经核查，被测系统仅收集和保存了业务必需用户个人信息，但未制定有关用户个人信息保护管理制度和流程，涉及测评对象**重要个人信息**。

**（5）对用户个人信息访问进行了限制，但未制定有关用户个人信息保护管理制度和流程**

经核查，被测系统对用户个人信息访问进行了限制，但未制定有关用户个人信息保护管理制度和流程，涉及测评对象**重要个人信息**。

### 其他系统或设备

#### 已有安全控制措施汇总分析

SanyMall 客户云商城系统不涉及其他系统或设备。

#### 主要安全问题汇总分析

SanyMall 客户云商城系统不涉及其他系统或设备。

## 安全管理中心

### 已有安全控制措施汇总分析

针对安全管理中心方面安全测评结果中存在的符合项进行汇总和分析，安全管理中心方面基本落实《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）的相关安全防护要求，总体安全保护措施相对较完善，具体措施如下：

在系统管理方面，通过腾讯云控制台对系统管理员进行身份鉴别，只允许管理员通过腾讯云控制台对系统进行管理操作，腾讯云控制台云审计云产品对这些操作进行审计等。

在审计管理方面，通过腾讯云控制台中的云审计云产品存储记录腾讯云账号内的所有操作行为；审计管理员通过登录到腾讯云控制台中的云审计云产品对日志进行管理，并对审计管理员的操作进行审计记录等。

在安全管理方面，被测系统相关相关云产品（Web应用防火墙、主机安全等）统一通过登录腾讯云企业子账号控制台进行管理访问，对云产品进行管理操作，且对操作进行审计记录等。

在集中管控方面，被测系统部署在腾讯云平台，通过腾讯云控制台云监控服务，可以对云安全产品、云服务器等运行状态进行集中监测并能依据设定的阀值实时报警；被测系统相关云产品（Web应用防火墙云产品、主机安全云产品等）通过腾讯云云审计云产品进行集中统一收集保存与审计分析等管理，日志留存时长可达到6个月，专职人员定期分析结合腾讯云平台为被测系统已提供部署的Web应用防火墙云产品、主机安全云产品等相关安全产品，对网络中发生的各类安全事件进行识别、报警和分析等。

### 主要安全问题汇总分析

安全管理中心存在的安全问题有:

**（1）未创未通过安全管理员对可信验证策略和安全标记策略进行配置和管理**

经核查，已设立安全管理员，安全管理员对安全策略进行配置和管理，但不包括可信验证策略和安全标记策略，涉及测评对象**安全管理中心**。

## 安全管理制度

### 已有安全控制措施汇总分析

针对安全管理制度方面安全测评结果中存在的符合项进行汇总和分析，安全管理制度方面基本落实《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）的相关安全防护要求，总体安全保护措施相对较完善，具体措施如下：

在安全策略方面，公司制定了《三一集团有限公司信息安全总体方针》、《三一集团有限公司集团信息安全委员会》制度文件，其中明确了组织机构与职责，明确了安全工作的总体目标与范围等。

在管理制度方面，针对日常重要管理活动建立了相关制度文件，如《三一集团有限公司数据中心管理规定》、《三一集团有限公司问责管理制度》、《三一集团有限公司备份管理制度》、《三一集团有限公司IT终端安全管理制度》、《三一集团有限公司IT服务台管理制度》、《三一集团有限公司防病毒系统管理规范》、《三一集团有限公司变更管理制度》、《三一集团有限公司信息安全事件处理与应急管理制度》、《三一集团有限公司信息系统权限管理制度》等相关安全管理制度等。

在制定和发布方面，由各部门负责本部门管辖业务的管理办法及管理标准的制订，走OA流程请示，由总经理和分管董事负责审批发布等。

在评审和修订方面，由各部门负责本部门安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订，走OA流程请示，由总经理和分管董事负责审批发布等。

### 主要安全问题汇总分析

经核查，安全管理制度方面暂未发现存在部分符合/不符合的测评项。

## 安全管理机构

### 已有安全控制措施汇总分析

针对安全管理机构方面安全测评结果中存在的符合项进行汇总和分析，安全管理机构方面基本落实《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）的相关安全防护要求，总体安全保护措施相对较完善，具体措施如下：

在岗位设置方面，公司信息安全工作领导委员会为网络安全管理工作的职能部门，并已设立系统管理员、审计管理员和安全管理员等岗位，并且在《三一集团有限公司IT体系内部职称评定管理规定》中明确各个部门及各个工作岗位的职责等。

在人员配备方面，配备了安全管理、审计管理员、系统管理员，负责公司日常系统网络管理运维工作。

在授权和审批方面，针对系统变更、物理访问和网络接入等事项建立了相关制度文件，明确了系统重大变更、重要操作和系统接入等事项需要进行审批。

在沟通和合作方面，公司有定期召开网络协调会议，有效的加强了各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通等。

在审核和检查方面，公司已落实安全巡检制度，每天巡检一次，巡检内容包含机房环境、设备状态、系统运行情况、数据备份等。

### 主要安全问题汇总分析

安全管理机构存在的安全问题有:

**（1）未明确安全主管、安全管理各方面负责人**

经核查，在《三一集团有限公司集团信息安全委员会》中指定了网络安全管理工作的职能部门（集团董办、集团总裁办等），明确了岗位职责。但未明确安全主管、安全管理各方面负责人名单，涉及测评对象**安全管理机构**。

**（2）未配备一定数量系统管理员、审计管理员和安全管理员**

经访谈，未配备一定数量的管理员，仅由雷杰一人担任系统管理员、黎勃利一人担任审计管理员、刘清香一人担任安全管理员，涉及测评对象**安全管理机构**。

## 安全管理人员

### 已有安全控制措施汇总分析

针对安全管理人员方面安全测评结果中存在的符合项进行汇总和分析，安全管理人员方面基本落实《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）的相关安全防护要求，总体安全保护措施相对较完善，具体措施如下：

在人员录用方面，由人资总部负责人员录用，人力资源部门会对被录用人员的身份、安全背景、专业资格或资质等进行审查等。

在人员离岗方面，人员岗位调整时，需经过部门领导的确认，调动流程通过后权限部门会关闭员工原岗位IT权限，若新岗位有IT权限需求，需重新申请走审批流程，岗位调动根据不同级别对应不同级别负责人审批；及人员岗位离职时，经过部门领导的确认，填写《离职工作交接单》、《解除终止劳动合同/实习协议申请书》经部门主管和总监签字确认，走SHR人资系统离职流程，将相关账户和访问权限清理，包括其使用的账号、密码、权限、各种身份证件等以及其他相关信息资料、资产和软硬件设备，归还资产的接收部门进行审核和确认等。

在安全意识教育和培训方面，单位针对新入职的员工会进行安全意识教育和岗位技能培训，并被告知相关的安全责任。

在外部人员访问管理方面，外部人员访问受控区域需向单位分管人事领导审批，方能进入，由专人全程陪同；外部人员接入受控网络访问系统需签署《商业秘密保密协议承诺函》《安全协议》并走流程审批，审批登记完成后方可接入等。

### 主要安全问题汇总分析

安全管理人员存在的安全问题有:

**（1）未与关键岗位（安全管理员等）签署岗位责任协议**

经访谈，未与关键岗位（安全管理员等）签署岗位责任协议，涉及测评对象**安全管理人员**。

## 安全建设管理

### 已有安全控制措施汇总分析

针对安全建设管理方面安全测评结果中存在的符合项进行汇总和分析，安全建设管理方面基本落实《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）的相关安全防护要求，总体安全保护措施相对较完善，具体措施如下：

在定级和备案方面，系统的定级结果已经过主管部门审批通过，已完成定级备案工作，已取得系统备案号等。

在安全方案设计方面，有组织集团相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，有提供相关会议纪要等。

在产品采购和使用方面，网络安全产品的采购均符合国家相关规定，均有相关销售许可等。

在自行软件开发方面，系统自行开发，测试环境和生产环境分开，测试数据和结果对内展示，均为受控成果；同时，公司建立了《三一重工软件开发管理规范》，对开发过程进行了规范等。

在工程实施方面，通过第三方工程监理（兴湘监理）及集团董办督办经理控制项目实施过程等。

在测试验收方面，依据测试验收方案实施测试验收，形成测试验收报告。

在系统交付方面，已制订项目交付清单，并对系统、设备和文档等进行了明确规定及软件开发单位提供了系统相关操作手册、培训资料等文档。

在等级测评方面，根据定级要求，定期每年进行一次等级测评，发现不符合相应等级保护标准要求的及时整改等。

在服务供应商选择方面，与湖南省金盾信息安全等级保护评估中心有限公司、网神信息技术股份有限公司、深信服科技股份有限公司等签订了安全服务合同，服务商具有相关资质，符合国家相关规定，在与安全服务商签订的安全服务合同中已明确双方应当履行的责任及安全服务内容等。

### 主要安全问题汇总分析

安全建设管理存在的安全问题有:

**（1）经核查，自行软件开发过程中未对恶意代码进行检测，无法保证软件安全性**

经核查，自行软件开发过程中未对恶意代码进行检测，无法保证软件安全性，涉及测评对象**安全建设管理**。

**（2）系统未进行上线前的安全性测试，未出具相关安全测试报告**

经访谈，系统未进行上线前的安全性测试，未出具相关安全测试报告，涉及测评对象**安全建设管理**。

## 安全运维管理

### 已有安全控制措施汇总分析

针对安全运维管理方面安全测评结果中存在的符合项进行汇总和分析，安全运维管理方面基本落实《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）的相关安全防护要求，总体安全保护措施相对较完善，具体措施如下：

在环境管理方面，公司建立了办公环境安全相关的管理制度，明确了来访人员接待区域，工作人员离开座位应确保终端计算机退出登录状态及桌面上不准放置包含敏感信息的文件文档等。

在资产管理方面，对信息系统相关资产进行标识管理，贴了资产标签，标明重要程度；同时，已建立《资产清单》，内容包括：资产名称、功能描述、数量、责任部门、责任人、使用人等。

在介质管理方面，公司已建立《三一集团有限公司存储介质管理办法》明确了将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点。

在设备维护管理方面，公司明确相关维护人员的职责分工，包括日常维护管理、计算机维修及服务审批等过程的管理等。

在漏洞和风险管理方面，公司对该系统定期每月进行安全漏洞扫描，且测评过程中涉及渗透测试和漏洞扫描，可以有效的发现安全漏洞和隐患及时进行修补或评估可能的影响后进行修补等。

在网络和系统安全管理方面，公司划分不同的管理员角色进行网络和系统的运维管理；由董办授权专干负责进行账户管理，对申请账户、建立账户、删除账户等进行控制；同时，每天一次对机房进行安全巡检，巡检内容主要是针对机房基础设施的环境、设备状态及公司建立了《三一集团有限公司网络管理办法》网络接入管理远程访问账号的申请必须获得相关部门审批，且符合远程访问控制满足一定安全的要求，如需对远程操作或使用的设备以及操作权限、允许访问的内部服务、允许访问时间、会话超时等进行严格控制。

在恶意代码防范管理方面，单位会不定期宣传防恶意代码知识，服务器及终端PC均安装了防恶意代码等安全防护软件，可以对外来存储设备进行恶意代码检查等；同时，公司建立的《三一集团有限公司计算机病毒防治管理办法》中明确规定各部门在从信息网络上下载软件、程序、数据和购置、维修、借入计算机设备时，必须先对其进行计算机病毒检测，经确认无毒后方可使用，所有设备接入系统前均需查杀病毒等。

在配置管理方面，如需改变服务器或软件系统相关配置参数，需经过部门相关领导的批准，及时更新基本配置信息库；在密码管理方面，购买的密码产品（如：门禁系统）已提供相关证明材料证明符合相关国家标准和行业标准。

在变更管理方面，公司在OA 系统中明确了变更流程，包括变更发起方、实施方的工作内容，变更发起方需提交变更方案，变更方案需经过相关领导的审批，对有可能影响客户利益的变更事先通知客户并得到客户的确认之后再进行变更操作等；同时，公司已建立《三一集团有限公司变更管理流程》，对变更过程进行控制规定。

在备份与恢复管理方面，公司已识别需要定期备份的重要业务信息（系统业务数据等），公司发布的《三一集团有限公司数据备份管理实施细则》中明确了备份方式、备份频度、存储介质、保存期等；同时，针对被测系统SanyMall 客户云商城系统相关业务等重要数据，制定了备份策略，对系统业务数据库采用实时备份等。

在安全事件方面，单位各部门或员工发现的安全弱点和可疑事件会及时向宣传信息科进行报告；同时，公司制定了《三一集团有限公司信息安全事件处理与应急预案管理制度》，明确了不同安全事件的报告、处置和响应流程等。

在应急预案管理方面，有制定《三一集团有限公司信息安全事件处理与应急管理制度》，包括应急处理流程、系统恢复流程等内容；同时，公司每年会组织一次应急演练，有形成相关演练记录；在外包运维管理方面，与外包运维服务商有签订相关协议，协议中有明确约定外包运维的范围和工作内容等。

### 主要安全问题汇总分析

经核查，安全运维管理方面暂未发现存在部分符合/不符合的测评项。

## 其他安全要求指标

### 已有安全控制措施汇总分析

SanyMall 客户云商城系统不涉及其他安全要求指标。

### 主要安全问题汇总分析

SanyMall 客户云商城系统不涉及其他安全要求指标。

## 验证测试

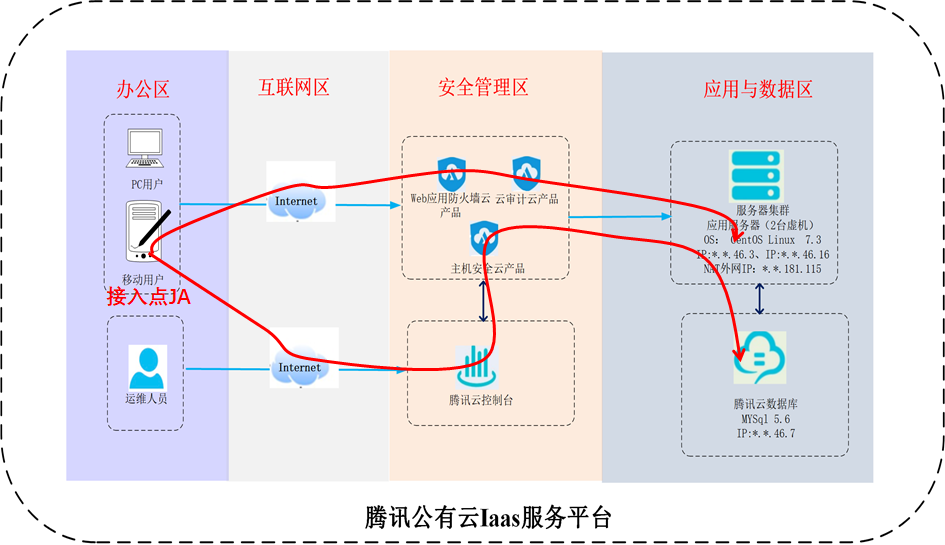
### 漏洞扫描

#### 漏洞扫描结果统计

本次等级测评采用的漏洞扫描工具主要包括：

| **序号** | **工具名称** | **型号** | **系统固件版本** | **系统漏洞库版本** | **工具描述** |
| --- | --- | --- | --- | --- | --- |
| 1 | 绿盟远程安全评估系统 | NX3 | V6.0R04F01 | 2021112901 | 绿盟远程安全评估系统能够全方位检测IT系统存在的脆弱性，发现信息系统存在的安全漏洞、安全配置问题、应用系统安全漏洞，核查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告，帮助安全管理人员先于攻击者发现安全问题，及时进行修补。 |

针对被测系统的网络边界和测评设备、主机和业务应用系统的情况，需要在被测系统及其互联网络中设置1个测试工具接入点――接入点JA，如图3-1所示，“接入点”标注表示进行工具测试时，需要从该接入点接入，对应的箭头路线表示工具测试数据的主要流向示意。



**图3-1 漏洞扫描工具接入测试示意图**

测试接入点JA:

测试目的：在三一集团有限公司办公区接入漏洞扫描工具，一是模拟通过Internet外部恶意用户测试系统是否存在可利用的漏洞，二是验证边界控制策略有效性。

**接入点JA漏洞扫描结果统计**

接入点JA的漏洞扫描结果汇总如下表所示。

**表 3‑1 接入点JA漏洞扫描结果汇总表**

| **序号** | **设备名称** | **系统及版本** | **安全漏洞数量** | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **高** | **中** | **低** | **小计** |
| 1 | 应用服务器-1 | CentOS Linux 7.3 | 0 | 0 | 7 | 7 |
| 2 | 应用服务器-2 | CentOS Linux 7.3 | 0 | 0 | 7 | 7 |
| 3 | 办公运维管理终端 | Windows10企业版 | 0 | 0 | 1 | 1 |
| 4 | SanyMall 客户云商城应用系统 | Ecstore V5.0.4 | 0 | 0 | 0 | 0 |
| 5 | 中间件 | Nginx 1.14.2 | 0 | 0 | 0 | 0 |
| 安全漏洞数量小计 | | | 0 | 0 | 15 | 15 |

说明：被测系统部署于腾讯公有云IaaS服务平台，为云服务客户业务应用

系统其基础设施与网络架构及网络设备均采用腾讯公有云IaaS服务平台服务，被测系统涉及的安全产品均为腾讯云上的云安全服务产品，无法对其自身进行漏洞扫描来发现可能存在的已知漏洞，故未纳入漏洞扫描范围。

#### 漏洞扫描问题描述

通过对漏洞扫描结果进行分析，SanyMall 客户云商城未发现存在高、中危安全漏洞，全部安全漏洞描述详见报告附录E。

### 渗透测试

#### 渗透测试过程说明

渗透测试的主要功能是通过模拟恶意黑客的攻击方法,攻击等级保护对象的应用程序、系统或者网络的安全功能,从而验证测评对象弱点、技术缺陷或漏洞的一种评估方法。

1. **渗透测试对象**

本次测试对象如下表所示：

|  |  |  |
| --- | --- | --- |
| **序号** | **测试系统名称** | **测试范围（域名/IP）** |
| 1 | SanyMall 客户云商城系统 | https://mall.sany.com.cn/ |

1. **渗透测试工具**

使用到的工具包括：

漏洞扫描工具：sqlmap、fscan、javaserializetools、Struts2、VulsTools、 ShiroExpoit、 Metasploit-Framework；

端口扫描工具：nmap；

应用抓包工具：burpsuite、fiddle ；

网络抓包工具：wireshark、httpcanary。

1. **渗透测试内容**

本次渗透测试主要测试系统是否有以下漏洞的存在:

（1）系统/服务类漏洞。由于操作系统、数据库、中间件等为应用系统提供服务或支撐的环境存在缺陷,所导致的安全漏洞,如缓冲区溢岀漏洞、堆/栈溢岀、内存泄露等,可能造成程序运行失败、系统宕机、重新启动等后果,更为严重的,可以导致程序执行非授权指令,甚至取得系统特权,进而进行各种非法操作。

（2）应用代码类漏洞。由于开发人员编写代码不规范或缺少必要的校验措施,导致应用系统存在安全漏洞,包括SQL注入、跨站脚本、任意上传文件等漏洞;攻击者可利用这些漏洞,对应用系统发起攻击,从而获得数据库中的敏感信息,更为严重的,可以导致服务器被控制。

（3）权限旁路类漏洞。由于对数据访问、功能模块访问控制规则不严或存在缺失,导致攻击者可非授权访问这些数据及功能模块。权限旁路类漏洞通常可分为越权访问及平行权限,越权访问是指低权限用户非授权访问高权限用户的功能模块或数据信息;平行权限是指攻击者利用自身权限的功能模块,非授权访问或操作他人的数据信息.

（4）配置不当类漏洞。由于未对配置文件进行安全加固,仅使用默认配置或配置不合理,所导致的安全风险。如中间件配置支持put方法,可能导致攻击者利用put方法上传木马文件,从而获得服务器控制权

（5）信息泄露类漏洞。由于系统未对重要数据及信息进行必要的保护,导致攻击者可从泄露的内容中获得有用的信息,从而为进一步攻击提供线索。如源代码泄露、默认错误信息中含有服务器信息/SQL语句等均属于信息泄露类漏洞。

（6）业务逻辑缺陷类漏洞。由于程序逻辑不严或逻辑太复杂,导致一些逻辑分支不能够正常处理或处理错误。如果出现这种情况,则用户可以根据业务功能的不同时行任意密码修改、越权访问、非正常金额交易等攻击。

#### 渗透测试问题描述

通过渗透测试发现，SanyMall 客户云商城系统存在的安全问题汇总如下表所示。

**表 3‑3 渗透测试结果汇总表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **安全问题** | **关联资产/域名** | **严重程度** | **修复情况** |
| 1 | 存在SQL注入漏洞 | https://mall.sany.com.cn/item-getSpecSku.html?item\_id=2010 | 高 | 已修复  详见“附录G回归测试”。 |
| 2 | 存在存储型跨站漏洞 | https://mall.sany.com.cn/ | 高 | 已修复  详见“附录G回归测试”。 |
| 3 | 存在敏感信息泄露漏洞 | https://malltest.sany.com.cn/shop-falshsale.html?shop\_id=1 | 中 | 暂未修复 |

注：本小节的严重程度为渗透测试结果，非报告最终结论。

## 单项测评小结

### 控制点符合情况汇总

根据单项测评结果汇总控制点符合情况如下表所示。

**表 3‑4 控制点符合情况汇总表**

| **序号** | **通用/扩展** | **安全类** | **控制点** | **控制点符合情况** | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **符合** | **部分符合** | **不符合** | **不适用** |
| **安全通用要求** | | | | | | | |
| 1 | 安全通用要求 | 安全物理环境 | 物理位置选择 |  |  |  | √ |
| 2 | 物理访问控制 |  |  |  | √ |
| 3 | 防盗窃和防破坏 |  |  |  | √ |
| 4 | 防雷击 |  |  |  | √ |
| 5 | 防火 |  |  |  | √ |
| 6 | 防水和防潮 |  |  |  | √ |
| 7 | 防静电 |  |  |  | √ |
| 8 | 温湿度控制 |  |  |  | √ |
| 9 | 电力供应 |  |  |  | √ |
| 10 | 电磁防护 |  |  |  | √ |
| 11 | 安全通信网络 | 网络架构 | √ |  |  |  |
| 12 | 通信传输 | √ |  |  |  |
| 13 | 可信验证 |  |  | √ |  |
| 14 | 安全区域边界 | 边界防护 | √ |  |  |  |
| 15 | 访问控制 | √ |  |  |  |
| 16 | 入侵防范 |  | √ |  |  |
| 17 | 恶意代码和垃圾邮件防范 | √ |  |  |  |
| 18 | 安全审计 | √ |  |  |  |
| 19 | 可信验证 |  |  | √ |  |
| 20 | 安全计算环境 | 身份鉴别 |  | √ |  |  |
| 21 | 访问控制 |  | √ |  |  |
| 22 | 安全审计 |  | √ |  |  |
| 23 | 入侵防范 |  | √ |  |  |
| 24 | 恶意代码防范 | √ |  |  |  |
| 25 | 可信验证 |  |  | √ |  |
| 26 | 数据完整性 |  | √ |  |  |
| 27 | 数据保密性 |  | √ |  |  |
| 28 | 数据备份恢复 |  | √ |  |  |
| 29 | 剩余信息保护 | √ |  |  |  |
| 30 | 个人信息保护 |  | √ |  |  |
| 31 | 安全管理中心 | 系统管理 | √ |  |  |  |
| 32 | 审计管理 | √ |  |  |  |
| 33 | 安全管理 |  | √ |  |  |
| 34 | 集中管控 | √ |  |  |  |
| 35 | 安全管理制度 | 安全策略 | √ |  |  |  |
| 36 | 管理制度 | √ |  |  |  |
| 37 | 制定和发布 | √ |  |  |  |
| 38 | 评审和修订 | √ |  |  |  |
| 39 | 安全管理机构 | 岗位设置 |  | √ |  |  |
| 40 | 人员配备 |  | √ |  |  |
| 41 | 授权和审批 | √ |  |  |  |
| 42 | 沟通和合作 | √ |  |  |  |
| 43 | 审核和检查 | √ |  |  |  |
| 44 | 安全管理人员 | 人员录用 |  | √ |  |  |
| 45 | 人员离岗 | √ |  |  |  |
| 46 | 安全意识教育和培训 | √ |  |  |  |
| 47 | 外部人员访问管理 | √ |  |  |  |
| 48 | 安全建设管理 | 定级和备案 | √ |  |  |  |
| 49 | 安全方案设计 | √ |  |  |  |
| 50 | 产品采购和使用 | √ |  |  |  |
| 51 | 自行软件开发 |  | √ |  |  |
| 52 | 外包软件开发 |  |  |  | √ |
| 53 | 工程实施 | √ |  |  |  |
| 54 | 测试验收 |  | √ |  |  |
| 55 | 系统交付 | √ |  |  |  |
| 56 | 等级测评 | √ |  |  |  |
| 57 | 服务供应商选择 | √ |  |  |  |
| 58 | 安全运维管理 | 环境管理 | √ |  |  |  |
| 59 | 资产管理 | √ |  |  |  |
| 60 | 介质管理 | √ |  |  |  |
| 61 | 设备维护管理 | √ |  |  |  |
| 62 | 漏洞和风险管理 | √ |  |  |  |
| 63 | 网络和系统安全管理 | √ |  |  |  |
| 64 | 恶意代码防范管理 | √ |  |  |  |
| 65 | 配置管理 | √ |  |  |  |
| 66 | 密码管理 | √ |  |  |  |
| 67 | 变更管理 | √ |  |  |  |
| 68 | 备份与恢复管理 | √ |  |  |  |
| 69 | 安全事件处置 | √ |  |  |  |
| 70 | 应急预案管理 | √ |  |  |  |
| 71 | 外包运维管理 |  |  |  | √ |
| **云计算安全扩展要求** | | | | | | | |
| 72 | 云计算安全扩展要求 | 安全物理环境 | 基础设施位置 |  |  |  | √ |
| 73 | 安全通信网络 | 网络架构 | √ |  |  |  |
| 74 | 安全区域边界 | 访问控制 | √ |  |  |  |
| 75 | 入侵防范 | √ |  |  |  |
| 76 | 安全审计 | √ |  |  |  |
| 77 | 安全计算环境 | 身份鉴别 | √ |  |  |  |
| 78 | 访问控制 |  |  |  | √ |
| 79 | 入侵防范 | √ |  |  |  |
| 80 | 镜像和快照保护 |  |  |  | √ |
| 81 | 数据完整性和保密性 | √ |  |  |  |
| 82 | 数据备份恢复 | √ |  |  |  |
| 83 | 剩余信息保护 |  |  |  | √ |
| 84 | 安全管理中心 | 集中管控 | √ |  |  |  |
| 85 | 安全建设管理 | 云服务商选择 | √ |  |  |  |
| 86 | 供应链管理 | √ |  |  |  |
| 87 | 安全运维管理 | 云计算环境管理 |  |  |  | √ |
| **安全控制点符合情况数量统计** | | | | 52 | 15 | 3 | 17 |

### 安全问题汇总

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

**表 3‑5 安全问题汇总表**

| **问题编号** | **安全问题** | **测评对象** | **通用/扩展** | **安全类** | **控制点** | **测评项** |
| --- | --- | --- | --- | --- | --- | --- |
| **安全通用要求** | | | | | | |
| T01 | 未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 | 安全通信网络 | 安全通用要求 | 安全通信网络 | 可信验证 | a）可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |
| T02 | 未采取技术措施对新型网络攻击行为进行分析。 | 虚拟网络边界 | 安全区域边界 | 入侵防范 | c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析； |
| T03 | 网络边界设备不具有可信根芯片或硬件，未基于可信根对通信设备的系统引导程序、系统程序、重要配置参数等进行可信验证。 | 虚拟网络边界 | 可信验证 | a）可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |
| T04 | 身份鉴别模块功能不完善（账户口令未定期更换）。 | SanyMall 客户云商城系统、腾讯云数据库 | 安全计算环境 | 身份鉴别 | a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； |
| T05 | 未启用登录失败处理功能。 | Web应用防火墙云产品、主机安全云产品、云审计云产品、腾讯云数据库 | b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； |
| T06 | 未采用两种或两种以上组合的鉴别技术。 | SanyMall 客户云商城系统、办公运维管理终端 | d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。 |
| T07 | 未限制默认账户访问权限。 | 应用服务器-1、应用服务器-2 | 访问控制 | a）应对登录的用户分配账户和权限； |
| T08 | 未授予不同账户为完成各自承担任务所需的最小权限。 | 腾讯云数据库 | d）应授予管理用户所需的最小权限，实现管理用户的权限分离； |
| T09 | 未提供实现安全标记功能。 | Web应用防火墙云产品、主机安全云产品、云审计云产品、SanyMall 客户云商城系统、应用服务器-1、应用服务器-2、办公运维管理终端、腾讯云数据库 | g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 |
| T10 | 日志存储时间可达到6个月，但未对日志进行定期备份。 | 办公运维管理终端 | 安全审计 | c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； |
| T11 | 未关闭危险端口。 | 办公运维管理终端 | 入侵防范 | b）应关闭不需要的系统服务、默认共享和高危端口； |
| T12 | 未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 | Web应用防火墙云产品、主机安全云产品、云审计云产品、SanyMall 客户云商城系统、应用服务器-1、应用服务器-2、办公运维管理终端、腾讯云数据库 | 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |
| T13 | 针对重要业务数据及重要个人信息未采用校验技术或密码技术保证存储过程中的完整性。 | 重要业务数据、重要个人信息 | 数据完整性 | b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 |
| T14 | SanyMall客户云商城系统针对重要业务数据及重要个人信息未采用密码技术保证存储过程中的保密性。 | 重要业务数据、重要个人信息 | 数据保密性 | b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 |
| T15 | 未提供异地数据备份功能。 | SanyMall 客户云商城系统、应用服务器-1、应用服务器-2、办公运维管理终端、腾讯云数据库、重要业务数据、重要个人信息 | 数据备份恢复 | b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； |
| T16 | 仅收集和保存了业务必需用户个人信息，但未制定有关用户个人信息保护管理制度和流程。 | SanyMall 客户云商城系统、腾讯云数据库、重要个人信息 | 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； |
| T17 | 对用户个人信息访问进行了限制，但未制定有关用户个人信息保护管理制度和流程。 | SanyMall 客户云商城系统、腾讯云数据库、重要个人信息 | b）应禁止未授权访问和非法使用用户个人信息。 |
| T18 | 未创未通过安全管理员对可信验证策略和安全标记策略进行配置和管理。 | 安全管理中心 | 安全管理中心 | 安全管理 | b）应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。 |
| T19 | 未明确安全主管、安全管理各方面负责人。 | 安全管理机构 | 安全管理机构 | 岗位设置 | b）应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责； |
| T20 | 未配备一定数量系统管理员、审计管理员和安全管理员。 | 安全管理机构 | 人员配备 | a）应配备一定数量的系统管理员、审计管理员和安全管理员等； |
| T21 | 未与关键岗位（安全管理员等）签署岗位责任协议 | 安全管理人员 | 安全管理人员 | 人员录用 | c）应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。 |
| T22 | 经核查，自行软件开发过程中未对恶意代码进行检测，无法保证软件安全性。 | 安全建设管理 | 安全建设管理 | 自行软件开发 | e）应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测； |
| T23 | 系统未进行上线前的安全性测试，未出具相关安全测试报告。 | 安全建设管理 | 测试验收 | b）应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。 |

# 整体测评

## 安全控制点间安全测评

安全控制间的安全测评主要考虑同一区域内、同一层面或不同层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用。

**安全计算环境：**

SanyMall客户云商城系统针对重要业务数据及重要个人信息未采用密码技术保证存储过程中的保密性。但针对SanyMall客户云商城系统重要业务数据及重要个人信息进行加密存储行业主管部门未明确规定要求，根据团体标准《T/ISEAA 001-2020 网络安全等级保护测评高风险判定指引》判定标准，此安全问题不适用高风险判定场景。

**安全建设管理：**

系统未进行上线前安全性测试，未出具相关安全测试报告。但针对被测系统有定期开展安全测评，上次测评2020年度有委托第三方测评机构进行过等级保护测评，且通过测评检测未发现系统存在高危风险隐患。从整体安全分析，以上措施一定程度上降低了安全隐患在系统上线运行前未被发现、系统一直带病运行、系统漏洞被利用攻击的安全风险；故由高风险降为中风险。

## 区域间安全测评

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

**安全计算环境安全与网络安全之间：**

1）未采用两种或两种以上组合的鉴别技术。经核查，SanyMall 客户云

商城系统采用用户名+口令一种鉴别技术对用户进行身份鉴别，未采用两种或两种以上组合的鉴别技术。但SanyMall客户云商城系统是面向用户线上购物平台，此平台主要用于三一集团线上销售产品展示、宣传及线上购买咨询等，是允许对外开公开，未涉及公司重要敏感数据；系统涉及资金业务交易时，会对接第三支付平台进行二次用户身份验证；且对SanyMall客户云商城系统后台及商家中心限制了访问地址范围，仅允许内网访问；从整体安全分析，以上措施一定程度上降低了登录口令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可能性；故由高风险降为中风险。

2）未关闭危险端口。被测系统重要终端（办公运维管理终端）操作系统开启了TCP 135、139、445、593、1025端口和UDP 135、137、138、445 端口等危险端口。但重要终端（办公运维管理终端）操作系统处于三一集团内网，互联网不能够直接访问；重要终端（办公运维终端）仅为一台办公运维管理终端，非关键主机设备；且在网络层面，已通过出口边界防火墙设备针对TCP 135、139、445、593、1025高危端口和UDP 135、137、138、445 高危端口通信进行了封堵；从整体安全分析，以上措施一定程度上降低了重要终端（办公运维终端）操作系统多余系统服务/默认共享/高危端口会被非法人员利用进行攻击的可能性；故由高风险降为中风险。

3）未提供异地数据备份功能。未提供异地备份措施，未通过网络将系统网络内的服务器上的重要数据及系统业务数据定期备份至备份场地。但此SanyMall 客户云商城系统部署在腾讯公有云IaaS服务平台，服务器采用的是腾讯公有云服务器，数据库采用的是腾讯云数据库；从整体安全分析，以上措施一定程度上降低了如机房遭受严重破坏等因素导致数据完全丢失的安全风险，故由高风险降为中风险。

## 整体测评结果汇总

经整体测评后安全问题严重程度变化情况如下表所示。

**表 4‑1 整体测评结果汇总表**

| **问题编号** | **安全问题** | **测评对象** | **整体测评描述** | **严重程度变化** |
| --- | --- | --- | --- | --- |
| **安全通用要求** | | | | |
| T06 | 未采用两种或两种以上组合的鉴别技术 | SanyMall 客户云商城系统、办公运维管理终端 | 未采用两种或两种以上组合的鉴别技术。经核查，SanyMall 客户云商城系统采用用户名+口令一种鉴别技术对用户进行身份鉴别，未采用两种或两种以上组合的鉴别技术。但SanyMall客户云商城系统是面向用户线上购物平台，此平台主要用于三一集团线上销售产品展示、宣传及线上购买咨询等，是允许对外开公开，未涉及公司重要敏感数据；系统涉及资金业务交易时，会对接第三支付平台进行二次用户身份验证；且对SanyMall客户云商城系统后台及商家中心限制了访问地址范围，仅允许内网访问；从整体安全分析，以上措施一定程度上降低了登录口令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可能性；故由高风险降为中风险。 | □升高  ☑降低 |
| T11 | 未关闭危险端口 | 办公运维管理终端 | 未关闭危险端口。被测系统重要终端（办公运维管理终端）操作系统开启了TCP 135、139、445、593、1025端口和UDP 135、137、138、445 端口等危险端口。但重要终端（办公运维管理终端）操作系统处于三一集团内网，互联网不能够直接访问；重要终端（办公运维终端）仅为一台办公运维管理终端，非关键主机设备；且在网络层面，已通过出口边界防火墙设备针对TCP 135、139、445、593、1025高危端口和UDP 135、137、138、445 高危端口通信进行了封堵；从整体安全分析，以上措施一定程度上降低了重要终端（办公运维终端）操作系统多余系统服务/默认共享/高危端口会被非法人员利用进行攻击的可能性；故由高风险降为中风险。 | □升高  ☑降低 |
| T14 | SanyMall客户云商城系统针对重要业务数据及重要个人信息未采用密码技术保证存储过程中的保密性。 | 重要业务数据、重要个人信息 | SanyMall客户云商城系统针对重要业务数据及重要个人信息未采用密码技术保证存储过程中的保密性。但针对SanyMall客户云商城系统重要业务数据及重要个人信息进行加密存储行业主管部门未明确规定要求，根据团体标准《T/ISEAA 001-2020 网络安全等级保护测评高风险判定指引》判定标准，此安全问题不适用高风险判定场景。 | □升高  ☑降低 |
| T15 | 未提供异地数据备份功能 | SanyMall 客户云商城系统、应用服务器-1、应用服务器-2、办公运维管理终端、腾讯云数据库、重要业务数据、重要个人信息 | 未提供异地数据备份功能。未提供异地备份措施，未通过网络将系统网络内的服务器上的重要数据及系统业务数据定期备份至备份场地。但此SanyMall 客户云商城系统部署在腾讯公有云IaaS服务平台，服务器采用的是腾讯公有云服务器，数据库采用的是腾讯云数据库；从整体安全分析，以上措施一定程度上降低了如机房遭受严重破坏等因素导致数据完全丢失的安全风险，故由高风险降为中风险。 | □升高  ☑降低 |
| T23 | 系统未进行上线前的安全性测试，未出具相关安全测试报告 | 安全建设管理 | 系统未进行上线前安全性测试，未出具相关安全测试报告。但针对被测系统有定期开展安全测评，上次测评2020年度有委托第三方测评机构进行过等级保护测评，且通过测评检测未发现系统存在高危风险隐患。从整体安全分析，以上措施一定程度上降低了安全隐患在系统上线运行前未被发现、系统一直带病运行、系统漏洞被利用攻击的安全风险；故由高风险降为中风险。 | □升高  ☑降低 |

# 安全问题风险分析

针对等级测评结果中存在的所有安全问题，结合关联资产和威胁分别分析安全问题可能产生的危害结果，找出可能对系统、单位、社会及国家造成的最大安全危害（损失），并根据最大安全危害（损失）的严重程度进一步确定安全问题的风险等级，结果为“高”、“中”或“低”。最大安全危害（损失）结果应结合安全问题所影响业务的重要程度、相关系统组件的重要程度、安全问题严重程度以及安全事件影响范围等进行综合分析。

**表 5‑1 安全问题风险分析**

| **序号** | **问题**  **编号** | **安全类** | **安全问题** | **关联资产** | **关联威胁** | **危害分析结果** | **风险等级** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **安全通用要求** | | | | | | | |
| 1 | T01 | 安全通信网络 | 未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 | 安全通信网络 | 网络攻击,篡改 | 通信设备不具有可信根芯片或硬件，未基于可信根对通信设备的系统引导程序、系统程序、重要配置参数等进行可信验证。无法检测及保证接入的网络设备真实可信。 | 中 |
| 2 | T02 | 安全区域边界 | 未采取技术措施对新型网络攻击行为进行分析。 | 虚拟网络边界 | 网络攻击 | 存在不能及时发现网络攻击行为，特别是新型网络攻击行为，而造成系统信息泄漏或损坏的风险。 | 中 |
| 3 | T03 | 网络边界设备不具有可信根芯片或硬件，未基于可信根对通信设备的系统引导程序、系统程序、重要配置参数等进行可信验证。 | 虚拟网络边界 | 网络攻击,篡改 | 无法检测及保证接入的网络边界设备真实可信。 | 中 |
| 4 | T04 | 安全计算环境 | 身份鉴别模块功能不完善（账户口令未定期更换）。 | SanyMall 客户云商城系统、腾讯云数据库 | 网络攻击 | 存在使用穷举法进行口令的暴力破解或口令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的可能性。 | 中 |
| 5 | T05 | 未启用登录失败处理功能。 | Web应用防火墙云产品、主机安全云产品、云审计云产品、腾讯云数据库 | 网络攻击、越权或滥用 | 身份鉴别机制不完善，使合法用户的鉴别信息更容易被攻击者所获取，从而使合法用户身份被冒用，对相关系统的正常运行带来影响。 | 中 |
| 6 | T06 | 未采用两种或两种以上组合的鉴别技术。 | SanyMall 客户云商城系统、办公运维管理终端 | 网络攻击 | 登录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 |
| 7 | T07 | 未限制默认账户访问权限。 | 应用服务器-1、应用服务器-2 | 越权或滥用 | 管理员权限过大，可能无法对管理员的行为进行监管、制约。 | 中 |
| 8 | T08 | 未授予不同账户为完成各自承担任务所需的最小权限。 | 腾讯云数据库 | 越权或滥用 | 管理员权限过大，可能导致无法在管理员级别形成权限相互制约。 | 中 |
| 9 | T09 | 未提供实现安全标记功能。 | Web应用防火墙云产品、主机安全云产品、云审计云产品、SanyMall 客户云商城系统、应用服务器-1、应用服务器-2、办公运维管理终端、腾讯云数据库 | 越权或滥用 | 存在帐号、口令、权限等重要参数被非授权访问的可能性。 | 低 |
| 10 | T10 | 日志存储时间可达到6个月，但未对日志进行定期备份。 | 办公运维管理终端 | 抵赖 | 可能会受到未预期的删除、修改或覆盖，或无法对安全事件进行追溯，存在一定的安全风险。 | 中 |
| 11 | T11 | 未关闭危险端口。 | 办公运维管理终端 | 网络攻击 | 开启不需要的系统服务、默认共享和高危端口，可能会被非法人员利用进行攻击，影响系统运行。 | 中 |
| 12 | T12 | 未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 | Web应用防火墙云产品、主机安全云产品、云审计云产品、SanyMall 客户云商城系统、应用服务器-1、应用服务器-2、办公运维管理终端、腾讯云数据库 | 网络攻击,篡改 | 无法检测及保证接入的设备、应用程序真实可信。 | 中 |
| 13 | T13 | 针对重要业务数据及重要个人信息未采用校验技术或密码技术保证存储过程中的完整性。 | 重要业务数据、重要个人信息 | 篡改 | 可能导致重要数据在存储过程中被恶意篡改。重要数据在存储过程中被攻击者篡改成功的可能性增大，会影响到信息系统的正常运行，进而可能使企业的业务运营、声誉、经济利益受损。 | 中 |
| 14 | T14 | SanyMall客户云商城系统针对重要业务数据及重要个人信息未采用密码技术保证存储过程中的保密性。 | 重要业务数据、重要个人信息 | 篡改 | 可能导致重要数据在存储过程中被恶意篡改。 | 中 |
| 15 | T15 | 未提供异地数据备份功能。 | SanyMall 客户云商城系统、应用服务器-1、应用服务器-2、办公运维管理终端、腾讯云数据库、重要业务数据、重要个人信息 | 软硬件故障 | 如机房遭受严重破坏，可能导致数据完全丢失。 | 中 |
| 16 | T16 | 仅收集和保存了业务必需用户个人信息，但未制定有关用户个人信息保护管理制度和流程。 | SanyMall 客户云商城系统、腾讯云数据库、重要个人信息 | 管理不到位 | 可能被未授权人员获取相关信息，导致信息泄露。 | 中 |
| 17 | T17 | 对用户个人信息访问进行了限制，但未制定有关用户个人信息保护管理制度和流程。 | SanyMall 客户云商城系统、腾讯云数据库、重要个人信息 | 泄密 | 可能被未授权人员获取相关信息，导致信息泄露。 | 中 |
| 18 | T18 | 安全管理中心 | 未创未通过安全管理员对可信验证策略和安全标记策略进行配置和管理。 | 安全管理中心 | 管理不到位 | 无法实现系统或设备用户帐号、权限及安全策略的统一集中管理，容易造成由于管理配置不当而引起系统面临各种安全风险。 | 中 |
| 19 | T19 | 安全管理机构 | 未明确安全主管、安全管理各方面负责人。 | 安全管理机构 | 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。 | 中 |
| 20 | T20 | 未配备一定数量系统管理员、审计管理员和安全管理员。 | 安全管理机构 | 管理不到位 | 影响信息安全管理工作连续性，可能对信息系统的正常运行产生影响。 | 低 |
| 21 | T21 | 安全管理人员 | 未与关键岗位（安全管理员等）签署岗位责任协议 | 安全管理人员 | 管理不到位、泄密 | 可能导致人员保密意识淡薄，造成泄密事件。 | 中 |
| 22 | T22 | 安全建设管理 | 经核查，自行软件开发过程中未对恶意代码进行检测，无法保证软件安全性。 | 安全建设管理 | 管理不到位、网络攻击、越权或滥用 | 可能存在后门未在上线前被发现及处理。 | 中 |
| 23 | T23 | 系统未进行上线前的安全性测试，未出具相关安全测试报告。 | 安全建设管理 | 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。 | 中 |

# 等级测评结论

等级测评结论由安全问题风险分析结果和综合得分共同确定，判定依据如下表所示。

**表 6‑1 等级测评结论判定依据**

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

综合得分计算方法如下：

设为被测对象的综合得分，，和根据下列公式计算。



其中，为关注系数，取值在0至1之间，由等级保护工作管理部门给出，默认值为0.5。为被测对象涉及的总测评项数（不含不适用项，下同），为技术方面对应的总测评项数，为技术方面的得分，为管理方面对应的总测评项数，为管理方面的得分，为测评项的重要程度（分为一般、重要和关键），为测评项的得分。

根据第5章安全问题风险分析结果统计高、中、低风险安全问题的数量，利用综合得分计算公式计算出被测对象的综合得分，并将相关结果填入下表。

**表 6‑2 安全问题统计和综合得分**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **被测对象名称** | **安全问题数量** | | | **综合得分** |
| **高风险** | **中风险** | **低风险** |
| SanyMall 客户云商城系统 | 0 | 21 | 2 | 86.41 |

依据GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》和GB/T 28448—2019《信息安全技术 网络安全等级保护测评要求》的第三级要求，经对SanyMall 客户云商城系统的安全保护状况进行综合分析评价后，等级测评结论如下：

SanyMall 客户云商城系统本次等级测评的综合得分为**86.41分**，不存在高等级风险，且系统中不存在高等级风险，等级测评结论为**良**。

# 安全问题整改建议

**表 7‑1 安全问题整改建议**

| **序号** | **问题**  **编号** | **安全类** | **安全问题** | **关联资产** | **整改建议** |
| --- | --- | --- | --- | --- | --- |
| **安全通用要求** | | | | | |
| 1 | T01 | 安全通信网络 | 未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 | 安全通信网络 | 建议通信设备采用可信根芯片或硬件，基于可信根对通信设备的系统引导程序、系统程序、重要配置参数等进行可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |
| 2 | T02 | 安全区域边界 | 未采取技术措施对新型网络攻击行为进行分析。 | 虚拟网络边界 | 建议购买配置APT、态势感知等安全服务，实现对新型网络攻击行为的分析。 |
| 3 | T03 | 网络边界设备不具有可信根芯片或硬件，未基于可信根对通信设备的系统引导程序、系统程序、重要配置参数等进行可信验证。 | 虚拟网络边界 | 建议网络边界设备采用可信根芯片或硬件，基于可信根对网络边界设备的系统引导程序、系统程序、重要配置参数等进行可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |
| 4 | T04 | 安全计算环境 | 身份鉴别模块功能不完善（账户口令未定期更换）。 | SanyMall 客户云商城系统、腾讯云数据库 | 建议被测系统腾讯云数据库及SanyMall 客户云商城系统对登录账户口令进行定期修改更换。 |
| 5 | T05 | 未启用登录失败处理功能。 | Web应用防火墙云产品、主机安全云产品、云审计云产品、腾讯云数据库 | 建议配置并启用被测系统相关安全产品(Web应用防火墙、主机安全云产品、云审计云产品)及腾讯云数据库登录失败处理功能，如限制非法登录次数5次、锁定10分钟，配置登录连接超时时间10分钟，登录连接超时后需重新登录。 |
| 6 | T06 | 未采用两种或两种以上组合的鉴别技术。 | SanyMall 客户云商城系统、办公运维管理终端 | 建议SanyMall 客户云商城系统及相关重要终端（办公运维管理终端）操作系统采用两种或两种以上组合的鉴别技术实现用户身份鉴别，其中一种使用密码技术，如数字证书、数字令牌等，或部署堡垒机实施双因子登录。 |
| 7 | T07 | 未限制默认账户访问权限。 | 应用服务器-1、应用服务器-2 | 建议限制系统网络内的服务器操作系统默认账户访问权限。 |
| 8 | T08 | 未授予不同账户为完成各自承担任务所需的最小权限。 | 腾讯云数据库 | 建议腾讯云数据库按最小权限原则，实现管理用户权限分离，区分设立管理员、审计员、安全员角色。 |
| 9 | T09 | 未提供实现安全标记功能。 | Web应用防火墙云产品、主机安全云产品、云审计云产品、SanyMall 客户云商城系统、应用服务器-1、应用服务器-2、办公运维管理终端、腾讯云数据库 | 建议对系统网络内的主要网络安全设备（Web应用防火墙云产品、主机安全云产品、云审计云产品等）及应用服务器、重要终端（办公运维管理终端）、腾讯云数据库、SanyMall 客户云商城系统内的重要信息设置安全标记，并控制对有安全标记信息资源的访问。 |
| 10 | T10 | 日志存储时间可达到6个月，但未对日志进行定期备份。 | 办公运维管理终端 | 建议采取相关技术措施，定期对被测系统重要终端（办公运维管理终端）日志进行定期备份。 |
| 11 | T11 | 未关闭危险端口。 | 办公运维管理终端 | 建议关闭被测系统相关重要终端（办公运维管理终端）操作系统TCP 135、139、445、593、1025端口和UDP 135、137、138、445端口等危险端口。 |
| 12 | T12 | 未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 | Web应用防火墙云产品、主机安全云产品、云审计云产品、SanyMall 客户云商城系统、应用服务器-1、应用服务器-2、办公运维管理终端、腾讯云数据库 | 建议系统网络中的主要计算设备(如：Web应用防火墙云产品、主机安全云产品、云审计云产品、应用服务器等)采用可信根芯片或硬件，基于可信根对计算设备的系统引导程序、系统程序、重要配置参数等进行可信验证，及对SanyMall 客户云商城系统应用程序等关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |
| 13 | T13 | 针对重要业务数据及重要个人信息未采用校验技术或密码技术保证存储过程中的完整性。 | 重要业务数据、重要个人信息 | 建议采用校验技术或密码技术保证SanyMall客户云商城系统重要业务数据及重要个人信息在存储过程中的完整性。 |
| 14 | T14 | SanyMall客户云商城系统针对重要业务数据及重要个人信息未采用密码技术保证存储过程中的保密性。 | 重要业务数据、重要个人信息 | 建议采用密码技术保证SanyMall客户云商城系统重要业务数据及重要个人信息在存储过程中的保密性。 |
| 15 | T15 | 未提供异地数据备份功能。 | SanyMall 客户云商城系统、应用服务器-1、应用服务器-2、办公运维管理终端、腾讯云数据库、重要业务数据、重要个人信息 | 建议利用通信网络将系统网络内的服务器配置数据及系统业务数据等重要数据定时批量传送至备用场地，实现异地数据异地备份。 |
| 16 | T16 | 仅收集和保存了业务必需用户个人信息，但未制定有关用户个人信息保护管理制度和流程。 | SanyMall 客户云商城系统、腾讯云数据库、重要个人信息 | 建议制定有关用户个人信息保护管理制度和流程，且需与系统实际情况一致。 |
| 17 | T17 | 对用户个人信息访问进行了限制，但未制定有关用户个人信息保护管理制度和流程。 | SanyMall 客户云商城系统、腾讯云数据库、重要个人信息 | 建议制定有关用户个人信息保护管理制度和流程，且需与系统实际情况一致。 |
| 18 | T18 | 安全管理中心 | 未创未通过安全管理员对可信验证策略和安全标记策略进行配置和管理。 | 安全管理中心 | 建议对所有主要网络设备及安全设备创建专门的安全管理员，设置仅有安全管理员对设备安全策略进行配置，包括对可信验证策略和安全标记策略配置和管理。 |
| 19 | T19 | 安全管理机构 | 未明确安全主管、安全管理各方面负责人。 | 安全管理机构 | 建议设立网络安全管理工作职能部门，设立安全主管、安全管理各方面负责人，并定义各负责人的职责。 |
| 20 | T20 | 未配备一定数量系统管理员、审计管理员和安全管理员。 | 安全管理机构 | 建议配备一定数量的系统管理员、网络管理员、安全管理员等，形成AB岗。 |
| 21 | T21 | 安全管理人员 | 未与关键岗位（安全管理员等）签署岗位责任协议 | 安全管理人员 | 建议与关键岗位（安全管理员等）签署岗位责任协议，明确岗位安全责任定义、协议的有效期限和责任人签字等内容。 |
| 22 | T22 | 安全建设管理 | 经核查，自行软件开发过程中未对恶意代码进行检测，无法保证软件安全性。 | 安全建设管理 | 建议软件开发过程中进行安全性测试，在软件安装前对恶意代码进行检测等。 |
| 23 | T23 | 系统未进行上线前的安全性测试，未出具相关安全测试报告。 | 安全建设管理 | 建议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，要求在系统建设验收阶段委托第三方进行安全测试，安全测试应包括密码应用安全性测试等。 |

【正文结束】

1. 被测对象资产
   1. 物理机房

被测系统三一集团有限公司SanyMall客户云商城系统为云服务客户业务应用系统，基础设施与网络环境由腾讯公有云IaaS服务平台提供，不涉及物理机房测评对象资产。

* 1. 网络设备

被测系统三一集团有限公司SanyMall客户云商城系统为云服务客户业务应用系统，基础设施与网络环境由腾讯公有云IaaS服务平台提供，不涉及网络设备测评对象资产。

* 1. 安全设备

**附录A 表-1 安全设备**

| **序号** | **设备名称** | **是否虚拟设备** | **系统及版本** | **品牌及型号** | **用途** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Web应用防火墙云产品 | 否 | 企业版 | 腾讯云 | 为云租户Web应用提供安全防护。 | 重要 | 设备数量：1套 |
| 2 | 主机安全云产品 | 否 | 专业版 | 腾讯云 | 为云租户主机提供入侵检测、漏洞管理、基线管理、高级防御等安全功能。 | 重要 | 设备数量：1套 |
| 3 | 云审计云产品 | 否 | / | 腾讯云 | 对云产品（Web应用防火墙云产品、主机安全云产品等）日志进行集中统一收集保存与审计分析等管理。 | 重要 | 设备数量：1套 |

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

* 1. 服务器/存储设备

**附录A 表-2 服务器/存储设备**

| **序号** | **设备名称** | **所属业务应用系统/平台名称** | **是否虚拟设备** | **操作系统及版本** | **数据库管理系统及版本** | **中间件及版本** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 应用服务器-1 | SanyMall 客户云商城系统 | 是 | CentOS Linux 7.3 | -- | Nginx 1.14.2 | 关键 | 设备数量：1台 |
| 2 | 应用服务器-2 | SanyMall 客户云商城系统 | 是 | CentOS Linux 7.3 | -- | Nginx 1.14.2 | 关键 | 设备数量：1台 |

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

* 1. 终端设备

**附录A 表-3 终端设备**

| **序号** | **设备名称** | **是否虚拟设备** | **操作系统/控制软件及版本** | **用途** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 办公运维管理终端 | 否 | Windows10企业版 | 用于日常办公及运维管理等。 | 重要 | 设备数量：1台 |

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

* 1. 其他系统或设备

SanyMall 客户云商城系统不涉及其他设备。

* 1. 系统管理软件/平台

**附录A 表-4 系统管理软件/平台**

| **序号** | **系统管理软件/平台名称** | **主要功能** | **版本** | **所在设备名称** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 腾讯云控制台 | 统一查看和管理腾讯云产品及服务的平台。 | -- | 腾讯云 | 重要 | 数量：1个 |
| 2 | 腾讯云数据库 | 数据存储 | MYSql 5.6 | 腾讯云 | 关键 | 数量：1个 |
| 3 | 中间件-1 | 网页发布 | Nginx 1.14.2 | 应用服务器-1 | 关键 | 数量：1个 |
| 4 | 中间件-2 | 网页发布 | Nginx 1.14.2 | 应用服务器-2 | 关键 | 数量：1个 |

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

* 1. 业务应用系统/平台

**附录A 表-5 业务应用系统/平台**

| **序号** | **业务应用系统/平台名称** | **主要功能** | **业务应用软件及版本** | **开发厂商** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | SanyMall 客户云商城系统 | SanyMall 客户云商城系统是三一集团商城系统，主要提供商城在线展示和交易功能，以最终用户为主要对象，提供三一整机、三一机械配件等系列终端产品和服务；致力于为客户提供方便快捷的产品选购渠道，完善智慧管理云平台生态圈。 | Ecstore V5.0.4 | 三一集团有限公司 | 关键 | 1套 |

* 1. 数据资源

**附录A 表-6 数据资源**

| **序号** | **数据类别** | **所属业务应用** | **安全防护需求** | **重要程度** |
| --- | --- | --- | --- | --- |
| 1 | 业务数据  （订单、交易明细等业务数据） | SanyMall 客户云商城系统 | 保密性：高  完整性：高 | 关键 |
| 2 | 个人信息数据  （用户名、手机号、邮箱、密码等个人信息数据） | 保密性：高  完整性：高 | 关键 |

* 1. 密码产品

SanyMall 客户云商城系统不涉及密码产品。

* 1. 安全相关人员

**附录A 表-7 安全相关人员**

| **序号** | **姓名** | **岗位/角色** | **联系方式** | **所属单位** |
| --- | --- | --- | --- | --- |
| 1 | 孟翔巍 | 安全主管 | 17770925562 | 三一集团有限公司 |
| 2 | 刘清香 | 安全管理员 | 15273150727 | 三一集团有限公司 |
| 3 | 谭智敏 | 网络管理员 | 17607310632 | 三一集团有限公司 |
| 4 | 雷杰 | 系统管理员 | 13808415415 | 三一集团有限公司 |
| 5 | 黎勃利 | 审计管理员 | 15274464567 | 三一集团有限公司 |
| 6 | 李三林 | 机房管理员 | 18073655130 | 三一集团有限公司 |

* 1. 安全管理文档

**附录A 表-8 安全管理文档**

| **序号** | **文档名称** | **主要内容** |
| --- | --- | --- |
| 1 | 《三一重工信息安全总体方针和策略》 | 主要涉及提高集团网络信息安全管理工作的水平，切实保障信息化健康发展，建立健全安全管理组织机构而发布的信息安全总体方针和策略。 |
| 2 | 《三一重工信息系统访问控制规定》 | 主要涉及严格控制信息系统的合法访问权限，保证信息系统的安全。 |
| 3 | 《三一重工数据安全管理制度》 | 主要涉及对数据资产的管理要求，规范员工操作行为，保障公司数据在创建、采集、存储、访问、下载、分发、流转、打印等全生命周期得到合理保护和共享。 |
| 4 | 《三一重工防病毒系统管理规范》 | 主要涉及通过制订防病毒系统管理规范，完善防病毒系统架构、标准化防病毒系统的管理以达到同意策略管理、提高病毒定义更新和加强系统安全性的目的。 |
| 5 | 《三一重工数据中心管理规定》 | 主要涉及规范数据中心的管理，确保数据中心所有设备的正常运行，确保应用系统的连续性。 |
| 6 | 《三一重工员工信息安全管理制度》 | 主要明确员工在司使用公司IT资源时的信息安全行为规范，提升员工信息安全意识，合规使用公司信息系统资源，保护公司信息资产。 |
| 7 | 《三一重工信息系统业务连续性管理流程》 | 主要涉及通过制订业务连续性计划，规范业务连续性文档发布过程，规范业务连续性演练工作，检验备份恢复策略是否有效，对演练中发现的问题进行改善，从而增强在面对风险是的处置能力。 |
| 8 | 《三一重工互联网系统发布管理制度》 | 主要涉及规范集团数据中心信息系统互联网发布安全标准，提升全体IT人员互联网信息系统安全意识，引导IT人员安全合规地建设使用互联网信息系统，保护公司信息资产。 |
| 9 | 《三一重工信息系统版本准入规范》 | 主要涉及三一集团信息系统版本管理，保证基础类软件使用安全可靠的版本，信息系统软件版本的选型与维护，明确各类软件使用版本准入要求。 |
| 10 | 《三一重工IT终端安全管理制度》 | 主要涉及规范三一集团终端与服务器的安全管控，确保集团内终端安全。 |
| 11 | 《三一重工信息安全事件处理与应急管理制度》 | 主要涉及加强三一集团信息安全事件管理，提升信息安全事件预防、响应、分析、处置及反馈的效率，降低信息安全事件造成的损失。 |
| 12 | 《三一重工信息系统权限管理制度》 | 主要涉及规范信息系统各类用户的权限管理，防止信息系统被非法授权、授权不当。规范IT协助处理业务数据的操作流程，保证IT协助处理业务数据结果的准确性、安全性。 |
| 13 | 《三一重工变更管理制度》 | 主要涉及规范IT系统运营环境变更行为，降低系统故障风险，保障系统可用率。 |
| 14 | 《三一重工备份管理制度》 | 主要涉及保护公司的业务数据免受意外损坏，确保业务的连续性。 |
| 15 | 《三一重工第三方人员信息安全管理规定》 | 主要涉及确保需接入公司IT资源的第三方人员安全、有效使用公司信息系统等资源，有效保护公司机密信息。 |
| 16 | 《三一重工软件开发管理规范》 | 主要涉及规范了软件开发相关人员和流程管控等内容。 |

1. 上次测评问题整改情况说明

湖南省金盾信息安全等级保护评估中心有限公司于 2020 年12月对三一集团有限公司SanyMall 客户云商城系统开展了等级测评工作，等级测评结论为良，综合得分93.95分。上次测评发现的主要安全问题以及被测单位针对主要安全问题的闭环整改工作情况如下：

**附录B 表-1 上次测评问题整改情况**

| **序号** | **安全问题** | **整改结果** | **情况说明** |
| --- | --- | --- | --- |
| 1 | 应用系统用户登录时未采用双因子鉴别方式。 | □已整改  ☑未整改 | 客户暂未整改。 |
| 2 | 数据库管理系统未授予不同管理账户为完成各 自承担任务所需的最小权限。 | □已整改  ☑未整改 | 客户暂未整改。 |
| 3 | 操作系统未限制终端远程接入地址。 | ☑已整改  □未整改 | 服务器只能通过腾讯云控制台进行登录访问控制，腾讯云控制台使用了SSH协议进行通信。 |
| 4 | 未提供异地数据备份功能。 | □已整改  ☑未整改 | 客户暂未整改。 |
| 5 | 未对敏感标记策略和可信验证策略进行配置。 | □已整改  ☑未整改 | 客户暂未整改。 |
| 6 | 关键岗位人员未签署岗位责任协议。 | □已整改  ☑未整改 | 客户暂未整改。 |
| 7 | 未根据系统的安全保护等级进行安全方案设计。 | ☑已整改  □未整改 | 有提供被测系统安全规划设计方案相关内容。 |
| 8 | 未组织相关部门和安全技术专家对安全整体规划及其配套文件的合理 性和正确性进行论证和审定。 | ☑已整改  □未整改 | 有提供安全规划方案评审相关会议纪要等相关文件。 |
| 9 | 未对系统恶意代码进行检测。 | □已整改  ☑未整改 | 当前系统已在线运行，软件开发过程中未进行安全性测试，未在软件安装前未进行恶意代码检测。 |
| 10 | 未聘请第三方工程监理控制项目的实施过程。 | ☑已整改  □未整改 | 有通过第三方工程监理（兴湘监理）及集团董办督办经理控制项目实施过程。 |
| 11 | 未进行上线前的安全性测试。 | □已整改  ☑未整改 | 当前系统已在线运行，系统上线前未进行安全性测试。 |
| 12 | 未提供详细的工程实施方案。 | ☑已整改  □未整改 | 有制订提供相关工程实施方案。 |
| 13 | 未在测试验收前根据设计方案要求制订测试验收方案。 | ☑已整改  □未整改 | 有制订提供测试验收方案及测试报告。 |

1. 单项测评结果汇总
   1. 安全通信网络

**附录 C 表-1 安全通信网络单项测评结果汇总（安全通用要求）**

| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | |
| --- | --- | --- | --- | --- | --- |
| **网络架构** | **通信传输** | **可信验证** |
| 1 | 安全通信网络 | 符合 | 5 | 2 | 0 |
| 部分符合 | 0 | 0 | 0 |
| 不符合 | 0 | 0 | 1 |
| 不适用 | 0 | 0 | 0 |
| 总计测评项8个，符合项7个，部分符合项0个，不符合项1个，不适用项0个 | | | | | |

**附录 C 表-2 安全通信网络单项测评结果汇总（安全扩展要求）**

| **序号** | **测评对象** | **符合情况** | **安全扩展要求** |
| --- | --- | --- | --- |
| **网络架构（云计算）** |
| 1 | 安全通信网络 | 符合 | 1 |
| 部分符合 | 0 |
| 不符合 | 0 |
| 不适用 | 4 |
| 总计测评项5个，符合项1个，部分符合项0个，不符合项0个，不适用项4个 | | | |

* 1. 安全区域边界

**附录 C 表-3 安全区域边界单项测评结果汇总（安全通用要求）**

| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **边界防护** | **访问控制** | **入侵防范** | **恶意代码和垃圾邮件防范** | **安全审计** | **可信验证** |
| 1 | 虚拟网络边界 | 符合 | 1 | 5 | 3 | 1 | 4 | 0 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 0 | 0 | 1 | 0 | 0 | 1 |
| 不适用 | 3 | 0 | 0 | 1 | 0 | 0 |
| 总计测评项20个，符合项14个，部分符合项0个，不符合项2个，不适用项4个 | | | | | | | | |

**附录 C 表-4 安全区域边界单项测评结果汇总（安全扩展要求）**

| **序号** | **测评对象** | **符合情况** | **安全扩展要求** | | |
| --- | --- | --- | --- | --- | --- |
| **访问控制（云计算）** | **入侵防范（云计算）** | **安全审计（云计算）** |
| 1 | 虚拟网络边界 | 符合 | 2 | 3 | 1 |
| 部分符合 | 0 | 0 | 0 |
| 不符合 | 0 | 0 | 0 |
| 不适用 | 0 | 1 | 1 |
| 总计测评项8个，符合项6个，部分符合项0个，不符合项0个，不适用项2个 | | | | | |

* 1. 安全计算环境
     1. 安全设备

**附录 C 表-5 安全设备单项测评结果汇总（安全通用要求）**

| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **身份鉴别** | **访问控制** | **安全审计** | **入侵防范** | **恶意代码防范** | **可信验证** | **数据完整性** | **数据保密性** | **数据备份恢复** | **剩余信息保护** | **个人信息保护** |
| 1 | Web应用防火墙云产品 | 符合 | 3 | 6 | 4 | 4 | - | 0 | 2 | 2 | 3 | - | - |
| 部分符合 | 0 | 0 | 0 | 0 | - | 0 | 0 | 0 | 0 | - | - |
| 不符合 | 1 | 1 | 0 | 0 | - | 1 | 0 | 0 | 0 | - | - |
| 不适用 | 0 | 0 | 0 | 2 | - | 0 | 0 | 0 | 0 | - | - |
| 2 | 主机安全云产品 | 符合 | 3 | 6 | 4 | 4 | - | 0 | 2 | 2 | 3 | - | - |
| 部分符合 | 0 | 0 | 0 | 0 | - | 0 | 0 | 0 | 0 | - | - |
| 不符合 | 1 | 1 | 0 | 0 | - | 1 | 0 | 0 | 0 | - | - |
| 不适用 | 0 | 0 | 0 | 2 | - | 0 | 0 | 0 | 0 | - | - |
| 3 | 云审计云产品 | 符合 | 3 | 6 | 4 | 3 | - | 0 | 2 | 2 | 3 | - | - |
| 部分符合 | 0 | 0 | 0 | 0 | - | 0 | 0 | 0 | 0 | - | - |
| 不符合 | 1 | 1 | 0 | 0 | - | 1 | 0 | 0 | 0 | - | - |
| 不适用 | 0 | 0 | 0 | 3 | - | 0 | 0 | 0 | 0 | - | - |
| 总计测评项87个，符合项71个，部分符合项0个，不符合项9个，不适用项7个 | | | | | | | | | | | | | |

**附录 C 表-6 安全设备单项测评结果汇总（安全扩展要求）**

| **序号** | **测评对象** | **符合情况** | **安全扩展要求** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **身份鉴别（云计算）** | **访问控制（云计算）** | **入侵防范（云计算）** | **镜像和快照保护（云计算）** | **数据完整性和保密性（云计算）** | **数据备份恢复（云计算）** | **剩余信息保护（云计算）** |
| 1 | Web应用防火墙云产品 | 符合 | - | - | - | - | - | - | - |
| 部分符合 | - | - | - | - | - | - | - |
| 不符合 | - | - | - | - | - | - | - |
| 不适用 | - | - | - | - | - | - | - |
| 2 | 主机安全云产品 | 符合 | - | - | - | - | - | - | - |
| 部分符合 | - | - | - | - | - | - | - |
| 不符合 | - | - | - | - | - | - | - |
| 不适用 | - | - | - | - | - | - | - |
| 3 | 云审计云产品 | 符合 | - | - | - | - | - | - | - |
| 部分符合 | - | - | - | - | - | - | - |
| 不符合 | - | - | - | - | - | - | - |
| 不适用 | - | - | - | - | - | - | - |
| 总计测评项0个，符合项0个，部分符合项0个，不符合项0个，不适用项0个 | | | | | | | | | |

* + 1. 服务器和终端

**附录 C 表-7 服务器和终端单项测评结果汇总（安全通用要求）**

| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **身份鉴别** | **访问控制** | **安全审计** | **入侵防范** | **恶意代码防范** | **可信验证** | **数据完整性** | **数据保密性** | **数据备份恢复** | **剩余信息保护** | **个人信息保护** |
| 1 | 应用服务器-1 | 符合 | 4 | 5 | 4 | 5 | 1 | 0 | 2 | 2 | 2 | 2 | - |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | - |
| 不符合 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | - |
| 不适用 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | - |
| 2 | 应用服务器-2 | 符合 | 4 | 5 | 4 | 5 | 1 | 0 | 2 | 2 | 2 | 2 | - |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | - |
| 不符合 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | - |
| 不适用 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | - |
| 3 | 办公运维管理终端 | 符合 | 3 | 5 | 3 | 3 | 1 | 0 | 2 | 2 | 2 | 2 | - |
| 部分符合 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | - |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | - |
| 不适用 | 0 | 1 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | - |
| 总计测评项96个，符合项77个，部分符合项4个，不符合项10个，不适用项5个 | | | | | | | | | | | | | |

**附录 C 表-8 服务器和终端单项测评结果汇总（安全扩展要求）**

| **序号** | **测评对象** | **符合情况** | **安全扩展要求** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **身份鉴别（云计算）** | **访问控制（云计算）** | **入侵防范（云计算）** | **镜像和快照保护（云计算）** | **数据完整性和保密性（云计算）** | **数据备份恢复（云计算）** | **剩余信息保护（云计算）** |
| 1 | 应用服务器-1 | 符合 | - | - | - | - | - | - | - |
| 部分符合 | - | - | - | - | - | - | - |
| 不符合 | - | - | - | - | - | - | - |
| 不适用 | - | - | - | - | - | - | - |
| 2 | 应用服务器-2 | 符合 | - | - | - | - | - | - | - |
| 部分符合 | - | - | - | - | - | - | - |
| 不符合 | - | - | - | - | - | - | - |
| 不适用 | - | - | - | - | - | - | - |
| 3 | 办公运维管理终端 | 符合 | - | - | - | - | - | - | - |
| 部分符合 | - | - | - | - | - | - | - |
| 不符合 | - | - | - | - | - | - | - |
| 不适用 | - | - | - | - | - | - | - |
| 总计测评项0个，符合项0个，部分符合项0个，不符合项0个，不适用项0个 | | | | | | | | | |

* + 1. 系统管理软件/平台

**附录 C 表-9 系统管理软件/平台单项测评结果汇总（安全通用要求）**

| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **身份鉴别** | **访问控制** | **安全审计** | **入侵防范** | **恶意代码防范** | **可信验证** | **数据完整性** | **数据保密性** | **数据备份恢复** | **剩余信息保护** | **个人信息保护** |
| 1 | 腾讯云控制台 | 符合 | - | - | - | - | - | - | - | - | - | - | - |
| 部分符合 | - | - | - | - | - | - | - | - | - | - | - |
| 不符合 | - | - | - | - | - | - | - | - | - | - | - |
| 不适用 | - | - | - | - | - | - | - | - | - | - | - |
| 2 | 腾讯云数据库 | 符合 | 2 | 5 | 4 | 1 | - | 0 | 2 | 2 | 2 | 2 | 0 |
| 部分符合 | 1 | 0 | 0 | 0 | - | 0 | 0 | 0 | 0 | 0 | 2 |
| 不符合 | 1 | 2 | 0 | 0 | - | 1 | 0 | 0 | 1 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 5 | - | 0 | 0 | 0 | 0 | 0 | 0 |
| 总计测评项33个，符合项20个，部分符合项3个，不符合项5个，不适用项5个 | | | | | | | | | | | | | |

**附录 C 表-10 系统管理软件/平台单项测评结果汇总（安全扩展要求）**

| **序号** | **测评对象** | **符合情况** | **安全扩展要求** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **身份鉴别（云计算）** | **访问控制（云计算）** | **入侵防范（云计算）** | **镜像和快照保护（云计算）** | **数据完整性和保密性（云计算）** | **数据备份恢复（云计算）** | **剩余信息保护（云计算）** |
| 1 | 腾讯云控制台 | 符合 | 1 | 0 | 2 | 0 | 1 | 1 | 0 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不适用 | 0 | 2 | 1 | 3 | 3 | 3 | 2 |
| 2 | 腾讯云数据库 | 符合 | - | - | - | - | - | - | - |
| 部分符合 | - | - | - | - | - | - | - |
| 不符合 | - | - | - | - | - | - | - |
| 不适用 | - | - | - | - | - | - | - |
| 总计测评项19个，符合项5个，部分符合项0个，不符合项0个，不适用项14个 | | | | | | | | | |

* + 1. 业务应用系统/平台

**附录 C 表-11 业务应用系统/平台单项测评结果汇总（安全通用要求）**

| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **身份鉴别** | **访问控制** | **安全审计** | **入侵防范** | **恶意代码防范** | **可信验证** | **数据完整性** | **数据保密性** | **数据备份恢复** | **剩余信息保护** | **个人信息保护** |
| 1 | SanyMall 客户云商城系统 | 符合 | 2 | 6 | 4 | 2 | - | 0 | 2 | 2 | 2 | 2 | 0 |
| 部分符合 | 1 | 0 | 0 | 0 | - | 0 | 0 | 0 | 0 | 0 | 2 |
| 不符合 | 1 | 1 | 0 | 0 | - | 1 | 0 | 0 | 1 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 4 | - | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 中间件-1 | 符合 | 0 | 0 | 4 | 1 | - | 0 | 0 | 0 | - | 0 | - |
| 部分符合 | 0 | 0 | 0 | 0 | - | 0 | 0 | 0 | - | 0 | - |
| 不符合 | 0 | 0 | 0 | 0 | - | 0 | 0 | 0 | - | 0 | - |
| 不适用 | 4 | 7 | 0 | 5 | - | 1 | 2 | 2 | - | 2 | - |
| 3 | 中间件-2 | 符合 | 0 | 0 | 4 | 1 | - | 0 | 0 | 0 | - | 0 | - |
| 部分符合 | 0 | 0 | 0 | 0 | - | 0 | 0 | 0 | - | 0 | - |
| 不符合 | 0 | 0 | 0 | 0 | - | 0 | 0 | 0 | - | 0 | - |
| 不适用 | 4 | 7 | 0 | 5 | - | 1 | 2 | 2 | - | 2 | - |
| 总计测评项89个，符合项32个，部分符合项3个，不符合项4个，不适用项50个 | | | | | | | | | | | | | |

**附录 C 表-12 业务应用系统/平台单项测评结果汇总（安全扩展要求）**

| **序号** | **测评对象** | **符合情况** | **安全扩展要求** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **身份鉴别（云计算）** | **访问控制（云计算）** | **入侵防范（云计算）** | **镜像和快照保护（云计算）** | **数据完整性和保密性（云计算）** | **数据备份恢复（云计算）** | **剩余信息保护（云计算）** |
| 1 | SanyMall 客户云商城系统 | 符合 | - | - | - | - | - | - | - |
| 部分符合 | - | - | - | - | - | - | - |
| 不符合 | - | - | - | - | - | - | - |
| 不适用 | - | - | - | - | - | - | - |
| 2 | 中间件-1 | 符合 | - | - | - | - | - | - | - |
| 部分符合 | - | - | - | - | - | - | - |
| 不符合 | - | - | - | - | - | - | - |
| 不适用 | - | - | - | - | - | - | - |
| 3 | 中间件-2 | 符合 | - | - | - | - | - | - | - |
| 部分符合 | - | - | - | - | - | - | - |
| 不符合 | - | - | - | - | - | - | - |
| 不适用 | - | - | - | - | - | - | - |
| 总计测评项0个，符合项0个，部分符合项0个，不符合项0个，不适用项0个 | | | | | | | | | |

* + 1. 数据资源

**附录 C 表-13 数据资源单项测评结果汇总（安全通用要求）**

| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **身份鉴别** | **访问控制** | **安全审计** | **入侵防范** | **恶意代码防范** | **可信验证** | **数据完整性** | **数据保密性** | **数据备份恢复** | **剩余信息保护** | **个人信息保护** |
| 1 | 重要业务数据 | 符合 | - | - | - | - | - | - | 1 | 1 | 2 | 2 | 0 |
| 部分符合 | - | - | - | - | - | - | 0 | 0 | 0 | 0 | 0 |
| 不符合 | - | - | - | - | - | - | 1 | 1 | 1 | 0 | 0 |
| 不适用 | - | - | - | - | - | - | 0 | 0 | 0 | 0 | 2 |
| 2 | 重要个人信息 | 符合 | - | - | - | - | - | - | 1 | 1 | 2 | 2 | 0 |
| 部分符合 | - | - | - | - | - | - | 0 | 0 | 0 | 0 | 2 |
| 不符合 | - | - | - | - | - | - | 1 | 1 | 1 | 0 | 0 |
| 不适用 | - | - | - | - | - | - | 0 | 0 | 0 | 0 | 0 |
| 总计测评项22个，符合项12个，部分符合项2个，不符合项6个，不适用项2个 | | | | | | | | | | | | | |

**附录 C 表-14 数据资源单项测评结果汇总（安全扩展要求）**

| **序号** | **测评对象** | **符合情况** | **安全扩展要求** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **身份鉴别（云计算）** | **访问控制（云计算）** | **入侵防范（云计算）** | **镜像和快照保护（云计算）** | **数据完整性和保密性（云计算）** | **数据备份恢复（云计算）** | **剩余信息保护（云计算）** |
| 1 | 重要业务数据 | 符合 | - | - | - | - | - | - | - |
| 部分符合 | - | - | - | - | - | - | - |
| 不符合 | - | - | - | - | - | - | - |
| 不适用 | - | - | - | - | - | - | - |
| 2 | 重要个人信息 | 符合 | - | - | - | - | - | - | - |
| 部分符合 | - | - | - | - | - | - | - |
| 不符合 | - | - | - | - | - | - | - |
| 不适用 | - | - | - | - | - | - | - |
| 总计测评项0个，符合项0个，部分符合项0个，不符合项0个，不适用项0个 | | | | | | | | | |

* 1. 安全管理中心

**附录 C 表-15 安全管理中心单项测评结果汇总（安全通用要求）**

| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **系统管理** | **审计管理** | **安全管理** | **集中管控** |
| 1 | 安全管理中心 | 符合 | 2 | 2 | 1 | 6 |
| 部分符合 | 0 | 0 | 1 | 0 |
| 不符合 | 0 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 |
| 总计测评项12个，符合项11个，部分符合项1个，不符合项0个，不适用项0个 | | | | | | |

**附录 C 表-16 安全管理中心单项测评结果汇总（安全扩展要求）**

| **序号** | **测评对象** | **符合情况** | **安全扩展要求** |
| --- | --- | --- | --- |
| **集中管控（云计算）** |
| 1 | 安全管理中心 | 符合 | 2 |
| 部分符合 | 0 |
| 不符合 | 0 |
| 不适用 | 2 |
| 总计测评项4个，符合项2个，部分符合项0个，不符合项0个，不适用项2个 | | | |

* 1. 安全管理制度

**附录 C 表-17 安全管理制度单项测评结果汇总（安全通用要求）**

| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **安全策略** | **管理制度** | **制定和发布** | **评审和修订** |
| 1 | 安全管理制度 | 符合 | 1 | 3 | 2 | 1 |
| 部分符合 | 0 | 0 | 0 | 0 |
| 不符合 | 0 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 |
| 总计测评项7个，符合项7个，部分符合项0个，不符合项0个，不适用项0个 | | | | | | |

* 1. 安全管理机构

**附录 C 表-18 安全管理机构单项测评结果汇总（安全通用要求）**

| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **岗位设置** | **人员配备** | **授权和审批** | **沟通和合作** | **审核和检查** |
| 1 | 安全管理机构 | 符合 | 2 | 1 | 3 | 3 | 3 |
| 部分符合 | 1 | 0 | 0 | 0 | 0 |
| 不符合 | 0 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 |
| 总计测评项14个，符合项12个，部分符合项1个，不符合项1个，不适用项0个 | | | | | | | |

* 1. 安全管理人员

**附录 C 表-19 安全管理人员单项测评结果汇总（安全通用要求）**

| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **人员录用** | **人员离岗** | **安全意识教育和培训** | **外部人员访问管理** |
| 1 | 安全管理人员 | 符合 | 2 | 2 | 3 | 4 |
| 部分符合 | 1 | 0 | 0 | 0 |
| 不符合 | 0 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 |
| 总计测评项12个，符合项11个，部分符合项1个，不符合项0个，不适用项0个 | | | | | | |

* 1. 安全建设管理

**附录 C 表-20 安全建设管理单项测评结果汇总（安全通用要求）**

| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **定级和备案** | **安全方案设计** | **产品采购和使用** | **自行软件开发** | **外包软件开发** | **工程实施** | **测试验收** | **系统交付** | **等级测评** | **服务供应商选择** |
| 1 | 安全建设管理 | 符合 | 4 | 3 | 3 | 6 | 0 | 3 | 1 | 3 | 3 | 3 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 0 |
| 总计测评项34个，符合项29个，部分符合项0个，不符合项2个，不适用项3个 | | | | | | | | | | | | |

**附录 C 表-21 安全建设管理单项测评结果汇总（安全扩展要求）**

| **序号** | **测评对象** | **符合情况** | **安全扩展要求** | |
| --- | --- | --- | --- | --- |
| **云服务商选择（云计算）** | **供应链管理（云计算）** |
| 1 | 安全建设管理 | 符合 | 5 | 3 |
| 部分符合 | 0 | 0 |
| 不符合 | 0 | 0 |
| 不适用 | 0 | 0 |
| 总计测评项8个，符合项8个，部分符合项0个，不符合项0个，不适用项0个 | | | | |

* 1. 安全运维管理

**附录 C 表-22 安全运维管理单项测评结果汇总（安全通用要求）**

| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **环境管理** | **资产管理** | **介质管理** | **设备维护管理** | **漏洞和风险管理** | **网络和系统安全管理** | **恶意代码防范管理** | **配置管理** | **密码管理** | **变更管理** | **备份与恢复管理** | **安全事件处置** | **应急预案管理** | **外包运维管理** |
| 1 | 安全运维管理 | 符合 | 1 | 3 | 2 | 3 | 2 | 10 | 2 | 2 | 2 | 3 | 3 | 4 | 4 | 0 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不适用 | 2 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 |
| 总计测评项48个，符合项41个，部分符合项0个，不符合项0个，不适用项7个 | | | | | | | | | | | | | | | | |

**附录 C 表-23 安全运维管理单项测评结果汇总（安全扩展要求）**

| **序号** | **测评对象** | **符合情况** | **安全扩展要求** |
| --- | --- | --- | --- |
| **云计算环境管理（云计算）** |
| 1 | 安全运维管理 | 符合 | 0 |
| 部分符合 | 0 |
| 不符合 | 0 |
| 不适用 | 1 |
| 总计测评项1个，符合项0个，部分符合项0个，不符合项0个，不适用项1个 | | | |

1. 单项测评结果记录
   1. 安全通信网络
      1. 安全通用要求部分

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 网络架构 | a）应保证网络设备的业务处理能力满足业务高峰期需要； | 经核查，被测系统部署于腾讯云上，在腾讯云上分配有专门的VPC，未出现由于设备性能存在瓶颈，而导致网络拥堵、阻断等情况。 | 符合 |
| b）应保证网络各个部分的带宽满足业务高峰期需要； | 经核查，被测应用系统部署于腾讯云上，在腾讯云上分配有专门的VPC网络区域，且已为该VPC区域分配了专门的网络地址，未出现接入网络和核心网络存在瓶颈情况。 | 符合 |
| c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址； | 经核查，被测应用系统部署于腾讯云上，在腾讯云上分配有专门的VPC网络区域，且已为该VPC区域分配了专门的网络地址。 | 符合 |
| d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段； | 经访谈管理员并查看腾讯云网络结构及物理网络部署：1、拓扑图与当前网络运行情况一致。2、重要网段未处在网络边界处。3、已开启有效的访问控制策略，可以防止非授权访问。 | 符合 |
| e）应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。 | 经访谈管理员并查看腾讯云网络结构及物理网络部署：1、腾讯云关键网络设备和线路已实现硬件冗余和线路冗余。2、云租户所有虚拟服务器均是采用了集群虚拟化部署，能保证系统的可用性。 | 符合 |
| 通信传输 | a）应采用校验技术或密码技术保证通信过程中数据的完整性； | 经核查，在管理网络系统云服务器及云安全产品均通过腾讯云企业子账号控制台进行管理访问，采用HTTPS协议登录腾讯云控制台，能够保证通信过程中数据的完整性。 | 符合 |
| b）应采用密码技术保证通信过程中数据的保密性。 | 经核查，在管理网络系统云服务器及云安全产品均通过腾讯云企业子账号控制台进行管理访问，采用HTTPS协议登录腾讯云控制台，能够保证通信过程中数据的保密性。 | 符合 |
| 可信验证 | a）可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 经核查，通信设备不具有可信根芯片或硬件，未基于可信根对通信设备的系统引导程序、系统程序、重要配置参数等进行可信验证。 | 不符合 |

* + 1. 云计算安全扩展要求部分

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 网络架构 | a）应保证云计算平台不承载高于其安全保护等级的业务应用系统； | 被测系统为云服务客户业务应用系统，安全保护等级为三级；应用系统部署在腾讯公有云IaaS服务平台，腾讯公有云IaaS服务平台安全保护等级为三级，腾讯公有云IaaS服务平台已通过网络安全等级测评(测评时间：2021.5、等级测评报告编号：440320-50052-00011-21-000008-01、测评结论：优、综合得分：96.3）。云计算平台承载的业务系统等级不高于云计算平台自身的安全保护等级。 | 符合 |
| b）应实现不同云服务客户虚拟网络之间的隔离； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 | 不适用 |
| c）应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 | 不适用 |
| d）应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 | 不适用 |
| e）应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务。 | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 | 不适用 |

* 1. 安全区域边界
     1. 安全通用要求部分
        1. 虚拟网络边界

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 边界防护 | a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信； | 经核查，被测系统部署在腾讯公有云IaaS服务平台，为云租户分配有专门的VPC网络区域，在VPC网络边界部署了高级版云防火墙访问控制设备，并配置了相应访问控制策略，对VPC边界的流量进行控制，实现VPC之间的隔离；云租户具有云防火墙管理权限，可根据业务需要或所发生的安全事件及时调整访问控制策略。 | 符合 |
| b）应能够对非授权设备私自联到内部网络的行为进行检查或限制； | 经核查，被测系统部署在腾讯公有云IaaS服务平台，为云服务客户业务应用系统，该项不适用。 | 不适用 |
| c）应能够对内部用户非授权联到外部网络的行为进行检查或限制； | 经核查，被测系统部署在腾讯公有云IaaS服务平台，为云服务客户业务应用系统，该项不适用。 | 不适用 |
| d）应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。 | 经核查，被测系统部署在腾讯公有云IaaS服务平台，未涉及部署无线网络，无无线用户，该项不适用。 | 不适用 |
| 访问控制 | a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信； | 经核查，被测系统部署在腾讯公有云IaaS服务平台，为云租户分配有专门的VPC网络区域，在VPC网络边界通过腾讯云安全组件云服务进行访问控制，有根据被测系统实际业务配置了相应出、入站规则。如：针对ping服务、系统业务访问端口、SSH(22)远程访问服务等通信设置了相应访问控制规则，默认情况下除允许通信外拒绝所有通信。 | 符合 |
| b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化； | 经核查，根据业务需求在腾讯云安全组件云服务上已配置了访问控制规则，不存在多余或无效的访问控制规则。 | 符合 |
| c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出； | 经核查，被测系统部署在腾讯公有云IaaS服务平台，为云租户分配有专门的VPC网络区域，在VPC网络边界通过腾讯云安全组件云服务进行访问控制，有根据被测系统实际业务配置了相应出、入站规则。如：针对ping服务、系统业务访问端口、SSH(22)远程访问服务等通信设置提供了相应访问控制规则，控制规则有精确到来源IP地址、目的IP地址及端口协议等。 | 符合 |
| d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力； | 经核查，被测系统部署在腾讯公有云IaaS服务平台，为云租户分配有专门的VPC网络区域，在VPC网络边界通过腾讯云安全组件云服务进行访问控制，有根据被测系统实际业务配置了相应出、入站规则。如：针对ping服务、系统业务访问端口、SSH(22)远程访问服务等通信设置提供了明确的访问控制规则，控制规则有精确到来源IP地址、目的IP地址及端口协议等。 | 符合 |
| e）应对进出网络的数据流实现基于应用协议和应用内容的访问控制。 | 经核查，为被测系统提供部署了Web应用防火墙云产品，且根据企业的需求已配置了安全策略；如已设置Web应用攻击防护、CC防护等。 | 符合 |
| 入侵防范 | a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为； | 经核查，为被测系统提供部署了主机安全云产品、Web应用防火墙云产品，主机安全云产品实现对云上虚拟服务器主机全量日志分析，对进程异常行为、异常账户、敏感文件篡改、异常网络连接等入侵行为进行检测及分析；同时，检测云上虚拟服务器主机恶意攻击行为，对进程、网络异常等行为进行预警。Web应用防火墙实现对Web应用进防护，防御各类OWASP常见Web攻击并过滤海量恶意CC攻击，保障网站业务安全性与可用性。 | 符合 |
| b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为； | 经核查，为被测系统提供部署了主机安全云产品、Web应用防火墙云产品，主机安全云产品实现对云上虚拟服务器主机全量日志分析，对进程异常行为、异常账户、敏感文件篡改、异常网络连接等入侵行为进行检测及分析；同时，检测云上虚拟服务器主机恶意攻击行为，对进程、网络异常等行为进行预警。Web应用防火墙实现对Web应用进防护，防御各类OWASP常见Web攻击并过滤海量恶意CC攻击，保障网站业务安全性与可用性。 | 符合 |
| c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析； | 经核查，未购买部署抗APT、态势感知等可检测新型网络攻击行为的安全服务。 | 不符合 |
| d）当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。 | 经核查，为被测系统提供部署了主机安全云产品、Web应用防火墙云产品，受到攻击时能够记录，如主机安全云产品中的高级防御告警信息：目标主机、目标端口、来源IP、来源端口、威胁类型、攻击方式、攻击时间及操作，并在发生严重入侵事件时提供告警机制。 | 符合 |
| 恶意代码和垃圾邮件防范 | a）应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新； | 经核查，为被测系统提供部署了主机安全云产品，通过主机安全云产品实现蠕虫病毒、勒索病毒、木马、网站后门等恶意代码的检测和隔离清除，自动升级相关恶意代码规则库，最近一次更新时间为：2021.12.20。 | 符合 |
| b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。 | 经核查，该应用系统不涉及邮件系统，故该项不适用。 | 不适用 |
| 安全审计 | a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； | 经核查，系统部署于腾讯云，被测系统相关云产品（Web应用防火墙云产品、主机安全云产品、云服务器等）所有操作行为通过云审计云产品进行审计；同时，通过主机安全云产品、Web应用防火墙云产品实现对网络中发生的各类安全事件进行审计。 | 符合 |
| b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 经核查，云审计操作日志，审计记录字段包括事件时间、操作者、事件名称、资源类型、资源名称、来源等与审计相关信息。 | 符合 |
| c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； | 经核查，由专人管理审计记录，无删改特定记录的权限，日志保存每天自动备份在指定对象存储空间上。 | 符合 |
| d）应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。 | 经核查，通过腾讯云企业子账号控制台进行管理访问相关云资源，用户对云服务资源的操作信息通过云审计云产品进行审计及分析。 | 符合 |
| 可信验证 | a）可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 1、网络边界设备不具有可信根芯片或硬件；2、未基于可信根对设备的系统引导程序、系统程序、重要配置参数等进行可信验证。 | 不符合 |

* + 1. 云计算安全扩展要求部分
       1. 虚拟网络边界

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 访问控制 | a）应在虚拟化网络边界部署访问控制机制，并设置访问控制规则； | 经核查，被测系统部署在腾讯公有云IaaS服务平台，为云租户分配有专门的VPC网络区域，在VPC网络边界通过腾讯云安全组件云服务进行访问控制，有根据被测系统实际业务配置了相应出、入站规则。如：针对ping服务、系统业务访问端口、SSH(22)远程访问服务等通信设置提供了相应访问控制规则，控制策略有达到端口级。 | 符合 |
| b）应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。 | 经访谈和核查，腾讯公有云IaaS服务平台在每个租户网络区域边界设置了访问控制，且该租户在边界处统一部署腾讯云安全组件云服务，设置访问控制规则，网络不存在其他非三级以外的网络区域边界。 | 符合 |
| 入侵防范 | a）应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 | 不适用 |
| b）应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； | 经访谈和核查，系统部署于腾讯云，为被测系统提供部署了主机安全云产品、Web应用防火墙云产品等相关安全服务，可以检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。 | 符合 |
| c）应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量； | 经访谈和核查，系统部署于腾讯云，为被测系统提供部署了主机安全云产品、Web应用防火墙云产品等相关安全服务；可以检测到虚拟机与宿主机、虚拟机之间的异常流量。 | 符合 |
| d）应在检测到网络攻击行为、异常流量情况时进行告警。 | 经访谈和核查，系统部署于腾讯云，为被测系统提供部署了主机安全云产品、Web应用防火墙云产品等相关安全服务；当检测到网络攻击行为、异常流量情况时以邮箱、短信形式实时告警。 | 符合 |
| 安全审计 | a）应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启； | 经访谈和核查，系统部署于腾讯云，为被测系统提供部署了云审计云产品，能对云服务商和云服务客户在远程管理时操作行为包括特权命令进行安全审计。 | 符合 |
| b）应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。 | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 | 不适用 |

* 1. 安全计算环境
     1. 安全通用要求部分
        1. 安全设备
           1. Web应用防火墙云产品

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 身份鉴别 | a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； | 经核查，管理Web应用防火墙云产品需要通过登录腾讯云企业子账号控制台进行管理访问，在腾讯云管理控制台账户中心安全设置中要求账号密码长度至少为8位，密码由数字+字母+特殊字符混合组成，设置账户的密码有效期为90天。 | 符合 |
| b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； | 经核查，设备未配置启用登录失败处理功能，未配置启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。 | 不符合 |
| c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 经核查，远程管理Web应用防火墙云产品需要登录腾讯云的企业账号，在控制端中对其进行安全管理。腾讯云使用的是https协议来进行远程通信，可防止鉴别数据在网络传输的过程中被窃听。 | 符合 |
| d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。 | 经核查，远程管理Web应用防火墙云产品需要通过腾讯云账号控制端。登录腾讯云账号要求通过用户名+口令和手机短信验证码进行身份鉴别；其中口令鉴别采用了密码技术（base64加私钥）实现。 | 符合 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经核查，管理员管理Web应用防火墙云产品需要通过登录腾讯云主账号控制台进行管理访问，该主账户具有对Web应用防火墙云产品的所有管理权限；未存在越权访问情况及未存在默认账户及匿名账户。 | 符合 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 经核查，管理Web应用防火墙云产品需要通过登录腾讯云控制台进行管理访问；腾讯云无默认账户和默认口令，子账号要求密码长度至少8位，必须包含数字+字母+特殊字符。 | 符合 |
| c）应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 经核查，目前管理Web应用防火墙云产品需要通过登录腾讯云控制台进行管理访问，当前腾讯云企业主账号具有所有权限，不存在其他账号，无多余、过期账户，也不存在多人共用一个账号的情况。 | 符合 |
| d）应授予管理用户所需的最小权限，实现管理用户的权限分离； | 经询问和核查，腾讯云为不同用户分配了不同权限账户进行管理，实现了管理用户的权限分离。 如腾讯云创建了系统管理员（sys\_admin)、安全管理员(sec\_admin)、审计管理员(audit\_admin)、运维用户(ops\_开头）和研发用户（dev\_开头），系统管理员主要是用于系统管理，拥有所有系统权限；安全管理员用于管理用户权限，授予云资源权限；审计管理员用于审计命令操作和系统操作日志，并定期检查；运维用户用于资源购买和分配；研发用户用于资源操作。 | 符合 |
| e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； | 经核查，由管理员对访问控制策略进行配置，且根据安全策略控制用户对信息的访问范围，未发现越权访问的情况。 | 符合 |
| f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； | 核查，访问控制的主体为用户，客体为产品配置文件。 | 符合 |
| g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 | 经核查，未对主体和客体设置安全标记，无法对系统账户和系统资源安全标记进行访问控制。 | 不符合 |
| 安全审计 | a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； | 经核查，Web应用防火墙云产品中已开启日志审计，日志类型包括攻击日志、访问日志等，审计范围覆盖重要的用户行为和重要安全事件。 | 符合 |
| b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 经核查攻击日志，日志记录字段包含时间、attack\_area、url、attack\_ip、attack\_type rule\_id、attack\_content risk\_level status count domain等与审计相关的信息内容。 | 符合 |
| c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； | 经核查，Web应用防火墙云产品上的审计记录默认保存180天，自动备份存储在指定空间中，无法删除修改日志内容。 | 符合 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经核查，Web应用防火墙云产品不支持手动关闭日志审计，因此不会遭到未经授权的中断。 | 符合 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经核查，此为Web应用防火墙云产品，遵循最小安装的原则，仅安装了需要的服务组件。 | 符合 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经核查，Web应用防火墙云产品只开启了必要的服务及端口如：https、443端口等，未开启其他端口及服务。 | 符合 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，该测评对象为腾讯云安全服务产品，只能通过腾讯云控制台进行访问控制，腾讯云控制台使用了https协议进行通信。 | 符合 |
| d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及安全产品，此项不适用。 | 不适用 |
| e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞； | 经核查，该测评对象为腾讯云上的安全产品，无法对其自身进行漏洞扫描来发现可能存在的已知漏洞，此项不适用。 | 不适用 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，该云安全产品具有针对Web网络攻击入侵防御功能，能对网络攻击入侵行为进行检测，并能提供报警。 | 符合 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 经核查：1、此产品不具有可信根芯片或硬件；2、未基于可信根对产品的系统引导程序、系统程序、重要配置参数等进行可信验证。 | 不符合 |
| 数据完整性 | a）应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 经核查，远程管理Web应用防火墙云产品需要登录腾讯云的企业账号，在控制端中对其进行安全管理。腾讯云使用的是https协议来进行远程通信，传输过程加密，可保证重要数据在传输过程中的完整性。 | 符合 |
| b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 | 经核查，腾讯云控制端针对用户鉴别数据采用SHA算法计算哈希值，用于完整性保护，能保证鉴别数据存储过程中的完整性。 | 符合 |
| 数据保密性 | a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； | 经核查，远程管理Web应用防火墙云产品需要登录腾讯云的企业账号，在控制端中对其进行安全管理。腾讯云使用的是https协议来进行远程通信，传输过程加密，可保证重要数据在传输过程中的保密性。 | 符合 |
| b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 | 经核查，腾讯云控制端针对用户口令采用加密算法进行加密，用户口令以密文形式保存，能保证鉴别数据存储过程中的保密性。 | 符合 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，腾讯云平台已针对云上安全产品的重要数据提供了本地备份与恢复。 | 符合 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 经核查，云上安全产品的重要数据由腾讯云平台负责管理，腾讯云平台已针对云上安全产品的重要数据提供了异地数据备份功能。 | 符合 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 腾讯云的云产品基于分布式操作系统高可用架构集群部署，支持用于基于业务处理能力，按照需求动态调整资源，能保证系统的高可用性。 | 符合 |

* + - * 1. 主机安全云产品

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 身份鉴别 | a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； | 经核查，管理主机安全云产品需要通过登录腾讯云企业子账号控制台进行管理访问，在腾讯云管理控制台账户中心安全设置中要求账号密码长度至少为8位，密码由数字+字母+特殊字符混合组成，设置账户的密码有效期为90天。 | 符合 |
| b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； | 经核查，设备未配置启用登录失败处理功能，未配置启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。 | 不符合 |
| c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 经核查，远程管理主机安全云产品需要登录腾讯云的企业账号，在控制端中对其进行安全管理。腾讯云使用的是https协议来进行远程通信，可防止鉴别数据在网络传输的过程中被窃听。 | 符合 |
| d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。 | 经核查，远程管理主机安全云产品需要通过腾讯云账号控制端。登录腾讯云账号要求通过用户名+口令和手机短信验证码进行身份鉴别；其中口令鉴别采用了密码技术（base64加私钥）实现。 | 符合 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经核查，管理员管理主机安全云产品需要通过登录腾讯云主账号控制台进行管理访问，该主账户具有对主机安全云产品的所有管理权限；未存在越权访问情况及未存在默认账户及匿名账户。 | 符合 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 经核查，管理主机安全云产品需要通过登录腾讯云控制台进行管理访问；腾讯云无默认账户和默认口令，子账号要求密码长度至少8位，必须包含数字+字母+特殊字符。 | 符合 |
| c）应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 经核查，目前管理主机安全云产品需要通过登录腾讯云控制台进行管理访问，当前腾讯云企业主账号具有所有权限，不存在其他账号，无多余、过期账户，也不存在多人共用一个账号的情况。 | 符合 |
| d）应授予管理用户所需的最小权限，实现管理用户的权限分离； | 经询问和核查，腾讯云为不同用户分配了不同权限账户进行管理，实现了管理用户的权限分离。 如腾讯云创建了系统管理员（sys\_admin)、安全管理员(sec\_admin)、审计管理员(audit\_admin)、运维用户(ops\_开头）和研发用户（dev\_开头），系统管理员主要是用于系统管理，拥有所有系统权限；安全管理员用于管理用户权限，授予云资源权限；审计管理员用于审计命令操作和系统操作日志，并定期检查；运维用户用于资源购买和分配；研发用户用于资源操作。 | 符合 |
| e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； | 经核查，由管理员对访问控制策略进行配置，且根据安全策略控制用户对信息的访问范围，未发现越权访问的情况。 | 符合 |
| f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； | 核查，访问控制的主体为用户，客体为产品配置文件。 | 符合 |
| g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 | 经核查，未对主体和客体设置安全标记，无法对系统账户和系统资源安全标记进行访问控制。 | 不符合 |
| 安全审计 | a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； | 经核查，主机安全云产品中已开启日志审计，日志类型包括入侵检测日志、高级防御日志等，审计范围覆盖重要的用户行为和重要安全事件。 | 符合 |
| b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 经核查入侵检测中的异常登录日志，日志记录字段包含服务器IP/名称 来源IP 来源地 登录用户名、登录时间、危险等级、状态等与审计相关的信息内容。 | 符合 |
| c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； | 经核查，主机安全云产品上的审计记录默认保存180天，自动备份存储在指定空间中，无法删除修改日志内容。 | 符合 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经核查，主机安全云产品不支持手动关闭日志审计，因此不会遭到未经授权的中断。 | 符合 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经核查，此为主机安全云产品，遵循最小安装的原则，仅安装了需要的服务组件。 | 符合 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经核查，主机安全云产品只开启了必要的服务及端口如：https、443端口等，未开启其他端口及服务。 | 符合 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，该测评对象为腾讯云安全服务产品，只能通过腾讯云控制台进行访问控制，腾讯云控制台使用了https协议进行通信。 | 符合 |
| d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及安全产品，此项不适用。 | 不适用 |
| e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞； | 经核查，该测评对象为腾讯云上的安全产品，无法对其自身进行漏洞扫描来发现可能存在的已知漏洞，此项不适用。 | 不适用 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，该云安全产品具有入侵检测及高级防御功能，能对入侵行为进行检测，并能提供报警。 | 符合 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 经核查：1、此产品不具有可信根芯片或硬件；2、未基于可信根对产品的系统引导程序、系统程序、重要配置参数等进行可信验证。 | 不符合 |
| 数据完整性 | a）应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 经核查，远程管理主机安全云产品需要登录腾讯云的企业账号，在控制端中对其进行安全管理。腾讯云使用的是https协议来进行远程通信，传输过程加密，可保证重要数据在传输过程中的完整性。 | 符合 |
| b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 | 经核查，腾讯云控制端针对用户鉴别数据采用SHA算法计算哈希值，用于完整性保护，能保证鉴别数据存储过程中的完整性。 | 符合 |
| 数据保密性 | a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； | 经核查，远程管理主机安全云产品需要登录腾讯云的企业账号，在控制端中对其进行安全管理。腾讯云使用的是https协议来进行远程通信，传输过程加密，可保证重要数据在传输过程中的保密性。 | 符合 |
| b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 | 经核查，腾讯云控制端针对用户口令采用加密算法进行加密，用户口令以密文形式保存，能保证鉴别数据存储过程中的保密性。 | 符合 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，腾讯云平台已针对云上安全产品的重要数据提供了本地备份与恢复。 | 符合 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 经核查，云上安全产品的重要数据由腾讯云平台负责管理，腾讯云平台已针对云上安全产品的重要数据提供了异地数据备份功能。 | 符合 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 腾讯云的云产品基于分布式操作系统高可用架构集群部署，支持用于基于业务处理能力，按照需求动态调整资源，能保证系统的高可用性。 | 符合 |

* + - * 1. 云审计云产品

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 身份鉴别 | a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； | 经核查，管理云审计云产品需要通过登录腾讯云企业子账号控制台进行管理访问，在腾讯云管理控制台账户中心安全设置中要求账号密码长度至少为8位，密码由数字+字母+特殊字符混合组成，设置账户的密码有效期为90天。 | 符合 |
| b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； | 经核查，设备未配置启用登录失败处理功能，未配置启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。 | 不符合 |
| c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 经核查，远程管理云审计云产品需要登录腾讯云的企业账号，在控制端中对其进行安全管理。腾讯云使用的是https协议来进行远程通信，可防止鉴别数据在网络传输的过程中被窃听。 | 符合 |
| d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。 | 经核查，远程管理云审计云产品需要通过腾讯云账号控制端。登录腾讯云账号要求通过用户名+口令和手机短信验证码进行身份鉴别；其中口令鉴别采用了密码技术（base64加私钥）实现。 | 符合 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经核查，管理员管理云审计云产品需要通过登录腾讯云主账号控制台进行管理访问，该主账户具有对云审计云产品的所有管理权限；未存在越权访问情况及未存在默认账户及匿名账户。 | 符合 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 经核查，管理云审计云产品需要通过登录腾讯云控制台进行管理访问；腾讯云无默认账户和默认口令，子账号要求密码长度至少8位，必须包含数字+字母+特殊字符。 | 符合 |
| c）应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 经核查，目前管理云审计云产品需要通过登录腾讯云控制台进行管理访问，当前腾讯云企业主账号具有所有权限，不存在其他账号，无多余、过期账户，也不存在多人共用一个账号的情况。 | 符合 |
| d）应授予管理用户所需的最小权限，实现管理用户的权限分离； | 经询问和核查，腾讯云为不同用户分配了不同权限账户进行管理，实现了管理用户的权限分离。 如腾讯云创建了系统管理员（sys\_admin)、安全管理员(sec\_admin)、审计管理员(audit\_admin)、运维用户(ops\_开头）和研发用户（dev\_开头），系统管理员主要是用于系统管理，拥有所有系统权限；安全管理员用于管理用户权限，授予云资源权限；审计管理员用于审计命令操作和系统操作日志，并定期检查；运维用户用于资源购买和分配；研发用户用于资源操作。 | 符合 |
| e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； | 经核查，由管理员对访问控制策略进行配置，且根据安全策略控制用户对信息的访问范围，未发现越权访问的情况。 | 符合 |
| f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； | 核查，访问控制的主体为用户，客体为产品配置文件。 | 符合 |
| g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 | 经核查，未对主体和客体设置安全标记，无法对系统账户和系统资源安全标记进行访问控制。 | 不符合 |
| 安全审计 | a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； | 经核查，云审计云产品能有效的记录下腾讯云账号内的所有操作行为，日志类型包括操作日志、历史日志等，审计范围覆盖重要的用户行为和重要安全事件。 | 符合 |
| b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 经核查操作日志，包括事件时间、操作者、事件名称、资源类型、资源名称等与审计相关的信息内容。 | 符合 |
| c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； | 经核查，云审计云产品上的审计记录能保存180天，自动备份存储在指定空间中，无法删除修改日志内容。 | 符合 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经核查，云审计云产品不支持手动关闭日志审计，因此不会遭到未经授权的中断。 | 符合 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经核查，此为云审计云产品，遵循最小安装的原则，仅安装了需要的服务组件。 | 符合 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经核查，云审计云产品只开启了必要的服务及端口如：https、443端口等，未开启其他端口及服务。 | 符合 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，该测评对象为腾讯云安全服务产品，只能通过腾讯云控制台进行访问控制，腾讯云控制台使用了https协议进行通信。 | 符合 |
| d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及安全产品，此项不适用。 | 不适用 |
| e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞； | 经核查，该测评对象为腾讯云上的安全产品，无法对其自身进行漏洞扫描来发现可能存在的已知漏洞，此项不适用。 | 不适用 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，该云安全产品为审计产品，不具备入侵检测功能，根据 GB/T 28448-2019，该项测评对象不涉及此产品，此项不适用。 | 不适用 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 经核查：1、此产品不具有可信根芯片或硬件；2、未基于可信根对产品的系统引导程序、系统程序、重要配置参数等进行可信验证。 | 不符合 |
| 数据完整性 | a）应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 经核查，远程管理云审计云产品需要登录腾讯云的企业账号，在控制端中对其进行安全管理。腾讯云使用的是https协议来进行远程通信，传输过程加密，可保证重要数据在传输过程中的完整性。 | 符合 |
| b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 | 经核查，腾讯云控制端针对用户鉴别数据采用SHA算法计算哈希值，用于完整性保护，能保证鉴别数据存储过程中的完整性。 | 符合 |
| 数据保密性 | a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； | 经核查，远程管理云审计云产品需要登录腾讯云的企业账号，在控制端中对其进行安全管理。腾讯云使用的是https协议来进行远程通信，传输过程加密，可保证重要数据在传输过程中的保密性。 | 符合 |
| b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 | 经核查，腾讯云控制端针对用户口令采用加密算法进行加密，用户口令以密文形式保存，能保证鉴别数据存储过程中的保密性。 | 符合 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，腾讯云平台已针对云上安全产品的重要数据提供了本地备份与恢复。 | 符合 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 经核查，云上安全产品的重要数据由腾讯云平台负责管理，腾讯云平台已针对云上安全产品的重要数据提供了异地数据备份功能。 | 符合 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 腾讯云的云产品基于分布式操作系统高可用架构集群部署，支持用于基于业务处理能力，按照需求动态调整资源，能保证系统的高可用性。 | 符合 |

* + - 1. 服务器和终端
         1. 应用服务器-1

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 身份鉴别 | a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； | 1、登录操作系统需要输入用户名和口令；2、操作系统用户具有唯一性，服务器为专人管理；3、经检测，未发现操作系统存在空口令用户；4、经检测，操作系统用户口令符合复杂性要求，口令由字母+数字+符号组成，位数8位以上；5、账户口令复杂度策略有按安全要求配置，相关策略设置如下(/etc/login.defs)： PASS\_MIN\_LEN 8，/etc/pam.d/system-auth文件，参数行password requisite后有添加pam\_cracklib.so try\_first\_pass retry=3 type= dcredit=1 lcredit=-1 miclass=2 minlen=8相关参数；6、账户口令定期90天更换。 | 符合 |
| b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； | 操作系统已设置启用登录失败处理功能，设置了限制非法登录次数及登录连接超时时间；相关参数配置： 1、经查看/etc/pam.d/sshd文件，参数行auth required后未添加 pam\_tally2.so deny=3 unlock\_time=120 even\_deny\_root root\_unlock\_time=60 相关参数；2、经查看/etc/Profile文件中已设置TMOUT1800等参数。 | 符合 |
| c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 经核查，远程管理服务器需要登录腾讯云的企业账号，在控制端中对其进行安全管理。腾讯云使用的是https协议来进行远程通信，可防止鉴别数据在网络传输的过程中被窃听。 | 符合 |
| d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。 | 经核查，远程管理服务器需要通过腾讯云账号控制端。登录腾讯云账号要求通过用户名+口令和手机短信验证码进行身份鉴别；其中口令鉴别采用了密码技术（base64加私钥）实现。 | 符合 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 操作系统为不同用户分配创建了不同登录账户及权限，如：root管理员、op审计员、security安全员用户；但未限制默认账户root访问权限。 | 部分符合 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、操作系统默认账户：root未进行重命名；2、操作系统默认账户：root的默认口令已修改。 | 符合 |
| c）应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 操作系统默认多余账户：bin、daemon、mail、lp、adm、nobody、operator等已被注释禁用。 | 符合 |
| d）应授予管理用户所需的最小权限，实现管理用户的权限分离； | 1、目前操作系统区分了管理员用户及审计员用户和安全员用户；2、已按最小权限原则，实现管理用户权限分离，区分设立了系统管理员、审计员、安全员角色。 | 符合 |
| e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； | 所有访问控制策略都由root账户负责配置，操作系统其它用户非root权限，访问控制策略已达到主体对客体的访问规则；及经测试验证，未用户存在越权访问情况。 | 符合 |
| f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； | 访问控制的粒度达到主体为用户，客体达到文件级。操作系统重要文件和目录权限(如：/etc/passwd、/etc/shadow等)设置合理。 | 符合 |
| g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 | 操作系统未提供设置安全标记功能。 | 不符合 |
| 安全审计 | a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； | 日志审计已开启，进程运行正常。 审计内容包括了用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、用户登录和退出等。 /etc/rsyslog.conf文件中有包含： \*.info;mail.none;authpriv.none;cron.none /var/log/messages等参数值。 | 符合 |
| b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 审计记录包括事件类型、日期与时间、详细信息等与审计相关信息内容。 | 符合 |
| c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； | 此服务器日志数据通过管理员设置备份策略进行定期备份，每45天备份一次，备份数据留存时长可达到6个月以上；且对备份数据进行了保护，非管理员无权进行删改。 | 符合 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经测试验证，对操作系统审计进程进行了保护，无法单独中断审计进程。 | 符合 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 操作系统安装遵循最小化安装原则，不存在业务所不需要的组件和应用程序。 | 符合 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | tak、talk、sendmail等非必要的系统服务已关闭，echo、shell、telnet、rsh、rlog等危险的服务已关闭，未存在默认共享。 | 符合 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，服务器只能通过腾讯云控制台进行访问控制，腾讯云控制台使用了SSH协议进行通信。 | 符合 |
| d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及操作系统层面，此项不适用。 | 不适用 |
| e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞； | 1、经漏扫（扫描设备型号：绿盟远程安全评估系统、系统版本：V6.0R04F01、漏洞库版本：2021112901），未发现此操作系统存在已知高危漏洞。2、经访谈系统管理员得知，对通过漏扫、渗透测试发现的问题经过充分测试评估后及时修补漏洞。 | 符合 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 操作系统已安装部署腾讯云主机安全云产品专业版，具备入侵防御功能，能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。自动升级相关入侵防御规则库，最近一次更新时间为：2021.12.20。 | 符合 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 操作系统已安装部署腾讯云主机安全云产品专业版，具备防恶意代码功能，能够及时识别入侵和病毒行为，并将其有效阻断。自动升级相关恶意代码规则库，最近一次更新时间为：2021.12.20。 | 符合 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 1、此主机不具有可信根芯片或硬件；2、未基于可信根对主机设备的系统引导程序、系统程序、重要配置参数等进行可信验证。 | 不符合 |
| 数据完整性 | a）应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 服务器采用SSH加密协议连接通信，传输过程加密，可保证重要数据在传输过程中的完整性。 | 符合 |
| b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 | 服务器针对用户鉴别数据采用SHA计算哈希值，用于完整性保护，能保证鉴别数据存储过程中的完整性。 | 符合 |
| 数据保密性 | a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； | 服务器采用SSH加密协议连接通信，传输过程加密，可保证重要数据在传输过程中的保密性。 | 符合 |
| b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 | 服务器针对鉴别数据(用户口令)采用DES加密算法进行加密以密文形式保存，可保证鉴别数据存储过程中的保密性。 | 符合 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 服务器操作系统重要数据(如：应用程序配置数据等)定期本地备份，一旦数据修改进行了更新，会即时备份；同时，已建立恢复测试机制，定期每半年对备份数据进行恢复测试验证。 | 符合 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 未提供异地实时备份环境，未利用通信网络将服务器上的重要数据(如：应用程序配置数据等)实时备份至备份场地。 | 不符合 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 此服务器为腾讯云平台虚机，采用集群虚拟化部署，能保证系统的高可用性。 | 符合 |
| 剩余信息保护 | a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除； | 经检查，断开服务器连接之后，内存存储数据会完全清除，重连服务器后，不会显示最终登录用户。 | 符合 |
| b）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。 | 经检查，断开服务器连接之后，内存存储数据会完全清除，重连服务器之前，存储数据会完全清除。 | 符合 |

* + - * 1. 应用服务器-2

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 身份鉴别 | a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； | 1、登录操作系统需要输入用户名和口令；2、操作系统用户具有唯一性，服务器为专人管理；3、经检测，未发现操作系统存在空口令用户；4、经检测，操作系统用户口令符合复杂性要求，口令由字母+数字+符号组成，位数8位以上；5、账户口令复杂度策略有按安全要求配置，相关策略设置如下(/etc/login.defs)： PASS\_MIN\_LEN 8 ，/etc/pam.d/system-auth文件，参数行password requisite后有添加pam\_cracklib.so try\_first\_pass retry=3 type= dcredit=1 lcredit=-1 miclass=2 minlen=8相关参数；6、账户口令定期90天更换。 | 符合 |
| b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； | 操作系统已设置启用登录失败处理功能，设置了限制非法登录次数及登录连接超时时间；相关参数配置： 1、经查看/etc/pam.d/sshd文件，参数行auth required后未添加 pam\_tally2.so deny=3 unlock\_time=120 even\_deny\_root root\_unlock\_time=60 相关参数；2、经查看/etc/Profile文件中已设置TMOUT1800等参数。 | 符合 |
| c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 经核查，远程管理服务器需要登录腾讯云的企业账号，在控制端中对其进行安全管理。腾讯云使用的是https协议来进行远程通信，可防止鉴别数据在网络传输的过程中被窃听。 | 符合 |
| d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。 | 经核查，远程管理服务器需要通过腾讯云账号控制端。登录腾讯云账号要求通过用户名+口令和手机短信验证码进行身份鉴别；其中口令鉴别采用了密码技术（base64加私钥）实现。 | 符合 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 操作系统为不同用户分配创建了不同登录账户及权限，如：root管理员、op审计员、security安全员用户；但未限制默认账户root访问权限。 | 部分符合 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1、操作系统默认账户：root未进行重命名；2、操作系统默认账户：root的默认口令已修改。 | 符合 |
| c）应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 操作系统默认多余账户：bin、daemon、mail、lp、adm、nobody、operator等已被注释禁用。 | 符合 |
| d）应授予管理用户所需的最小权限，实现管理用户的权限分离； | 1、目前操作系统区分了管理员用户及审计员用户和安全员用户；2、已按最小权限原则，实现管理用户权限分离，区分设立了系统管理员、审计员、安全员角色。 | 符合 |
| e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； | 所有访问控制策略都由root账户负责配置，操作系统其它用户非root权限，访问控制策略已达到主体对客体的访问规则；及经测试验证，未用户存在越权访问情况。 | 符合 |
| f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； | 访问控制的粒度达到主体为用户，客体达到文件级。操作系统重要文件和目录权限(如：/etc/passwd、/etc/shadow等)设置合理。 | 符合 |
| g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 | 操作系统未提供设置安全标记功能。 | 不符合 |
| 安全审计 | a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； | 日志审计已开启，进程运行正常。 审计内容包括了用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、用户登录和退出等。 /etc/rsyslog.conf文件中有包含： \*.info;mail.none;authpriv.none;cron.none /var/log/messages等参数值。 | 符合 |
| b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 审计记录包括事件类型、日期与时间、详细信息等与审计相关信息内容。 | 符合 |
| c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； | 此服务器日志数据通过管理员设置备份策略进行定期备份，每45天备份一次，备份数据留存时长可达到6个月以上；且对备份数据进行了保护，非管理员无权进行删改。 | 符合 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经测试验证，对操作系统审计进程进行了保护，无法单独中断审计进程。 | 符合 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 操作系统安装遵循最小化安装原则，不存在业务所不需要的组件和应用程序。 | 符合 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | tak、talk、sendmail等非必要的系统服务已关闭，echo、shell、telnet、rsh、rlog等危险的服务已关闭，未存在默认共享。 | 符合 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，服务器只能通过腾讯云控制台进行访问控制，腾讯云控制台使用了SSH协议进行通信。 | 符合 |
| d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及操作系统层面，此项不适用。 | 不适用 |
| e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞； | 1、经漏扫（扫描设备型号：绿盟远程安全评估系统、系统版本：V6.0R04F01、漏洞库版本：2021112901），未发现此操作系统存在已知高危漏洞。2、经访谈系统管理员得知，对通过漏扫、渗透测试发现的问题经过充分测试评估后及时修补漏洞。 | 符合 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 操作系统已安装部署腾讯云主机安全云产品专业版，具备入侵防御功能，能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。自动升级相关入侵防御规则库，最近一次更新时间为：2021.12.20。 | 符合 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 操作系统已安装部署腾讯云主机安全云产品专业版，具备防恶意代码功能，能够及时识别入侵和病毒行为，并将其有效阻断。自动升级相关恶意代码规则库，最近一次更新时间为：2021.12.20。 | 符合 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 1、此主机不具有可信根芯片或硬件；2、未基于可信根对主机设备的系统引导程序、系统程序、重要配置参数等进行可信验证。 | 不符合 |
| 数据完整性 | a）应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 服务器采用SSH加密协议连接通信，传输过程加密，可保证重要数据在传输过程中的完整性。 | 符合 |
| b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 | 服务器针对用户鉴别数据采用SHA计算哈希值，用于完整性保护，能保证鉴别数据存储过程中的完整性。 | 符合 |
| 数据保密性 | a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； | 服务器采用SSH加密协议连接通信，传输过程加密，可保证重要数据在传输过程中的保密性。 | 符合 |
| b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 | 服务器针对鉴别数据(用户口令)采用DES加密算法进行加密以密文形式保存，可保证鉴别数据存储过程中的保密性。 | 符合 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 服务器操作系统重要数据(如：应用程序配置数据等)定期本地备份，一旦数据修改进行了更新，会即时备份；同时，已建立恢复测试机制，定期每半年对备份数据进行恢复测试验证。 | 符合 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 未提供异地实时备份环境，未利用通信网络将服务器上的重要数据(如：应用程序配置数据等)实时备份至备份场地。 | 不符合 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 此服务器为腾讯云平台虚机，采用集群虚拟化部署，能保证系统的高可用性。 | 符合 |
| 剩余信息保护 | a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除； | 经检查，断开服务器连接之后，内存存储数据会完全清除，重连服务器后，不会显示最终登录用户。 | 符合 |
| b）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。 | 经检查，断开服务器连接之后，内存存储数据会完全清除，重连服务器之前，存储数据会完全清除。 | 符合 |

* + - * 1. 办公运维管理终端

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 身份鉴别 | a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； | 1、此终端为华为桌面云，通过域控账户进行身份标识和鉴别，使用用户名+口令认证方式进行登录；2、操作系统用户具有唯一性，为专人使用管理；3、操作系统用户口令符合复杂性要求，由字母+数字+符号混合组成，位数8位以上，且域控针对密码复杂度策略设置下发了统一策略，相关策略设置如下：  a）密码必须符合复杂度要求：已启用；  b）密码长度最小值：8个字符； c）强制密码历史：5个记住的密码  4、域控针对域账户设置为90天修改一次密码。 | 符合 |
| b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； | 此终端为华为桌面云，通过域控账户进行认证登录，域控针对登录失败设置下发了统一策略：账户连接错误登录6次锁定账户5分钟及登录会话空闲时间30分钟自动断开。 | 符合 |
| c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 此终端为华为桌面云，通过桌面接入网关代理访问对应的桌面，同桌面接入网关之间采用SSL加密的HDP协议进行信息传输，能防止鉴别信息在网络传输过程中被窃听。 | 符合 |
| d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。 | 此终端操作系统采用用户名+口令一种鉴别技术对用户身份进行认证鉴别，未采用两种或两种以上组合的鉴别技术。此主机仅为一台办公运维管理终端，非关键主机设备。 | 不符合 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 1、此办公运维终端为专人使用；2、操作系统%systemdrive%\windows\system重要目录Users组拥有读取和执行权限，everyone组无权限；%systemroot%\%system32\config等重要目录Users组、everyone组无权限。 | 符合 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 此终端为华为桌面云，通过域控账户进行身份标识和鉴别，未涉及存在本地默认登录账户。 | 不适用 |
| c）应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 此终端为华为桌面云，通过域控账户进行身份标识和鉴别功能，未存在多余的、过期的本地账户。 | 符合 |
| d）应授予管理用户所需的最小权限，实现管理用户的权限分离； | 1、此仅为一台办公运维管理终端，非关键主机设备，能通过域账户登录管理；2、经查看用户权限分配，“管理审核和安全日志”、“配置文件单一进程”等赋予administratos管理组拥有权限。 | 符合 |
| e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； | 1、配置访问控制策略的用户为操作系统域控管理账户：sanyits，为安全管理员角色；2、经查看本地重要文件目录权限设置合理，Users组拥有读取和执行权限，everyone组无权限；3、经测试验证，未用户存在越权访问情况。 | 符合 |
| f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； | 访问控制的粒度达到主体为用户，客体达到文件级。操作系统%systemdrive%\windows\system重要目录Users组仅拥有读取和执行权限，everyone组无权限。、 %systemroot%\%system32\config等重要目录Users组、everyone组无权限。 | 符合 |
| g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 | 操作系统未提供设置安全标记功能。 | 不符合 |
| 安全审计 | a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； | 操作系统日志审计功能已配置开启，审计范围覆盖到了所有重要用户行为和重要安全事件，相关参数配置如下： 审计账户登录事件：成功、失败； 审计账户管理：成功、失败； 审计目录服务访问：成功、失败； 审计登录事件：成功、失败； 审计对象访问：成功、失败； 审计策略更改：成功、失败； 审计特权使用：成功、失败； 审计系统事件：成功、失败。 | 符合 |
| b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 审计记录包括日期和时间、级别、来源、事件ID、任务类别、详细信息等与审计相关信息。 | 符合 |
| c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； | 此为一台办公运维终端，非关键主机设备，操作系统应用程序日志最大存储容量空间为80000，系统日志最大存储容量空间为29952KB，安全日志最大存储容量空间为99968KB；经核查，本地日志能查询到6个月以内的审计记录；对日志记录进行了保护，普通用户无法删改日志；但未对日志进行定期备份。 | 部分符合 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 只有administrator组具有“管理审核和安全日志”的权限。 | 符合 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 1、操作系统遵循最小安装原则，仅安装一些与工作相关软件；2、操作系统针对重大漏洞补丁进行了定期及时更新，最近一次更新时间为：2021.01.27。 | 符合 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 1、操作系统telnet等非必要的系统服务及默认共享已关闭；2、操作系统开启了135、139、445等危险端口服务。 | 部分符合 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 此终端为华为桌面云，通地域控账户登录，操作系统本地未开启远程管理服务。 | 不适用 |
| d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及主机操作系统，针对应用层面，此项不适用。 | 不适用 |
| e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞； | 1、经漏扫（扫描设备型号：绿盟远程安全评估系统、系统版本：V6.0R04F01、漏洞库版本：2021112901），未发现此操作系统存在已知高危漏洞。2、经访谈系统管理员得知，对通过漏扫、渗透测试发现的问题经过充分测试评估后及时修补漏洞。 | 符合 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 操作系统已安装部署云主机深度安全防护系统（系统版本：20.0.0.235），具有入侵检测功能，同时，相应特征库有自动在线升级更新至最新；当发生入侵事件时能提供报警。 | 符合 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 1、操作系统已安装部署云主机深度安全防护系统（系统版本：20.0.0.235 病毒库码：17.163.60），具有恶意代码防范功能，同时，相应特征库有自动在线升级更新至最新。2、经病毒查杀，未发现存在病毒和木马。 | 符合 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 1、此主机不具有可信根芯片或硬件；2、未基于可信根对主机设备的系统引导程序、系统程序、重要配置参数等进行可信验证。 | 不符合 |
| 数据完整性 | a）应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 此终端为华为桌面云，通过桌面接入网关代理访问对应的桌面，同桌面接入网关之间采用SSL加密的HDP协议进行信息传输，可保证重要数据在传输过程中的完整性。 | 符合 |
| b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 | 此终端为华为桌面云，通过桌面接入网关代理访问对应的桌面，针对鉴别数据采用SHA计算哈希值，用于完整性保护，能保证鉴别数据存储过程中的完整性。 | 符合 |
| 数据保密性 | a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； | 此终端为华为桌面云，通过桌面接入网关代理访问对应的桌面，同桌面接入网关之间采用SSL加密的HDP协议进行信息传输，可保证重要数据在传输过程中的保密性。 | 符合 |
| b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 | 终端对鉴别数据(用户口令)采用DES加密算法进行加密以密文形式保存，可保证鉴别数据存储过程中的保密性。 | 符合 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，此终端为桌面云，数据集中存储在华为桌面云平台数据中心；且管理员能够在出现故障后通过华为桌面云平台数据中心进行恢复。 | 符合 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 未提供异地备份环境，未利用通信网络将重要数据实时备份至备份场地。 | 不符合 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 经核查，此终端为桌面云，采用虚拟化集群部署。 | 符合 |
| 剩余信息保护 | a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除； | 经核查，操作系统用户的鉴别信息释放措施设置符合安全要求，设置如下： 安全选项“不显示最后的用户名”->已启用。 | 符合 |
| b）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。 | 操作系统存有敏感数据的存储空间被释放或重新分配前措施设置符合安全要求，设置如下：  安全选项“关机：清除虚拟内存页面文件”->已启用。 | 符合 |

* + - 1. 系统管理软件/平台
         1. 腾讯云数据库

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 身份鉴别 | a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； | 1、登录数据库控制台需输入账户与口令，用户标识唯一；2、数据库由专人管理，用户身份标识唯一，不存在同名用户；3、经测试验证，未存在空口令用户；4、数据库登录口令符合复杂性要求，口令由大写字母+小写字母+数字+字符，其中两种组成，位数8位以上；但口令未定期修改更换。 | 部分符合 |
| b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； | 经核查，数据库未配置启用登录失败处理功能，未配置启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。 | 不符合 |
| c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 经核查，远程管理数据库需要登录腾讯云的企业账号，在控制端中对其进行安全管理。腾讯云使用的是https协议来进行远程通信，可防止鉴别数据在网络传输的过程中被窃听。 | 符合 |
| d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。 | 经核查，远程管理数据库需要通过腾讯云账号控制端。登录腾讯云账号要求通过用户名+口令和手机短信验证码进行身份鉴别；其中口令鉴别采用了密码技术（base64加私钥）实现。 | 符合 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 数据库为不同登录用户分配创建了不同账户(root、khymall、sanykhy等)及权限；但未限制默认账户root访问权限。 | 符合 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 经核查，数据库对root默认账户未进行重命名，但对默认账户的默认登录口令进行了修改。 | 符合 |
| c）应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 数据库不存在多余的帐号。 | 符合 |
| d）应授予管理用户所需的最小权限，实现管理用户的权限分离； | 未制定提供用户权限表，未按不同用户角色创建不同用户(管理员、审计员、操作员),目前数据库仅设置了管理用户及业务应用用户。 | 不符合 |
| e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； | 所有访问控制策略都由数据库管理员账户负责配置，访问控制策略已达到主体对客体的访问规则；及经测试验证，未用户存在越权访问情况。 | 符合 |
| f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； | 访问控制的粒度达到主体为用户，客体达到数据库表级。 | 符合 |
| g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 | 不具备对主客体设置敏感标记的功能。 | 不符合 |
| 安全审计 | a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； | 日志审计已配置并启用，审计范围覆盖了重要的用户行为和重要安全事件。相关参数配置如下： 控制台-操作日志-慢日志明细、错误日志明细等。 | 符合 |
| b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 经查看，审计记录包括日期、事件类型、详细内容、状态等与审计相关的信息内容。 | 符合 |
| c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； | 此数据库日志备份至腾讯云北京备份中心，备份数据留存时长为180天；且对备份数据进行了保护，非管理员无权进行删改。 | 符合 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 数据库有保护审计进程，审计进程启动用户为root，仅root能修改审计进程。 | 符合 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及数据库系统，此项不适用。 | 不适用 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及数据库系统，此项不适用。 | 不适用 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及数据库系统，此项不适用。 | 不适用 |
| d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及数据库，针对应用层面，此项不适用。 | 不适用 |
| e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞； | 1、经漏扫（扫描设备型号：绿盟远程安全评估系统、系统版本：V6.0R04F01、漏洞库版本：2021112901），未发现此数据库存在已知高危漏洞。2、经访谈系统管理员得知，对通过漏扫、渗透测试发现的问题经过充分测试评估后及时修补漏洞。 | 符合 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 此项一般在具备入侵检测功能设备上实现，数据库不涉及该核查项，此项不适用。 | 不适用 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 1、数据库所在的服务器主机不具有可信根芯片或硬件；2、未基于可信根对数据库所在的服务器主机设备的系统引导程序、系统程序、重要配置参数等进行可信验证。 | 不符合 |
| 数据完整性 | a）应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 此数据库为腾讯云数据库，采用HTTPS协议通过腾讯云管理控制台登录访问腾讯云数据库，传输过程加密；可保证重要数据在传输过程中的完整性。 | 符合 |
| b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 | 经核查，腾讯云控制端针对用户鉴别数据采用SHA算法计算哈希值，用于完整性保护，能保证鉴别数据存储过程中的完整性。 | 符合 |
| 数据保密性 | a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； | 此数据库为腾讯云数据库，采用HTTPS协议通过腾讯云管理控制台登录访问腾讯云数据库，传输过程加密；可保证重要数据在传输过程中的保密性。 | 符合 |
| b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 | 经核查，腾讯云控制端针对用户口令采用DES加密算法进行了加密，用户口令以密文形式保存，能保证鉴别数据存储过程中的保密性。 | 符合 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 此数据库为腾讯云数据库，系统业务数据库采用实时备份，备份位置：北京腾讯云备份中心；同时，已建立恢复测试机制，定期每半年对备份数据进行恢复测试验证。 | 符合 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 未提供异地实时备份环境，未利用通信网络将系统上的业务等重要数据实时备份至备份场地。 | 不符合 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 此数据库为腾讯云数据库，能保证数据库服务的高可用性。 | 符合 |
| 剩余信息保护 | a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除； | 经测试验证，删除数据库账户后，无法用此账户再进行登录及此账户相关鉴别信息也随之被完全清除。 | 符合 |
| b）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。 | 经测试验证，删除数据库账户后，跟此账户相关存储的敏感数据也随之被完全清除。 | 符合 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 数据库仅采集和保存了业务必需的用户个人信息，如：用户名、手机号、邮箱、密码等；但未制定有关用户个人信息保护管理制度和流程。 | 部分符合 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 数据库存储的SanyMall客户云商城系统个人用户详细信息只有管理人员及相关权限人员才能查询到；但未制定有关用户个人信息保护管理制度和流程。 | 部分符合 |

* + - * 1. 中间件-1

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 身份鉴别 | a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。 | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| c）应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| d）应授予管理用户所需的最小权限，实现管理用户的权限分离； | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及中间件，此项不适用。 | 不适用 |
| g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及中间件，此项不适用。 | 不适用 |
| 安全审计 | a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； | 日志审计已开启，进程运行正常。审计范围覆盖重要安全事件，相关设置： 经查看/usr/local/nginx/logs文件，相关参数配置如下：  error\_log /var/log/nginx/error.log notice；  access\_log /data/applogs/khymall.access.log common。 | 符合 |
| b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 日志记录包括事件的日期、时间、用户、事件类型等消息内容。 | 符合 |
| c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； | 中间件日志通过管理员备份策略，实时备份至服务器本机，能查询到6个月以内的日志，能避免受到未预期的删除、修改或覆盖等。 | 符合 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 审计进程与中间件主进程关联，无法单独中断审计进程。 | 符合 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及中间件，此项不适用。 | 不适用 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及中间件，此项不适用。 | 不适用 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及中间件，此项不适用。 | 不适用 |
| d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及中间件，此项不适用。 | 不适用 |
| e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞； | 1、经漏扫（扫描设备型号：绿盟远程安全评估系统、系统版本：V6.0R04F01、漏洞库版本：2021112901），未发现此中间件存在已知高危漏洞。2、经访谈系统管理员得知，对通过漏扫、渗透测试发现的问题经过充分测试评估后及时修补漏洞。 | 符合 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及中间件，此项不适用。 | 不适用 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及中间件，此项不适用。 | 不适用 |
| 数据完整性 | a）应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| 数据保密性 | a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| 剩余信息保护 | a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除； | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| b）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。 | 经核查，中间件管理控制台未配置启用。 | 不适用 |

* + - * 1. 中间件-2

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 身份鉴别 | a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。 | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| c）应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| d）应授予管理用户所需的最小权限，实现管理用户的权限分离； | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及中间件，此项不适用。 | 不适用 |
| g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及中间件，此项不适用。 | 不适用 |
| 安全审计 | a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； | 日志审计已开启，进程运行正常。审计范围覆盖重要安全事件，相关设置： 经查看/usr/local/nginx/logs文件，相关参数配置如下：  error\_log /var/log/nginx/error.log notice；  access\_log /data/applogs/khymall.access.log common。 | 符合 |
| b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 日志记录包括事件的日期、时间、用户、事件类型等消息内容。 | 符合 |
| c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； | 中间件日志通过管理员备份策略，实时备份至服务器本机，能查询到6个月以内的日志，能避免受到未预期的删除、修改或覆盖等。 | 符合 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 审计进程与中间件主进程关联，无法单独中断审计进程。 | 符合 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及中间件，此项不适用。 | 不适用 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及中间件，此项不适用。 | 不适用 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及中间件，此项不适用。 | 不适用 |
| d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及中间件，此项不适用。 | 不适用 |
| e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞； | 1、经漏扫（扫描设备型号：绿盟远程安全评估系统、系统版本：V6.0R04F01、漏洞库版本：2021112901），未发现此中间件存在已知高危漏洞。2、经访谈系统管理员得知，对通过漏扫、渗透测试发现的问题经过充分测试评估后及时修补漏洞。 | 符合 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及中间件，此项不适用。 | 不适用 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及中间件，此项不适用。 | 不适用 |
| 数据完整性 | a）应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| 数据保密性 | a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| 剩余信息保护 | a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除； | 经核查，中间件管理控制台未配置启用。 | 不适用 |
| b）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。 | 经核查，中间件管理控制台未配置启用。 | 不适用 |

* + - 1. 业务应用系统/平台
         1. SanyMall 客户云商城系统

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 身份鉴别 | a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； | 经核查，SanyMall客户云商城系统采用B/S架构，系统提供了一种登录方式。1、后台通过用户名+口令进行身份鉴别。2、商家中心通过用户名+口令+验证码进行身份鉴别。3、商城前台用户由树根系统统一身份验证。可保障鉴别及标识具有唯一性。同时，系统设置提供了身份鉴别信息复杂度校验功能，密码必须包含字母及数字，密码长度要求（不能小于8位)；但对口令未强制要求进行定期更换。 | 部分符合 |
| b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； | 经核查，系统设置了登录失败处理功能，连续登录失败达到10次，锁定10个小时，10个小时后自动解锁；及设置了登录会话空闲时间15分钟自动断开连接。 | 符合 |
| c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 经测试，系统针对用户鉴别信息（如：用户登录口令）采用了加密技术（Bcrypt加密）进行传输，可实现通信过程的保密性。 | 符合 |
| d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。 | 经核查：1、SanyMall客户云商城系统后台采用用户名+口令一种鉴别技术实现用户身份鉴别，SanyMall客户云商城系统商家中心通过用户名+口令+图形验证码一种鉴别技术实现用户身份鉴别，未采用两种或两种以上组合的鉴别技术实现用户身份鉴别，但后台及商家中心限制了访问地址范围，仅允许内网访问；2、SanyMall客户云商城系统前台用户由树根系统统一身份验证（采用用户名+口令），未采用两种或两种以上组合的鉴别技术实现用户身份鉴别。 | 不符合 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 经核查，SanyMall客户云商城系统根据不同用户工作需求给予不同权限，系统划分为：平台总运营、平台基础运营、商城报表查询、订单管理、聚合页配置等5个不同权限组。每个权限组又可以依据不同用途划分不同栏目权限；及未存在匿名、默认账户。 | 符合 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 经核查，SanyMall客户云商城系统不存在默认账户及默认口令。 | 符合 |
| c）应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 经核查，SanyMall客户云商城系统中不存在过期或多余的账户，不存在用户共享的情况。 | 符合 |
| d）应授予管理用户所需的最小权限，实现管理用户的权限分离； | 经核查，SanyMall客户云商城系统区分设立系统管理员、操作员、审计员相关角色用户，按最小权限原则，实现管理用户权限分离。 | 符合 |
| e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； | 经核查，SanyMall客户云商城系统访问控制策略均由管理员进行设定，根据用户工作需求所设定访问规则；及经测试验证，系统用户未存在越权访问情况。 | 符合 |
| f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； | 经核查，SanyMall客户云商城系统访问控制策略均以达到系统功能的每个子项，且可对每个子项的查看、管理权限进行细分。 | 符合 |
| g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 | 经核查，系统未对重要主体和客体设置安全标记。 | 不符合 |
| 安全审计 | a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； | 经核查，系统开启了安全审计功能，审计内容覆盖到了所有用户，对重要用户行为和重要安全事件进行了安全审计。 | 符合 |
| b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 经核查，SanyMall客户云商城系统审计记录包括：记录了时间、用户名、IP地址、操作内容、结果等。用户登录日志保存在system\_adminloginlog表中。操作日志保存在system\_seller\_log表中。 | 符合 |
| c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； | 经核查，SanyMall客户云商城系统所有审计记录均保存在服务器上，以文本形式保存，前台用户无法对其进行删除、修改及覆盖等操作。日志留储时间系统上线（2019年4月上线）至今。保存时间超过6个月。 | 符合 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 经核查，经核查，SanyMall客户云商城系统为B/S应用程序，审计进程无法单独中断。 | 符合 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 经核查，SanyMall客户云商城系统为B/S应用程序，为应用系统，固该项不适用。 | 不适用 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经核查，SanyMall客户云商城系统为B/S应用程序，为应用系统，固该项不适用。 | 不适用 |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及应用系统，此项不适用。 | 不适用 |
| d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； | 经渗透测试验证，发现该系统存在SQL注入高危漏洞及存储型跨站高危漏洞，但经回归测试已经修复该漏洞，应用系统对数据有效性进行了校验，对无效或非法数据进行了过滤。 | 符合 |
| e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞； | 1、经漏扫（扫描设备型号：绿盟远程安全评估系统、系统版本：V6.0R04F01、漏洞库版本：2021112901），未发现此系统存在已知高危漏洞；2、经渗透测试，发现该系统存在SQL注入高危漏洞及存储型跨站高危漏洞，经回归测试已经修复该漏洞；2、经访谈管理员得知，对通过漏扫、渗透测试发现的问题经过充分测试评估后会及时修补漏洞。 | 符合 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，根据 GB/T 28448-2019，该项测评对象不涉及应用系统，此项不适用。 | 不适用 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 经核查，系统未基于可信根对应用程序等关键执行环节进行动态可信验证。 | 不符合 |
| 数据完整性 | a）应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 经核查，SanyMall客户云商城系统为B/S架构，在传输过程中采用了密码技术https加密协议，可保证重要数据在传输过程中的完整性。 | 符合 |
| b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 | 经核查，系统对用户鉴别数据采用Hash加密算法计算哈希值，用于完整性保护，能保证鉴别数据存储过程中的完整性。 | 符合 |
| 数据保密性 | a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； | 经核查，SanyMall客户云商城系统为B/S架构，在传输过程中采用了密码技术https加密协议，可保证重要数据在传输过程中的保密性。 | 符合 |
| b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 | 经核查，系统对用户密码采用了Bcrypt加密工具进行加密，用户口令以密文形式保存，能保证鉴别数据存储过程中的保密性。 | 符合 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，被测系统数据库采用的是腾讯云数据库，系统业务数据采用实时备份，备份位置：北京腾讯云备份中心；同时，已建立恢复测试机制，定期每半年对备份数据进行恢复测试验证。 | 符合 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 未提供异地实时备份环境，未利用通信网络将系统上业务等重要数据实时备份至备份场地。 | 不符合 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 系统服务器为腾讯云平台虚机，采用集群虚拟化部署，能保证系统的高可用性。 | 符合 |
| 剩余信息保护 | a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除； | 经核查，SanyMall客户云商城系统在注消后可释放cookie信息，可保证身份鉴别信息完全清除。 | 符合 |
| b）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。 | 经核查，SanyMall客户云商城系统为B/S应用系统，所有查询、添加、修改等动作均为数据操作。当完成动作后数据库会自动释放或重新分配空间。 | 符合 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 经核查，SanyMall客户云商城系统仅采集和保存了业务必需用户个人信息；如：用户名、手机号、邮箱、密码等；但未制定有关用户个人信息保护管理制度和流程。 | 部分符合 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 经核查，SanyMall客户云商城系统用户个人详细信息只有管理人员及相关权限人员才能查询到；但未制定有关用户个人信息保护管理制度和流程。 | 部分符合 |

* + - 1. 数据资源
         1. 重要业务数据

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 数据完整性 | a）应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 经核查，SanyMall客户云商城系统为B/S架构，在传输过程中采用了密码技术https加密协议，可保证重要数据在传输过程中的完整性。 | 符合 |
| b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 | 核查，SanyMall客户云商城系统针对重要业务数据未采用校验技术或密码技术保证存储过程中的完整性。 | 不符合 |
| 数据保密性 | a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； | 经核查，SanyMall客户云商城系统为B/S架构，在传输过程中采用了密码技术https加密协议，可保证重要数据在传输过程中的保密性。 | 符合 |
| b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 | 经核查，SanyMall客户云商城系统针对重要业务数据未采用密码技术保证存储过程中的保密。 | 不符合 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，被测系统数据库采用的是腾讯云数据库，系统业务数据采用实时备份，备份位置：北京腾讯云备份中心；同时，已建立恢复测试机制，定期每半年对备份数据进行恢复测试验证。 | 符合 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 未提供异地实时备份环境，未利用通信网络将系统上业务等重要数据实时备份至备份场地。 | 不符合 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 系统服务器为腾讯云平台虚机，采用集群虚拟化部署，能保证系统的高可用性。 | 符合 |
| 剩余信息保护 | a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除； | 经核查，SanyMall客户云商城系统在注消后可释放cookie信息，可保证身份鉴别信息完全清除。 | 符合 |
| b）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。 | 经核查，SanyMall客户云商城系统为B/S应用系统，所有查询、添加、修改等动作均为数据操作。当完成动作后数据库会自动释放或重新分配空间。 | 符合 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 经核查，该项针对个人信息，不涉及重要业务数据测评对象，此项不适用。 | 不适用 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 经核查，该项针对个人信息，不涉及重要业务数据测评对象，此项不适用。 | 不适用 |

* + - * 1. 重要个人信息

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 数据完整性 | a）应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 经核查，SanyMall客户云商城系统为B/S架构，在传输过程中采用了密码技术https加密协议，可保证重要数据在传输过程中的完整性。 | 符合 |
| b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 | 经核查，SanyMall客户云商城系统针对重要个人信息未采用校验技术或密码技术保证存储过程中的完整性。 | 不符合 |
| 数据保密性 | a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； | 经核查，SanyMall客户云商城系统为B/S架构，在传输过程中采用了密码技术https加密协议，可保证重要数据在传输过程中的保密性。 | 符合 |
| b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 | 经核查，SanyMall客户云商城系统针对重要个人信息未采用密码技术保证存储过程中的保密。 | 不符合 |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | 经核查，被测系统数据库采用的是腾讯云数据库，系统业务数据采用实时备份，备份位置：北京腾讯云备份中心；同时，已建立恢复测试机制，定期每半年对备份数据进行恢复测试验证。 | 符合 |
| b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | 未提供异地实时备份环境，未利用通信网络将系统上业务等重要数据实时备份至备份场地。 | 不符合 |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 系统服务器为腾讯云平台虚机，采用集群虚拟化部署，能保证系统的高可用性。 | 符合 |
| 剩余信息保护 | a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除； | 经核查，SanyMall客户云商城系统在注消后可释放cookie信息，可保证身份鉴别信息完全清除。 | 符合 |
| b）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。 | 经核查，SanyMall客户云商城系统为B/S应用系统，所有查询、添加、修改等动作均为数据操作。当完成动作后数据库会自动释放或重新分配空间。 | 符合 |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 经核查，SanyMall客户云商城系统仅采集和保存了业务必需用户个人信息；如：用户名、手机号、邮箱、密码等；但未制定有关用户个人信息保护管理制度和流程。 | 部分符合 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 经核查，SanyMall客户云商城系统用户个人详细信息只有管理人员及相关权限人员才能查询到；但未制定有关用户个人信息保护管理制度和流程。 | 部分符合 |

* + 1. 云计算安全扩展要求部分
       1. 系统管理软件/平台
          1. 腾讯云控制台

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 身份鉴别 | a）当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。 | 当通过腾讯云控制台远程管理腾讯公有云Iaas服务平台上的服务器、云数据库等产品及服务时，通过HTTPS实现了双向认证。 | 符合 |
| 访问控制 | a）应保证当虚拟机迁移时，访问控制策略随其迁移； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 | 不适用 |
| b）应允许云服务客户设置不同虚拟机之间的访问控制策略。 | 被测系统部署在腾讯公有云IaaS服务平台，为云服务客户业务应用系统，该项不适用。 | 不适用 |
| 入侵防范 | a）应能检测虚拟机之间的资源隔离失效，并进行告警； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 | 不适用 |
| b）应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警； | 经核查，当非授权对新建虚拟机或重新启用虚拟机，会提示进行告警。 | 符合 |
| c）应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。 | 经核查，为被测系统提供部署了主机安全云产品，具有恶意代码检测功能；当检测虚拟机感染恶意代码时，会进行提醒告警。 | 符合 |
| 镜像和快照保护 | a）应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 | 不适用 |
| b）应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 | 不适用 |
| c）应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 | 不适用 |
| 数据完整性和保密性 | a）应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定； | 被测系统为云服务客户业务应用系统，部署在腾讯公有云Iaas服务平台，数据存储在中国境内，服务模式为：IaaS模式。 | 符合 |
| b）应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 | 不适用 |
| c）应使用校验码或密码技术确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 | 不适用 |
| d）应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。 | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 | 不适用 |
| 数据备份恢复 | a）云服务客户应在本地保存其业务数据的备份； | 云计算平台提供了备份功能，被测系统数据库采用的是腾讯云数据库，系统业务数据采用实时备份，备份位置：北京腾讯云备份中心。 | 符合 |
| b）应提供查询云服务客户数据及备份存储位置的能力； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 | 不适用 |
| c）云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 | 不适用 |
| d）应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。 | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 | 不适用 |
| 剩余信息保护 | a）应保证虚拟机所使用的内存和存储空间回收时得到完全清除； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 | 不适用 |
| b）云服务客户删除业务应用数据时，云计算平台应将云存储在所有副本删除。 | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 | 不适用 |

* 1. 安全管理中心
     1. 安全通用要求部分

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 系统管理 | a）应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计； | 经核查，通过腾讯云控制台对系统管理员进行身份鉴别，只允许管理员通过腾讯云控制台对系统进行管理操作，腾讯云控制台云审计云产品对这些操作进行审计。 | 符合 |
| b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。 | 经核查，系统管理员使用腾讯云控制台对系统的资源和运行进行配置、控制和管理，包括用户身份、资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复。 | 符合 |
| 审计管理 | a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计； | 经核查，通过腾讯云控制台中的云审计云产品存储记录腾讯云账号内的所有操作行为；审计管理员通过登录到腾讯云控制台中的云审计云产品对日志进行管理，并对审计管理员的操作进行审计记录。 | 符合 |
| b）应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。 | 经核查，通过腾讯云控制台中的云审计云产品存储记录腾讯云账号内的所有操作行为；审计管理员通过登录到腾讯云控制台中的云审计云产品对日志进行管理，审计管理员通过登录到腾讯云控制台中的云审计云产品对日志进行存储、管理和查询等。 | 符合 |
| 安全管理 | a）应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计； | 经核查，相关云产品（Web应用防火墙、主机安全等）统一通过登录腾讯云企业子账号控制台进行管理访问，对云产品进行管理操作，且对操作进行审计记录。 | 符合 |
| b）应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。 | 经核查，已设立安全管理员，安全管理员对安全策略进行配置和管理，但不包括可信验证策略和安全标记策略。 | 部分符合 |
| 集中管控 | a）应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控； | 经核查，腾讯云为租户已分配了专用VPC，对安全产品、服务器等进行统一管控。 | 符合 |
| b）应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理； | 经核查，相关云产品（Web应用防火墙、主机安全等）统一通过登录腾讯云企业子账号控制台进行管理访问，腾讯云控制台采用https协议进行登录访问，传输过程加密。 | 符合 |
| c）应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测； | 经核查，被测系统部署在腾讯云平台，通过腾讯云控制台云监控服务，可以对云安全产品、云服务器等运行状态进行集中监测并能依据设定的阀值实时报警。 | 符合 |
| d）应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求； | 经核查，系统相关云产品（Web应用防火墙云产品、主机安全云产品等）通过腾讯云云审计云产品进行集中统一收集保存与审计分析等管理，日志留存时长可达到6个月，专职人员定期分析。 | 符合 |
| e）应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理； | 经核查，Web应用防火墙云产品、主机安全云产品及云审计云产品安全策略，云服务器操作系统病毒库及补丁升级均由腾讯云的企业账号在腾讯云控制台进行统一集中管理。 | 符合 |
| f）应能对网络中发生的各类安全事件进行识别、报警和分析。 | 经核查，已购买部署Web应用防火墙云产品、主机安全云产品等相关安全产品，能对网络中发生的各类安全事件进行识别、报警和分析。 | 符合 |

* + 1. 云计算安全扩展要求部分

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 集中管控 | a）应能对物理资源和虚拟资源按照策略做统一管理调度与分配； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 | 不适用 |
| b）应保证云计算平台管理流量与云服务客户业务流量分离； | 被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 | 不适用 |
| c）应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计； | 经核查，系统部署于腾讯云，为被测系统提供部署了云审计云产品；对安全服务进行集中审计；及云租户可对审计日志进行查看并可对日志进行审计。 | 符合 |
| d）应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。 | 经核查，腾讯云控制台实现操作审计、职权管控、安全认证功能，记录所有操作记录；各设备的运行状态由阿里云控制台统一查看，进行集中监测。 | 符合 |

* 1. 安全管理制度
     1. 安全通用要求部分

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 安全策略 | a）应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。 | 经核查，制定了《三一集团有限公司信息安全总体方针》、《三一集团有限公司集团信息安全委员会》制度文件，其中明确了组织机构与职责，明确了安全工作的总体目标与范围。 | 符合 |
| 管理制度 | a）应对安全管理活动中的各类管理内容建立安全管理制度； | 经核查，已建立《三一集团有限公司数据中心管理规定》、《三一集团有限公司问责管理制度》、《三一集团有限公司备份管理制度》、《三一集团有限公司IT终端安全管理制度》、《三一集团有限公司IT服务台管理制度》、《三一集团有限公司防病毒系统管理规范》、《三一集团有限公司变更管理制度》、《三一集团有限公司信息安全事件处理与应急管理制度》、《三一集团有限公司信息系统权限管理制度》等方面管理制度，明确了对上述管理活动的相关要求。 | 符合 |
| b）应对管理人员或操作人员执行的日常管理操作建立操作规程； | 经核查，已形成《三一集团有限公司IT服务台管理制度》、《三一集团有限公司IT计算与存储资源需求管理规定》、《三一集团有限公司系统安全补丁管理制度》等操作规范。 | 符合 |
| c）应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。 | 经核查，已形成由安全策略、管理制度、操作规程、记录表单等1-4级文件构成的较全面安全管理制度体系。 | 符合 |
| 制定和发布 | a）应指定或授权专门的部门或人员负责安全管理制度的制定； | 经核查，在《三一集团有限公司信息安全总体方针》中明确规定由流程信息化总部负责集团信息安全具体工作，包括安全管理制度的制定。各事业部、职能部门主要负责人是落实信息安全管理制度的第一责任人。 | 符合 |
| b）安全管理制度应通过正式、有效的方式发布，并进行版本控制。 | 经访谈，由各部门负责本部门管辖业务的管理办法及管理标准的制订，走OA流程请示，由总经理和分管董事负责审批发布。 | 符合 |
| 评审和修订 | a）应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。 | 经访谈，由各部门负责本部门安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订，走OA流程请示，由总经理和分管董事负责审批发布。 | 符合 |

* 1. 安全管理机构
     1. 安全通用要求部分

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 岗位设置 | a）应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权； | 经核查，在《三一集团有限公司集团信息安全委员会》中设定成立了信息安全工作领导委员会，主任：向文波、副主任：易小刚。 | 符合 |
| b）应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责； | 经核查，在《三一集团有限公司集团信息安全委员会》中指定了网络安全管理工作的职能部门（集团董办、集团总裁办等），明确了岗位职责。但未明确安全主管、安全管理各方面负责人名单。 | 部分符合 |
| c）应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。 | 经访谈，已设立系统管理员（雷杰）、审计管理员（黎勃利）和安全管理员（刘清香）等岗位，并且在《三一集团IT体系内部职称评定管理规定》中明确各个部门及各个工作岗位的职责。 | 符合 |
| 人员配备 | a）应配备一定数量的系统管理员、审计管理员和安全管理员等； | 经访谈，未配备一定数量的管理员，仅由雷杰一人担任系统管理员、黎勃利一人担任审计管理员、刘清香一人担任安全管理员。 | 不符合 |
| b）应配备专职安全管理员，不可兼任。 | 经访谈，已配备安全管理员刘清香未兼任其他岗位。 | 符合 |
| 授权和审批 | a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等； | 经核查，已建立《三一集团有限公司信息系统权限管理制度》其中根据各部门和岗位的职责明确授权审批事项、审批部门和批准人等。 | 符合 |
| b）应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，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； | 经核查，已建立《三一集团有限公司变更管理制度》、《三一集团有限公司第三方人员管理制度》、《三一集团有限公司数据中心管理规定》，针对系统变更、重要操作、物理访问和系统接入等事项建立了审批程序，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。 | 符合 |
| 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。 | 经核查，已定期对审批事项、审批部门、审批人等信息进行审查及更新。 | 符合 |
| 沟通和合作 | a）应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题； | 经核查，有定期召开网络协调会议，有效的加强了各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通。 | 符合 |
| b）应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通； | 经访谈，与湖南省金盾信息安全等级保护评估中心有限公司、网神信息技术股份有限公司、深信服科技股份有限公司等，签订安全服务合同，并与其他安全服务商均有沟通合作。 | 符合 |
| c）应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。 | 经核查，已建立通讯录的方式建立了外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。 | 符合 |
| 审核和检查 | a）应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况； | 经核查，已落实安全巡检制度，每天巡检一次，巡检内容包含机房环境、设备状态、系统运行情况、数据备份等；现场提供了巡检记录表单。 | 符合 |
| b）应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； | 经访谈，已定期每年一次进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。 | 符合 |
| c）应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。 | 经核查，已制定了日常巡检的表格，检查内容包括机房温湿度、UPS主机情况、电力供应情况、硬件运行情况等，并形成了安全检查报告。 | 符合 |

* 1. 安全管理人员
     1. 安全通用要求部分

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 人员录用 | a）应指定或授权专门的部门或人员负责人员录用； | 经访谈，由人资总部负责人员录用。 | 符合 |
| b）应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核； | 经访谈，由人资总部负责对被录用人员的身份、安全背景、专业资格或资质等进行审查，并对被录用人员的专业技能进行考核。 | 符合 |
| c）应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。 | 经核查，签署劳动合同时，合同第六条中已与被录用人员约定了保密协议；但与关键岗位未签署岗位责任协议。 | 部分符合 |
| 人员离岗 | a）应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备； | 经核查：1、人员岗位调整时，需经过部门领导的确认，调动流程通过后权限部门会关闭员工原岗位IT权限，若新岗位有IT权限需求，需重新申请走审批流程，岗位调动根据不同级别对应不同级别负责人审批。2、人员岗位离职时，经过部门领导的确认，填写《离职工作交接单》、《解除终止劳动合同/实习协议申请书》经部门主管和总监签字确认，走SHR人资系统离职流程，将相关账户和访问权限清理，包括其使用的账号、密码、权限、各种身份证件等以及其他相关信息资料、资产和软硬件设备，归还资产的接收部门进行审核和确认。 | 符合 |
| b）应办理严格的调离手续，并承诺调离后的保密义务后方可离开。 | 经访谈，人员离岗需经过SHR人资系统的确认和审批，将相关账户和访问权限清理，包括其使用的账号名、密码、权限、各种身份证件等以及其他相关信息资料、资产和软硬件设备，接收部门进行审核和确认。  经核查，签署劳动合同时，合同第六条中已与被录用人员约定了保密协议。 | 符合 |
| 安全意识教育和培训 | a）应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施； | 经核查，《三一集团有限公司员工信息安全管理制度》第5章中明确了信息安全培训与要求，对无故缺席公司组织的信息安全培训与考试，信息安全考试未及格的，对其处罚上升一级。 | 符合 |
| b）应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训； | 经核查，已建立每年一次员工安全意识培训，根据不同岗位制定不同培训计划，对安全基础知识、岗位操作规程等进行培训。 | 符合 |
| c）应定期对不同岗位的人员进行技能考核。 | 经核查，每年一次信息安全意识线上学习及考试，对于未按期完成线上学习的员工，考试未参加或未及格的员工，予以处罚。 | 符合 |
| 外部人员访问管理 | a）应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案； | 经核查，《三一集团有限公司数据中心管理规定》中规定外部人员进出均需登记，第三方人员如需访问物理机房等重要区域时，应填写《数据中心出入登记表》进行申请，对第三方人员进入机房内部全程陪同监督。 | 符合 |
| b）应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案； | 经核查，《三一集团有限公司第三方人员信息安全管理规定》中明确规定，临时外部人员如需接入内部网络，需签署《商业秘密保密协议承诺函》《安全协议》并走流程审批。审批登记完成后方可接入。 | 符合 |
| c）外部人员离场后应及时清除其所有的访问权限； | 经核查，《三一集团有限公司第三方人员信息安全管理规定》中明确规定了对外部人员完成工作后，业务负责人应参照《三一集团有限公司信息系统权限管理制度》内容及时关闭其权限，并于一周内归还所使用资产，将所有工作资料进行存档，便于后续跟踪检查。 | 符合 |
| d）获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。 | 经核查，《三一集团有限公司第三方人员信息安全管理规定》中明确规定外部人员需提交申请并报分管人事领导审批，并全程均由相关人员陪同监督。 | 符合 |

* 1. 安全建设管理
     1. 安全通用要求部分

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 定级和备案 | a）应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由； | 经核查，被测系统已完成定级备案工作，在《三一集团有限公司SanyMall客户云商城系统网络安全等级保护定级报告》中已明确安全保护等级及定级理由，将三一集团有限公司SanyMall客户云商城系统等级定为第S3A3级。 | 符合 |
| b）应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定； | 经核查，被测系统定级结果已经过相关部门和安全技术专家评审，已完成定级备案工作，已取得系统备案号。 | 符合 |
| c）应保证定级结果经过相关部门的批准； | 经核查，系统的定级结果已经过主管部门审批通过，已完成定级备案工作，已取得系统备案号。 | 符合 |
| d）应将备案材料报主管部门和相应公安机关备案。 | 经核查，系统备案材料已上报主管部门和公安机关备案，已取得系统备案号。此次测评为二次测评，需测评工作结束并出具测评报告且结果为符合之后公安部门才会出具备案证明。 | 符合 |
| 安全方案设计 | a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施； | 经核查，系统定级备案附件材料中已明确要求项目建设严格遵照国家《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）第三级等级保护技术等相关文件要求，建立集技术、管理及监管为一体的统一安全防护体系。此次为二次测评，后续会根据等保测评及风险评估结果对安全措施进行调整。 | 符合 |
| b）应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件； | 经核查，已提供《应用系统安全自查表》明确了对集团应用系统安全进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件。 | 符合 |
| c）应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。 | 经核查，有组织集团相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，有提供相关会议纪要。 | 符合 |
| 产品采购和使用 | a）应确保网络安全产品采购和使用符合国家的有关规定； | 经核查，网络安全产品的采购均符合国家相关规定，均有相关销售许可，现场有提供。 | 符合 |
| b）应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求； | 经核查，相关密码产品已提供相关材料证明符合国家密码管理主管部门的要求。 | 符合 |
| c）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。 | 经核查，具有商品采购清单，设备采购前会由需求部门的技术人员根据设备各方面性能进行对比筛选。 | 符合 |
| 自行软件开发 | a）应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制； | 经核查，系统自行开发，测试环境和生产环境分开，测试数据和结果对内展示，均为受控成果。 | 符合 |
| b）应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则； | 经核查，《三一重工软件开发管理规范》规范了相关人员和流程管控等内容。 | 符合 |
| c）应制定代码编写安全规范，要求开发人员参照规范编写代码； | 经核查，已制定代码安全编写规范，要求开发人员参照规范编写代码。 | 符合 |
| d）应具备软件设计的相关文档和使用指南，并对文档使用进行控制； | 经核查，系统已提供软件使用说明手册。 | 符合 |
| e）应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测； | 经核查，自行软件开发过程中未对恶意代码进行检测，无法保证软件安全性。 | 不符合 |
| f）应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制； | 经核查，《三一重工软件开发管理规范》已提对程序资源的变更修改进行了要求。 | 符合 |
| g）应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。 | 经核查，软件开发人员均为专职人员，开发活动规范、受控。 | 符合 |
| 外包软件开发 | a）应在软件交付前检测其中可能存在的恶意代码； | 经访谈，被测系统为集团自行开发，未涉及外包软件开发。 | 不适用 |
| b）应保证开发单位提供软件设计文档和使用指南； | 经访谈，被测系统为集团自行开发，未涉及外包软件开发。 | 不适用 |
| c）应保证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。 | 经访谈，被测系统为集团自行开发，未涉及外包软件开发。 | 不适用 |
| 工程实施 | a）应指定或授权专门的部门或人员负责工程实施过程的管理； | 经访谈，已指定营销与风控总部负责对工程的实时过程进行管控。 | 符合 |
| b）应制定安全工程实施方案控制工程实施过程； | 经核查，有制定提供详细的工程实施方案。 | 符合 |
| c）应通过第三方工程监理控制项目的实施过程。 | 经核查，有通过第三方工程监理（兴湘监理）及集团董办督办经理控制项目实施过程。 | 符合 |
| 测试验收 | a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告； | 经核查，有制订测试验收方案及提供测试报告。 | 符合 |
| b）应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。 | 经访谈，未提供上线前的安全性测试报告。 | 不符合 |
| 系统交付 | a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点； | 经访谈，已制订项目交付清单，并对系统、设备和文档等进行了明确规定。 | 符合 |
| b）应对负责运行维护的技术人员进行相应的技能培训； | 经访谈，已对负责系统维护的技术人员进行相应的技能培训，由厂商在会议室统一进行技术培训和产品说明。 | 符合 |
| c）应提供建设过程文档和运行维护文档。 | 经核查，已提供SanyMall客户云商城系统操作手册、培训资料等文档。 | 符合 |
| 等级测评 | a）应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改； | 经访谈，本次测评为第二次测评，根据定级要求，定期每年进行一次等级测评，发现不符合相应等级保护标准要求的及时整改。 | 符合 |
| b）应在发生重大变更或级别发生变化时进行等级测评； | 经访谈，本次测评为第二次测评，根据定级要求，定期每年进行一次等级测评，暂未发生过重大变更。 | 符合 |
| c）应确保测评机构的选择符合国家有关规定。 | 经访谈，此次为第二次测评，测评机构为湖南省金盾信息安全等级保护评估中心有限公司，该公司具有等保测评资质。 | 符合 |
| 服务供应商选择 | a）应确保服务供应商的选择符合国家的有关规定； | 经访谈，与湖南省金盾信息安全等级保护评估中心有限公司、网神信息技术股份有限公司、深信服科技股份有限公司等，签订安全服务合同，服务商具有系统运维及开发资质。 | 符合 |
| b）应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务； | 经访谈，在与服务商（湖南省金盾信息安全等级保护评估中心有限公司、网神信息技术股份有限公司、深信服科技股份有限公司）签订的安全服务合同中已明确双方应当履行的责任及安全服务内容。 | 符合 |
| c）应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。 | 经访谈，已定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。 | 符合 |

* + 1. 云计算安全扩展要求部分

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 云服务商选择 | a）应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力； | 被测系统为云服务客户业务应用系统，安全保护等级为三级；应用系统部署在腾讯公有云IaaS服务平台，腾讯公有云IaaS服务平台安全保护等级为三级，腾讯公有云IaaS服务平台已通过网络安全等级测评(测评时间：2021.5、等级测评报告编号：440320-50052-00011-21-000008-01、测评结论：优、综合得分：96.3）。云计算平台承载的业务系统等级不高于云计算平台自身的安全保护等级。 | 符合 |
| b）应在服务水平协议中规定云服务的各项服务内容和具体技术指标； | 经核查，单位与腾讯云计算(北京)有限责任公司签订了服务协议。服务协议明确了各项服务内容及具体指标等内容。 | 符合 |
| c）应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等； | 经核查，单位与腾讯云计算(北京)有限责任公司签订了服务协议。服务协议明确了腾讯云计算(北京)有限责任公司的权限与责任。 | 符合 |
| d）应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除； | 经核查，单位与腾讯云计算(北京)有限责任公司签订了服务协议。服务协议明确了规定了服务合约到期时，承诺数据安全的相关内容。 | 符合 |
| e）应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据。 | 经核查，单位与腾讯云计算(北京)有限责任公司签订了服务协议。服务协议中含有保密协议章节内容。 | 符合 |
| 供应链管理 | a）应确保供应商的选择符合国家有关规定； | 经核查，采购符合国家和单位相关法律和规章制度。通过公开招标完成采购。 | 符合 |
| b）应将供应链安全事件信息或安全威胁信息及时传达到云服务客户； | 经核查，云平台服务商通过邮件、短信、电话及时把各类安全事件信息或安全威胁信息传达单位。 | 符合 |
| c）应将供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。 | 经核查，云平台服务商针对重要变更会及时通过邮件、短信、电话传达到单位。并会对变更产生的风险及提前需要采取的控制措施进行告知。 | 符合 |

* 1. 安全运维管理 
     1. 安全通用要求部分

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 环境管理 | a）应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理； | 系统部署于腾讯公有云IaaS服务平台，机房由云平台侧负责管理。 | 不适用 |
| b）应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定； | 系统部署于腾讯公有云IaaS服务平台，机房由云平台侧负责管理。 | 不适用 |
| c）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。 | 经核查，《三一集团有限公司员工信息安全管理制度》，规定了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、不在重要区接待来访人员、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文件文档。 | 符合 |
| 资产管理 | a）应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容； | 经核查，已建立《资产清单》，内容包括：资产名称、功能描述、数量、责任部门、责任人、使用人等。 | 符合 |
| b）应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施； | 经核查，对信息系统相关资产进行标识管理，贴了资产标签，标明重要程度；重要信息系统资产保存在机房内。 | 符合 |
| c）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。 | 经核查，已建立《集团各体系数据分类分级表》，对信息分类与标识方法进行说明，对信息的使用、传输和存储等进行规定。 | 符合 |
| 介质管理 | a）应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点； | 经核查，已建立《三一集团有限公司存储介质管理办法》明确了将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点。 | 符合 |
| b）应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。 | 经核查，已建立《三一集团有限公司存储介质管理办法》明确了对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。 | 符合 |
| 设备维护管理 | a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理； | 系统部署于腾讯公有云IaaS服务平台，机房各种设备、线路等设施由云平台侧负责管理。 | 不适用 |
| 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、维修和服务的审批、维修过程的监督控制等； | 经核查，已建立《三一集团有限公司设备管理办法》，明确相关维护人员的职责分工，包括日常维护管理、计算机维修及服务审批等过程的管理。 | 符合 |
| c）信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密； | 经访谈，信息处理设备带离机房或办公地点时，需向机房管理员提出申请，并由机房管理员填写《中心机房设备出入登记表》。 | 符合 |
| d）含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。 | 经访谈，含有存储介质的设备在报废或重用前，机房管理员填写《设备报废清单》和相关报告，经相关部室领导审批后进行集中处置，对机房报废设备进行存储介质消磁并对存储介质粉碎，及对其他敏感信息进行相应的清理工作，并进行相关工作记录后由机房管理员存档保存。 | 符合 |
| 漏洞和风险管理 | a）应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补； | 经访谈，公司对该系统定期每月进行安全漏洞扫描，且测评过程中涉及渗透测试和漏洞扫描，可以有效的发现安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。 | 符合 |
| b）应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。 | 经核查，本系统已完成信息系统定级备案工作，根据三级系统要求，每年会进行一次等保测评工作，并依据等保测评结果进行安全整改。此次测评为第二次测评。 | 符合 |
| 网络和系统安全管理 | a）应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限； | 经核查，已明确系统管理员雷杰、网络管理员谭智敏、安全管理员刘清香、审计管理员黎勃利等角色的责任和权限。 | 符合 |
| b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制； | 经核查，已建立《三一集团有限公司信息系统权限管理制度》由董办授权专干负责进行账户管理，对申请账户、建立账户、删除账户等进行控制。 | 符合 |
| c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定； | 经核查，已建立《三一集团有限公司网络安全管理办法》、《三一集团有限公司系统安全管理办法》、《三一集团有限公司信息系统变更管理办法》等相应管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁等方面作出了相应规定及要求。 | 符合 |
| d）应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等； | 经核查，已提供《深信服产品使用手册》《网神产品使用手册》等网络设备、安全设备、业务系统等配置和操作手册。 | 符合 |
| e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容； | 经核查，每天一次对机房进行安全巡检，巡检内容主要是针对机房基础设施的环境、设备状态，已形成相关运维记录（参数配置、修改等）已提供《平台日常运维记录表》。 | 符合 |
| f）应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为； | 经访谈，由平台管理部负责对防火墙、上网行为管理设备、IPS等安全设备日志进行查看、分析、统计，发现可疑行为及时上报及处理。 | 符合 |
| g）应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库； | 经核查，对系统组件或配置参数进行变更需经过审批流程，并对变更内容并进行记录，内容包括运维情况一览表，包括故障次数等、OA 权限设置、新增业务（变更）、操作系统请求（变更等内容）；操作过程产生的审计日志，不能进行更改；且操作结束后会同步更新配置信息库。 | 符合 |
| h）应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据； | 经核查，对运维工具的使用需经过审批流程，通过堡垒机对被测系统相关设备、系统资源进行运维，堡垒机能保留不可更改的审计日志；操作结束后对相关敏感数据进行删除。 | 符合 |
| i）应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道； | 经核查，远程运维通过VPN接入，使用堡垒机对被测系统相关设备、系统资源进行操作运维；单位严格按照《三一集团有限公司网络管理办法》执行，对VPN及堡垒机访问开通需经过审批，VPN及堡垒机能保留不可更改的审计日志；且操作结束后会关闭VPN及堡垒机的访问权限。 | 符合 |
| j）应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。 | 经核查，已建立《三一集团有限公司网络管理办法》网络接入管理办公网没有连通外网，笔记本可通过 WIFI 上外网，WIFI 的账号和密码严格控制；控制网络外联措施：上网行为管理可控制网络外联。 | 符合 |
| 恶意代码防范管理 | a）应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等； | 经核查，《三一集团有限公司计算机病毒防治管理办法》中明确规定各部门在从信息网络上下载软件、程序、数据和购置、维修、借入计算机设备时，必须先对其进行计算机病毒检测，经确认无毒后方可使用，所有设备接入系统前均需查杀病毒。 | 符合 |
| b）应定期验证防范恶意代码攻击的技术措施的有效性。 | 经核查，平台管理部定期自动升级恶意代码库，采集防病毒服务器的病毒和木马情况的日志记录，并及时采取相应的病毒防御措施。 | 符合 |
| 配置管理 | a）应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等； | 经核查，存储管理员对网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等均进行了备份。 | 符合 |
| b）应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。 | 经访谈，如需改变服务器或软件系统相关配置参数，需经过部门相关领导的批准，及时更新基本配置信息库。 | 符合 |
| 密码管理 | a）应遵循密码相关国家标准和行业标准； | 经核查，购买的密码产品（如：门禁系统）已提供相关证明材料证明符合相关国家标准和行业标准。 | 符合 |
| b）应使用国家密码管理主管部门认证核准的密码技术和产品。 | 购买的密码产品（如：门禁系统）已提供相关证明材料证明是使用国家密码管理主管部门认证核准的密码技术和产品。 | 符合 |
| 变更管理 | a）应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施； | 经核查，OA 系统中明确了变更流程，包括变更发起方、实施方的工作内容，变更发起方需提交变更方案，变更方案需经过相关领导的审批，对有可能影响客户利益的变更事先通知客户并得到客户的确认之后再进行变更操作。 | 符合 |
| b）应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程； | 经核查，已建立《三一集团有限公司变更管理流程》，包括变更申报、审批程序；已查看相关变更过程记录文档：《三一集团有限公司变更实施步骤报告》。 | 符合 |
| c）应建立中止变更并从失败变更中恢复的程序，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。 | 经核查，已建立《三一集团有限公司信息系统投产及变更管理办法》，平台管理部和相关业务管理部门制定重要信息系统投产及变更应急预案,并根据投产及变更回退时间跨度制定相应的系统回退和应急处置计划和流程；已查看相关文档：《三一集团有限公司一般变更上线操作及回退步骤》，内容包括变更失败的回退方案。 | 符合 |
| 备份与恢复管理 | a）应识别需要定期备份的重要业务信息、系统数据及软件系统等； | 经核查，已识别出了需要备份的重要业务数据，配置文件备份方式是通过管理员手工进行备份，日志文件通过日志服务器进行自动备份；网络管理员负责网络设备、安全设备的文件备份，系统管理员负责应用相关文件备份。 | 符合 |
| b）应规定备份信息的备份方式、备份频度、存储介质、保存期等； | 经核查，已建立《三一集团有限公司数据备份管理实施细则》，对数据备份的范围、备份策略、备份方式、存储介质、保存期等进行了说明。 | 符合 |
| c）应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。 | 经访谈，系统管理员已制定了数据备份策略，每天会对重要业务数据进行一次完全备份。 | 符合 |
| 安全事件处置 | a）应及时向安全管理部门报告所发现的安全弱点和可疑事件； | 经访谈，平台管理部运维人员在发现网络问题、设备故障、其他安全事件时，及时向平台管理部报告。 | 符合 |
| b）应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等； | 经核查，《三一集团有限公司信息安全事件处理与应急预案管理制度》，明确信息安全事件的定义与分类分级，人员职责，信息安全事件报告流程，信息安全事件的处理过程，事件处理流程的改进。 | 符合 |
| c）应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训； | 经核查，已根据网络与信息安全突发公共事件的发生过程、性质和特征，网络与信息安全突发公共事件可划分为网络安全突发事件和信息安全突发事件，当前未发生过安全事情。 | 符合 |
| d）对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。 | 经核查，已建立《三一集团有限公司信息安全事件处理与应急预案管理制度》，为不同安全事件制定了不同的处理和报告程序的内容。 | 符合 |
| 应急预案管理 | a）应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容； | 经核查，已制定《三一集团有限公司信息安全事件处理与应急管理制度》，其中包括了启动预案的条件、应急组织构成、应急资源保障等方面内容。 | 符合 |
| b）应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容； | 经核查，已制定《三一集团有限公司信息安全事件处理与应急管理制度》，其中包括了应急处理流程、系统恢复流程等相关内容。 | 符合 |
| c）应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练； | 经核查，每年会组织一次应急预案培训及应急演练，有提供相应的应急预案培训记录和演练记录，如：《SanyMall 客户云商城系统灾难恢复演练过程文档》、《TAS灾难恢复演练》、《TAS灾难恢复应急演练培训记录》等。 | 符合 |
| d）应定期对原有的应急预案重新评估，修订完善。 | 经访谈，定期每年对原有应急预案重新评估，修订完善。 | 符合 |
| 外包运维管理 | a）应确保外包运维服务商的选择符合国家的有关规定； | 系统部署于腾讯公有云IaaS服务平台，系统不涉及外包运维，此项不适用。 | 不适用 |
| b）应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容； | 系统部署于腾讯公有云IaaS服务平台，系统不涉及外包运维，此项不适用。 | 不适用 |
| c）应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确； | 系统部署于腾讯公有云IaaS服务平台，系统不涉及外包运维，此项不适用。 | 不适用 |
| d）应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对IT 基础设施中断服务的应急保障要求等。 | 系统部署于腾讯公有云IaaS服务平台，系统不涉及外包运维，此项不适用。 | 不适用 |

* + 1. 云计算安全扩展要求部分

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| 云计算环境管理 | a）云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。 | 经核查，被测系统为云服务客户业务应用系统，非云计算平台，此项不涉及，不适用。 | 不适用 |

1. 漏洞扫描结果记录

**附录E 表-1漏洞扫描安全漏洞**

| **序号** | **危险程度** | **漏洞名称** | **影响IP或URL** | **漏洞描述** | **解决方法** |
| --- | --- | --- | --- | --- | --- |
| 1 | 低 | 允许Traceroute探测 | \*.\*.181.115 | 本插件使用Traceroute探测来获取扫描器与远程主机之间的路由信息。攻击者也可以利用这些信息来了解目标网络的网络拓扑。 | 在防火墙中禁用Time Exceeded类型的ICMP包。 |
| 2 | 低 | 检测到目标主机加密通信支持的SSL加密算法【原理扫描】 | \*.\*.181.115 | 该插件连接到目标主机服务，检测到目标服务加密通信使用的SSL加密算法。 | 该漏洞仅仅是一个信息获取的漏洞，可以不做修复。 |
| 3 | 低 | 服务器允许SSL会话恢复【原理扫描】 | \*.\*.181.115 | 服务器允许SSL会话恢复。 | 该漏洞仅仅是对SSL会话恢复的检测，可以不修复。 |
| 4 | 低 | 可通过HTTPS获取远端WWW服务信息 | \*.\*.181.115 | 可通过HTTPS获取远端HTTP服务器信息。这可能使得攻击者了解远程系统类型以便进行下一步的攻击。 | 改变您的HTTP服务器的缺省banner。 |
| 5 | 低 | 可通过HTTP获取远端WWW服务信息 | \*.\*.181.115 | 本插件检测远端HTTP Server信息。这可能使得攻击者了解远程系统类型以便进行下一步的攻击。 | 改变您的HTTP服务器的缺省banner。 |
| 6 | 低 | 探测到服务器支持的SSL加密协议【原理扫描】 | \*.\*.181.115 | 为了保护敏感数据在传送过程中的安全，全球许多知名企业采用SSL（Security Socket Layer）加密机制。 SSL是Netscape公司所提出的安全保密协议。 | 该漏洞仅仅是一个信息获取的漏洞，可以不做修复。 |
| 7 | 低 | 允许Traceroute探测 | \*.\*.181.115 | 本插件使用Traceroute探测来获取扫描器与远程主机之间的路由信息。攻击者也可以利用这些信息来了解目标网络的网络拓扑。 | 在防火墙中禁用Time Exceeded类型的ICMP包。 |

1. 渗透测试结果记录

**1）渗透过程记录**

| **安全控制点** | **要求项** | **测试漏洞类型** | **渗透结果** |
| --- | --- | --- | --- |
| 身份鉴别 | a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； | 任意用户登录、任意用户注册和覆盖注册、空口令和弱口令、其他认证缺陷、任意用户密码重置 | 未发现安全漏洞 |
| b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； | 账户枚举和可猜解用户账户、口令爆破、验证码缺失/绕过、失败登录限制缺失/绕过、撞库 | 未发现安全漏洞 |
| c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 鉴别信息明文传输 | 未发现安全漏洞 |
| d) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。 | 双因子认证缺失/绕过、短信验证码绕过 | 未发现安全漏洞 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 未授权访问 | 未发现安全漏洞 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 存在默认账户、默认口令 | 未发现安全漏洞 |
| c）应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 存在测试帐号、存在后门帐号 | 未发现安全漏洞 |
| d)应授予管理用户所需的最小权限，实现管理用户的权限分离； | 权限设置不当 | 未发现安全漏洞 |
| e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； | 垂直越权、平行越权 | 未发现安全漏洞 |
| f)访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； | 同步错误、cookie设置不当、过程验证缺失、flash 配置不当、CSRF漏洞、可预测的资源位置、接口调用次数无限制、环境错误 | 未发现安全漏洞 |
| g)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 | 敏感信息标记配置不当 | 发现安全漏洞 |
| 安全审计 | a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； | 伪造审计记录 | 未发现安全漏洞 |
| c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； | 删除审计记录 | 未发现安全漏洞 |
| d) 应对审计进程进行保护，防止未经授权的中断。 | 中断审计进程 | 未发现安全漏洞 |
| 入侵防范 | c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 管理地址对外 | 未发现安全漏洞 |
| d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； | SQL注入、LDAP注入、ORM注入、XML注入、SSI注入、Xpath注入、CRLF注入、IMAP/SMTP注入、其它代码注入、命令执行、任意文件上传、任意文件下载、本地文件包含、远程文件包含、存储型XSS、反射型XSS、基于DOM的XSS、基于flash的XSS、路径遍历、SSRF漏洞、URL重定向漏洞、格式化字符串处理、缓冲区溢出、意外处理错误、点击劫持、HTTP参数污染 | 详见F.1 SanyMall 客户云商城系统存在SQL注入漏洞安全问题及详见F.2 SanyMall 客户云商城系统存在存储型跨站漏洞安全问题。 |
| 数据完整性 | a) 应采用校验码技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 会话劫持、报文未增加防重放机制和哈希校验完整性机制 | 未发现安全漏洞 |
| b) 应采用校验码技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 | 存储的敏感数据可被篡改 | 未发现安全漏洞 |
| 数据保密性 | a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； | 敏感信息明文传输、不安全的加密算法 | 详见F.3 SanyMall 客户云商城系统存在敏感信息泄露漏洞安全问题。 |
| b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 | 敏感信息明文存储 | 未发现安全漏洞 |
| 剩余信息保护 | a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除； | Cookie敏感信息泄露 | 未发现安全漏洞 |
| b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。 | 资源释放后重利用、OpenSSL心脏滴血漏洞 | 未发现安全漏洞 |
| 个人信息保护 | a)应仅采集和保存业务必需的用户个人信息； | 采集不必要用户信息 | 未发现安全漏洞 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 用户信息泄露 | 未发现安全漏洞 |

**2）渗透发现问题**

* 1. SanyMall 客户云商城系统存在Sql注入漏洞安全问题

|  |  |
| --- | --- |
| 漏洞名称 | 存在SQL注入漏洞 |
| 风险等级 | 高 |
| 目标系统 | SanyMall 客户云商城系统 |
| 漏洞URL/IP | https://mall.sany.com.cn/item-getSpecSku.html?item\_id=2010 |
| 内网系统 | 否 |
| 漏洞危害 | SanyMall客户云商城系统的item\_id参数没有进行严格过滤，导致可带入SQL语句进行查询。攻击者利用此漏洞可读取整个数据库的信息（包括后台管理员的账号和密码），如果网站的数据库连接账号具有最高权限，即可直接执行系统命令或者上传网站后门程序，完全控制服务器。 |
| 修复建议 | 严格过滤网站链接传递的参数，对数据库的SQL语句特征字符进行排除，防止完整的语句被带入数据库查询。 |
| 详细渗透过程截图 | |
| 测试环境中    生产环境中 | |

* 1. SanyMall 客户云商城系统存在存储型跨站漏洞安全问题

|  |  |
| --- | --- |
| 漏洞名称 | 存在存储型跨站漏洞 |
| 风险等级 | 高 |
| 目标系统 | SanyMall 客户云商城系统 |
| 漏洞URL/IP | https://mall.sany.com.cn/ |
| 内网系统 | 否 |
| 漏洞危害 | SanyMall客户云商城系统未对提交参数没有进行严格过滤，导致用户可以提交一些特意构造的语句，一般都是带有像JavaScript等这类脚本代码。攻击者利用此漏洞可偷取管理员COOKIE，利用获得的COOKIE值可直接登录网站后台，进行任意操作。 |
| 修复建议 | 过滤特殊字符在网站程序处过滤特殊字符，这是防范跨站脚本攻击最为有效和彻底的方法。在不影响网站程序正常运行的前提下，我们可以在网站程序的表单输入处过滤掉“javascript”、“<script>”、“#”、“&”等字符，这样就可以防范大部分的跨站攻击。 |
| 详细渗透过程截图 | |
| 打印出cookie    执行的脚本 | |

* 1. SanyMall 客户云商城系统存在敏感信息泄露漏洞安全问题

|  |  |
| --- | --- |
| 漏洞名称 | 存在敏感信息泄露漏洞 |
| 风险等级 | 中 |
| 目标系统 | SanyMall 客户云商城系统 |
| 漏洞URL/IP | https://malltest.sany.com.cn/shop-falshsale.html?shop\_id=1 |
| 内网系统 | 否 |
| 漏洞危害 | 可通过该报错页面获取到大量服务器、web相关敏感信息。 |
| 修复建议 | 建议开启容错模式，不对用户直接返回详细的错误代码。 |
| 详细渗透过程截图 | |
| E:\2021\金盾\三一重工\渗透测试\商城\捕获.JPG  测试环境中 | |

1. 回归测试
   1. SanyMall 客户云商城系统存在Sql注入漏洞安全问题

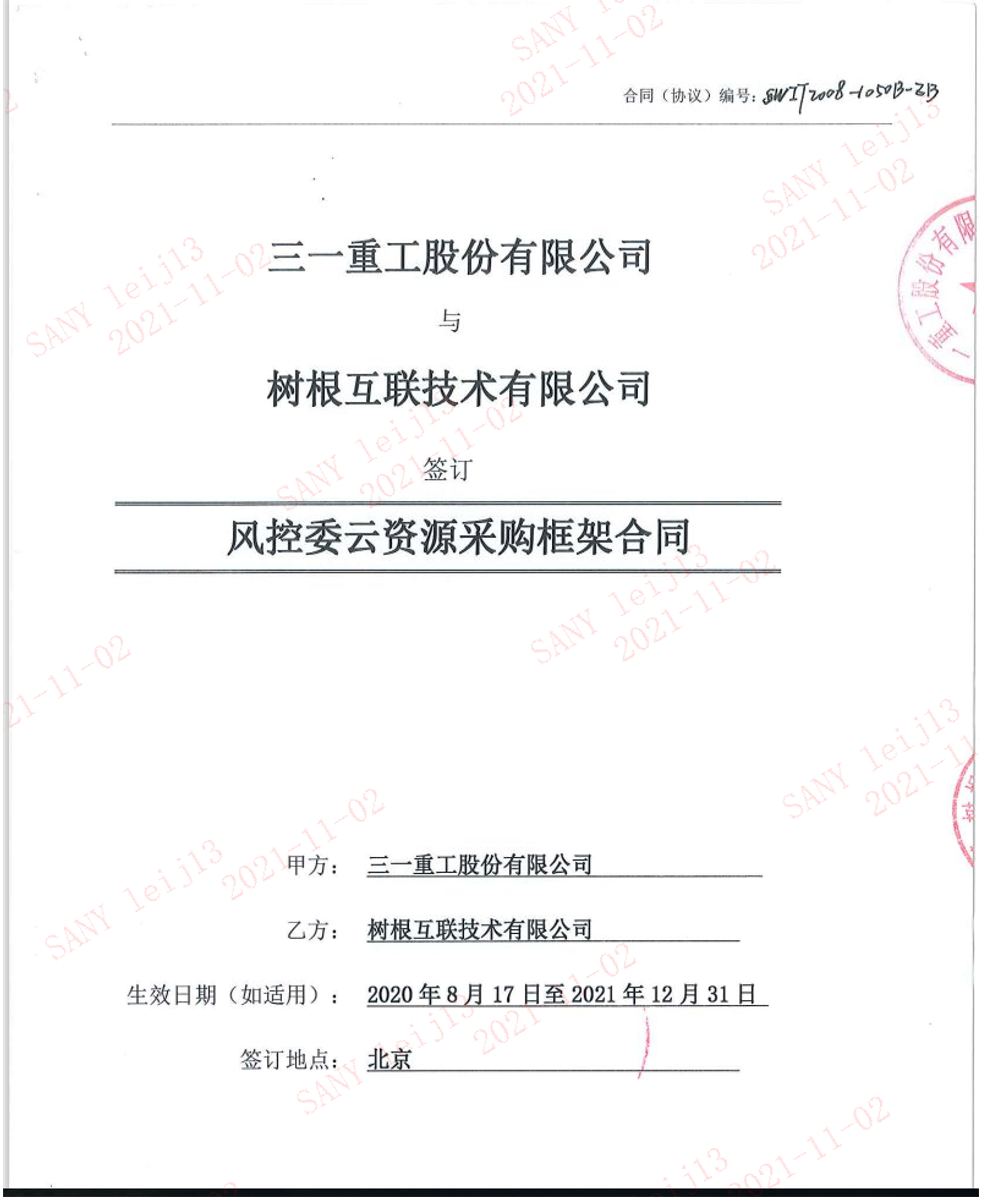
|  |  |
| --- | --- |
| 漏洞名称 | 存在SQL注入漏洞 |
| 风险等级 | 高 |
| 目标系统 | SanyMall 客户云商城系统 |
| 漏洞URL/IP | https://mall.sany.com.cn/item-getSpecSku.html?item\_id=2010 |
| 内网系统 | 否 |
| 漏洞危害 | SanyMall客户云商城系统的item\_id参数没有进行严格过滤，导致可带入SQL语句进行查询。攻击者利用此漏洞可读取整个数据库的信息（包括后台管理员的账号和密码），如果网站的数据库连接账号具有最高权限，即可直接执行系统命令或者上传网站后门程序，完全控制服务器。 |
| 修复情况 | 已修复 |
| 漏洞修复证明截图 | |
|  | |

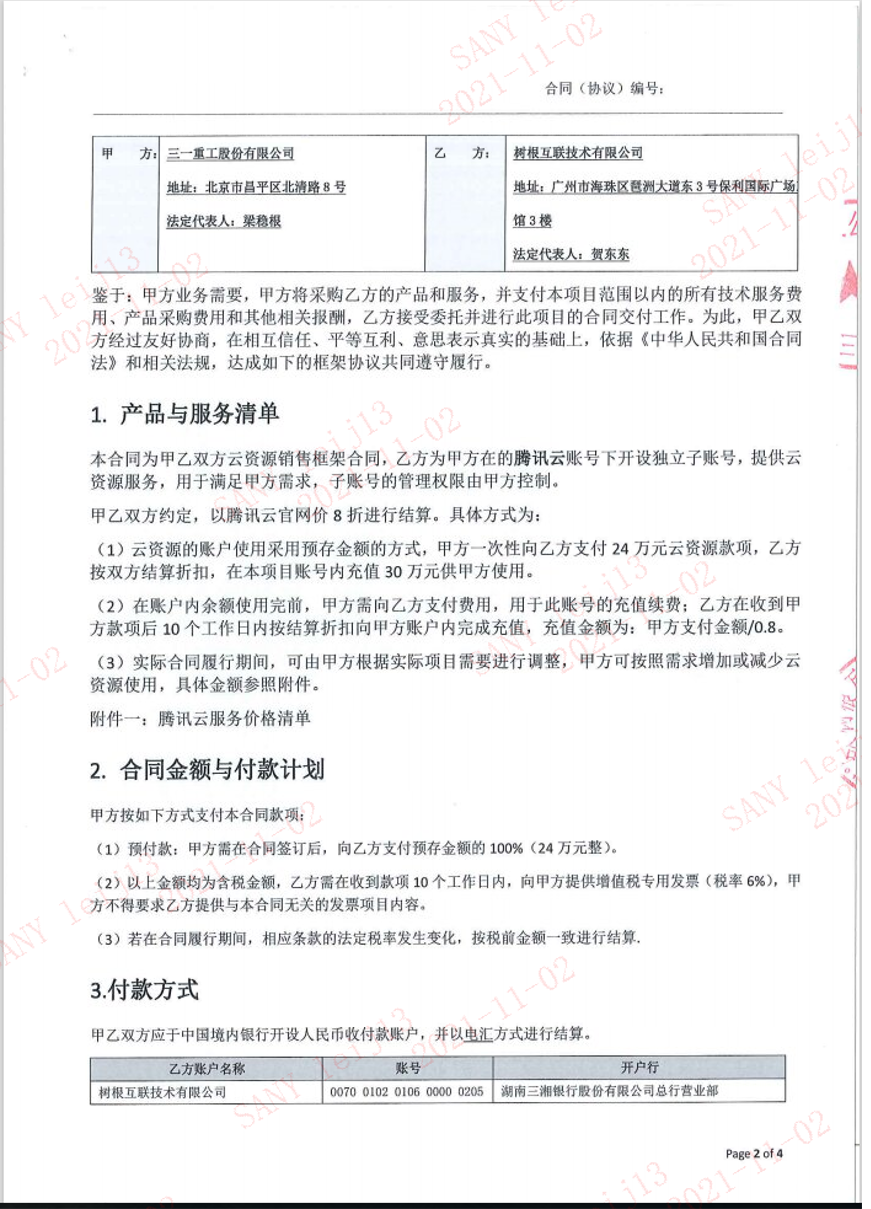
* 1. SanyMall 客户云商城系统存在存储型跨站漏洞安全问题

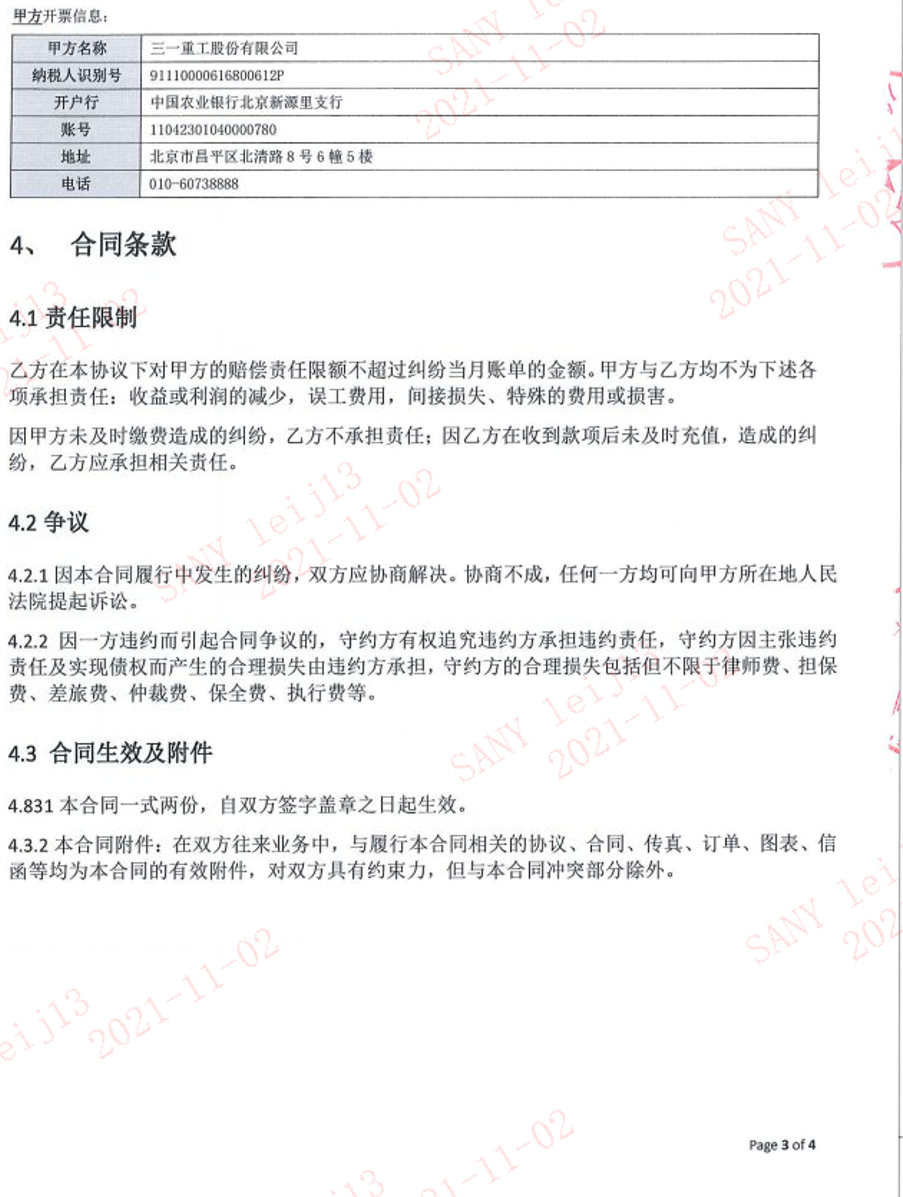
|  |  |
| --- | --- |
| 漏洞名称 | 存在存储型跨站漏洞 |
| 风险等级 | 高 |
| 目标系统 | SanyMall 客户云商城系统 |
| 漏洞URL/IP | https://mall.sany.com.cn/ |
| 内网系统 | 否 |
| 漏洞危害 | SanyMall客户云商城系统未对提交参数没有进行严格过滤，导致用户可以提交一些特意构造的语句，一般都是带有像JavaScript等这类脚本代码。攻击者利用此漏洞可偷取管理员COOKIE，利用获得的COOKIE值可直接登录网站后台，进行任意操作。 |
| 修复情况 | 已修复 |
| 漏洞修复证明截图 | |
|  | |

1. 腾讯云采购框架协议
2. 三一重工股份有限公司与树根互联技术有限公司风控委云资源采购框架

合同



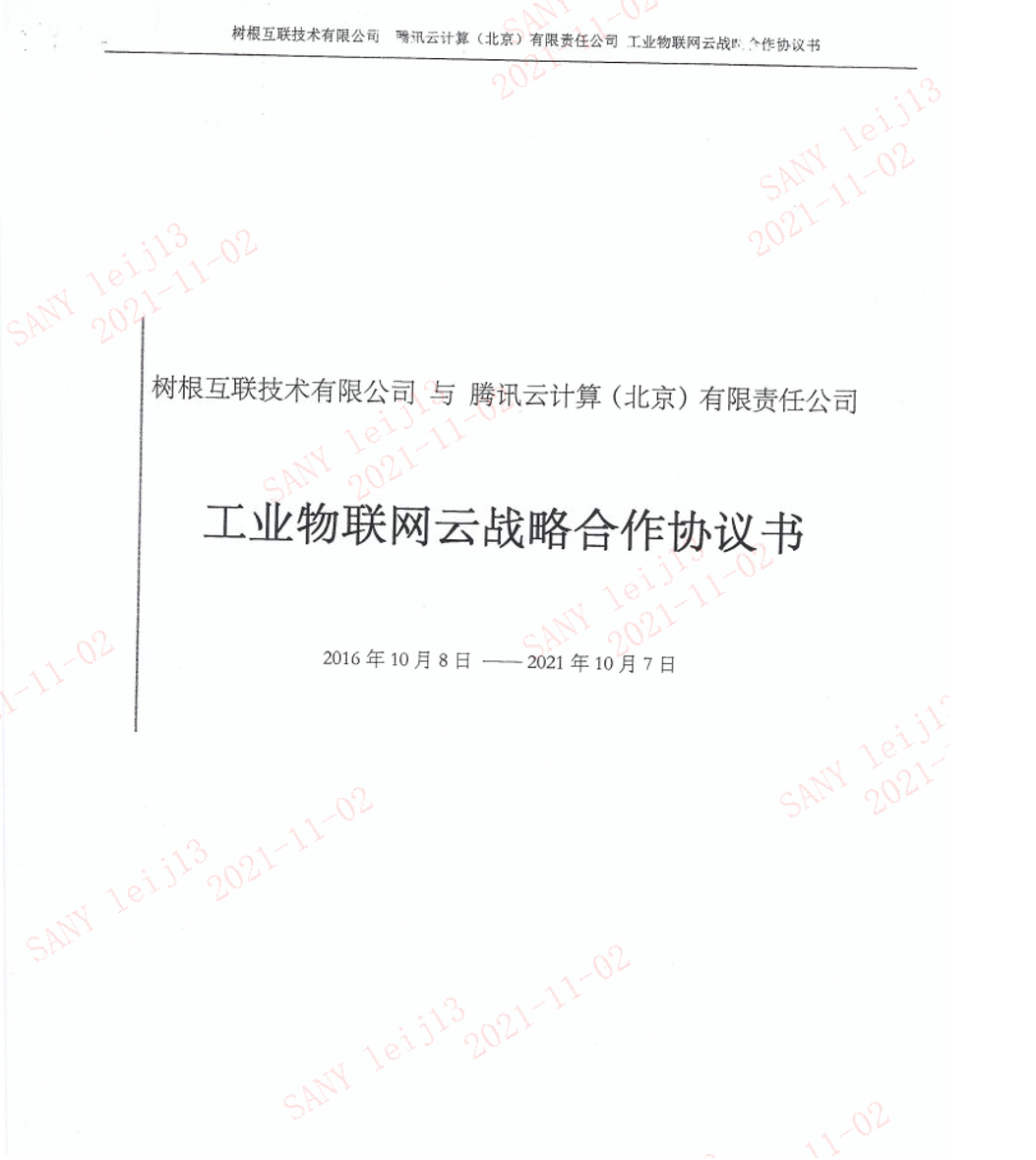






1. 树根互联技术有限公司与腾讯云计算（北京）有限责任公司工业物联网云

战略合作协议书



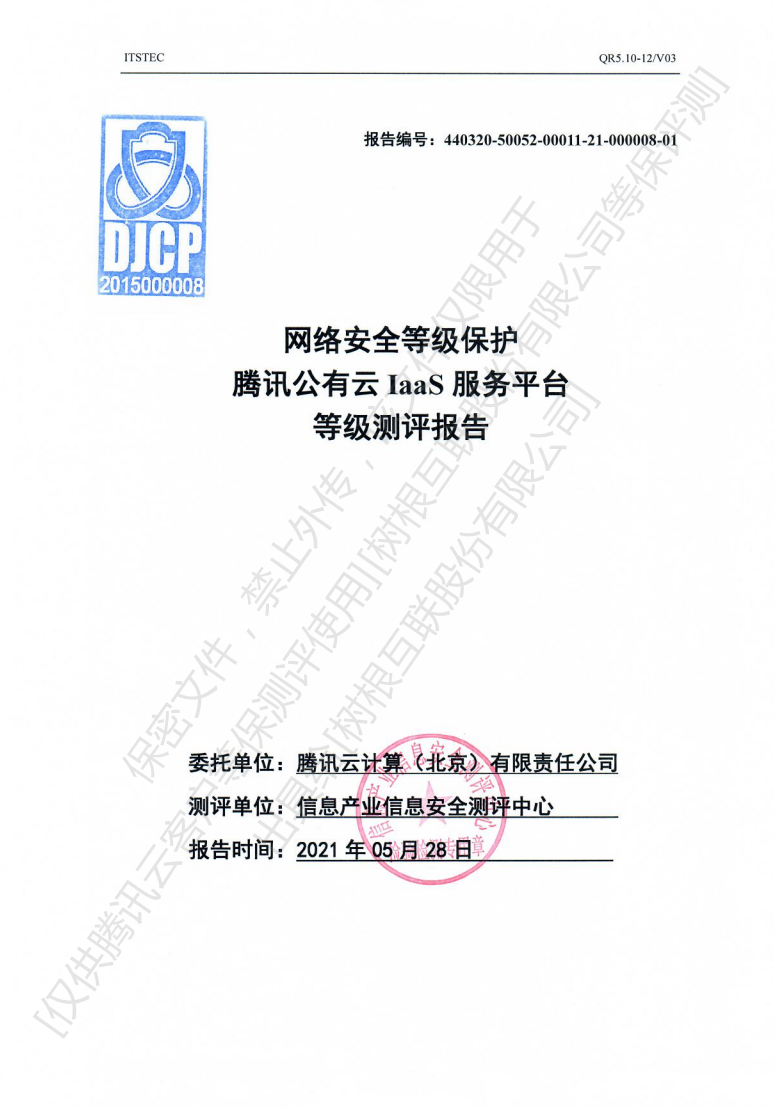


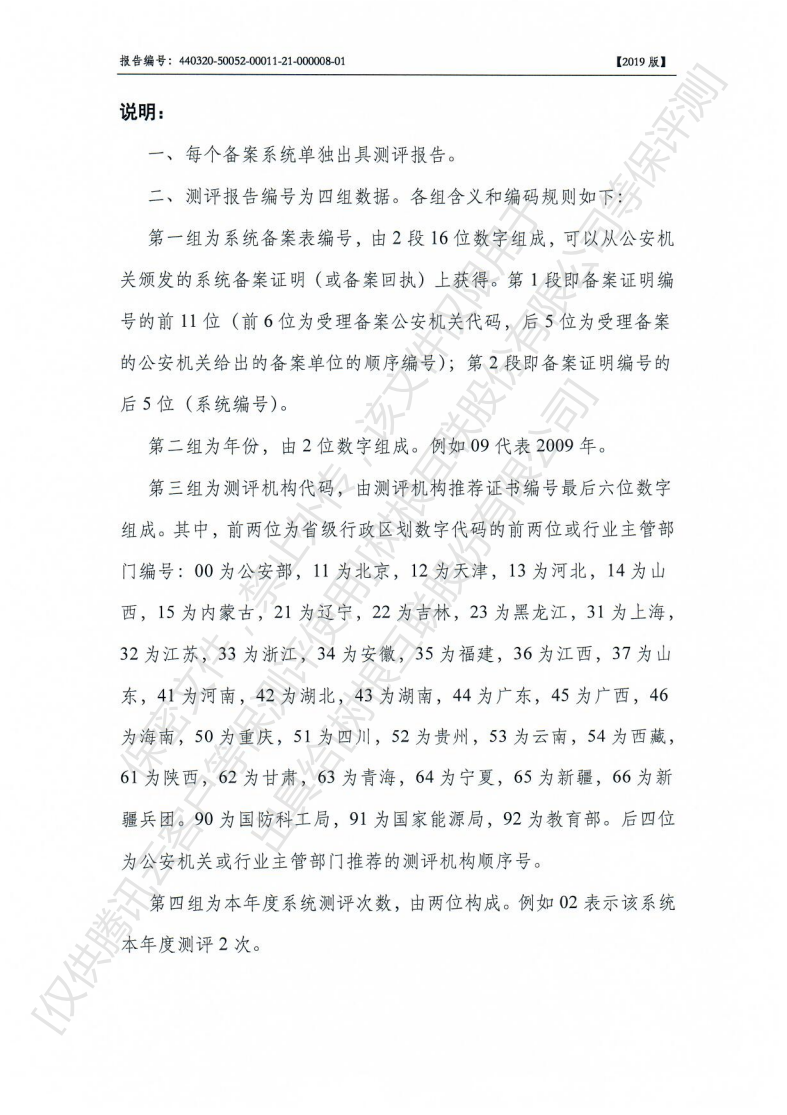
1. 威胁列表

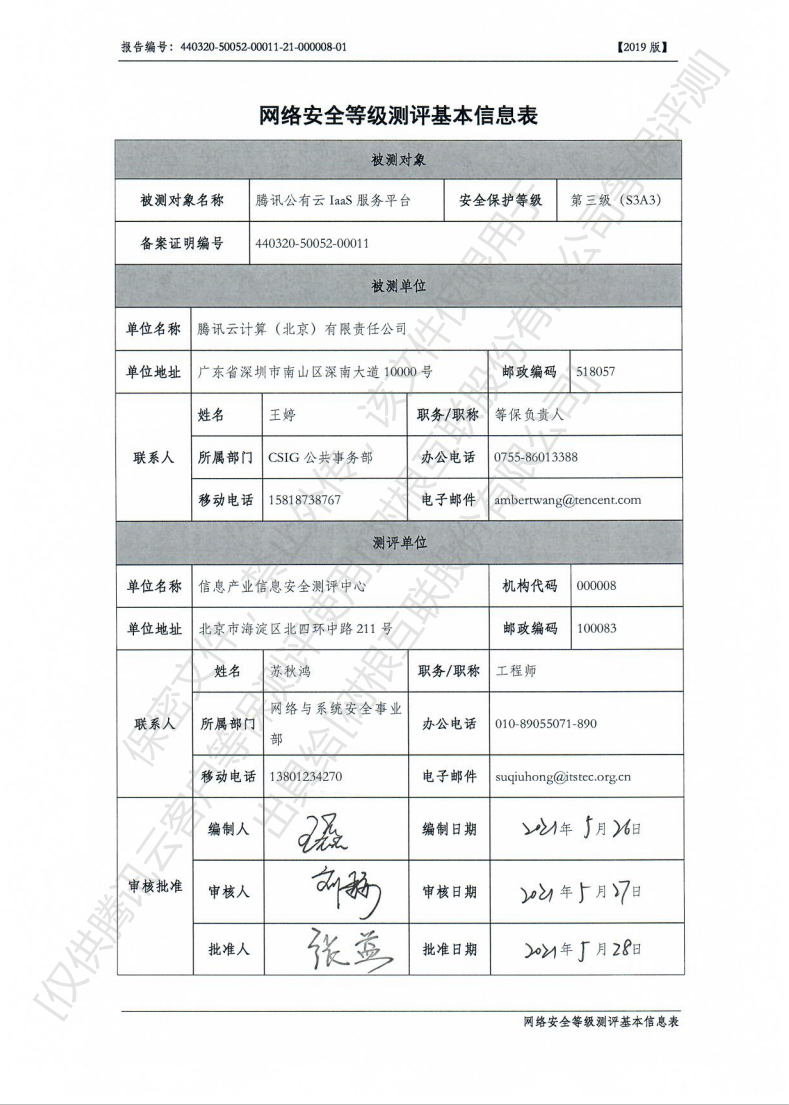
**附录I 表-1威胁列表**

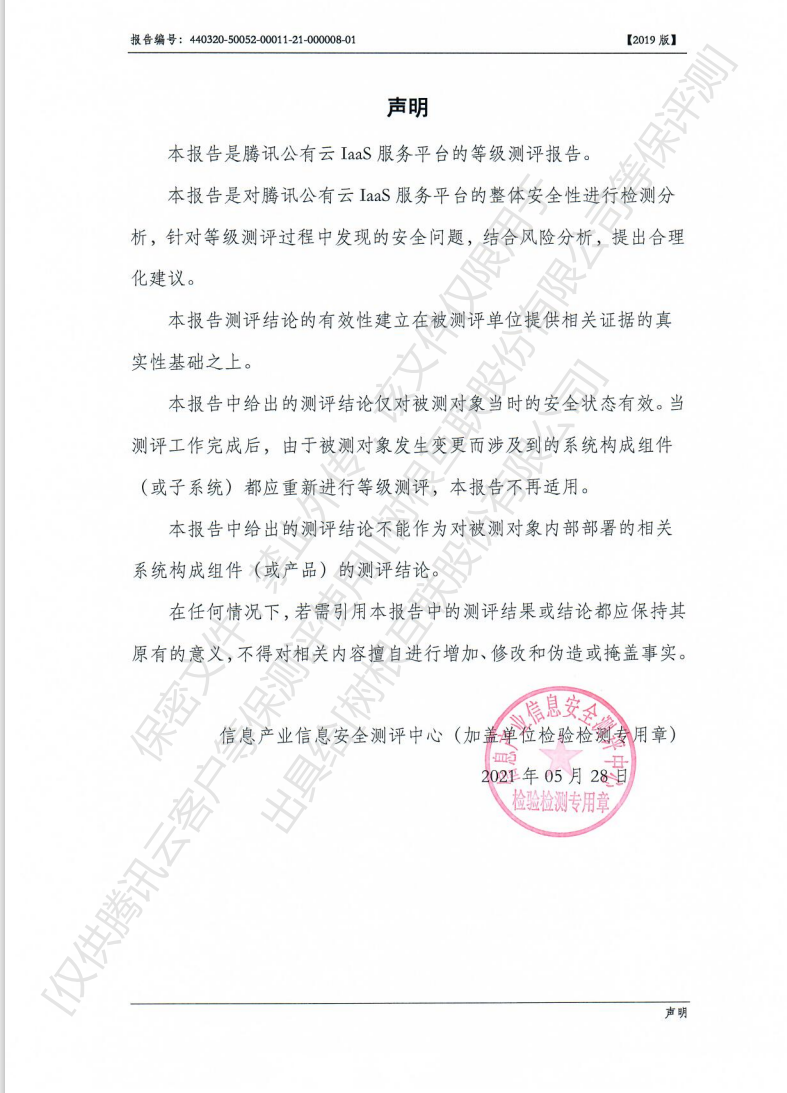
| **序号** | **威胁分(子)类** | **威胁描述** |
| --- | --- | --- |
| 1 | 软硬件故障 | 对业务实施或系统运行产生影响的设备硬件故障、通讯链路中断、系统本身或软件缺陷等问题 |
| 2 | 物理环境影响 | 对信息系统正常运行造成影响的物理环境问题和自然灾害 |
| 3 | 无作为或操作失误 | 应该执行而没有执行相应的操作，或无意执行了错误的操作 |
| 4 | 管理不到位 | 安全管理无法落实或不到位，从而破坏信息系统正常有序运行 |
| 5 | 恶意代码 | 故意在计算机系统上执行恶意任务的程序代码 |
| 6 | 越权或滥用 | 通过采用一些措施，超越自己的权限访问了本来无权访问的资源，或者滥用自己的权限，做出破坏信息系统的行为 |
| 7 | 网络攻击 | 利用工具和技术通过网络对信息系统进行攻击和入侵 |
| 8 | 物理攻击 | 通过物理的接触造成对软件、硬件、数据的破坏 |
| 9 | 泄密 | 信息泄露给不应了解的他人 |
| 10 | 篡改 | 非法修改信息，破坏信息的完整性使系统的安全性降低或信息不可用 |
| 11 | 抵赖 | 不承认收到的信息和所作的操作和交易 |
| 12 | 资源不足 | 系统重要设备负载较高，不满足业务需求，一旦设备因负载较高而出现故障将影响业务连续性 |
| 13 | 敏感信息泄漏 | 敏感信息包括用户信息、 公民信息、地理信息，数量级0~1万、1~10万、10~100万、100万以上 |
| 14 | 网页篡改 | 针对连接互联网的网站面临被篡改的可能性较大 |

1. 云计算平台测评及整改情况
2. **云计算平台测评情况**

****

****

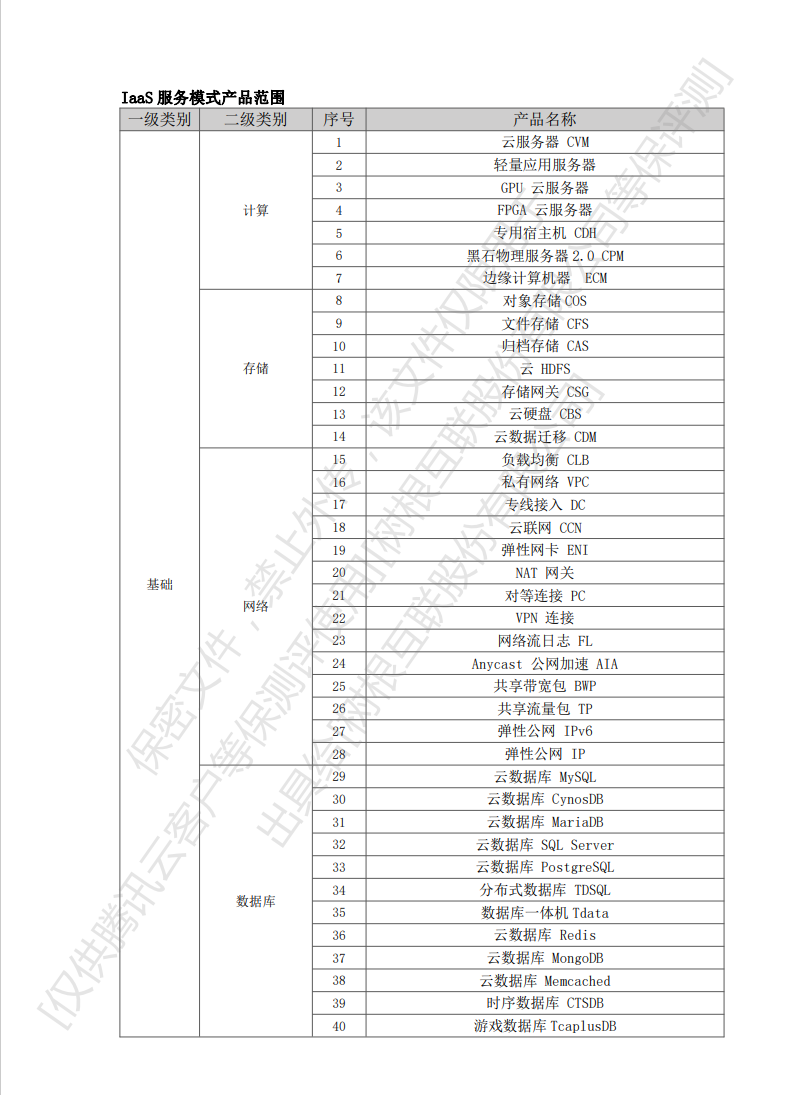
****

****

****

****

****

****

1. **云计算平台整改情况**

经与云服务商腾讯云计算（北京）有限责任公司沟通确认，针对腾讯公有云IaaS服务平台整改情况无法提供。

【全文结束】