**报告编号：33012199039-00002-21-XXXXXX-01**

**网络安全等级保护**

**私有云等级测评报告**

|  |  |
| --- | --- |
| **被测单位：** | **浙江省建设投资集团股份有限公司** |
| **测评单位：** | **杭州中尔网络科技有限公司** |
| **报告时间：** | **2021年12月** |

说明：

一、每个备案系统单独出具测评报告。

二、测评报告编号为四组数据。各组含义和编码规则如下：

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

第二组为年份，由2位数字组成。例如09代表2009年。

第三组为测评机构代码，由测评机构推荐证书编号最后六位数字组成。其中，前两位为省级行政区划数字代码的前两位或行业主管部门编号：00为公安部，11为北京，12为天津，13为河北，14为山西，15为内蒙古，21为辽宁，22为吉林，23为黑龙江，31为上海，32为江苏，33为浙江，34为安徽，35为福建，36为江西，37为山东，41为河南，42为湖北，43为湖南，44为广东，45为广西，46为海南，50为重庆，51为四川，52为贵州，53为云南，54为西藏，61为陕西，62为甘肃，63为青海，64为宁夏，65为新疆，66为新疆兵团。90为国防科工局，91为国家能源局，92为教育部。后四位为公安机关或行业主管部门推荐的测评机构顺序号。

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** | | 私有云 | | | **安全保护等级** | | 第三级（S3A3） | |
| **备案证明编号** | | 33012199039-00002 | | | | | | |
| **被测单位** | | | | | | | | |
| **单位名称** | 浙江省建设投资集团股份有限公司 | | | | | | | |
| **单位地址** | 浙江省杭州市文三西路52号浙江建投大厦 | | | | | **邮政编码** | | 310013 |
| **联系人** | **姓名** | | 李任华 | **职务/职称** | | 信息主管 | | |
| **所属部门** | | 科技信息部 | **办公电话** | | 0571-88235655 | | |
| **移动电话** | | 19805812519 | **电子邮件** | | lirh@cnzgc.com | | |
| **测评单位** | | | | | | | | |
| **单位名称** | 杭州中尔网络科技有限公司 | | | | | **机构代码** | | 0114 |
| **单位地址** | 浙江省杭州市余杭区五常街道溪沁街258号B幢501、502、503室 | | | | | **邮政编码** | | 311100 |
| **联系人** | **姓名** | | 孟洪亮 | **职务/职称** | | 项目经理 | | |
| **所属部门** | | 技术中心 | **办公电话** | | 0571-86123793 | | |
| **移动电话** | | 13588085940 | **电子邮件** | | mhl@hzzekj.com | | |
| **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

本报告是私有云的等级测评报告。

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。

杭州中尔网络科技有限公司

（加盖单位等级测评业务专用章）

2021年12月

等级测评结论

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **测评结论和综合得分** | | | | | |
| **被测对象名称** | 私有云 | **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** | 浙江省建设投资集团股份有限公司是浙江省最大的建筑业企业集团，有着六十多年的发展历史，是浙江省的“国有企业长子”，系省政府出资设立的国有控股集团。前身是浙江建筑公司，成立于1949年8月15日，随后经历了浙江省建筑工业管理局、浙江省城市建设局、浙江省建筑工业厅和浙江省基本建设局等14次变革，2002年3月28日正式更名为浙江省建设投资集团股份有限公司。作为省政府直属厅局中第一家整体转制、走向市场的省属大型国有企业，2009年完成整体改制，实现了产权多元化。“十二五”期间，集团将把整体上市将作为重点工作之一。私有云采用新华三的云计算平台架构进行搭建，主要用于为集团数据化资源提供本地虚拟化服务，为集团内部应用业务系统各子公司提供计算资源服务。目前该系统由浙江省建设投资集团股份有限公司科技信息部负责运行维护。浙江省建设投资集团股份有限公司是该信息系统定级的责任单位。浙江省建设投资集团股份有限公司科技信息部是该信息系统业务的主管部门。 | | | | |
| **安全状况描述** | 该被测对象测评结论为中,高风险数量为0，高风险描述为，中风险数量为33，中风险描述为未在远程管理云平台中设备时，在管理终端和云平台间建立双向身份验证机制。云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。未采取措施对关键设备实施电磁屏蔽防护。未采取措施对非授权设备私自连入内部网络的行为进行检查和限制。未采取措施针对网络访问的数据流量实现基于应用协议和应用内容的访问控制。未配置口令有效期策略。未配置登录连接超时策略。未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。未重命名或删除默认账户。未部署主机入侵防护软件，无法对主机重要节点进行入侵行为进行检查、限制并报警。未安装防恶意代码软件，无法识别入侵和病毒行为，并将其有效阻断。未采用校验技术或密码技术保证重要审计数据在传输过程中的完整性。 | | | | |
| **等级测评结论** | 中 | | **综合得分** | 76.59 | |

*…………………………本页结束，以下为空白…………………………*

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：） | | | | |
| **云计算平台**  **名称** | 私有云 | | **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 |
| f)应提供对虚拟资源的主体和客体设置安全标记的能力，保证云服务客户可以依据安全标记和强制访问控制规则确定主体对客体的访问； | | | | 符合 |
| g) 应提供通信协议转换或通信协议隔离等的数据交换方式，保证云服务客户可以根据业务需求自主选择边界数据交换方式； | | | | 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 |
| 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。 | | | | 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 | 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 |
| 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。 | | | | 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中所有副本删除。 | | | | 符合 |
| 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； | | | | 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； | | | | 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** | | 中 | **云计算平台综合得分** | | 76.59 |

*…………………………本页结束，以下为空白…………………………*

总体评价

浙江省建设投资集团股份有限公司在网络安全技术防护措施的建设和安全管理制度体系建设方面，开展了一定的工作，初步建立了一套满足自身业务发展的网络安全防护体系，能够基本保障私有云日常有效的运行。其中：

在安全物理环境中，安全保护状况如下：浙江建投大厦设置又避雷针。配电柜和列头柜已配备部署有施耐德防雷开关和LKX雷科星防雷器进行保护，可防止感应雷。机房建设位于杭州市西湖区文三西路52号浙江建投大厦15层，该建筑具备防震验收文档，具备良好的防震、防雨和防风的能力，机房内不存在雨水渗漏、墙体开裂等情况。机房使用3台Emerson艾默生精密空调进行温湿度控制，当前机房温度为23℃，湿度为45%，温湿度均在适宜可控范围内。机房采用桥架方式，将通信线缆铺设于机柜上方的走线架中。机房电源线采用下走线方式，通信线缆采用上走线方式部署再桥架当中。

在安全通信网络中，安全保护状况如下：云平台开放第三方API接口，云服务客户可通过申请和工单的形式，在通过审批后可按照云服务客户的要求对接第三方安全服务或部署第三方安全产品。当前系统为浙江省建设投资集团股份有限公司自建私有云，该云平台的网络安全保护等级为第三级（S3A3G3），其私有云上没有承载高于其安全保护等级的业务系统。当前主干核心线路均采用双线聚合互联，关键核心交换、Spine交换机、Leaf交换机，关键出口安全设备，关键资源池服务器等均采用两台至多台进行热冗余部署，保证系统的高可用性。云平台部署有CloudOS平台、SAN平台、CAS平台，支持云服务客户自主定义安全策略，并自主选择所需要的安全服务或组件。网络设备、服务器采用SSH的方式进行远程连接管理，安全设备、应用系统采用HTTPS的方式进行远程管理，可保证通信过程中数据的保密性。

在安全区域边界中，安全保护状况如下：互联网边界通过飞塔防火墙配置策略对跨越边界的网络数据进行控制，且已配置并启用访问控制规则，对不符合策略的数据采取拒绝操作，最后一条策略为双向拒绝所有网络通信。云平台部署有威胁感知大数据平台，云平台服务器边界服务器防火墙集成IPS功能，均已配置监控及报警策略，针对云服务客户发起的网络攻击行为进行记录，其设备规则库版本为20211110，均已升级至最新版本。互联网边界飞塔防火墙、深信服上网行为管理等设备均已启用审计功能，能够针对边界的访问流量，每个用户的访问行为以及重要安全事件等进行审计。服务器边界部署服务器防火墙对进出网络的数据进行控制，数据在指定端口进行传输，通过访问控制策略对数据出入进行控制，仅允许指定端口跨越边界进行网络通信。云平台网络安全保护等级为第三级（S3A3G3），云服务客户不同的等级区域通过VPC组进行隔离，云平台不同等级的网络区域通过CloudOS平台创建服务链配置不同NetWork网络进行隔离。

在安全计算环境中，安全保护状况如下：当前使用admin管理员、aud\*\*\*审计管理员、sec\*\*\*安全管理员、sys\*\*\*系统管理员等角色权限，各账户仅分配所需的最小权限，实现管理用户权限分离。登录设备需要使用用户名加口令进行身份鉴别，身份标识唯一，当前口令长度8位以上，口令组成包含特殊字符，大小写字母和数字，已开启口令复杂度策略Password-control enable，要求口令长度至少8位，口令组成必须包含大小写字母、数字和特殊字符，每半年进行一次口令更换。帕拉迪堡垒机主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的保密性。综合日志审计系统采用HTTPS的远程管理方式，用户鉴别信息加密传输，防止鉴别信息在网络传输中被窃听。云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。

在安全管理中心中，安全保护状况如下：所有测评对象已进行三权分立，仅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。云平台通过CAS平台、SNA平台和CloudOS平台对物理资源和虚拟资源按照管理员策略意愿做统一管理调度与分配。通过CAS平台、CloudOS平台对云平台各服务器运行状况，网络设备、网络链路等进行集中监控，并可依据其工作状态及设定阈值实时报警。云服务商和云租户客户可通过账户划分，对各虚拟网络设备、虚拟机、虚拟安全设备等进行自主控制管理。当前部署有威胁感知大数据平台，能够对网络当中各类安全事件进行识别、分析，监测范围覆盖系统网络所有关键路径，在发生重要安全事件时通过邮件的方式告警管理员。

在安全管理制度中，安全保护状况如下：已制定《ZJJT-XX-17-2020信息安全机构管理制度》、《ZJJT-XX-03-2020计算机病毒防治管理制度》、《ZJJT-XX-04-2020数据备份与恢复管理制度》、《ZJJT-XX-08-2020信息系统巡检管理制度》、《ZJJT-XX-11-2020外部人员访问控制管理制度》、《ZJJT-XX-16-2020信息系统安全补丁管理制度》等制度，相关制度中包含对系统维护、系统配置、用户操作等访问的规定。《ZJJT-XX-01-2020信息安全策略》对安全工作的总体方针和安全策略做了相关说明，对机构安全工作的总体目标、范围、原则和安全框架等进行了阐明，包括组织机构及岗位职责，人员安全管理、环境和资产安全管理、系统安全建设管理 系统安全运行管理、事件处置和应急响应等。指定科技信息科负责安全管理制度的制定。已制定《ZJJT-XX-02-2020网络与信息安全管理制度》、《ZJJT-XX-05-2020机房管理制度 》、《ZJJT-XX-06-2020信息资产管理制度》、《ZJJT-XX-07-2020信息设备运维管理制度》、《ZJJT-XX-08-2020信息系统巡检管理制度》、《ZJJT-XX-09-2020信息网络管理制度》、《ZJJT-XX-14-2020业务应用系统软件安全管理制度》、《ZJJT-XX-18-2020信息系统管理授权审批管理制度》、《ZJJY-XX-19-2020系统安全管理制度》、《ZJJY-XX-24-2020信息系统数据质量管理制度》等制度，相关制度中包含服务运维、系统运维、系统数据安全等管理内容。浙江省建设投资集团股份有限公司的安全管理制度通过红头文件的形式进行发布，其管理制度文件通过内部办公OA系统进行正式发布，且进行了版本控制。

在安全管理机构中，安全保护状况如下：已制定《ZJJT-XX-18-2020信息系统管理授权审批管理制度》，明确各个部门岗位的具体职责划分以及授权审批事项、审批部门和批准人等内容。设立网络安全管理工作的职能部门科技信息部，设立安全主管岗位，《ZJJT-XX-17-2020信息安全机构管理制度》说明部门职责及各个工作岗位的职责。查看到具有《aZJJT-XXBG-02-2020-B网络与信息系统安全运行月报2021年2月》，相关记录表单为《a定期全面信息系统安全检查表》，每季度进行安全检测，报告内容包括系统日常运维、文档、数据备份、系统漏洞等情况。当前配备有系统管理员3名，审计管理员2名、安全管理员2名，网络管理员1名、机房管理员1名、应用管理员1名，其中李明明兼任系统管理员和审计管理员，关俭兼任系统管理员和应用管理员，赖晋宝兼容网络管理员和机房管理员。《ZJJT-XX-01-2020信息安全策略》中已明确成立网络安全工作领导小组，并通过红头文件发布有《关于成立信息安全管理工作领导小组的通知》，明确了人员构成情况和相关职责。

在安全管理人员中，安全保护状况如下：《ZJJT-XX-10-2020信息安全员管理制度》中规定了人员调离手续和离岗要求等，《aZJJT-XXBG-10-2020-A人员离岗交接清单》中按照人员管理文档中的离岗程序办理人员调离手续。已指定人事部专门负责对人员录用。已制定《ZJJT-XX-11-2020外部人员访问控制管理制度》规定了在外部人员接入受控网络访问系统前先提出书面申请，填写《aZJJT-XXBG-11-2020-A外部人员访问申请授权表》，批准后由专人开设账户、分配权限，并登记备案。在《ZJJT-XX-10-2020信息安全员管理制度》规定所有人员离职时的操作流程：删除该人员的信息系统访问账号和权限；明确保密事项，不得泄露原单位信息秘密，不得使用原单位的知识产权。《ZJJT-XX-11-2020外部人员访问控制管理制度》对系统访问情况进行了规定，获得系统访问授权的外部人员应签署保密协议，协议中明确了外部人员的保密义务，包含不得进行非授权操作，不得复制信息等内容。

在安全建设管理中，安全保护状况如下：该系统相关网络安全产品均采用公开招投标、邀请招标、单一来源等方式开展采购，招投标文件、流程符合国家《中华人民共和国招投标法》的有关要求，且网络安全产品均具备销售许可证。在发生安全事件时，云服务商通过邮件或电话方式通知云服务客户，并向云服务客户提交安全事件报告或威胁报告，报告内容包括响应流程响应和处理的范围、程度及处理方法等。在确定该信息系统的安全保护等级后，并未发生较大变更，未调整安全保护级别，系统发生重大变更或级别发生变化时及时进行等级测评。浙江省建设投资集团股份有限公司私有云的定级材料已提交杭州西湖区网安进行备案，具有公安出具的备案证明。已和新华三技术有限公司、浙江乾冠信息安全研究院有限公司签订相关服务合同，服务合同中明确了甲乙双方的责任和义务。

在安全运维管理中，安全保护状况如下：已制定《ZJJT-XX-02-2020网络与信息安全管理制度》、《ZJJT-XX-07-2020信息设备运维管理制度》、《ZJJT-XX-08-2020信息系统巡检管理制度》等制定，明确了在日常运维工作中的安全策略、账户管理、配置管理、日志管理等的操作规程。已在《ZJJT-XX-11-2020外部人员访问控制管理制度》中规定，来访人员在会议室接待，敏感机制不得随意存放，避免外部人员接触，含有敏感信息的纸质文件和移动介质不得随意放置在办公桌面等位置。《ZJJT-XX-02-2020网络与信息安全管理制度》明确如发生安全事件，事后应详细分析事件发生的原因，记录处理过程，总结经验教训等。已制定《ZJJT-XX-07-2020信息设备运维管理制度》，制度中要求含有存储介质的设备在报废或重用前，须对数据进行加密，以确保其所存储信息完全清除或被安全覆盖，不可恢复，且具备详细的清除记录。已制定《ZJJT-XX-05-2020机房管理制度》，制度中已明确对机房人员进出、物品的带进带出和日常安全环境管理等进行规定，具备《机房出入登录表》、《aZJJT-XXBG-08-2020-A巡视记录表》等记录表单。

综合上述评价结果，浙江省建设投资集团股份有限公司私有云在本次测评中，测评项符合率为76.76%，其中部分符合率为8.10%，不符合率为15.14%，其中测评项总数2193个，符合项总数1450个，部分符合项总数153个，不符合项总数286个，不适用项总数304个。问题数（含验证测试）总计37个，其中高风险问题0个，中风险问题数33个，低风险问题4个。结合风险评价与风险对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成的危害情况，最终风险值为：76.59。通过对网络安全等级保护基本安全保护状态的分析，浙江省建设投资集团股份有限公司私有云等级测评结论为中。

**综合判定：浙江省建设投资集团股份有限公司私有云在网络安全等级保护第3级（S3A3G3）保护要求中综合得分76.59。测评结论为中。**

*…………………………本页结束，以下为空白…………………………*

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，私有云存在的主要问题及整改建议如下：

1、安全物理环境

1）**中风险，未采取措施对关键设备实施电磁屏蔽防护。**

建议采取电磁屏蔽措施，如使用电磁屏蔽机房、电磁屏蔽机柜等，对关键设备进行电磁屏蔽防护，以保证关键设备的保密性。涉及测评对象：物理机房。

2、安全通信网络

1）**低风险，未基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。**

建议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。涉及测评对象：安全通信网络。

3、安全区域边界

1）**中风险，未采取措施对非授权设备私自连入内部网络的行为进行检查和限制。**

建议部署准入控制系统防范非法内联行为。涉及测评对象：互联网边界、服务器边界。

2）**中风险，未采取措施针对网络访问的数据流量实现基于应用协议和应用内容的访问控制。**

建议在网络边界处部署应用层防护设备，并开启内容过滤策略防范应用层面的攻击。涉及测评对象：服务器边界、互联网边界。

3）**低风险，未采取措施基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。**

建议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。涉及测评对象：互联网边界、服务器边界。

4、安全计算环境

1）**中风险，未在远程管理云平台中设备时，在管理终端和云平台间建立双向身份验证机制。**

建议在远程管理云平台中设备时，在管理终端和云平台间建立双向身份验证机制。涉及测评对象：核心交换机A、核心交换机B、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、业务数据、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2、亚信安全服务器深度安全防护系统。

2）**中风险，云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。**

建议采取措施对非授权新建虚拟机或者重新启用虚拟机等进行检测并告警。涉及测评对象：核心交换机A、核心交换机B、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、业务数据、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2、亚信安全服务器深度安全防护系统。

3）**中风险，未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。**

建议采取密码技术或其他技术手段对虚拟机镜像、快照中敏感资源进行防护。涉及测评对象：核心交换机A、核心交换机B、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、业务数据、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2、亚信安全服务器深度安全防护系统。

4）**中风险，未配置口令有效期策略。**

建议配置口令的有效期策略，定期更换口令，防止口令被轻易破解。涉及测评对象：CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02。

5）**中风险，未配置登录连接超时策略。**

建议配置登录连接超时策略，严格限制登录超时时间。涉及测评对象：CloudOS3、CloudOS2、CloudOS1。

6）**中风险，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。**

建议采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，并且其中一种鉴别技术为密码技术，如：数字证书、动态口令等。涉及测评对象：亚信安全服务器深度安全防护系统、SDN03、SDN02、SDN01、CVM02、CVM01、CVK05、CVK04、CVK03、CVK02、CVK01、CloudOS3、CloudOS2、CloudOS1、飞塔防火墙B、飞塔防火墙A、综合日志审计系统、深信服上网行为管理B、深信服上网行为管理A、服务器防火墙、帕拉迪堡垒机B、帕拉迪堡垒机A、威胁感知大数据平台、H3C防火墙B、H3C防火墙A、SNA平台、CloudOS平台、CAS平台、核心交换机B、核心交换机A、Spine交换机B、Spine交换机A、Leaf交换机B、Leaf交换机A。

5、安全管理中心

1）**中风险，未限制网络设备、安全设备、服务器等仅通过堡垒机进行运维管理，并对系统管理员的操作进行审计。**

建议限制网络设备、安全设备、服务器仅通过堡垒机进行运维管理，并对系统管理员的操作进行审计。涉及测评对象：安全管理中心。

2）**中风险，未限制网络设备、安全设备、服务器等仅通过堡垒机进行运维管理，并对安全管理员的操作进行审计。**

建议限制网络设备、安全设备、服务器等仅通过堡垒机进行运维管理，并对安全管理员的操作进行审计。涉及测评对象：安全管理中心。

3）**中风险，未采取措施对安全策略、恶意代码、补丁升级等进行统一集中管理。**

建议采取措施对安全策略、恶意代码防范策略、系统或设备的补丁升级进行统一管理。涉及测评对象：安全管理中心。

6、安全管理制度

1）**中风险，未定期对安全管理制度进行论证、审定以及修订。**

建议定期对安全管理制度进行论和审定，并根据审查结果对安全管理制度进行修订。涉及测评对象：制度或记录类文档。

7、安全建设管理

1）**中风险，未组织相关部分和有关专家对安全方案进行论证和审查。**

建议组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。涉及测评对象：制度或记录类文档。

2）**中风险，该系统未使用密码产品，未采购和使用国家密码主管部门要求的密码产品。**

建议采购和使用符合国家密码主管部门的要求的密码产品。涉及测评对象：制度或记录类文档。

3）**中风险，未对源代码进行审计工作，并出具相关审计报告。**

建议对源代码进行审计并出具相关审计报告。涉及测评对象：制度或记录类文档。

4）**中风险，未聘请第三方工程监理控制项目的实施过程。**

建议聘请第三方工程监理的方式控制项目的实施过程，保障项目质量。涉及测评对象：制度或记录类文档。

5）**中风险，安全测试未包含密码相关安全性测试内容。**

建议对系统开展密码应用安全性测试或测评工作并遵照国家密码管理局印发的有关规定执行。涉及测评对象：制度或记录类文档。

8、安全运维管理

1）**中风险，未建立介质管理制度对介质进行控制和保护，也未指定专人或专门的部门对介质进行管理并定期清算盘点。**

建议建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定，并指定专人或专门的部分对介质进行管理并定期进行清算盘点。涉及测评对象：制度或记录类文档。

2）**中风险，未对介质在物理传输过程中的人员选择、打包、交付等进行控制，也未对介质的归档和查询等进行登记记录。**

建议对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，对介质归档和查询等进行登记记录。涉及测评对象：制度或记录类文档。

3）**中风险，系统未使用密码产品，未遵循密码相关国家标准和行业标准。**

建议使用的密码遵循密码相关的国家标准和行业标准。涉及测评对象：制度或记录类文档。

4）**中风险，未建立密码使用管理制度，未使用符合国家密码管理规定的密码技术和产品。**

建议建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。涉及测评对象：制度或记录类文档。

5）**中风险，未建立终止变更并从失败变更中恢复的程序。**

建议建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。涉及测评对象：制度或记录类文档。

6）**中风险，未定期对原有的应急预案重新评估并定期修订完善。**

建议定期对应急预案进行审查和根据实际情况更新的内容，并定期进行修订完善。涉及测评对象：制度或记录类文档。

*…………………………本页结束，以下为空白…………………………*

目录

[网络安全等级测评基本信息表 I](#_Toc88414597)

[声明 II](#_Toc88414598)

[等级测评结论 III](#_Toc88414599)

[等级测评结论扩展表（云计算安全） V](#_Toc88414600)

[总体评价 VII](#_Toc88414601)

[主要安全问题及整改建议 XIV](#_Toc88414602)

[目录 XXI](#_Toc88414603)

[1 测评项目概述 1](#_Toc88414604)

[1.1 测评目的 1](#_Toc88414605)

[1.2 测评依据 1](#_Toc88414606)

[1.3 测评过程 2](#_Toc88414607)

[1.4 报告分发范围 4](#_Toc88414608)

[2 被测对象描述 5](#_Toc88414609)

[2.1 被测对象概述 5](#_Toc88414610)

[2.1.1 定级结果 5](#_Toc88414611)

[2.1.2 业务和采用的技术 5](#_Toc88414612)

[2.1.3 网络结构 6](#_Toc88414613)

[2.2 测评指标 8](#_Toc88414614)

[2.2.1 安全通用要求指标 8](#_Toc88414615)

[2.2.2 安全扩展要求指标 11](#_Toc88414616)

[2.2.3 其他安全要求指标 12](#_Toc88414617)

[2.2.4 不适用安全要求指标 12](#_Toc88414618)

[2.3 测评对象 14](#_Toc88414619)

[2.3.1 测评对象选择方法 14](#_Toc88414620)

[2.3.2 测评对象选择结果 16](#_Toc88414621)

[3 单项测评结果分析 26](#_Toc88414622)

[3.1 安全物理环境 26](#_Toc88414623)

[3.1.1 已有安全控制措施汇总分析 26](#_Toc88414624)

[3.1.2 主要安全问题汇总分析 28](#_Toc88414625)

[3.2 安全通信网络 28](#_Toc88414626)

[3.2.1 已有安全控制措施汇总分析 28](#_Toc88414627)

[3.2.2 主要安全问题汇总分析 29](#_Toc88414628)

[3.3 安全区域边界 30](#_Toc88414629)

[3.3.1 已有安全控制措施汇总分析 30](#_Toc88414630)

[3.3.2 主要安全问题汇总分析 32](#_Toc88414631)

[3.4 安全计算环境 33](#_Toc88414632)

[3.4.1 网络设备 33](#_Toc88414633)

[3.4.2 安全设备 38](#_Toc88414634)

[3.4.3 服务器和终端 44](#_Toc88414635)

[3.4.4 系统管理软件/平台 50](#_Toc88414636)

[3.4.5 业务应用系统/平台 54](#_Toc88414637)

[3.4.6 数据资源 59](#_Toc88414638)

[3.4.7 其他系统或设备 62](#_Toc88414639)

[3.5 安全管理中心 63](#_Toc88414640)

[3.5.1 已有安全控制措施汇总分析 63](#_Toc88414641)

[3.5.2 主要安全问题汇总分析 64](#_Toc88414642)

[3.6 安全管理制度 64](#_Toc88414643)

[3.6.1 已有安全控制措施汇总分析 64](#_Toc88414644)

[3.6.2 主要安全问题汇总分析 66](#_Toc88414645)

[3.7 安全管理机构 66](#_Toc88414646)

[3.7.1 已有安全控制措施汇总分析 66](#_Toc88414647)

[3.7.2 主要安全问题汇总分析 68](#_Toc88414648)

[3.8 安全管理人员 68](#_Toc88414649)

[3.8.1 已有安全控制措施汇总分析 68](#_Toc88414650)

[3.8.2 主要安全问题汇总分析 70](#_Toc88414651)

[3.9 安全建设管理 70](#_Toc88414652)

[3.9.1 已有安全控制措施汇总分析 70](#_Toc88414653)

[3.9.2 主要安全问题汇总分析 72](#_Toc88414654)

[3.10 安全运维管理 73](#_Toc88414655)

[3.10.1 已有安全控制措施汇总分析 73](#_Toc88414656)

[3.10.2 主要安全问题汇总分析 78](#_Toc88414657)

[3.11 其他安全要求指标 79](#_Toc88414658)

[3.12 验证测试 79](#_Toc88414659)

[3.12.1 漏洞扫描 79](#_Toc88414660)

[3.12.2 渗透测试 86](#_Toc88414661)

[3.13 单项测评小结 88](#_Toc88414662)

[3.13.1 控制点符合情况汇总 88](#_Toc88414663)

[3.13.2 安全问题汇总 92](#_Toc88414664)

[4 整体测评 111](#_Toc88414665)

[4.1 安全控制点间安全测评 111](#_Toc88414666)

[4.2 区域间安全测评 112](#_Toc88414667)

[4.3 整体测评结果汇总 113](#_Toc88414668)

[5 安全问题风险分析 116](#_Toc88414669)

[6 等级测评结论 151](#_Toc88414670)

[7 安全问题整改建议 153](#_Toc88414671)

[附录A 被测对象资产 169](#_Toc88414672)

[A.1 物理机房 169](#_Toc88414673)

[A.2 网络设备 169](#_Toc88414674)

[A.3 安全设备 170](#_Toc88414675)

[A.4 服务器/存储设备 171](#_Toc88414676)

[A.5 终端设备 173](#_Toc88414677)

[A.6 其他系统或设备 173](#_Toc88414678)

[A.7 系统管理软件/平台 173](#_Toc88414679)

[A.8 业务应用系统/平台 174](#_Toc88414680)

[A.9 数据资源 174](#_Toc88414681)

[A.10 密码产品 174](#_Toc88414682)

[A.11 安全相关人员 175](#_Toc88414683)

[A.12 安全管理文档 175](#_Toc88414684)

[附录B 上次测评问题整改情况说明 180](#_Toc88414685)

[附录C 单项测评结果汇总 181](#_Toc88414686)

[C.1 安全物理环境 181](#_Toc88414687)

[C.2 安全通信网络 181](#_Toc88414688)

[C.3 安全区域边界 182](#_Toc88414689)

[C.4 安全计算环境 183](#_Toc88414690)

[C.4.1 网络设备 183](#_Toc88414691)

[C.4.2 安全设备 186](#_Toc88414692)

[C.4.3 服务器和终端 191](#_Toc88414693)

[C.4.4 系统管理软件/平台 197](#_Toc88414694)

[C.4.5 业务应用系统/平台 198](#_Toc88414695)

[C.4.6 数据资源 200](#_Toc88414696)

[C.4.7 其他系统或设备 201](#_Toc88414697)

[C.5 安全管理中心 201](#_Toc88414698)

[C.6 安全管理制度 202](#_Toc88414699)

[C.7 安全管理机构 202](#_Toc88414700)

[C.8 安全管理人员 203](#_Toc88414701)

[C.9 安全建设管理 203](#_Toc88414702)

[C.10 安全运维管理 204](#_Toc88414703)

[C.11 其他安全要求指标 205](#_Toc88414704)

[附录D 单项测评结果记录 206](#_Toc88414705)

[D.1 安全物理环境 206](#_Toc88414706)

[D.1.1 安全通用要求部分 206](#_Toc88414707)

[D.1.2 安全扩展要求部分 208](#_Toc88414708)

[D.2 安全通信网络 209](#_Toc88414709)

[D.2.1 安全通用要求部分 209](#_Toc88414710)

[D.2.2 安全扩展要求部分 210](#_Toc88414711)

[D.3 安全区域边界 211](#_Toc88414712)

[D.3.1 安全通用要求部分 211](#_Toc88414713)

[D.3.2 安全扩展要求部分 218](#_Toc88414714)

[D.4 安全计算环境 221](#_Toc88414715)

[D.4.1 安全通用要求部分 221](#_Toc88414716)

[D.4.2 安全扩展要求部分 387](#_Toc88414717)

[D.5 安全管理中心 486](#_Toc88414718)

[D.5.1 安全通用要求部分 486](#_Toc88414719)

[D.5.2 安全扩展要求部分 488](#_Toc88414720)

[D.6 安全管理制度 488](#_Toc88414721)

[D.7 安全管理机构 490](#_Toc88414722)

[D.8 安全管理人员 493](#_Toc88414723)

[D.9 安全建设管理 495](#_Toc88414724)

[D.9.1 安全通用要求部分 495](#_Toc88414725)

[D.9.2 安全扩展要求部分 499](#_Toc88414726)

[D.10 安全运维管理 501](#_Toc88414727)

[D.10.1 安全通用要求部分 501](#_Toc88414728)

[D.10.2 安全扩展要求部分 508](#_Toc88414729)

[D.11 其他安全要求 508](#_Toc88414730)

[附录E 漏洞扫描结果记录 510](#_Toc88414731)

[附录F 渗透测试结果记录 512](#_Toc88414732)

[F.1 CloudOS平台存在Docker Engine API信息泄露 512](#_Toc88414733)

[F.2 CAS平台存在点击劫持 512](#_Toc88414734)

[附录G 威胁列表 514](#_Toc88414735)

[附录H 云计算平台测评及整改情况 515](#_Toc88414736)

[附录I 大数据平台测评及整改情况 516](#_Toc88414737)

# 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，浙江省建设投资集团股份有限公司委托杭州中尔网络科技有限公司（XXXXX）对私有云实施等级测评，以期发现被测评对象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 17859—1999 《计算机信息系统 安全保护等级划分准则》
2. 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》）
3. GB/T 28448—2019 《信息安全技术 网络安全等级保护测评要求》
4. GB/T 28449—2018 《信息安全技术 网络安全等级保护测评过程指南》
5. GB/T 20984—2007 《信息安全技术 信息安全风险评估规范》

## 测评过程

等级测评过程分为四个基本测评活动：测评准备阶段、方案编制阶段、现场测评阶段、分析与报告编制阶段。测评双方之间的沟通与洽谈贯穿整个等级测评过程。

2021年11月23日至2021年11月24日期间为测评准备阶段，测评项目组通过调查表格等方式，完成了浙江省建设投资集团股份有限公司私有云基本情况的调查，并针对调研结果进行了静态分析。

2021年11月24日至2021年11月25日期间为方案编制阶段，测评项目组编制完成《浙江省建设投资集团股份有限公司网络安全等级保护测评方案》，并得到浙江省建设投资集团股份有限公司现场测评授权，于2021年11月29日至2021年12月02日实施现场测评。

2021年11月29日至2021年12月02日期间为现场测评阶段，网络安全等级测评小组按照测评现场工作计划，在浙江省建设投资集团股份有限公司开展了网络安全等级保护测评工作。测评组投入相关测试人员，完成了安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面的网络安全等级保护测评。

2021年12月02日，测评项目组同浙江省建设投资集团股份有限公司召开了信息安全等级保护测评问题会议，就现场安全等级保护测评情况进行了总结，讨论并确认了管理和技术方面所发现的问题，编制问题汇总表。

2021年12月07日至2021年12月XX日期间为分析与报告编制阶段，测评项目组对现场测评结果进行整理，并与等级保护要求进行差距分析、整体测评，对发现问题进行风险分析和评价，依据此次测评指标完成信息安全等级测评报告编制工作。

具体流程如下图所示：



## 报告分发范围

本报告一式3份，其中1份提交浙江省建设投资集团股份有限公司，1份提交备案机关，1份由杭州中尔网络科技有限公司留存。

*…………………………本页结束，以下为空白…………………………*

# 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** |
| --- | --- | --- | --- |
| 私有云 | 3级 | 3级 | 3级 |

### 业务和采用的技术

浙江省建设投资集团股份有限公司是浙江省最大的建筑业企业集团，有着六十多年的发展历史，是浙江省的“国有企业长子”，系省政府出资设立的国有控股集团。前身是浙江建筑公司，成立于1949年8月15日，随后经历了浙江省建筑工业管理局、浙江省城市建设局、浙江省建筑工业厅和浙江省基本建设局等14次变革，2002年3月28日正式更名为浙江省建设投资集团股份有限公司。作为省政府直属厅局中第一家整体转制、走向市场的省属大型国有企业，2009年完成整体改制，实现了产权多元化。“十二五”期间，集团将把整体上市将作为重点工作之一。私有云采用新华三的云计算平台架构进行搭建，主要用于为集团数据化资源提供本地虚拟化服务，为集团内部应用业务系统各子公司提供计算资源服务。

私有云系统采用华三云的云平台技术架构，提供资源虚拟化，网络虚拟化，云安全组、云防火墙，且旁路部署有资源池提供入侵防护、恶意代码防护、脆弱性感知、主机层防护等安全防护功能。

### 网络结构

浙江省建设投资集团股份有限公司私有云的网络结构主要包括：边界区、核心层、计算资源池和安全管理区。

1、边界区

（1）互联网边界采用飞塔防火墙FG-600E，实施网络访问控制、入侵防护、恶意代码防护等功能，为边界提供一定的安全防护能力。

（2）服务器边界采用服务器防火墙AF-1000，实施网络访问控制、入侵防护、恶意代码防护等功能，为边界提供一定的安全防护能力。

2、核心层

核心层网络主要提供用户、服务器的数据交换功能。使用两台H3CS10606作为核心交换机，两台H3CS9850作为Spine交换机，两台H3CS6800作为Leaf交换机，均通过IRF虚拟化技术进行热冗余部署保证高可用性，并通过ACL进行提供一定的访问控制能力。

3、安全管理区

安全管理区域主要提供安全审计、安全运维、态势感知、虚拟主机防护等功能。设备均采用旁路方式进行部署，使用综合日志审计系统、威胁感知大数据平台、亚信安全服务器深度安全防护系统，实现日志集中审计、态势感知、虚拟主机安全防护等。

3、计算资源池

计算资源池部署有私有云的5台资源池服务器，专为云计算平台提供计算资源。

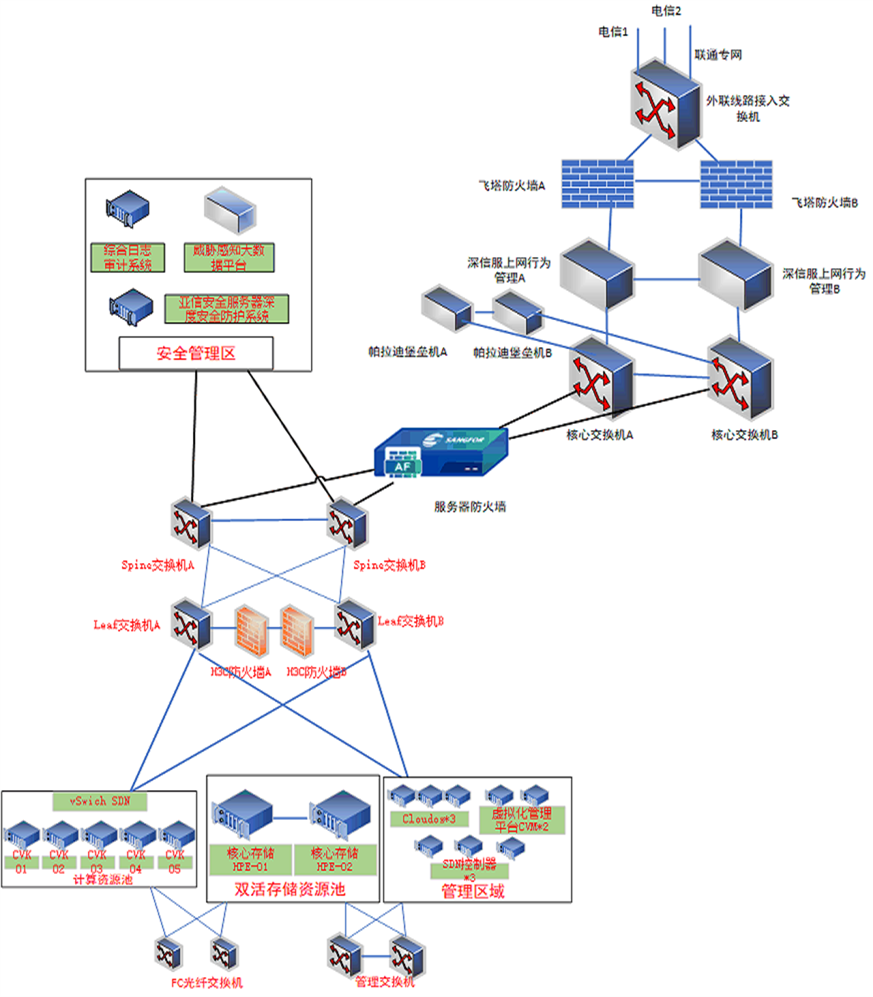
4、管理区域

管理区域部署有CloudOS平台、CAS平台、SNA平台等服务器，为云计算平台的资源池提供资源控制、网络划分等情况。

5、备份情况

网络设备、安全设备的配置数据由管理员定期或在重大配置更新前对设备配置文件进行手工备份，备份地点：自身电脑和服务器。服务器重要数据通过数腾备份软件备份；备份策略：增量备份；备份频率：每天；备份地点：本地服务器。且通过软件介质实时同步，将重要数据备份至宁波建投子公司。

其中管理交换机、FC光纤交换机、外联线路接入交换机均为纯二层交换机，不进行管理，故未纳入测评范围。核心存储HEP-01、核心存储HEP-02仅作为磁盘存储，故未纳入测评范围。



**图 2‑1网络结构拓扑图**

## 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 | 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 |

### 其他安全要求指标

本次检测不包含其他安全要求指标。

### 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** |
| --- | --- | --- | --- |
| 安全区域边界 | 边界防护 | 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。 | 该系统未使用无线网络。 |
| 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。 | 该系统未涉及邮件系统。 |
| 安全计算环境 | 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； | CloudOS平台、CAS平台、SNA平台仅作为私有云的管理控制平台，不涉及用户个人信息。 |
| b)应禁止未授权访问和非法使用用户个人信息。 | CloudOS平台、CAS平台、SNA平台仅作为私有云的管理控制平台，不涉及用户个人信息。 |
| 安全建设管理 | 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； | 不涉及自行软件开发。 |
| 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； | 不涉及自行软件开发。 |
| c)应制定代码编写安全规范，要求开发人员参照规范编写代码； | 不涉及自行软件开发。 |
| 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； | 不涉及自行软件开发。 |
| 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； | 不涉及自行软件开发。 |
| 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； | 不涉及自行软件开发。 |
| 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。 | 不涉及自行软件开发。 |
| 安全计算环境（云计算安全扩展要求） | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 |
| 安全建设管理（云计算安全扩展要求） | 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； | 该系统为云计算平台，故该条款不适用。 |
| 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； | 该系统为云计算平台，故该条款不适用。 |
| 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； | 该系统为云计算平台，故该条款不适用。 |
| 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； | 该系统为云计算平台，故该条款不适用。 |
| 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。 | 该系统为云计算平台，故该条款不适用。 |

## 测评对象

### 测评对象选择方法

浙江省建设投资集团股份有限公司私有云为第三级系统。第三级定级对象的等级测评，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,抽查的测评对象种类主要考虑以下几个方面：

——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局部(包括整体)或对定级对象的局部(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；

——存储被测定级对象重要数据的介质的存放环境；

——办公场地；

——整个系统的网络拓扑结构；

——安全设备,包括防火墙、入侵检测设备和防病毒网关等；

——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；

——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、汇聚层交换机、路由器等；

——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)；

——管理终端和主要业务应用系统终端；

——能够完成被测定级对象不同业务使命的业务应用系统；

——业务备份系统；

——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；

——涉及到定级对象安全的所有管理制度和记录。

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

**表 2‑5物理机房**

| **序号** | **机房名称** | **物理位置** | **重要程度** |
| --- | --- | --- | --- |
| 1 | 物理机房 | 浙江省杭州市西湖区古荡街道文三西路52号15楼 | 关键 |

#### 网络设备

**表 2‑6网络设备**

| **序号** | **设备名称** | **是否虚拟设备** | **系统及版本** | **品牌及型号** | **用途** | **重要程度** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 核心交换机A | 否 | Version 7.1.045, Release 7184 | H3C S10506 | 核心数据交换 | 关键 |
| 2 | Spine交换机A | 否 | Version 7.1.070, Release 6607 | H3C S9850 | 数据交换 | 关键 |
| 3 | Leaf交换机A | 否 | Version 7.1.070, Release 2702 | H3C S6800 | 数据交换 | 关键 |
| 4 | 核心交换机B | 否 | Version 7.1.045, Release 7184 | H3C S10506 | 核心数据交换 | 关键 |
| 5 | Spine交换机B | 否 | Version 7.1.070, Release 6607 | H3C S9850 | 数据交换 | 关键 |
| 6 | Leaf交换机B | 否 | Version 7.1.070, Release 2702 | H3C S6800 | 数据交换 | 关键 |

#### 安全设备

**表 2‑7安全设备表**

| **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** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 飞塔防火墙A | 否 | V6.4.3 build1778(GA) | 飞塔FG-600E | 访问控制、入侵防护、恶意代码防护 | 关键 |
| 2 | 飞塔防火墙B | 否 | V6.4.3 build1778(GA) | 飞塔FG-600E | 访问控制、入侵防护、恶意代码防护 | 关键 |
| 3 | 深信服上网行为管理A | 否 | AC11.9R1 | 深信服AC-3300-HY | 行为审计和外联控制 | 重要 |
| 4 | 深信服上网行为管理B | 否 | AC11.9R1 | 深信服AC-3300-HY | 行为审计和外联控制 | 重要 |
| 5 | 帕拉迪堡垒机A | 否 | ST00001B090 | 帕拉迪Core4A-UTM | 安全运维 | 重要 |
| 6 | 帕拉迪堡垒机B | 否 | ST00001B090 | 帕拉迪Core4A-UTM | 安全运维 | 重要 |
| 7 | H3C防火墙A | 否 | Vesion 7.1.064,Release 9608P30 | H3C F5030-D | 东西向流量访问控制 | 重要 |
| 8 | H3C防火墙B | 否 | Vesion 7.1.064,Release 9608P30 | H3C F5030-D | 东西向流量访问控制 | 重要 |
| 9 | 综合日志审计系统 | 否 | E1107 | H3C CSAP-SA | 日志审计 | 重要 |
| 10 | 服务器防火墙 | 否 | AF8.0.35 | 深信服AF-1000 | 访问控制、入侵防护、恶意代码防护 | 关键 |
| 11 | 威胁感知大数据平台 | 否 | V5.4.26 | 迪普 | 威胁集中分析和报警 | 重要 |

#### 服务器/存储设备

**表 2‑8服务器/存储设备**

| **序号** | **设备名称** | **所属业务应用系统/平台** | **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** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | CVK01 | / | 否 | Centos7.6 | / | / | 关键 |
| 2 | CVK02 | / | 否 | Centos7.6 | / | / | 关键 |
| 3 | CVK03 | / | 否 | Centos7.6 | / | / | 关键 |
| 4 | CVK04 | / | 否 | Centos7.6 | / | / | 关键 |
| 5 | CVK05 | / | 否 | Centos7.6 | / | / | 关键 |
| 6 | CloudOS1 | CloudOS平台 | 否 | Centos7.6 | / | / | 重要 |
| 7 | CloudOS2 | CloudOS平台 | 否 | Centos7.6 | / | / | 重要 |
| 8 | CloudOS3 | CloudOS平台 | 否 | Centos7.6 | / | / | 重要 |
| 9 | CVM01 | CAS平台 | 否 | Centos7.6 | / | / | 重要 |
| 10 | CVM02 | CAS平台 | 否 | Centos7.6 | / | / | 重要 |
| 11 | SDN01 | SNA平台 | 否 | H3Linux Release 1.1.2 | / | / | 重要 |
| 12 | SDN02 | SNA平台 | 否 | H3Linux Release 1.1.2 | / | / | 重要 |
| 13 | SDN03 | SNA平台 | 否 | H3Linux Release 1.1.2 | / | / | 重要 |

#### 终端设备

**表 2‑9终端设备**

| **序号** | **设备名称** | **是否虚拟设备** | **操作系统及版本** | **用途** | **重要程度** |
| --- | --- | --- | --- | --- | --- |
| 1 | 运维终端1 | 否 | Windows 10 | 运维管控 | 一般 |
| 2 | 运维终端2 | 否 | Windows 10 | 运维管控 | 一般 |

#### 其他设备

本次测评不包含此表格。

#### 系统管理软件/平台

**表 2‑10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 | 亚信安全服务器深度安全防护系统 | 主机层恶意代码防护 | 10.0.5129 | / | 重要 |

该系统为浙江省建设投资集团股份有限公司提供云计算虚拟资源服务，且不提供租户侧的数据库服务，均由租户自行搭建和运维管理。

#### 业务应用系统/平台

**表 2‑11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 | CloudOS平台 | 用于私有云平台创建网络及虚拟机。 | / | 新华三技术有限公司 | 关键 |
| 2 | CAS平台 | 用于私有云平台底层资源创建和控制。 | / | 新华三技术有限公司 | 关键 |
| 3 | SNA平台 | 用于私有云平台控制网络虚拟化功能。 | / | 新华三技术有限公司 | 关键 |

#### 数据资源

**表 2‑12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 | CloudOS平台、CAS平台、SNA平台 | 保密性、完整性、备份和恢复 | 重要 |

#### 安全相关人员

**表 2‑13安全相关人员**

| **序号** | **姓名** | **岗位/角色** | **联系方式** | **所属单位** |
| --- | --- | --- | --- | --- |
| 1 | 郑辉 | 安全管理员 | 0571-88260691 | 浙江省建设投资集团股份有限公司 |
| 2 | 李明明 | 系统管理员/审计管理员 | 13626815240 | 浙江省建设投资集团股份有限公司 |
| 3 | 关俭 | 系统管理员/应用管理员 | 13588759167 | 浙江省建设投资集团股份有限公司 |
| 4 | 张振 | 审计管理员 | 13454113928 | 浙江省建设投资集团股份有限公司 |
| 5 | 赖晋宝 | 网络管理员/机房管理员 | 13758191743 | 浙江省建设投资集团股份有限公司 |
| 6 | 李任华 | 安全管理员 | 19805812519 | 浙江省建设投资集团股份有限公司 |

#### 安全管理文档

**表 2‑14安全管理文档**

| **序号** | **文档名称** | **主要内容** |
| --- | --- | --- |
| 1 | 《ZJJT-XX-01-2020信息安全策略》 | 包含总体适用范围、信息安全职责等。 |
| 2 | 《ZJJT-XX-02-2020网络与信息安全管理制度》 | 包含人员管理、信息安全建设、信息安全事件严重程度级别划分等。 |
| 3 | 《ZJJT-XX-04-2020数据备份与恢复管理制度》 | 包含数据备份及恢复措施等。 |
| 4 | 《ZJJT-XX-05-2020机房管理制度》 | 包含机房进出管理、机房守则、机房建设等。 |
| 5 | 《ZJJT-XX-06-2020信息资产管理制度》 | 包含信息资产分类、处理管理办法。 |
| 6 | 《ZJJT-XX-10-2020信息安全员管理制度》 | 包含信息安全员聘用和管理、信息安全教育培训和考核等。 |
| 7 | 《ZJJT-XX-11-2020外部人员访问控制管理制度》 | 包含外部人员访问控制与管理等。 |
| 8 | 《ZJJT-XX-12-2020信息安全人员培训和教育管理制度》 | 包含培训要求、培训内容等。 |
| 9 | 《ZJJT-XX-16-2020信息系统安全补丁管理制度》 | 包含补丁更新、补丁测试等。 |
| 10 | 《ZJJT-XX-17-2020信息安全机构管理制度》 | 包含安全管理员、安全审计员等各岗位职责以及各岗位人员统计。 |
| 11 | 《ZJJT-XX-18-2020信息系统管理授权审批管理制度》 | 包含信息系统的授权审批流程。 |
| 12 | 《ZJJY-XX-21-2020信息安全产品采购管理制度》 | 包含设备采购、软件采购等采购管理制度。 |
| 13 | 《ZJJY-XX-22-2020信息安全外包运维管理制度》 | 包含外包服务合同管理要求、外包服务监控与评价等。 |
| 14 | 《ZJJY-XX-23-2020信息系统工程实施管理制度》 | 包含工程实施管理、实施人员行为准则等。 |
| 15 | 《aZJJT-XXBG-02-2020-B网络与信息系统安全运行月报》 | 网络与信息系统安全运行月报。 |
| 16 | 《ZJJT-XX-03-2020计算机病毒防治管理制度》 | 包含计算机病毒防治管理、指定计算机病毒防治工作的管理部门以及具体职责。 |
| 17 | 《ZJJT-XX-07-2020信息设备运维管理制度》 | 包含网络管理员具体职责、运维操作管理等。 |
| 18 | 《ZJJT-XX-08-2020信息系统巡检管理制度》 | 包含巡检的方式、过程等管理办法。 |
| 19 | 《ZJJT-XX-09-2020信息网络管理制度》 | 包含网络接入管理、网络运行管理等。 |
| 20 | 《ZJJT-XX-13-2020网络设备安全管理制度》 | 包含网络设备/安全设备安全管理、系统升级和补丁安全等。 |
| 21 | 《ZJJT-XX-14-2020业务应用系统软件安全管理制度》 | 包含业务应用系统软件的具体配置要求等。 |
| 22 | 《ZJJT-XX-15-2020计算机网络系统测试管理制度》 | 包含计算机网络系统测试要求、测试实施步骤、测试方案等。 |
| 23 | 《ZJJY-XX-19-2020系统安全管理制度》 | 包含用户账户管理、文件系统管理、系统安全管理、数据库管理、日志安全管理等。 |
| 24 | 《ZJJY-XX-20-2020软件开发管理制度》 | 包含外包软件开发管理、信息系统安全整体测试等。 |
| 25 | 《ZJJY-XX-24-2020信息系统数据质量管理制度》 | 包含数据质量管理职责、检查与考核等。 |
| 26 | 《aZJJT-XXBG-02-2020-A网络与信息安全事故情况报告表》 | 包含网络与信息安全事故的记录表单。 |
| 27 | 《aZJJT-XXBG-02-2020-C网络与重要信息系统敏感时期安全运行日报》 | 包含网络与重要信息系统敏感时期的运行日报记录内容。 |
| 28 | 《aZJJT-XXBG-02-2020-D离岗保密承诺书》 | 包含离岗保密协议相关内容。 |
| 29 | 《aZJJT-XXBG-02-2020-F保密协议(供应商)》 | 包含供应商保密协议相关内容。 |
| 30 | 《aZJJT-XXBG-03-2020-A恶意代码分析报告》 | 包含恶意代码分析相关内容。 |
| 31 | 《aZJJT-XXBG-03-2020-B恶意代码特征库更新记录表》 | 包含恶意代码规则库更新记录表单。 |
| 32 | 《aZJJT-XXBG-07-2020-A系统（设备）操作记录表》 | 包含系统和设备操作记录内容。 |
| 33 | 《aZJJT-XXBG-07-2020-C配置变更记录表》 | 包含系统变更相关记录内容。 |
| 34 | 《aZJJT-XXBG-08-2020-A巡视记录表》 | 包含巡检记录相关内容。 |
| 35 | 《aZJJT-XXBG-08-2020-B设备巡查记录表》 | 包含设备巡检记录表单内容。 |
| 36 | 《aZJJT-XXBG-10-2020-A人员离岗交接清单》 | 包含人员离岗时交接的内容清单。 |
| 37 | 《aZJJT-XXBG-10-2020-C保密协议》 | 包含建投集团保密协议内容。 |
| 38 | 《aZJJT-XXBG-11-2020-A外部人员访问申请授权表》 | 包含外部人员访问申请的相关记录内容。 |
| 39 | 《aZJJT-XXBG-12-2020-培训记录表》 | 包含培训有关记录表单。 |
| 40 | 《aZJJT-XXBG-16-2020系统补丁更新记录表》 | 包含系统补丁更新记录相关内容。 |
| 41 | 《a机房出入登记表》 | 包含机房出入登记相关内容。 |
| 42 | 《网络安全培训计划》 | 包含安全培训计划、方案、时间、地点等内容。 |
| 43 | 《03浙江省建设投资集团股份有限公司私有云系统应急预案》 | 包含私有云系统相关应急预案方案。 |
| 44 | 《04浙江省建设投资集团股份有限公司私有云系统应急演练记录》 | 包含私有云系统应急演练相关记录。 |
| 45 | 《关于成立信息安全管理工作领导小组的通知》 | 包含信息安全领导小组成立的红头文件的详细内容。 |
| 46 | 《私有云安全设计方案》 | 包含私有云安全方案设计的相关内容。 |
| 47 | 《产品选型测试记录表》 | 包含产品选型测试相关记录表单。 |
| 48 | 《私有云测试验收方案》 | 包含私有云系统验收测试方法、验收测试内容、验收测试预期结果。 |
| 49 | 《浙江省建设投资集团股份有限公司私有云风险评估报告》 | 包含私有云的风险评估过程、内容和结果。 |
| 50 | 《私有云系统实施方案》 | 包含私有云实施建设的全部流程，以及合理建议。 |
| 51 | 《技术培训记录》 | 包含运行维护人员相关培训情况，包括培训内容、培训时间、参与人员等。 |
| 52 | 《私有云操作手册》 | 包含私有云系统日常运行维护以及详细操作指导。 |
| 53 | 《浙江省建设投资集团股份有限公司安全整改报告》 | 包含私有云系统针对风评的结果，进行安全整改的记录过程。 |
| 54 | 《华三交换机操作手册》 | 包含华三交换机详细的操作流程及命令更能等。 |
| 55 | 《深信服防火墙操作手册》 | 包含深信服防火墙详细的操作流程及功能配置。 |
| 56 | 《运维审批记录》 | 包含运维开通，运维工具，运维权限分配、审核等相关记录。 |
| 57 | 《漏洞修补记录表》 | 包含系统和设备漏洞修补的维护记录内容。 |
| 58 | 《技能考核记录》 | 包含对不同岗位的人员技能考核记录。 |

# 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

安全物理环境方面，在基础设施位置、物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应方面采用了严格的安全措施。在电磁防护方面采用了一定的安全措施。云计算服务器、存储设备及网络安全设备均部署于浙江省杭州市西湖区文三西路52号浙江建投大厦的物理机房内部，该云计算设施位于中国境内。机房建设位于杭州市西湖区文三西路52号浙江建投大厦15层，该建筑具备防震验收文档，具备良好的防震、防雨和防风的能力，机房内不存在雨水渗漏、墙体开裂等情况。机房建设在杭州市西湖区文三西路52号浙江建投大厦15楼，不处于楼顶和地下室，整体地板下方进行了防渗水、防潮措施，机房周围没有用水设备通过，精密空调底部水管采用防水层与防水棉，并设置有漏水检测措施。机房出入口已配备电子门禁系统，并配置电子门禁卡，能够控制、鉴别和记录进入的人员，记录保存时间长达6个月，且具备《机房出入登记表》，记录计入机房人员的姓名、进出时间、进出事由等相关信息。机房的主要部件均固定在机架当中，采用螺丝进行固定，且各设备上均粘贴有不易除去机打标签，标注为建投集团资产卡。机房采用桥架方式，将通信线缆铺设于机柜上方的走线架中。机房部署有7个海康威视的监控摄像头，覆盖整个机房视角，机房具有专人值守的视频监控区，海康威视的视频硬盘共8块，每块5个T的空间大小，能保存6个月以上的回放时间，且每个机柜门需要输入对应密码才能打开。机房当中所有机柜和设备均通过接地线接入静电地板底部的铜排，再连入整个大楼接地系统。浙江建投大厦设置又避雷针。配电柜和列头柜已配备部署有施耐德防雷开关和LKX雷科星防雷器进行保护，可防止感应雷。机房已部署七氟丙烷自动灭火系统，安装有烟感探头，当前系统运行方式为手动，系统运转正常。当前有4个气罐，气压在正常范围内。可实现自动检测火情、自动报警、自动灭火。机房大门采用防火门，工作室两面采用钢筋混凝土材质，另外两面采用DFB-08-C1.50防火玻璃，均为耐火等级材质。机房划分有核心区域、动力区域、运营商区域等，各区域之间采用DFB-08-C1.50防火玻璃进行隔离，具备隔离防火措施。机房无窗户存在，屋顶和墙壁等位置未出现过漏水、渗透和返潮现象，且通过防水涂层进行防水处理。机房使用Emerson艾默生精密空调进行温湿度调节防止水蒸气结露，精密空调下方的排水管采取密封防漏处理，且设置有排水管道防范地下积水。精密空调下方部署有水浸绳与动环系统相连，如果发生漏水等异常情况，能够进行告警并及时通知管理员。机房地面已采用防静电地板进行铺设，且各区域机柜、配电柜、设备等均进行了接地，并与整个大楼的接地系统相连。在机房出入口配置有静电消除器，可防止静电产生。机房使用3台Emerson艾默生精密空调进行温湿度控制，当前机房温度为23℃，湿度为45%，温湿度均在适宜可控范围内。机房配电柜的供电线路已配备施耐德稳压器和过压保护装置。采用蓝代斯克UPS电池组作为备用电力供应，在外部电路切断的情况下，UPS电池组能至少提供2个小时的电力供应。机房电力供应通过双路市电接到UPS再双路加入配电柜中，再双路连接机柜两个PDU，能再断电后1秒的时候进行切换。机房电源线采用下走线方式，通信线缆采用上走线方式部署再桥架当中。

### 主要安全问题汇总分析

安全物理环境存在的安全问题有：

**未采取措施对关键设备实施电磁屏蔽防护。**

可能导致非授权人员通过特殊设备接收电磁信号，并从中分析窃取重要系统数据，涉及测评对象：**物理机房。**

## 安全通信网络

### 已有安全控制措施汇总分析

安全通信网络方面，在网络架构、通信传输方面配置了严格的安全策略。当前系统为浙江省建设投资集团股份有限公司自建私有云，该云平台的网络安全保护等级为第三级（S3A3G3），其私有云上没有承载高于其安全保护等级的业务系统。不同云服务客户之间均采用独立的VPC网络进行组网，由CloudOS平台创建不同的NetWork网络，通过配置服务链对虚拟网络进行隔离，不能互访。私有云使用华三的云平台架构进行搭建，云平台部署有云安全组、边界防火墙并集成入侵防护和恶意代码防护功能以及威胁感知大数据平台等安全设备，可为云服务客户提供通信传输、边界防护、入侵防范等安全能力。云平台部署有CloudOS平台、SAN平台、CAS平台，支持云服务客户自主定义安全策略，并自主选择所需要的安全服务或组件。云平台开放第三方API接口，云服务客户可通过申请和工单的形式，在通过审批后可按照云服务客户的要求对接第三方安全服务或部署第三方安全产品。当前接入交换机CPU2%，内存使用44%；核心交换机CPU15%，内存45%，Spine交换机CPU5%，内存25%；Leaf交换机CPU10%，内存42%，且通过CAS平台、CloudOS平台可查看各核心主要网络设备资源均占用较低，可满足业务高峰期使用需求。外部线路采用两条电信两百兆带宽、一条联通一百兆专线，内部主干线路采用双线聚合互联，当前各主要线路带宽占用率低于30%，可满足业务高峰期使用需求。已根据实际安全需求，依据工作职能、重要性、程度等通过核心交换机、Spine交换机、Leaf交换机划分不同的VLAN，例如按照楼层，服务器，有线，会议等原则，并合理分配网络地址。网络拓扑图与实际运行环境一致，重要网段部署在网络边界内部区域，重要私有云服务器区域通过服务器防火墙，并配置访问控制策略进行逻辑隔离，网络出口边界采用飞塔防火墙进行逻辑隔离，可有效避免非授权访问。当前主干核心线路均采用双线聚合互联，关键核心交换、Spine交换机、Leaf交换机，关键出口安全设备，关键资源池服务器等均采用两台至多台进行热冗余部署，保证系统的高可用性。网络设备、服务器采用SSH的方式进行远程连接管理，安全设备、应用系统采用HTTPS的方式进行远程管理，可保证通信过程中数据的完整性。网络设备、服务器采用SSH的方式进行远程连接管理，安全设备、应用系统采用HTTPS的方式进行远程管理，可保证通信过程中数据的保密性。

### 主要安全问题汇总分析

安全通信网络存在的安全问题有：

**未基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。**

无可信链和可信验证，无法通过主动免疫可信验证技术提高系统自身安全防护能力，无法实现积极主动防御，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

安全区域边界方面，在入侵防范、安全审计、恶意代码和垃圾邮件防范方面配置了严格的安全策略。在访问控制、边界防护方面配置了一定的安全策略。在虚拟化网络边界部署有访问控制机制，在云计算平台和云服务客户业务系统间部署云安全组，云计算平台网络边界处部署服务器防火墙，不同云服务客户之间通过VPC组进行隔离，各设备均已配置并启用访问控制策略，且策略有效。云平台网络安全保护等级为第三级（S3A3G3），云服务客户不同的等级区域通过VPC组进行隔离，云平台不同等级的网络区域通过CloudOS平台创建服务链配置不同NetWork网络进行隔离。云平台部署有威胁感知大数据平台，云平台服务器边界服务器防火墙集成IPS功能，均已配置监控及报警策略，针对云服务客户发起的网络攻击行为进行记录，其设备规则库版本为20211110，均已升级至最新版本。云平台部署有威胁感知大数据平台，云平台服务器边界服务器防火墙集成IPS功能，已配置监控及报警策略，针对虚拟网络节点的攻击行为为进行记录，其设备规则库版本为20211110，均已升级至最新版本。通过CAS平台针对虚拟机与宿主机、虚拟机与虚拟机之间的端口流量进行监控，当流量超出阈值时，会在平台进行告警。云平台部署有威胁感知大数据平台，已配置相应安全策略，对网络攻击行为，异常流量情况进行检测，其设备规则库版本为20211110，均已升级至最新版本，并通过邮件方式告警。通过CloudOS平台记录云服务商和云租户的操作进行记录，内容包含登录日志、重启或删除虚拟机日志等。云服务商对云租户客户的操作日志会在CloudOS平台进行体现，云服务客户管理员可通过云平台查看系统和数据的审计记录，云服务商操作可备云服务客户审计。服务器边界部署服务器防火墙对进出网络的数据进行控制，数据在指定端口进行传输，通过访问控制策略对数据出入进行控制，仅允许指定端口跨越边界进行网络通信。部署有深信服上网行为管理，并配置权限策略拒绝采用远程软件远程服务器组，并配置上网认证，外联检查等功能，针对对非授权连接外部网络的行为进行检查或限制。通过服务器防火墙配置策略对跨越边界的网络数据进行控制，且已配置启用访问控制规则，对不符合策略的数据采取拒绝操作，且最后一条策略为双向拒绝所有。互联网边界飞塔防火墙当前无多余或无效的访问控制策略，不同的访问控制策略前后无包含关系，已使得访问控制列表最小化。服务器防火墙配置策略对数据包的源地址、目标地址、协议等内容进行检查，根据防火墙安全策略对数据进行放行或拒绝。例如仅允许源地址（总部员工有线10.\*.1.\*/24，机房运维10.\*.2.\*/24）访问目的地址（内部服务器10.\*.58.\*/24网段），协议（22、443、3389）等。通过飞塔防火墙对进出数据量提供明确的允许/拒绝访问的能力，可查询到详细的访问控制记录，并为进出数据流提供明确的允许或拒绝的能力，且策略有效。飞塔防火墙已集成IPS功能，边界飞塔防火墙已配置并开启入侵防护策略，策略范围覆盖所有IP网络节点，针对外部网络攻击行为进行检测和限制，当前IPS库版本为18.00039，更新时间为2021.11.15，规则库策略：每天自动进行更新，其规则库版本已至最新。网络边界服务器防火墙已集成IPS功能，且部署有威胁感知大数据平台，已配置对应入侵防护策略，策略范围覆盖所有IP网络节点，当前入侵防护规则库版本为2021.11.10，规则库策略：每天自动进行更新，其规则库已至最新版本可针对内部网络攻击行为进行检测和限制。部署有威胁感知大数据平台，已配置并开启相关安全策略，策略合理有效，能够针对网络攻击及新型网络攻击行为进行检测分析。通过边界服务器防火墙、威胁感知大数据平台对攻击行为进行分析和记录，记录内容包含攻击者IP、攻击类型、目标IP、攻击时间等内容，且发生严重入侵事件时将通过邮件的方式及时告警管理员。互联网部署有飞塔防火墙，已集成恶意代码防护功能，针对边界配置有恶意代码防护策略，当前恶意代码库版本为84.00787，杀毒引擎版本为6.00154，规则库更新时间：2021.11.15，规则库更新策略：每天自动进行更新，其恶意代码库已更新至最新版本，可对恶意代码进行检测和清除。互联网边界飞塔防火墙、深信服上网行为管理等设备均已启用审计功能，能够针对边界的访问流量，每个用户的访问行为以及重要安全事件等进行审计。审计记录包含具体时间、登录用户、登录名称、登录IP、操作内容，漏洞名称、目标IP、结果等内容。飞塔防火墙、深信服上网行为管理等设备审计记录已接入综合日志审计系统对审计记录进行保护，审计记录每季度进行备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达6个月。通过帕拉迪堡垒机针对远程访问的用户行为进行单独审计，通过深信服上网行为管理针对访问互联网的用户行为进行单独审计。

### 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）未采取措施对非授权设备私自连入内部网络的行为进行检查和限制。**

可能导致黑客通过技术手段接入内部网络，进而攻击应用系统，涉及测评对象：**互联网边界、服务器边界。**

**2）未采取措施针对网络访问的数据流量实现基于应用协议和应用内容的访问控制。**

增加了应用系统受到网络攻击的风险，涉及测评对象：**服务器边界、互联网边界。**

**3）未采取措施基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。**

无可信链和可信验证，无法通过主动免疫可信验证技术提高系统自身安全防护能力，无法实现积极主动防御，涉及测评对象：**互联网边界、服务器边界。**

## 安全计算环境

### 网络设备

#### 已有安全控制措施汇总分析

安全计算环境网络设备方面，在数据完整性和保密性、剩余信息保护、安全审计、数据保密性方面配置了严格的安全策略。在身份鉴别、访问控制、入侵防范、镜像和快照保护、数据备份恢复、数据完整性方面配置了一定的安全策略。通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。登录设备需要使用用户名加口令进行身份鉴别，身份标识唯一，当前口令长度8位以上，口令组成包含特殊字符，大小写字母和数字，已开启口令复杂度策略Password-control enable，要求口令长度至少8位，口令组成必须包含大小写字母、数字和特殊字符，每半年进行一次口令更换。已开启登录失败处理功能，password-control login-attempt 5 exceed lock-time 10，口令尝试次数：5次，措施：锁定账户10分钟；登录连接超时自动退出时间为：idle-timeout＝5分钟。Leaf交换机通过SSH的方式对设备进行远程管理，在通信过程采用SSL协议传输数据，用户口令信息加密传输，防止鉴别信息在网络传输过程中呗窃听。当前使用admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员等账户进行登录，不存在匿名账户，并为其分配相关权限。未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。当前使用admin、she\*\*\*、an\*\*\*、xi\*\*\*等账户，分别管理员、审计管理员、安全管理员security-admin、系统管理员network-operator等角色权限，各账户仅分配所需的最小权限，实现管理用户的权限分离。由管理员依据具体业务划分情况对账户进行具体权限划分，未发现越权访问情况。当前设备访问控制粒度达到主体为用户级，客体为命令级。核心交换机已开启info-center与logfile功能，可对每个用户的重要用户行为和重要事件进行记录。审计记录包含具体时间、用户、OID、端口、MAC、IP地址、具体消息等内容。核心交换机的审计记录已通过SYSLOG发送至综合日志审计系统当中进行保护，审计记录每季度备份至本地，管理员无法对审计记录进行删除、修改或覆盖，审计记录保存时间长达6个月。由底层软件对审计进程进行保护，非授权用户无法中断审计。底层OS及必要服务由设备厂商出厂前配置完成，用户无需登录底层操作系统并验证组件，系统遵循最小化安全原则，仅安装自身所需要的组件和程序。当前设备不存在默认共享，已关闭不必要的端口，仅开启业务所需端口。通过配置策略限制仅允许总部员工有线、机房运维、网络监控平台等网段可远程登录管理。建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。核心交换机主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的保密性。Leaf交换机主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的保密性。当前交换机使用两台设备采用IRF堆叠技术进行热冗余部署，保证系统高可用性。

#### 主要安全问题汇总分析

安全计算环境网络设备存在的安全问题有：

**1）未在远程管理云平台中设备时，在管理终端和云平台间建立双向身份验证机制。**

可能导致攻击者不可信管理终端接入，或者攻击者通过钓鱼或伪造云计算平台服务界面的形式诱骗管理员提供敏感数据，导致管理终端和云计算平台间通信被劫持或伪造，涉及测评对象：**核心交换机A、核心交换机B、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B。**

**2）云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。**

恶意用户可能通过获取虚拟机管理器权限或修改虚拟机管理权限等方式，非授权新建或重启虚拟机，存在潜在的安全隐患，涉及测评对象：**核心交换机A、核心交换机B、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B。**

**3）未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。**

可能导致虚拟机镜像、快照中可能存在的敏感资源被攻击者非法访问，使敏感信息遭遇泄漏，涉及测评对象：**核心交换机A、核心交换机B、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B。**

**4）未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。**

用户名和口令安全强度有限，如果未采用双因素认证，一旦用户名和口令被嗅探和泄露，将再没有其它技术进行身份鉴别，存在非授权访问的风险，涉及测评对象：**核心交换机B、核心交换机A、Spine交换机B、Spine交换机A、Leaf交换机B、Leaf交换机A。**

**5）未重命名或删除默认账户。**

恶意人员可能利用默认账户对系统进行试探攻击，存在潜在的安全隐患，涉及测评对象：**核心交换机B、核心交换机A、Spine交换机B、Spine交换机A、Leaf交换机B、Leaf交换机A。**

**6）未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。**

恶意用户可能通过修改用户权限等方法，非授权访问重要信息资源，存在潜在的安全隐患，涉及测评对象：**Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B。**

**7）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。**

无可信链和可信验证，不能通过主动免疫可信验证技术提高系统自身安全防护能力，不能实现积极主动防御，涉及测评对象：**Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B。**

**8）未采用校验技术或密码技术保证重要审计数据在传输过程中的完整性。**

可能导致重要数据在传输过程中被攻击者劫持、篡改，使重要数据的完整性遭到破坏，涉及测评对象：**核心交换机B、核心交换机A、Spine交换机B、Spine交换机A、Leaf交换机B、Leaf交换机A。**

**9）未采用校验技术或密码技术保证重要审计数据和重要配置数据在存储过程中的完整性。**

可能导致重要数据在存储过程中被恶意篡改，影响信息系统的正常运行，涉及测评对象：**Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B。**

**10）未使用备份文件进行过备份恢复测试。**

一旦出现故障，可能由于各种原因无法利用备份数据进行恢复，造成重要数据丢失，涉及测评对象：**核心交换机B、核心交换机A、Spine交换机B、Spine交换机A、Leaf交换机B、Leaf交换机A。**

### 安全设备

#### 已有安全控制措施汇总分析

安全计算环境安全设备方面，在数据完整性和保密性、剩余信息保护、安全审计、数据保密性方面配置了严格的安全策略。在身份鉴别、访问控制、入侵防范、镜像和快照保护、数据备份恢复、数据完整性方面配置了一定的安全策略。通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。登录设备需要使用用户名加口令进行身份鉴别，身份标识唯一，口令长度8位以上，口令组成包含特殊字符，大小写字母和数字，已开启口令复杂度策略，口令长度最小8位，口令组成不允许包含用户名或颠倒用户名，不允许包含连续三个或以上的相同字符，必须包含大小写字母、数字和特殊字符，每半年进行一次口令更换。已开启登录失败处理功能，登录失败次数：5次，登录失败措施：锁定账户1800秒；网络登录连接空闲超时自动退出时间：30分钟。H3C防火墙采用HTTPS进行远程管理，用户口令信息加密传输，防止鉴别信息被窃取。当前使用admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员等账户进行登录，不存在匿名账户，并为其分配相关权限。未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。当前使用admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员等角色权限，各账户仅分配所需的最小权限，不同账户具备不同的访问权限，实现管理用户权限分离。依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。当前设备访问控制粒度达到主体为用户级，客体为界面级。设备已开启审计功能，可对重要的用户行为和重要安全事件进行审计。审计记录包含具体时间、IP地址、操作内容、端口状态，是否成功等信息。飞塔防火墙已配置SYSLOG日志上传至综合日志审计系统进行收集和保护，审计记录每季度备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达6个月。由系统底层和综合日志审计系统对审计进程进行保护，非授权用户无法中断审计。底层OS及必要服务由设备厂商出厂前配置完成，用户无需登录底层操作系统并验证组件，系统遵循最小化安全原则，仅安装自身所需要的组件和程序。当前设备不存在默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的系统服务。通过边界配置ACL3001，仅允许10.\*.1.\*，192.\*.9.\*远程管理设备。建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。威胁感知大数据平台可对重要节点入侵行为进行检查，已配置并开启对应安全策略，策略范围覆盖系统内部所有网络地址，在发生严重入侵事件时，将通过邮件方式进行告警。综合日志审计系统主要涉及鉴别数据、重要审计数据和重要配置数据，其中重要审计数据和重要配置数据不进行传输，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的完整性。飞塔防火墙主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的保密性。H3C防火墙主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的保密性。当前设备采用两台设备虚拟化热冗余部署，并已配置主备模式，保证系统稳定运行。

#### 主要安全问题汇总分析

安全计算环境安全设备存在的安全问题有：

**1）未在远程管理云平台中设备时，在管理终端和云平台间建立双向身份验证机制。**

可能导致攻击者不可信管理终端接入，或者攻击者通过钓鱼或伪造云计算平台服务界面的形式诱骗管理员提供敏感数据，导致管理终端和云计算平台间通信被劫持或伪造，涉及测评对象：**H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B。**

**2）云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。**

恶意用户可能通过获取虚拟机管理器权限或修改虚拟机管理权限等方式，非授权新建或重启虚拟机，存在潜在的安全隐患，涉及测评对象：**H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B。**

**3）未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。**

可能导致虚拟机镜像、快照中可能存在的敏感资源被攻击者非法访问，使敏感信息遭遇泄漏，涉及测评对象：**H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B。**

**4）未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。**

用户名和口令安全强度有限，如果未采用双因素认证，一旦用户名和口令被嗅探和泄露，将再没有其它技术进行身份鉴别，存在非授权访问的风险，涉及测评对象：**飞塔防火墙B、飞塔防火墙A、综合日志审计系统、深信服上网行为管理B、深信服上网行为管理A、服务器防火墙、帕拉迪堡垒机B、帕拉迪堡垒机A、威胁感知大数据平台、H3C防火墙B、H3C防火墙A。**

**5）未重命名或删除默认账户。**

恶意人员可能利用默认账户对系统进行试探攻击，存在潜在的安全隐患，涉及测评对象：**飞塔防火墙B、飞塔防火墙A、综合日志审计系统、深信服上网行为管理B、深信服上网行为管理A、服务器防火墙、帕拉迪堡垒机B、帕拉迪堡垒机A、威胁感知大数据平台、H3C防火墙B、H3C防火墙A。**

**6）未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。**

恶意用户可能通过修改用户权限等方法，非授权访问重要信息资源，存在潜在的安全隐患，涉及测评对象：**H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B。**

**7）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。**

无可信链和可信验证，不能通过主动免疫可信验证技术提高系统自身安全防护能力，不能实现积极主动防御，涉及测评对象：**H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B。**

**8）未采用校验技术或密码技术保证重要审计数据在传输过程中的完整性。**

可能导致重要数据在传输过程中被攻击者劫持、篡改，使重要数据的完整性遭到破坏，涉及测评对象：**飞塔防火墙B、飞塔防火墙A、深信服上网行为管理B、深信服上网行为管理A、服务器防火墙、帕拉迪堡垒机B、帕拉迪堡垒机A、威胁感知大数据平台、H3C防火墙B、H3C防火墙A。**

**9）未采用校验技术或密码技术保证重要审计数据和重要配置数据在存储过程中的完整性。**

可能导致重要数据在存储过程中被恶意篡改，影响信息系统的正常运行，涉及测评对象：**H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B。**

**10）未使用备份文件进行过备份恢复测试。**

一旦出现故障，可能由于各种原因无法利用备份数据进行恢复，造成重要数据丢失，涉及测评对象：**飞塔防火墙B、飞塔防火墙A、综合日志审计系统、深信服上网行为管理B、深信服上网行为管理A、服务器防火墙、帕拉迪堡垒机B、帕拉迪堡垒机A、威胁感知大数据平台、H3C防火墙B、H3C防火墙A。**

### 服务器和终端

#### 已有安全控制措施汇总分析

安全计算环境服务器和终端方面，在数据完整性和保密性、剩余信息保护、安全审计、数据保密性方面配置了严格的安全策略。在身份鉴别、访问控制、入侵防范、镜像和快照保护、数据备份恢复、恶意代码防范、数据完整性方面配置了一定的安全策略。通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。使用用户名加口令身份验证方式对用户进行鉴别； 用户名作为用户唯一身份标识； 无空口令账户； 口令复杂度包含数字、大小写、特殊字符； 口令长度8位以上； 定期更换口令时间为90； 已配置口令复杂度策略： lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1； 口令策略： PASS\_MAX\_DAYS 90 PASS\_MIN\_DAYS 0 PASS\_MIN\_LEN 8 PASS\_WARN\_AGE 7 已配置口令复杂度策略及口令有限期策略。在本地安全策略中已配置账户锁定时间:30分钟； 账户锁定阀值:5次无效登录； 复位账户锁定计数器:30分钟之后。服务器采用SSH方式进行远程管理，通信过程中基于SSL协议传输数据，用户口令信息加密传输，可防止鉴别信息在网络传输过程中被窃听。当前使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等账户，不存在匿名账户，并为其分配了相关权限。未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。服务器使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等角色权限，各账户仅分配所需的最小权限，实现管理用户权限分离。依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。已配置访问控制功能，主体为用户级，客体为文件级。已在组策略中开启审计功能，可对所有重要的用户行为和重要安全事件进行审计，审计范围覆盖系统内所有用户。审计记录包括事件的日期（年月日等），时间、类型、成功与否、事件内容、IP地址等。能够查看到半年的日志，且管理员会定期对日志进行备份至移动硬盘，能够有效避免受到未预期的删除、修改或覆盖等。通过综合日志审计系统对审计记录进行保护对审计进程进行保护，非授权用户无法中断审计。运维终端已遵循最小化安装原则，仅安装必要的组件和程序。服务器未开启非必要的端口，不存在默认共享和高危端口的使用。通过服务器防火墙配置策略仅允许地址范围总部有线网段，机房运维网段可进行远程管理。建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。运维终端已安装了360杀毒软件，当前软件版本为12.0.0.2131，恶意代码库版本为2021-11-17，当前规则库已更新至最新，规则库更新频率：每天自动进行更新。服务器主要涉及鉴别数据，鉴别数据采用SSH的方式，能够保证鉴别数据在传输过程中的保密性。服务器主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的保密性。通过数腾软件对重要服务器数据每天进行增量备份，然后通过软件介质实时同步，将重要数据备份至宁波建投子公司。服务器采用多设备热备方式部署，可实现热冗余，保证系统高可用性。linux系统退出时自动对鉴别信息所在的存储空间进行完全的清除。HISTSIZE=1000，history无法查询上次登录的命令，可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。

#### 主要安全问题汇总分析

安全计算环境服务器和终端存在的安全问题有：

**1）未在远程管理云平台中设备时，在管理终端和云平台间建立双向身份验证机制。**

可能导致攻击者不可信管理终端接入，或者攻击者通过钓鱼或伪造云计算平台服务界面的形式诱骗管理员提供敏感数据，导致管理终端和云计算平台间通信被劫持或伪造，涉及测评对象：**CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2。**

**2）云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。**

恶意用户可能通过获取虚拟机管理器权限或修改虚拟机管理权限等方式，非授权新建或重启虚拟机，存在潜在的安全隐患，涉及测评对象：**CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2。**

**3）未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。**

可能导致虚拟机镜像、快照中可能存在的敏感资源被攻击者非法访问，使敏感信息遭遇泄漏，涉及测评对象：**CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2。**

**4）未配置口令有效期策略。**

账户口令可能被长时间使用，恶意人员可通过猜解或暴力破解的方式获取账户口令，存在非授权访问的风险，涉及测评对象：**CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02。**

**5）未配置登录连接超时策略。**

设备易被非授权人员恶意操作，存在非授权访问的风险，涉及测评对象：**CloudOS3、CloudOS2、CloudOS1。**

**6）未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。**

用户名和口令安全强度有限，如果未采用双因素认证，一旦用户名和口令被嗅探和泄露，将再没有其它技术进行身份鉴别，存在非授权访问的风险，涉及测评对象：**SDN03、SDN02、SDN01、CVM02、CVM01、CVK05、CVK04、CVK03、CVK02、CVK01、CloudOS3、CloudOS2、CloudOS1。**

**7）未重命名或删除默认账户。**

恶意人员可能利用默认账户对系统进行试探攻击，存在潜在的安全隐患，涉及测评对象：**运维终端2、运维终端1、SDN03、SDN02、SDN01、CVM02、CVM01、CVK05、CVK04、CVK03、CVK02、CVK01、CloudOS3、CloudOS2、CloudOS1。**

**8）未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。**

恶意用户可能通过修改用户权限等方法，非授权访问重要信息资源，存在潜在的安全隐患，涉及测评对象：**CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03。**

**9）未部署主机入侵防护软件，无法对主机重要节点进行入侵行为进行检查、限制并报警。**

无法及时发现入侵行为，不便于对入侵行为进行分析并迅速响应，涉及测评对象：**CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2。**

**10）未安装防恶意代码软件，无法识别入侵和病毒行为，并将其有效阻断。**

可能导致木马、病毒等恶意代码程序通过网络、存储介质对生产操作系统进行传染和破坏，对系统稳定和数据安全造成影响，涉及测评对象：**SDN03、SDN02、SDN01、CVM02、CVM01、CVK05、CVK04、CVK03、CVK02、CVK01、CloudOS3、CloudOS2、CloudOS1。**

### 系统管理软件/平台

#### 已有安全控制措施汇总分析

安全计算环境系统管理软件平台方面，在数据完整性和保密性、剩余信息保护、安全审计、数据保密性方面配置了严格的安全策略。在身份鉴别、访问控制、入侵防范、镜像和快照保护、数据备份恢复、数据完整性方面配置了一定的安全策略。通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。登录设备需要使用用户名加口令进行身份鉴别，身份标识唯一，口令长度8位以上，口令组成包含特殊字符，大小写字母和数字，已开启密码复杂度校验功能，口令长度至少8位，口令组成必须包含大小写字母、数字和特殊字符，每半年进行一次口令更换。已开启登录失败处理功能，登录失败次数：5次，措施：永久锁定账户，网络登录连接空闲超时自动退出时间：30分钟。当前设备远程管理采用HTTPS，用户口令信息加密传输，防止鉴别信息在网络传输中被窃听。当前使用MasterAdmin管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等账户，不存在匿名账户，并为其分配了相关权限。已重命名默认账户为MasterAdmin，已修改默认口令为复杂口令。未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。当前使用MasterAdmin管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员，各账户仅分配所需的最小权限，实现管理用户权限分离。依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。当前设备访问控制粒度达到主体为用户级，客体为界面级。设备已开启审计功能，可对重要的用户行为和重要安全事件进行审计。审计记录包含具体时间、计算机、原因、操作、排序、方向、接口、源目IP、源目MAC等重要信息。审计记录已通过SYSLOG的方式上传至综合日志审计系统当中进行保护，审计每季度备份至本地，审计记录无法受到非预期的删除、修改或覆盖，审计记录保存时间长达6个月。由系统底层对审计进程进行保护，非授权用户无法中断审计。底层OS及必要服务由设备厂商出厂前配置完成，用户无需登录底层操作系统并验证组件，系统遵循最小化安全原则，仅安装自身所需要的组件和程序。当前设备不存在默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的系统服务。通过配置策略限制仅允许总部员工有线、机房运维、网络监控平台等网段可远程登录管理。建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。亚信安全服务器深度安全防护系统主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的保密性。亚信安全服务器深度安全防护系统主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的保密性。系统登录时不自动保存和显示历史账号和口令，在用户退出后及时清空cookie和会话session，无法通过回退操作访问退出前界面，用户的鉴别信息所在的存储空间被释放或重新分配前能够得到完全清除。

#### 主要安全问题汇总分析

安全计算环境系统管理软件平台存在的安全问题有：

**1）未在远程管理云平台中设备时，在管理终端和云平台间建立双向身份验证机制。**

可能导致攻击者不可信管理终端接入，或者攻击者通过钓鱼或伪造云计算平台服务界面的形式诱骗管理员提供敏感数据，导致管理终端和云计算平台间通信被劫持或伪造，涉及测评对象：**亚信安全服务器深度安全防护系统。**

**2）云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。**

恶意用户可能通过获取虚拟机管理器权限或修改虚拟机管理权限等方式，非授权新建或重启虚拟机，存在潜在的安全隐患，涉及测评对象：**亚信安全服务器深度安全防护系统。**

**3）未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。**

可能导致虚拟机镜像、快照中可能存在的敏感资源被攻击者非法访问，使敏感信息遭遇泄漏，涉及测评对象：**亚信安全服务器深度安全防护系统。**

**4）未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。**

用户名和口令安全强度有限，如果未采用双因素认证，一旦用户名和口令被嗅探和泄露，将再没有其它技术进行身份鉴别，存在非授权访问的风险，涉及测评对象：**亚信安全服务器深度安全防护系统。**

**5）未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。**

恶意用户可能通过修改用户权限等方法，非授权访问重要信息资源，存在潜在的安全隐患，涉及测评对象：**亚信安全服务器深度安全防护系统。**

**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。**

无可信链和可信验证，不能通过主动免疫可信验证技术提高系统自身安全防护能力，不能实现积极主动防御，涉及测评对象：**亚信安全服务器深度安全防护系统。**

**7）未采用校验技术或密码技术保证重要审计数据在传输过程中的完整性。**

可能导致重要数据在传输过程中被攻击者劫持、篡改，使重要数据的完整性遭到破坏，涉及测评对象：**亚信安全服务器深度安全防护系统。**

**8）未采用校验技术或密码技术保证重要审计数据和重要配置数据在存储过程中的完整性。**

可能导致重要数据在存储过程中被恶意篡改，影响信息系统的正常运行，涉及测评对象：**亚信安全服务器深度安全防护系统。**

**9）未使用备份文件进行过备份恢复测试。**

一旦出现故障，可能由于各种原因无法利用备份数据进行恢复，造成重要数据丢失，涉及测评对象：**亚信安全服务器深度安全防护系统。**

**10）系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。**

如机房遭受严重破坏，可能导致部分数据丢失，涉及测评对象：**亚信安全服务器深度安全防护系统。**

### 业务应用系统/平台

#### 已有安全控制措施汇总分析

安全计算环境业务应用系统平台方面，在数据完整性和保密性、剩余信息保护、安全审计、数据保密性方面配置了严格的安全策略。在身份鉴别、访问控制、入侵防范、镜像和快照保护、数据备份恢复、数据完整性方面配置了一定的安全策略。通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。登录系统采用用户名和口令的方式进行身份鉴别，身份标识具有唯一性，当前口令8位以上，采用大小写字符、数字和特殊字符组成，已开启口令复杂度策略，要求口令最小长度8位，口令组成必须包含字母、数字和特殊字符，每半年人为进行一次口令更换。已开启登录失败处理功能，登录失败次数：5次，措施：锁定账户30分钟；登录连接超时自动退出时间为：30分钟。CAS平台采用HTTPS的方式进行远程管理，用户鉴别信息加密传输，防止鉴别信息在网络传输过程中被窃取。当前使用admin管理员、xitong系统管理员、anquan安全管理员、shenji审计管理员等账户，不存在匿名账户，并为其分配了不同权限。CAS平台未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。SNA平台创建xitong系统管理员、anquan安全管理员、shenji审计管理员等账户角色权限，各账户仅分配所需的最小权限，不同账户具备不同的访问权限，实现管理用户权限分离。已由授权主体配置访问控制策略，管理员具有概览、一键、云资源、主机池管理、集群管理、主机管理、虚拟机管理、云业务管理、云安全、系统管理、虚拟化、拓扑、自定义菜单、监控管理、告警管理等权限，普通用户仅有部分权限，审计管理员仅有日志查看权限。当前设备访问控制粒度达到主体为用户级，客体为界面级。SNA平台已启用安全审计功能，审计包括操作日志、系统日志、诊断日志，审计内容覆盖到每个用户、对重要用户的行为和重要安全事件进行审计。操作日志审计记录包括登录名、操作员姓名、完成时间、登录地址、操作分类、操作对象、操作描述、执行结果、失败原因等内容。SNA平台审计记录保存在本地，操作日志、系统日志最早可查看到2020/09/03，审计记录每季度进行备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达6个月。系统底层已对审计进程进行保护，非授权用户不可被中断。通过配置策略限制仅允许总部员工有线、机房运维、网络监控平台等网段可远程登录管理SNA平台。应用系统已对数据有效性进行校验，针对改动的数据格式，配置等要求进行校验，不满足要求无法生效，对于不符合的相关链接内容会弹出403的错误界面。建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。SNA平台主要涉及鉴别数据、重要审计数据和重要配置数据，其中重要审计数据和重要配置数据不进行传输，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的完整性。SNA平台主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的保密性。CAS平台主要涉及鉴别数据，鉴别数据采用SHA256+8位salt的方式进行保存，能够保证鉴别数据在存储过程中的保密性。系统登录时不自动保存和显示历史账号和口令，在用户退出后及时清空cookie和会话session，无法通过回退操作访问退出前界面，用户的鉴别信息所在的存储空间被释放或重新分配前能够得到完全清除。

#### 主要安全问题汇总分析

安全计算环境业务应用系统平台存在的安全问题有：

**1）未在远程管理云平台中设备时，在管理终端和云平台间建立双向身份验证机制。**

可能导致攻击者不可信管理终端接入，或者攻击者通过钓鱼或伪造云计算平台服务界面的形式诱骗管理员提供敏感数据，导致管理终端和云计算平台间通信被劫持或伪造，涉及测评对象：**CAS平台、CloudOS平台、SNA平台。**

**2）云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。**

恶意用户可能通过获取虚拟机管理器权限或修改虚拟机管理权限等方式，非授权新建或重启虚拟机，存在潜在的安全隐患，涉及测评对象：**CAS平台、CloudOS平台、SNA平台。**

**3）未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。**

可能导致虚拟机镜像、快照中可能存在的敏感资源被攻击者非法访问，使敏感信息遭遇泄漏，涉及测评对象：**CAS平台、CloudOS平台、SNA平台。**

**4）未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。**

用户名和口令安全强度有限，如果未采用双因素认证，一旦用户名和口令被嗅探和泄露，将再没有其它技术进行身份鉴别，存在非授权访问的风险，涉及测评对象：**SNA平台、CloudOS平台、CAS平台。**

**5）未重命名或删除默认账户。**

恶意人员可能利用默认账户对系统进行试探攻击，存在潜在的安全隐患，涉及测评对象：**SNA平台、CloudOS平台、CAS平台。**

**6）未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。**

恶意用户可能通过修改用户权限等方法，非授权访问重要信息资源，存在潜在的安全隐患，涉及测评对象：**CAS平台、CloudOS平台、SNA平台。**

**7）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。**

无可信链和可信验证，不能通过主动免疫可信验证技术提高系统自身安全防护能力，不能实现积极主动防御，涉及测评对象：**CAS平台、CloudOS平台、SNA平台。**

**8）未采用校验技术或密码技术保证重要审计数据和重要配置数据在存储过程中的完整性。**

可能导致重要数据在存储过程中被恶意篡改，影响信息系统的正常运行，涉及测评对象：**CAS平台、CloudOS平台、SNA平台。**

**9）未使用备份文件进行过备份恢复测试。**

一旦出现故障，可能由于各种原因无法利用备份数据进行恢复，造成重要数据丢失，涉及测评对象：**SNA平台、CloudOS平台、CAS平台。**

**10）系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。**

如机房遭受严重破坏，可能导致部分数据丢失，涉及测评对象：**CAS平台、CloudOS平台、SNA平台。**

### 数据资源

#### 已有安全控制措施汇总分析

安全计算环境数据资源方面，在访问控制、数据完整性和保密性、剩余信息保护方面配置了严格的安全策略。在入侵防范、镜像和快照保护、数据备份恢复、数据完整性、数据保密性方面配置了一定的安全策略。通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。CloudOS平台、CAS平台、SNA平台主要涉及重要业务数据，重要业务数据采用HTTPS的方式，能够保证重要业务数据在传输过程中的完整性。CloudOS平台、CAS平台、SNA平台主要涉及重要业务数据，重要业务数据采用HTTPS的方式，能够保证中亚业务数据在传输过程中的保密性。CloudOS平台、CAS平台、SNA平台均采用的多台服务器高可用集群方式进行部署，可保证系统的高可用性。CloudOS平台、CAS平台、SNA平台系统登录时不自动保存和显示历史账号和口令，在用户退出后及时清空cookie和会话session，无法通过回退操作访问退出前界面，用户的鉴别信息所在的存储空间被释放或重新分配前能够得到完全清除。

#### 主要安全问题汇总分析

安全计算环境数据资源存在的安全问题有：

**1）未在远程管理云平台中设备时，在管理终端和云平台间建立双向身份验证机制。**

可能导致攻击者不可信管理终端接入，或者攻击者通过钓鱼或伪造云计算平台服务界面的形式诱骗管理员提供敏感数据，导致管理终端和云计算平台间通信被劫持或伪造，涉及测评对象：**业务数据。**

**2）云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。**

恶意用户可能通过获取虚拟机管理器权限或修改虚拟机管理权限等方式，非授权新建或重启虚拟机，存在潜在的安全隐患，涉及测评对象：**业务数据。**

**3）未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。**

可能导致虚拟机镜像、快照中可能存在的敏感资源被攻击者非法访问，使敏感信息遭遇泄漏，涉及测评对象：**业务数据。**

**4）未采用校验技术或密码技术保证重要业务数据在存储过程中的完整性。**

可能导致重要数据在存储过程中被恶意篡改，影响信息系统的正常运行，涉及测评对象：**业务数据。**

**5）未采用密码技术保证重要业务数据在存储过程中的保密性。**

可能导致重要数据在存储过程中被攻击者直接盗用，使私密信息遭遇泄漏，涉及测评对象：**业务数据。**

**6）未使用备份文件进行过备份恢复测试。**

一旦出现故障，可能由于各种原因无法利用备份数据进行恢复，造成重要数据丢失，涉及测评对象：**业务数据。**

**7）系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。**

如机房遭受严重破坏，可能导致部分数据丢失，涉及测评对象：**业务数据。**

### 其他系统或设备

#### 已有安全控制措施汇总分析

本次测评不包含安全计算环境其他系统和设备的检测内容。

#### 主要安全问题汇总分析

本次测评不包含安全计算环境其他系统和设备的检测内容。未发现安全计算环境其他系统和设备中的安全问题。

## 安全管理中心

### 已有安全控制措施汇总分析

安全管理中心方面，在审计管理方面配置了严格的安全策略。在集中管控、系统管理、安全管理方面配置了一定的安全策略。云平台通过CAS平台、SNA平台和CloudOS平台对物理资源和虚拟资源按照管理员策略意愿做统一管理调度与分配。平台本身物理流量和租户的业务流量分离，云计算平台的管理流量通过各管理平台进行管控和监测，云租户的流量通过安装CasTools，并通过CAS平台进行管控。云服务商和云服务客户的审计记录通过综合日志审计平台和控制台进行收集，并创建不同的管理账户，各管理账户仅能查看自建所拥有的设备相关权限。云服务商和云租户客户可通过账户划分，对各虚拟网络设备、虚拟机、虚拟安全设备等进行自主控制管理。所有测评对象已进行三权分立，仅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。部署有综合日志审计系统，通过用户名加口令的方式对审计管理员进行身份鉴别，并在所有设备上均单独创建有审计管理员账户she\*\*\*，对这些操作进行审计。部署有综合日志审计系统，仅通过审计管理员对审计记录进行分析，并根据分析结果进行处理。所有测评对象已进行三权分立，仅通过安全管理员对系统中的安全策略进行配置。网络中已划分出单独的安全管理区用于部署安全设备及安全组件，网络安全设备及安全组件均部署在该区域。网络中的安全设备和安全组件均采用HTTPS的方式进行远程管理。通过CAS平台、CloudOS平台对云平台各服务器运行状况，网络设备、网络链路等进行集中监控，并可依据其工作状态及设定阈值实时报警。部署有综合日志审计系统对各个设备的日志进行统一收集管理，且各个设备均已开启安全审计功能，审计记录保存时间长达6个月。当前部署有威胁感知大数据平台，能够对网络当中各类安全事件进行识别、分析，监测范围覆盖系统网络所有关键路径，在发生重要安全事件时通过邮件的方式告警管理员。

### 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）未限制网络设备、安全设备、服务器等仅通过堡垒机进行运维管理，并对系统管理员的操作进行审计。**

无法对安全事件进行追溯，同时无法及时了解设备实际运行状况以及存在的安全隐患，涉及测评对象：**安全管理中心。**

**2）未限制网络设备、安全设备、服务器等仅通过堡垒机进行运维管理，并对安全管理员的操作进行审计。**

无法对安全事件进行追溯，同时无法及时了解设备实际运行状况以及存在的安全隐患，涉及测评对象：**安全管理中心。**

**3）未采取措施对安全策略、恶意代码、补丁升级等进行统一集中管理。**

无法对保护对象进行统一监视和控制，当安全事件发生时无法及时对威胁源进行阻断和干预，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

安全管理制度方面，在安全策略、管理制度、制定和发布方面制定了一系列的安全管理制度。《ZJJT-XX-01-2020信息安全策略》对安全工作的总体方针和安全策略做了相关说明，对机构安全工作的总体目标、范围、原则和安全框架等进行了阐明，包括组织机构及岗位职责，人员安全管理、环境和资产安全管理、系统安全建设管理 系统安全运行管理、事件处置和应急响应等。已制定《ZJJT-XX-02-2020网络与信息安全管理制度》、《ZJJT-XX-05-2020机房管理制度 》、《ZJJT-XX-06-2020信息资产管理制度》、《ZJJT-XX-07-2020信息设备运维管理制度》、《ZJJT-XX-08-2020信息系统巡检管理制度》、《ZJJT-XX-09-2020信息网络管理制度》、《ZJJT-XX-14-2020业务应用系统软件安全管理制度》、《ZJJT-XX-18-2020信息系统管理授权审批管理制度》、《ZJJY-XX-19-2020系统安全管理制度》、《ZJJY-XX-24-2020信息系统数据质量管理制度》等制度，相关制度中包含服务运维、系统运维、系统数据安全等管理内容。已制定《ZJJT-XX-17-2020信息安全机构管理制度》、《ZJJT-XX-03-2020计算机病毒防治管理制度》、《ZJJT-XX-04-2020数据备份与恢复管理制度》、《ZJJT-XX-08-2020信息系统巡检管理制度》、《ZJJT-XX-11-2020外部人员访问控制管理制度》、《ZJJT-XX-16-2020信息系统安全补丁管理制度》等制度，相关制度中包含对系统维护、系统配置、用户操作等访问的规定。已制定《ZJJT-XX-02-2020网络与信息安全管理制度》、《ZJJT-XX-05-2020机房管理制度 》、《ZJJT-XX-06-2020信息资产管理制度》、《ZJJT-XX-07-2020信息设备运维管理制度》、《ZJJT-XX-08-2020信息系统巡检管理制度》、《ZJJT-XX-09-2020信息网络管理制度》、《ZJJT-XX-14-2020业务应用系统软件安全管理制度》、《ZJJT-XX-18-2020信息系统管理授权审批管理制度》、《ZJJY-XX-19-2020系统安全管理制度》、《ZJJY-XX-24-2020信息系统数据质量管理制度》、《ZJJT-XX-17-2020信息安全机构管理制度》、《ZJJT-XX-03-2020计算机病毒防治管理制度》、《ZJJT-XX-04-2020数据备份与恢复管理制度》、《ZJJT-XX-08-2020信息系统巡检管理制度》、《ZJJT-XX-11-2020外部人员访问控制管理制度》、《ZJJT-XX-16-2020信息系统安全补丁管理制度》等制度，并留存相关记录表单，形成全面的安全管理制度体系。指定科技信息科负责安全管理制度的制定。浙江省建设投资集团股份有限公司的安全管理制度通过红头文件的形式进行发布，其管理制度文件通过内部办公OA系统进行正式发布，且进行了版本控制。

### 主要安全问题汇总分析

安全管理制度存在的安全问题有：

**未定期对安全管理制度进行论证、审定以及修订。**

可能导致安全管理体系与现实情况不符，导致管理文档无法落地，涉及测评对象：**制度或记录类文档。**

## 安全管理机构

### 已有安全控制措施汇总分析

安全管理机构方面，在岗位设置、人员配备、授权和审批、沟通和合作、审核和检查方面制定了一系列的安全管理制度。《ZJJT-XX-01-2020信息安全策略》中已明确成立网络安全工作领导小组，并通过红头文件发布有《关于成立信息安全管理工作领导小组的通知》，明确了人员构成情况和相关职责。设立网络安全管理工作的职能部门科技信息部，设立安全主管岗位，《ZJJT-XX-17-2020信息安全机构管理制度》说明部门职责及各个工作岗位的职责。浙江省建设投资集团股份有限公司已对安全管理岗位进行划分，在《ZJJT-XX-17-2020信息安全机构管理制度》中明确设立了系统管理员、安全审计员、安全管理员、网络管理员、应用管理员等岗位，并明确各个工作岗位的职责。当前配备有系统管理员3名，审计管理员2名、安全管理员2名，网络管理员1名、机房管理员1名、应用管理员1名，其中李明明兼任系统管理员和审计管理员，关俭兼任系统管理员和应用管理员，赖晋宝兼容网络管理员和机房管理员。当前已配置两名安全管理员：李任华、郑辉，不存在兼任的情况。已制定《ZJJT-XX-18-2020信息系统管理授权审批管理制度》，明确各个部门岗位的具体职责划分以及授权审批事项、审批部门和批准人等内容。已制定《ZJJT-XX-18-2020信息系统管理授权审批管理制度》、《ZJJY-XX-19-2020系统安全管理制度》、《ZJJY-XX-20-2020软件开发管理制度》等制度，对系统变更，重要操作、物理访问和系统接入等事项执行过程进行了审批和流程规定，具体工作在内部OA办公系统中审批。每年对各类审批项目、审批部门和审批人进行更新，记录表单类文档中具有更新需授权和审批的项目、审批部门和审批人等信息，记录日期与审查周期一致。已建立各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通机制，每年组织一次工作会议进行沟通合作，共同协调处理信息安全相关问题，具备相关会议记录。与中国电信股份有限公司、杭州西湖区网警、外包供应商：新华三技术有限公司、业界专家、安全公司、安全组织等，定期进行沟通、合作，通过会议、电话、邮件等方式进行交流沟通，具备沟通合作记录。已建立浙江省建设投资集团股份有限公司的《外联单位联系表》，内容包括外联单位名称、合作内容、联系人和联系方式等信息。查看到具有《aZJJT-XXBG-02-2020-B网络与信息系统安全运行月报2021年2月》，相关记录表单为《a定期全面信息系统安全检查表》，每季度进行安全检测，报告内容包括系统日常运维、文档、数据备份、系统漏洞等情况。每年进行一次全面的安全检查，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，且具备检查记录《a定期全面信息系统安全检查表》。具备安全检查表格、安全检查记录、安全检查报告、安全检查结果通报记录等；安全检查表记录包含常规检查、全面检查的相关数据，每年形成安全检查报告，通过邮件、会议等方式对安全检查结果进行通报。

### 主要安全问题汇总分析

经安全管理机构检测结果分析，所有检测项均符合相应级别的网络安全等级保护要求。

## 安全管理人员

### 已有安全控制措施汇总分析

安全管理人员方面，在人员录用、人员离岗、安全意识教育和培训、外部人员访问管理方面制定了一系列的安全管理制度。已指定人事部专门负责对人员录用。已制定《ZJJT-XX-10-2020信息安全员管理制度》规定在人员录用时对被录用人身份、安全背景、专业资格或资质等进行了审查，对其技术能力进行了考核，且具备相关审查记录及考核记录。已制定《ZJJT-XX-10-2020信息安全员管理制度》，与正式员工签署有保密协议，与关键岗位人员签署有岗位责任协议；保密协议中包含保密范围、保密责任、违约责任、协议的有效期限和责任人签字等内容；岗位责任协议中包含岗位安全责任定义、协议的有效期限和责任人签字等内容。在《ZJJT-XX-10-2020信息安全员管理制度》规定所有人员离职时的操作流程：删除该人员的信息系统访问账号和权限；明确保密事项，不得泄露原单位信息秘密，不得使用原单位的知识产权。《ZJJT-XX-10-2020信息安全员管理制度》中规定了人员调离手续和离岗要求等，《aZJJT-XXBG-10-2020-A人员离岗交接清单》中按照人员管理文档中的离岗程序办理人员调离手续。。《ZJJT-XX-12-2020信息安全人员培训和教育管理制度》规定了各类人员的安全意识教育和岗位技能培训，并明确了相关安全责任和惩戒措施，具备《aZJJT-XXBG-12-2020-培训记录表》。《ZJJT-XX-12-2020信息安全人员培训和教育管理制度》，具有不同岗位的培训计划，培训计划包含了培训目的、培训方式、培训对象、培训内容，对不同岗位指定了不同的培训计划，对安全基础知识、岗位操作等进行培训，具备《aZJJT-XXBG-12-2020-培训记录表》。信息安全内部培训与考核。培训应长期进行开展，并覆盖公司全员。针对公司安全管理员、安全审计员、系统管理员、网络管理员、数据库管理员、应用管理员、机房管理员应根据岗位不同，对员工进行相关的信息安全培训，并在培训后实行书面信息安全考核，具备《技能考核记录》。已制定《ZJJT-XX-11-2020外部人员访问控制管理制度》规定了外部人员的访问情况，在外部人员物理访问受控区域前先提出书面申请，填写《aZJJT-XXBG-11-2020-A外部人员访问申请授权表》，由系统管理员批准，通过审批后由专人全程陪同，并登记备案。已制定《ZJJT-XX-11-2020外部人员访问控制管理制度》规定了在外部人员接入受控网络访问系统前先提出书面申请，填写《aZJJT-XXBG-11-2020-A外部人员访问申请授权表》，批准后由专人开设账户、分配权限，并登记备案。在《ZJJT-XX-11-2020外部人员访问控制管理制度》中已规定外部人员离场后须及时清除其所有的访问权限，具备外部人员访问系统登记记录，记录中包含访问权限的清除时间等内容。《ZJJT-XX-11-2020外部人员访问控制管理制度》对系统访问情况进行了规定，获得系统访问授权的外部人员应签署保密协议，协议中明确了外部人员的保密义务，包含不得进行非授权操作，不得复制信息等内容。

### 主要安全问题汇总分析

经安全管理人员检测结果分析，所有检测项均符合相应级别的网络安全等级保护要求。

## 安全建设管理

### 已有安全控制措施汇总分析

安全建设管理方面，在供应链管理、定级和备案、系统交付、等级测评、服务供应商选择方面制定了一系列的安全管理制度。在安全方案设计、产品采购和使用、外包软件开发、工程实施、测试验收方面制定了一系列的安全管理制度。云服务商选择的供应商为：新华三技术有限公司，具备销售许可证、服务资质等，符合国家规定。在发生安全事件时，云服务商通过邮件或电话方式通知云服务客户，并向云服务客户提交安全事件报告或威胁报告，报告内容包括响应流程响应和处理的范围、程度及处理方法等。云服务商对每次供应商的重要变更均进行风险评估并采取控制措施，在供应商发生重要变更后云服务商通过邮件或电话方式通知云服务客户。已在浙江省建设投资集团股份有限公司私有云定级报告中明确了该系统的网络安全保护等级为第三级（S3A3G3），在报告中详细描述了网络安全保护等级的确定方法和理由。浙江省建设投资集团股份有限公司私有云的定级结果已经通过了专家评审，由安全技术专家对系统定级结果的合理性和正确性进行论证，具备专家定级评审反馈意见表。定级结果已通过杭州西湖区网安批准及信息安全部门的批准，具备私有云定级情况审批意见。浙江省建设投资集团股份有限公司私有云的定级材料已提交杭州西湖区网安进行备案，具有公安出具的备案证明。该系统具备《浙江省建设投资集团股份有限公司私有云风险评估报告》，报告中已明确根据等级保护第三级（S3A3G3）的要求对系统进行分析，并依据风险分析的结果补充和调整系统的安全性措施。《私有云安全设计方案》中包含与其他系统交互的整体规划设计部分，其中包括不同级别系统间如何进行数据传输以及采用何种密码算法等内容，且整体规划设计详细实施方案具备配套执行文件。该系统相关网络安全产品均采用公开招投标、邀请招标、单一来源等方式开展采购，招投标文件、流程符合国家《中华人民共和国招投标法》的有关要求，且网络安全产品均具备销售许可证。由科技信息部负责产品的选型测试，形成了产品候选范围，并根据安全需求及市场变动，调整并更新了候选产品，留存有《产品选择测试记录表》。在《ZJJT-XX-17-2020信息安全机构管理制度》中包含外包软件开发，在系统上线前，需由软件开发商对软件包中可能存在的恶意代码进行检测，具备《aZJJT-XXBG-03-2020-A恶意代码分析报告》。在《ZJJT-XX-17-2020信息安全机构管理制度》中包含外包软件开发，规定开发单位需提供软件涉及文档和使用指南。具体包含系统设计流程图、需求说明文档、系统概要设计文档等。科技信息部负责信息系统工程实施过程的管理工作。已制定《ZJJY-XX-23-2020信息系统工程实施管理制度》在工程实施之前，由工程实施单位制定详细的工程实施方案《私有云系统实施方案》对实施过程进行控制，该方案需要经信息安全管理工作领导小组批准认可后方可实施。在测试验收前制订《私有云测试验收方案》，《私有云测试验收方案》详细记录了时间、人员、现场操作过程、测试验收结果等方面内容，并形成《私有云系统测试验收报告》。制定有交付清单，系统交付清单包括系统设计流程图、效果图、需求说明文档、概要设计、详细设计、开发过程文档及系统操作手册等。由科技信息部人员进行系统的运行维护；在系统正式运行前对运行维护人员进行培训；主要针对的方面：操作、问题处理、功能介绍等；具备相关《技术培训记录》，内容包括培训内容、培训时间、参与人员等。已提供系统建设过程中的文档和指导用户进行系统运行维护的文档，包括系统建设文档、指导用户进行系统运维的文档、系统培训手册《私有云操作手册》。该系统定级为第三级（S3A3G3），本次为首次测评。在确定该信息系统的安全保护等级后，并未发生较大变更，未调整安全保护级别，系统发生重大变更或级别发生变化时及时进行等级测评。等级测评单位名称：杭州中尔网络科技有限公司；该单位具有相关技术资质、安全资质。信息系统选择的安全服务商：新华三技术有限公司、浙江乾冠信息安全研究院有限公司，均具备相应服务资质，且资质在有效期内，符合国家有关规定。已和新华三技术有限公司、浙江乾冠信息安全研究院有限公司签订相关服务合同，服务合同中明确了甲乙双方的责任和义务。新华三技术有限公司、浙江乾冠信息安全研究院有限公司具备每年的安全服务报告交付物，目前安全服务商未发起服务变更申请，无需对变更进行审核，在合同中明确了评价指标、考核内容、进入及退出机制等。

### 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）未组织相关部分和有关专家对安全方案进行论证和审查。**

可能存在安全策略缺乏合理性和可行性，导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要，涉及测评对象：**制度或记录类文档。**

**2）该系统未使用密码产品，未采购和使用国家密码主管部门要求的密码产品。**

可能存在安全隐患，导致保护机制失效或恶意人员利用产品自身漏洞攻击信息系统，涉及测评对象：**制度或记录类文档。**

**3）未对源代码进行审计工作，并出具相关审计报告。**

可能存在后门未在上线前被发现及处理，涉及测评对象：**制度或记录类文档。**

**4）未聘请第三方工程监理控制项目的实施过程。**

可能导致工程实施缺少组织性，工程实施管理不到位，涉及测评对象：**制度或记录类文档。**

**5）安全测试未包含密码相关安全性测试内容。**

安全隐患可能在系统上线运行前未被发现并作出相应的处理，涉及测评对象：**制度或记录类文档。**

## 安全运维管理

### 已有安全控制措施汇总分析

安全运维管理方面，在云计算环境管理、环境管理、资产管理、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、备份与恢复管理、安全事件处置、外包运维管理方面制定了一系列的安全管理制度。在变更管理、应急预案管理方面制定了一系列的安全管理制度。云平台运维地点位于浙江省杭州市西湖区古荡街道文三西路52号15楼，属于中国境内，云平台无境外远程运维操作。已制定《ZJJT-XX-05-2020机房管理制度》，机房管理员由信息科技部指定专人担任，具备《a机房出入登记表》，机房供配电、空调、温湿度设备等的定期巡检和维护记录。已制定《ZJJT-XX-05-2020机房管理制度》，制度中已明确对机房人员进出、物品的带进带出和日常安全环境管理等进行规定，具备《机房出入登录表》、《aZJJT-XXBG-08-2020-A巡视记录表》等记录表单。已在《ZJJT-XX-11-2020外部人员访问控制管理制度》中规定，来访人员在会议室接待，敏感机制不得随意存放，避免外部人员接触，含有敏感信息的纸质文件和移动介质不得随意放置在办公桌面等位置。已制定《ZJJT-XX-06-2020信息资产管理制度》，相关制度中已对信息资产分类进行规定，并留存有资产清单表，包括资产责任部门、重要程度和所处位置等内容。已制定《ZJJT-XX-06-2020信息资产管理制度》，相关制度中已明确了资产的标识方法，以及对不同资产的管理措施要求，同时资产清单中设备具有相应标识，符合相应制度要求。在《ZJJT-XX-06-2020信息资产管理制度》中，所有信息资产都应指定资产责任人，并由资产责任人负责进行相关资产的识别、统计、分类、分级，以便相关人员采取相应的保护措施。机房内的各类线路及设备指定信息科负责运行维护，具备《ZJJT-XX-07-2020信息设备运维管理制度》，文档中明确了设备维护管理的责任部门为科技信息部，每天进行一次维护管理工作。已制定《ZJJT-XX-07-2020信息设备运维管理制度》，信息资产日常使用管理过程中涉及维修的，原则上要求服务商现场维修，确需送外单位维修时，应彻底清除所存的工作相关信息，并与设备维修厂商签订保密协议，具备《aZJJT-XXBG-07-2020-A系统（设备）操作记录表》。含有重要数据的设备带出机房/工作环境要进行加密处理，并进行申请，经过本部门经理签字后方可带离，且留存有审批记录表。已制定《ZJJT-XX-07-2020信息设备运维管理制度》，制度中要求含有存储介质的设备在报废或重用前，须对数据进行加密，以确保其所存储信息完全清除或被安全覆盖，不可恢复，且具备详细的清除记录。已制定《ZJJT-XX-07-2020信息设备运维管理制度》，中规定由信息科技部，定期对私有云系统进行漏洞扫描，且与联通签订由协议，每半年进行一次漏洞扫描和渗透测试工作，具有漏洞扫描报告及渗透测试报告，报告描述了存在的漏洞、严重等级、原因分析和改进意见等方面，具备《aZJJT-XXBG-16-2020系统补丁更新记录表》。每年对私有云进行安全测评，并出具《浙江省建设投资集团股份有限公司私有云风险评估报告》，中报告日期符合每年开展安全测评的要求，具备《浙江省建设投资集团股份有限公司安全整改报告》，且依据上述风险分析报告所发现的问题进行了分析和整改。在《ZJJT-XX-17-2020信息安全机构管理制度》中已划分有系统管理员、网络管理员和安全管理员等角色，具备人员职责划分文档，文档中明确了各个角色的具体责任和权限。指定信息科技部负责账户管理，创建账户、修改账户权限、删除账户等操作，经过审批后方可执行；具备相关审批记录。已制定《ZJJT-XX-02-2020网络与信息安全管理制度》、《ZJJT-XX-07-2020信息设备运维管理制度》、《ZJJT-XX-08-2020信息系统巡检管理制度》等制定，明确了在日常运维工作中的安全策略、账户管理、配置管理、日志管理等的操作规程。具有《华三交换机操作手册》、《深信服防火墙操作手册》等重要设备的配置操作手册，包含了设备的操作步骤，参数配置等内容。具备《aZJJT-XXBG-08-2020-A巡视记录表》，包括日常巡检记录、运行维护记录、参数的设置和修改等内容。指定审计管理员每周对系统进行巡检，对日志、监测和报警数据等进行分析、统计，并出《aZJJT-XXBG-08-2020-A巡视记录表》，表中包含对日志、监测和报警数据等进行分析、统计的内容。该系统具备配置信息库，调整配置参数后立即同步更新配置信息库，配置库版本为最新；运维管理员需填写《aZJJT-XXBG-07-2020-C配置变更记录表》，通过审批后方可进行系统连接、安装系统组件或调整配置参数等活动。运维人员使用帕拉迪堡垒机对系统进行运维，使用运维工具接入系统时，须提交审批申请，经部门领导签字确认后方可接入系统，所有操作日志留存在堡垒机当中。系统在日常运维过程中存在远程运维，远程运维使用帕拉迪堡垒机进行，远程运维的开通须填写审批单，留存有《运维审批记录》；远程运维的帕拉迪堡垒机开启了审计日志功能，审计内容有时间、操作人员、操作内容等内容，审计日志不可更改。应用系统以及终端所有需与外部链接的端口和IP需经过上级信息部门的批准。《ZJJT-XX-16-2020信息系统安全补丁管理制度》中规定，所有联网和非联网计算机，要按照要求统一安装办法的防恶意代码软件，并定期更新（升级）计算机病毒防范产品的版本，具备《aZJJT-XXBG-03-2020-B恶意代码特征库更新记录表》。已制定《ZJJT-XX-03-2020计算机病毒防治管理制度》，制度中已规定须在服务器及终端均安装企业版防恶意代码软件，并定期对恶意代码库进行更新，并进行检测分析，且具备《aZJJT-XXBG-03-2020-B恶意代码特征库更新记录表》、《aZJJT-XXBG-03-2020-A恶意代码分析报告》等。已记录和保存系统基本配置信息；配置信息文档包含网络拓扑结构、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信息。基本配置信息变更后已及时更新配置信息库；制定有配置信息变更相应的申报审批程序，相关审批内容须经部门领导签字确认。已制定《ZJJT-XX-18-2020信息系统管理授权审批管理制度》，制度中已明确变更前需根据变更需求制定变更方案，方案内容须包括变更类型，变更原因，变更过程、变更前评估等内容，具有《aZJJT-XXBG-07-2020-C配置变更记录表》。已制定《ZJJT-XX-18-2020信息系统管理授权审批管理制度》，制度中已规定变更控制的申报和审批程序，具有《aZJJT-XXBG-07-2020-C配置变更记录表》，审批记录包含变更类型、申报流程、审批部门、批准人等方面内容。在《ZJJT-XX-04-2020数据备份与恢复管理制度》中已明确需要定期备份的信息为系统重要业务数据、系统软件配置信，具备备份记录。已制定《ZJJT-XX-04-2020数据备份与恢复管理制度》，制定中已对备份方式、备份频率、备份介质、备份保存时长等内容进行了规定。《ZJJT-XX-04-2020数据备份与恢复管理制度》规定对重要数据制定数据恢复策略、备份程序和恢复程序，并定期对策略、程序等进行实用性验证。《ZJJT-XX-02-2020网络与信息安全管理制度》明确系统运维人员在发现安全弱点和可疑事件时及时向安全管理部及时报告。《ZJJT-XX-02-2020网络与信息安全管理制度》已明确针对计算机病毒、网络攻击事件的威胁隔离、信息的收集、消除隐患等方面的内容。《ZJJT-XX-02-2020网络与信息安全管理制度》明确如发生安全事件，事后应详细分析事件发生的原因，记录处理过程，总结经验教训等。已制定《ZJJT-XX-02-2020网络与信息安全管理制度》，制度中规定了对造成系统中断和造成信息泄密的安全事件采用不同的处理程序和报告程序，且实际工作中对造成系统中断和造成信息泄漏的重大安全事件制定了不同的处理程序和报告程序。《03浙江省建设投资集团股份有限公司私有云系统应急预案》，制度中明确了应急预案工作小组由组长、副组长及组员组成，并对职责进行了详细描述；具有统一的应急预案框架描述，包括启动应急预案的条件、应急组织构成、应急资源保障、事后教育和培训等方面内容。《03浙江省建设投资集团股份有限公司私有云系统应急预案》，中对应急事件的处置流程、恢复流程等进行了说明。已根据《03浙江省建设投资集团股份有限公司私有云系统应急预案》要求，每年进行一次应急培训，培训记录包含培训对象、培训内容、培训结果等内容；每半年组织一次系统相关人员进行预案的演练，《04浙江省建设投资集团股份有限公司私有云系统应急演练记录》包含演练时间、主要操作内容、演练结果等内容。选择新华三技术有限公司作为系统运维服务商，符合国家相关规定。已和新华三技术有限公司签订相关的协议，对运维内容、范围等进行确定，并签订相关协议。浙江省建设投资集团股份有限公司与外包运维服务商签订的外包运维合同中有乙方应具备依据等级保护标准要求提供服务的能力以及相关要求。浙江省建设投资集团股份有限公司与外包运维服务商签订的外包运维服务商签署的合同中明确了敏感信息及应急保障方面安全要求。

### 主要安全问题汇总分析

安全运维管理存在的安全问题有：

**1）未建立介质管理制度对介质进行控制和保护，也未指定专人或专门的部门对介质进行管理并定期清算盘点。**

可能导致介质被未授权人员访问，导致系统敏感信息泄露等，涉及测评对象：**制度或记录类文档。**

**2）未对介质在物理传输过程中的人员选择、打包、交付等进行控制，也未对介质的归档和查询等进行登记记录。**

可能导致归档介质的丢失，而不能及时发现，使介质的安全管理不到位，涉及测评对象：**制度或记录类文档。**

**3）系统未使用密码产品，未遵循密码相关国家标准和行业标准。**

密码使用管理不到位，存在违反国家政策的风险，涉及测评对象：**制度或记录类文档。**

**4）未建立密码使用管理制度，未使用符合国家密码管理规定的密码技术和产品。**

导致信息系统所使用的密码密钥及密码设备等管理不到位，存在违反国家政策的风险，涉及测评对象：**制度或记录类文档。**

**5）未建立终止变更并从失败变更中恢复的程序。**

可能在变更过程中或变更后出现问题的情况下，存在无法回退的风险，涉及测评对象：**制度或记录类文档。**

**6）未定期对原有的应急预案重新评估并定期修订完善。**

未及时更新应急预案，导致使用时出现错误或导致无法在规定时间内完成应急工作，涉及测评对象：**制度或记录类文档。**

## 其他安全要求指标

本次检测不包含其他安全要求指标。

## 验证测试

### 漏洞扫描

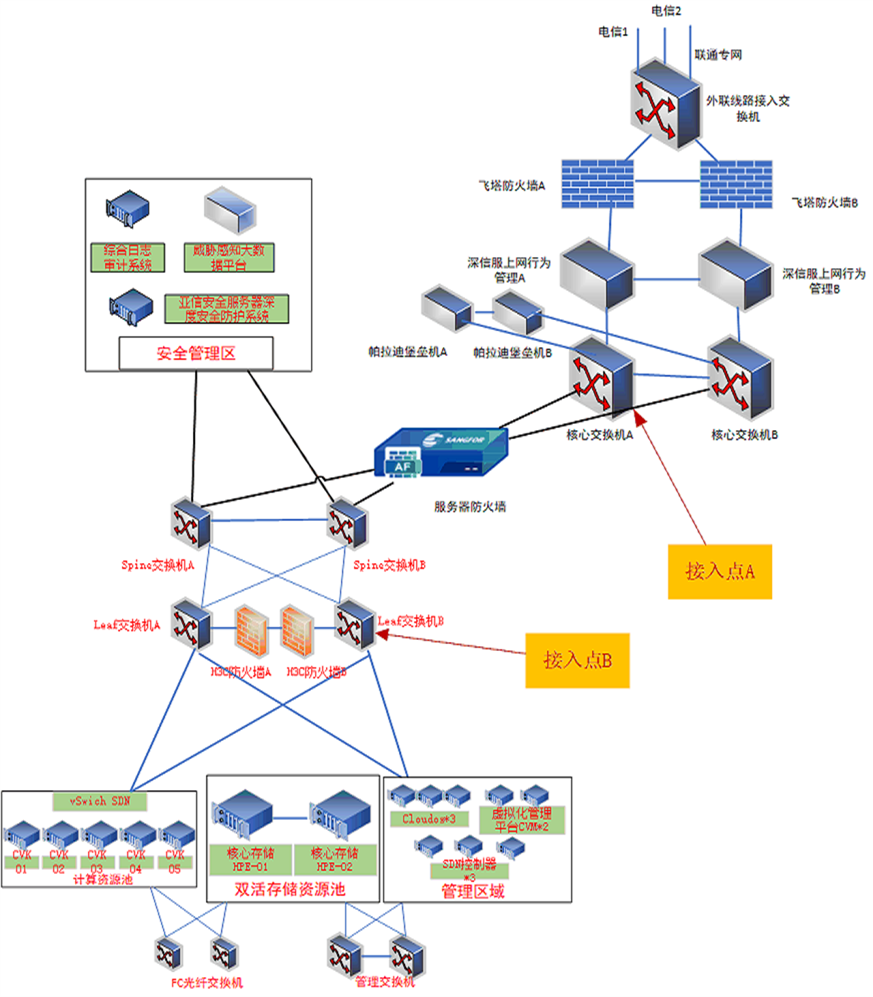
#### 漏洞扫描结果统计

接入点A：测试者在核心交换机上对区域内的设备通过工具扫描的方式发现其存在的脆弱点，主要检测内容包括系统漏洞的检测、协议漏洞的检测、多余端口和多余服务的检测等。同时通过应用扫描工具对系统应用进行SQL注入、Cookie注入、XPath注入、LDAP注入、跨站脚本、代码注入、表单绕过、弱口令、敏感文件和目录、管理后台、敏感数据等内容的测试。并且测试者对区域边界已设置的访问控制策略的有效性进行测试。

接入点B：测试者在Leaf核心交换机核心交换机上对区域内的设备通过工具扫描并进行渗透测试发现其存在的脆弱点，主要检测内容包括系统漏洞的检测、协议漏洞的检测、多余端口和多余服务的检测等。同时通过应用扫描工具对系统应用进行SQL注入、Cookie注入、XPath注入、LDAP注入、跨站脚本、代码注入、表单绕过、弱口令、敏感文件和目录、管理后台、敏感数据等内容的测试。

表 3-1 漏洞扫描与测试工具

| **序号** | **工具名称** | **工具版本** | **工具用途** |
| --- | --- | --- | --- |
| 1 | 安恒等级保护工具箱 | V2.3 | 网络设备、安全设备、服务器、web漏洞扫描 |



**图 3‑1接入点示意图**

**（1）接入点A漏洞扫描结果统计**

接入点A的漏洞扫描结果汇总如下表所示。

**表 3‑1 接入点A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 | 核心交换机A | Version 7.1.045, Release 7184 | 0 | 2 | 6 | 8 |
| 2 | Spine交换机A | Version 7.1.070, Release 6607 | 0 | 2 | 6 | 8 |
| 3 | Leaf交换机A | Version 7.1.070, Release 2702 | 0 | 2 | 6 | 8 |
| 4 | 核心交换机B | Version 7.1.045, Release 7184 | 0 | 2 | 6 | 8 |
| 5 | Spine交换机B | Version 7.1.070, Release 6607 | 0 | 2 | 6 | 8 |
| 6 | Leaf交换机B | Version 7.1.070, Release 2702 | 0 | 2 | 6 | 8 |
| 7 | 飞塔防火墙A | V6.4.3 build1778(GA) | 0 | 0 | 0 | 0 |
| 8 | 飞塔防火墙B | V6.4.3 build1778(GA) | 0 | 0 | 0 | 0 |
| 9 | 深信服上网行为管理A | AC11.9R1 | 0 | 0 | 0 | 0 |
| 10 | 深信服上网行为管理B | AC11.9R1 | 0 | 0 | 0 | 0 |
| 11 | 帕拉迪堡垒机A | ST00001B090 | 0 | 0 | 0 | 0 |
| 12 | 帕拉迪堡垒机B | ST00001B090 | 0 | 0 | 0 | 0 |
| 13 | H3C防火墙A | Vesion 7.1.064,Release 9608P30 | 0 | 0 | 0 | 0 |
| 14 | H3C防火墙B | Vesion 7.1.064,Release 9608P30 | 0 | 0 | 0 | 0 |
| 15 | 综合日志审计系统 | E1107 | 0 | 0 | 0 | 0 |
| 16 | 服务器防火墙 | AF8.0.35 | 0 | 0 | 0 | 0 |
| 17 | 威胁感知大数据平台 | V5.4.26 | 0 | 0 | 0 | 0 |
| 18 | CVK01 | Centos7.6 | 0 | 0 | 2 | 2 |
| 19 | CVK02 | Centos7.6 | 0 | 0 | 2 | 2 |
| 20 | CVK03 | Centos7.6 | 0 | 0 | 2 | 2 |
| 21 | CVK04 | Centos7.6 | 0 | 0 | 2 | 2 |
| 22 | CVK05 | Centos7.6 | 0 | 0 | 2 | 2 |
| 23 | CloudOS1 | Centos7.6 | 0 | 0 | 2 | 2 |
| 24 | CloudOS2 | Centos7.6 | 0 | 0 | 2 | 2 |
| 25 | CloudOS3 | Centos7.6 | 0 | 0 | 2 | 2 |
| 26 | CVM01 | Centos7.6 | 0 | 0 | 2 | 2 |
| 27 | CVM02 | Centos7.6 | 0 | 0 | 2 | 2 |
| 28 | SDN01 | H3Linux Release 1.1.2 | 0 | 0 | 2 | 2 |
| 29 | SDN02 | H3Linux Release 1.1.2 | 0 | 0 | 2 | 2 |
| 30 | SDN03 | H3Linux Release 1.1.2 | 0 | 0 | 2 | 2 |
| 31 | 亚信安全服务器深度安全防护系统 | 10.0.5129 | 0 | 0 | 1 | 1 |
| 32 | CloudOS平台 | / | 0 | 0 | 1 | 1 |
| 33 | CAS平台 | / | 0 | 0 | 3 | 3 |
| 34 | SNA平台 | / | 0 | 0 | 0 | 0 |
| **安全漏洞数量小计** | | | 0 | 12 | 67 | 79 |

**（2）接入点B漏洞扫描结果统计**

接入点B的漏洞扫描结果汇总如下表所示。

**表 3‑2 接入点B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 | 核心交换机A | Version 7.1.045, Release 7184 | 0 | 2 | 6 | 8 |
| 2 | Spine交换机A | Version 7.1.070, Release 6607 | 0 | 2 | 6 | 8 |
| 3 | Leaf交换机A | Version 7.1.070, Release 2702 | 0 | 2 | 6 | 8 |
| 4 | 核心交换机B | Version 7.1.045, Release 7184 | 0 | 2 | 6 | 8 |
| 5 | Spine交换机B | Version 7.1.070, Release 6607 | 0 | 2 | 6 | 8 |
| 6 | Leaf交换机B | Version 7.1.070, Release 2702 | 0 | 2 | 6 | 8 |
| 7 | 飞塔防火墙A | V6.4.3 build1778(GA) | 0 | 0 | 0 | 0 |
| 8 | 飞塔防火墙B | V6.4.3 build1778(GA) | 0 | 0 | 0 | 0 |
| 9 | 深信服上网行为管理A | AC11.9R1 | 0 | 0 | 0 | 0 |
| 10 | 深信服上网行为管理B | AC11.9R1 | 0 | 0 | 0 | 0 |
| 11 | 帕拉迪堡垒机A | ST00001B090 | 0 | 0 | 0 | 0 |
| 12 | 帕拉迪堡垒机B | ST00001B090 | 0 | 0 | 0 | 0 |
| 13 | H3C防火墙A | Vesion 7.1.064,Release 9608P30 | 0 | 0 | 0 | 0 |
| 14 | H3C防火墙B | Vesion 7.1.064,Release 9608P30 | 0 | 0 | 0 | 0 |
| 15 | 综合日志审计系统 | E1107 | 0 | 0 | 0 | 0 |
| 16 | 服务器防火墙 | AF8.0.35 | 0 | 0 | 0 | 0 |
| 17 | 威胁感知大数据平台 | V5.4.26 | 0 | 0 | 0 | 0 |
| 18 | CVK01 | Centos7.6 | 0 | 0 | 2 | 2 |
| 19 | CVK02 | Centos7.6 | 0 | 0 | 2 | 2 |
| 20 | CVK03 | Centos7.6 | 0 | 0 | 2 | 2 |
| 21 | CVK04 | Centos7.6 | 0 | 0 | 2 | 2 |
| 22 | CVK05 | Centos7.6 | 0 | 0 | 2 | 2 |
| 23 | CloudOS1 | Centos7.6 | 0 | 0 | 2 | 2 |
| 24 | CloudOS2 | Centos7.6 | 0 | 0 | 2 | 2 |
| 25 | CloudOS3 | Centos7.6 | 0 | 0 | 2 | 2 |
| 26 | CVM01 | Centos7.6 | 0 | 0 | 2 | 2 |
| 27 | CVM02 | Centos7.6 | 0 | 0 | 2 | 2 |
| 28 | SDN01 | H3Linux Release 1.1.2 | 0 | 0 | 2 | 2 |
| 29 | SDN02 | H3Linux Release 1.1.2 | 0 | 0 | 2 | 2 |
| 30 | SDN03 | H3Linux Release 1.1.2 | 0 | 0 | 2 | 2 |
| 31 | 亚信安全服务器深度安全防护系统 | 10.0.5129 | 0 | 0 | 1 | 1 |
| 32 | CloudOS平台 | / | 0 | 0 | 1 | 1 |
| 33 | CAS平台 | / | 0 | 0 | 3 | 3 |
| 34 | SNA平台 | / | 0 | 0 | 0 | 0 |
| **安全漏洞数量小计** | | | 0 | 12 | 67 | 79 |

#### 漏洞扫描问题描述

通过对漏洞扫描结果进行分析，私有云存在的主要安全漏洞汇总如下表所示。

**表 3‑3主要安全漏洞汇总表**

| **序号** | **安全漏洞名称** | **关联资产/域名** | **严重程度** |
| --- | --- | --- | --- |
| 1 | RC4 加密问题漏洞 | 核心交换机A、核心交换机B、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B | 中危 |
| 2 | TLS/SSL协议 RC4算法安全漏洞(CVE-2013-2566) | 核心交换机A、核心交换机B、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B | 中危 |
| 3 | 支持SSH弱MAC算法 | 核心交换机A、核心交换机B、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B | 低危 |
| 4 | SSH版本信息可被获取 | 核心交换机A、核心交换机B、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、CVK01、CVK02、CVK03、CVK04、CVK05、CloudOS1、CloudOS2、CloudOS3、CVM01、CVM02、SDN01、SDN02、SND03 | 低危 |
| 5 | SSH协议支持的算法 | 核心交换机A、核心交换机B、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、CVK01、CVK02、CVK03、CVK04、CVK05、CloudOS1、CloudOS2、CloudOS3、CVM01、CVM02、SDN01、SDN02、SND03 | 低危 |
| 6 | 服务器加密通信支持的SSL加密算法（原理扫描） | 核心交换机A、核心交换机B、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B | 低危 |
| 7 | 服务器支持的SSL加密协议（原理扫描） | 核心交换机A、核心交换机B、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B | 低危 |
| 8 | HTTP Server类型和版本号 | 核心交换机A、核心交换机B、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、亚信安全服务器深度安全防护系统 | 低危 |
| 9 | 错误页面Web应用服务器版本泄露 | CloudOS平台 | 低危 |
| 10 | E-Mail地址 | CAS平台 | 低危 |
| 11 | 内网IP | CAS平台 | 低危 |
| 12 | 电话号码 | CAS平台 | 低危 |

### 渗透测试

#### 渗透测试过程说明

渗透测试由信息安全专业人员采用攻击者的视角、使用同攻击者相同的技术和工具来发现信息系统风险。

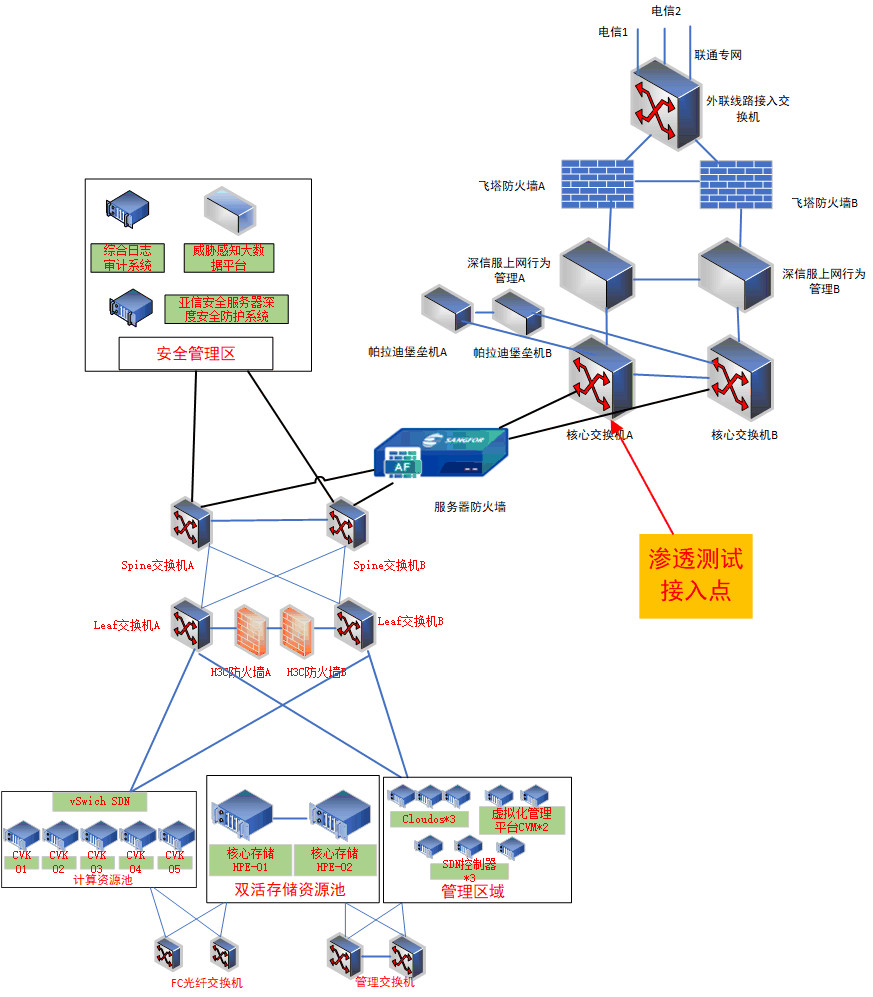
本次渗透测试针对应用服务层面进行，测试范围及流程如下：系统信息收集、配置管理测试、认证授权测试、会话管理测试、数据验证测试和业务逻辑安全测试等。

本次测试使用的工具包括：

| **序号** | **工具名称** | **工具描述（厂商、版本、功能）** |
| --- | --- | --- |
|  | Burpsuite Professional | V2021.5.1 web攻击工具平台 |
|  | SQLMap | V1.5.6 SQL注入漏洞测试工具 |
|  | Acunetix Web Vulnerability Scanner | V14应用安全扫描工具 |
|  | Nmap | V7.91 端口扫描工具 |

本次测试的对象包括：

| **序号** | **被测对象名称** | **URL地址** |
| --- | --- | --- |
| 1 | CloudOS平台 | https://10.0.58.121 |
| 2 | CAS平台 | https://10.0.58.123:8080 |
| 3 | SNA平台 | https://10.0.58.122:10443/portal |

【渗透测试接入点】

#### 渗透测试问题描述

通过渗透测试发现，私有云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** |
| --- | --- | --- | --- |
| 1 | CloudOS平台存在Docker Engine API信息泄露 | CloudOS平台 | 中危 |
| 2 | CAS平台存在点击劫持 | CAS平台 | 低危 |

## 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 3‑3控制点符合情况汇总表**

| **序号** | **通用/扩展** | **安全类** | **控制点** | **控制点符合情况** | | |
| --- | --- | --- | --- | --- | --- | --- |
| **符合** | **部分符合** | **不符合** |
| 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 | 安全管理中心 | 系统管理 |  | √ |  |
| 31 | 审计管理 | √ |  |  |
| 32 | 安全管理 |  | √ |  |
| 33 | 集中管控 |  | √ |  |
| 34 | 安全管理制度 | 安全策略 | √ |  |  |
| 35 | 管理制度 | √ |  |  |
| 36 | 制定和发布 | √ |  |  |
| 37 | 评审和修订 |  |  | √ |
| 38 | 安全管理机构 | 岗位设置 | √ |  |  |
| 39 | 人员配备 | √ |  |  |
| 40 | 授权和审批 | √ |  |  |
| 41 | 沟通和合作 | √ |  |  |
| 42 | 审核和检查 | √ |  |  |
| 43 | 安全管理人员 | 人员录用 | √ |  |  |
| 44 | 人员离岗 | √ |  |  |
| 45 | 安全意识教育和培训 | √ |  |  |
| 46 | 外部人员访问管理 | √ |  |  |
| 47 | 安全建设管理 | 定级和备案 | √ |  |  |
| 48 | 安全方案设计 |  | √ |  |
| 49 | 产品采购和使用 |  | √ |  |
| 50 | 外包软件开发 |  | √ |  |
| 51 | 工程实施 |  | √ |  |
| 52 | 测试验收 |  | √ |  |
| 53 | 系统交付 | √ |  |  |
| 54 | 等级测评 | √ |  |  |
| 55 | 服务供应商选择 | √ |  |  |
| 56 | 安全运维管理 | 环境管理 | √ |  |  |
| 57 | 资产管理 | √ |  |  |
| 58 | 介质管理 |  |  | √ |
| 59 | 设备维护管理 | √ |  |  |
| 60 | 漏洞和风险管理 | √ |  |  |
| 61 | 网络和系统安全管理 | √ |  |  |
| 62 | 恶意代码防范管理 | √ |  |  |
| 63 | 配置管理 | √ |  |  |
| 64 | 密码管理 |  |  | √ |
| 65 | 变更管理 |  | √ |  |
| 66 | 备份与恢复管理 | √ |  |  |
| 67 | 安全事件处置 | √ |  |  |
| 68 | 应急预案管理 |  | √ |  |
| 69 | 外包运维管理 | √ |  |  |
| 70 | 云计算安全扩展要求 | 安全物理环境 | 基础设施位置 | √ |  |  |
| 71 | 安全通信网络 | 网络架构 | √ |  |  |
| 72 | 安全区域边界 | 访问控制 | √ |  |  |
| 73 | 入侵防范 | √ |  |  |
| 74 | 安全审计 | √ |  |  |
| 75 | 安全计算环境 | 身份鉴别 |  |  | √ |
| 76 | 访问控制 | √ |  |  |
| 77 | 入侵防范 |  | √ |  |
| 78 | 镜像和快照保护 |  | √ |  |
| 79 | 数据完整性和保密性 | √ |  |  |
| 80 | 数据备份恢复 | √ |  |  |
| 81 | 剩余信息保护 | √ |  |  |
| 82 | 安全管理中心 | 集中管控 | √ |  |  |
| 83 | 安全建设管理 | 供应链管理 | √ |  |  |
| 84 | 安全运维管理 | 云计算环境管理 | √ |  |  |
| **控制点符合情况数量统计** | | | | **55** | **22** | **7** |

### 安全问题汇总

**表 3‑4安全问题汇总表**

| **问题编号** | **安全问题** | **测评对象** | **通用/扩展** | **安全类** | **控制点** | **测评项** |
| --- | --- | --- | --- | --- | --- | --- |
| T1 | 未采取措施对关键设备实施电磁屏蔽防护。 | 物理机房 | 安全通用要求 | 安全物理环境 | 电磁防护 | b)应对关键设备实施电磁屏蔽。 |
| T2 | 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 | 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。 |
| T3 | 未采取措施对非授权设备私自连入内部网络的行为进行检查和限制。 | 互联网边界、服务器边界 | 安全通用要求 | 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； |
| T4 | 未采取措施针对网络访问的数据流量实现基于应用协议和应用内容的访问控制。 | 互联网边界、服务器边界 | 安全通用要求 | 安全区域边界 | 访问控制 | 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。 |
| T5 | 未采取措施基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 | 互联网边界、服务器边界 | 安全通用要求 | 安全区域边界 | 可信验证 | 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。 |
| T6 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 安全通用要求 | 安全计算环境 | 身份鉴别 | 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。 |
| T7 | 未重命名或删除默认账户。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 安全通用要求 | 安全计算环境 | 访问控制 | b)应重命名或删除默认账户，修改默认账户的默认口令； |
| T8 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 安全通用要求 | 安全计算环境 | 访问控制 | 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。 |
| T9 | 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。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 安全通用要求 | 安全计算环境 | 可信验证 | 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。 |
| T10 | 未采用校验技术或密码技术保证重要审计数据和重要配置数据在存储过程中的完整性。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 安全通用要求 | 安全计算环境 | 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。 |
| T11 | 未使用备份文件进行过备份恢复测试。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、业务数据、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 安全通用要求 | 安全计算环境 | 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； |
| T12 | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、业务数据、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 安全通用要求 | 安全计算环境 | 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； |
| T13 | 未在远程管理云平台中设备时，在管理终端和云平台间建立双向身份验证机制。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、业务数据、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 云计算安全扩展要求 | 安全计算环境 | 身份鉴别 | 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。 |
| T14 | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、业务数据、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 云计算安全扩展要求 | 安全计算环境 | 入侵防范 | 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； |
| T15 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、业务数据、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 云计算安全扩展要求 | 安全计算环境 | 镜像和快照保护 | 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。 |
| T16 | 未采用校验技术或密码技术保证重要审计数据在传输过程中的完整性。 | H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、飞塔防火墙A、飞塔防火墙B、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 安全通用要求 | 安全计算环境 | 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； |
| T17 | 未采用校验技术或密码技术保证重要业务数据在存储过程中的完整性。 | 业务数据 | 安全通用要求 | 安全计算环境 | 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。 |
| T18 | 未采用密码技术保证重要业务数据在存储过程中的保密性。 | 业务数据 | 安全通用要求 | 安全计算环境 | 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。 |
| T19 | 未配置口令有效期策略。 | CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02 | 安全通用要求 | 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； |
| T20 | 未配置登录连接超时策略。 | CloudOS1、CloudOS2、CloudOS3 | 安全通用要求 | 安全计算环境 | 身份鉴别 | 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； |
| T21 | 未部署主机入侵防护软件，无法对主机重要节点进行入侵行为进行检查、限制并报警。 | CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2 | 安全通用要求 | 安全计算环境 | 入侵防范 | 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。 |
| T22 | 未安装防恶意代码软件，无法识别入侵和病毒行为，并将其有效阻断。 | CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03 | 安全通用要求 | 安全计算环境 | 恶意代码防范 | 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。 |
| T23 | 未限制网络设备、安全设备、服务器等仅通过堡垒机进行运维管理，并对系统管理员的操作进行审计。 | 安全管理中心 | 安全通用要求 | 安全管理中心 | 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； |
| T24 | 未限制网络设备、安全设备、服务器等仅通过堡垒机进行运维管理，并对安全管理员的操作进行审计。 | 安全管理中心 | 安全通用要求 | 安全管理中心 | 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； |
| T25 | 未采取措施对安全策略、恶意代码、补丁升级等进行统一集中管理。 | 安全管理中心 | 安全通用要求 | 安全管理中心 | 集中管控 | 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； |
| T26 | 未定期对安全管理制度进行论证、审定以及修订。 | 制度或记录类文档 | 安全通用要求 | 安全管理制度 | 评审和修订 | 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。 |
| T27 | 未组织相关部分和有关专家对安全方案进行论证和审查。 | 制度或记录类文档 | 安全通用要求 | 安全建设管理 | 安全方案设计 | c)应组织相关部门和有关安全专家对安全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。 |
| T28 | 该系统未使用密码产品，未采购和使用国家密码主管部门要求的密码产品。 | 制度或记录类文档 | 安全通用要求 | 安全建设管理 | 产品采购和使用 | 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； |
| T29 | 未对源代码进行审计工作，并出具相关审计报告。 | 制度或记录类文档 | 安全通用要求 | 安全建设管理 | 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。 |
| T30 | 未聘请第三方工程监理控制项目的实施过程。 | 制度或记录类文档 | 安全通用要求 | 安全建设管理 | 工程实施 | c)应通过第三方工程监理控制项目的实施过程。 |
| T31 | 安全测试未包含密码相关安全性测试内容。 | 制度或记录类文档 | 安全通用要求 | 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。 |
| T32 | 未建立介质管理制度对介质进行控制和保护，也未指定专人或专门的部门对介质进行管理并定期清算盘点。 | 制度或记录类文档 | 安全通用要求 | 安全运维管理 | 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； |
| T33 | 未对介质在物理传输过程中的人员选择、打包、交付等进行控制，也未对介质的归档和查询等进行登记记录。 | 制度或记录类文档 | 安全通用要求 | 安全运维管理 | 介质管理 | 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。 |
| T34 | 系统未使用密码产品，未遵循密码相关国家标准和行业标准。 | 制度或记录类文档 | 安全通用要求 | 安全运维管理 | 密码管理 | a)应遵循密码相关国家标准和行业标准； |
| T35 | 未建立密码使用管理制度，未使用符合国家密码管理规定的密码技术和产品。 | 制度或记录类文档 | 安全通用要求 | 安全运维管理 | 密码管理 | 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。 |
| T36 | 未建立终止变更并从失败变更中恢复的程序。 | 制度或记录类文档 | 安全通用要求 | 安全运维管理 | 变更管理 | 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。 |
| T37 | 未定期对原有的应急预案重新评估并定期修订完善。 | 制度或记录类文档 | 安全通用要求 | 安全运维管理 | 应急预案管理 | d)应定期对原有的应急预案重新评估，修订完善。 |

# 整体测评

## 安全控制点间安全测评

**入侵防范对身份鉴别的安全功能修正（安全计算环境）**

安全计算环境层面的身份鉴别中要求“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”，检查中发现未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。虽然所有测评对象身份鉴别方式仅采用用户名加口令的方式，未采取两种或两种以上的鉴别方式，但是所有测评对象的远程管理进行了地址限制，例如：通过边界配置ACL3001，仅允许10.\*.1.\*，192.\*.9.\*远程管理设备，通过服务器防火墙策略限制仅允许总部员工有线、机房运维、网络监控平台等网段可远程管理设备等，在一定程度上降低了设备未采取双因子认证带来的威胁。对该问题起到一定补充作用，问题风险降低。

**测试验收对外包软件开发的安全功能修正（安全建设管理）**

安全建设管理层面的外包软件开发中要求“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”，检查中发现未对源代码进行审计工作，并出具相关审计报告。虽然未对代码进行审计，但是该系统为云计算平台，采用新华三的云计算平台架构进行部署，该系统内部边界可控，仅允许总部员工有线10.\*.1.\*/24，机房运维10.\*.2.\*/24等访问内部服务器10.\*.58.\*/24网段和应用系统，且内部部署威胁感知大数据平台实时监控攻击行为等，在一定程度上减小了未对代码进行审计所带来的风险。对该问题起到一定补充作用，问题风险降低。

## 区域间安全测评

**安全区域边界对安全计算环境的安全功能修正**

安全计算环境层面的入侵防范中要求“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”，检查中发现未部署主机入侵防护软件，无法对主机重要节点进行入侵行为进行检查、限制并报警。虽然主机层面未安装入侵防护软件，但是网络层面部署有飞塔防火墙、服务器防火墙均集成入侵防护功能，已配置并启用相关策略，策略范围覆盖所有网络节点，可针对内外部入侵行为进行检测和限制，在发生严重入侵行为时通过邮件告警管理员，且已部署威胁感知大数据平台，可针对内部的网络行为进行集中监控和告警，在一定程度上降低了主机层面未安装入侵防护软件所带来的风险。对该问题起到一定补充作用，问题风险降低。

**安全区域边界对安全计算环境的安全功能修正**

安全计算环境层面的恶意代码防范中要求“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”，检查中发现未安装防恶意代码软件，无法识别入侵和病毒行为，并将其有效阻断。虽然主机层面未安装恶意代码防护软件，但是网络层面部署有飞塔防火墙、服务器防火墙均集成恶意代码防护功能，已配置并启用相关策略，策略范围覆盖所有网络节点，可针对网络层面的恶意代码进行检测和清除，在一定程度上降低了主机层面未安装恶意代码防护软件所带来的风险。对该问题起到一定补充作用，问题风险降低。

## 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修正后的安全问题汇总表**

| **问题编号** | **安全问题** | **测评对象** | **整体测评描述** | **严重程度变化** |
| --- | --- | --- | --- | --- |
| T6 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 虽然所有所有测评对象身份鉴别方式仅采用用户名加口令的方式，未采取两种或两种以上的鉴别方式，但是所有测评对象的远程管理进行了地址限制，例如：通过边界配置ACL3001，仅允许10.\*.1.\*，192.\*.9.\*远程管理设备，通过服务器防火墙策略限制仅允许总部员工有线、机房运维、网络监控平台等网段可远程管理设备等，在一定程度上降低了设备未采取双因子认证带来的威胁。 | □升高  ☑降低 |
| T21 | 未部署主机入侵防护软件，无法对主机重要节点进行入侵行为进行检查、限制并报警。 | CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2 | 虽然主机层面未安装入侵防护软件，但是网络层面部署有飞塔防火墙、服务器防火墙均集成入侵防护功能，已配置并启用相关策略，策略范围覆盖所有网络节点，可针对内外部入侵行为进行检测和限制，在发生严重入侵行为时通过邮件告警管理员，且已部署威胁感知大数据平台，可针对内部的网络行为进行集中监控和告警，在一定程度上降低了主机层面未安装入侵防护软件所带来的风险。 | □升高  ☑降低 |
| T22 | 未安装防恶意代码软件，无法识别入侵和病毒行为，并将其有效阻断。 | CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03 | 虽然主机层面未安装恶意代码防护软件，但是网络层面部署有飞塔防火墙、服务器防火墙均集成恶意代码防护功能，已配置并启用相关策略，策略范围覆盖所有网络节点，可针对网络层面的恶意代码进行检测和清除，在一定程度上降低了主机层面未安装恶意代码防护软件所带来的风险。 | □升高  ☑降低 |
| T29 | 未对源代码进行审计工作，并出具相关审计报告。 | 制度或记录类文档 | 虽然未对代码进行审计，但是该系统为云计算平台，采用新华三的云计算平台架构进行部署，该系统内部边界可控，仅允许总部员工有线10.\*.1.\*/24，机房运维10.\*.2.\*/24等访问内部服务器10.\*.58.\*/24网段和应用系统，且内部部署威胁感知大数据平台实时监控攻击行为等，在一定程度上减小了未对代码进行审计所带来的风险。 | □升高  ☑降低 |

*…………………………本页结束，以下为空白…………………………*

# 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，采用风险分析的方法进行危害分析和风险等级判定，得到被测对象安全问题风险分析表见表5-1。

风险分析主要结合关联资产和关联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或损失（风险等级）。风险分析结果的判断综合了相关系统组件的重要程度、安全问题的严重程度、安全问题被关联威胁利用的可能性、所影响的相关业务应用以及发生安全事件可能的影响范围等因素。风险等级根据最大安全危害的严重程度进一步确定为“高”、“中”、“低”。

**表 5‑1安全问题风险分析**

| **序号** | **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** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 安全物理环境 | 未采取措施对关键设备实施电磁屏蔽防护。 | 物理机房 | 物理环境影响 | 可能导致非授权人员通过特殊设备接收电磁信号，并从中分析窃取重要系统数据。 | 中 |
| 2 | 安全通信网络 | 未基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 | 安全通信网络 | 恶意攻击 | 无可信链和可信验证，无法通过主动免疫可信验证技术提高系统自身安全防护能力，无法实现积极主动防御。 | 低 |
| 3 | 安全区域边界 | 未采取措施对非授权设备私自连入内部网络的行为进行检查和限制。 | 互联网边界、服务器边界 | 恶意攻击 | 可能导致黑客通过技术手段接入内部网络，进而攻击应用系统。 | 中 |
| 4 | 未采取措施针对网络访问的数据流量实现基于应用协议和应用内容的访问控制。 | 互联网边界、服务器边界 | 恶意攻击 | 增加了应用系统受到网络攻击的风险。 | 中 |
| 5 | 未采取措施基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 | 互联网边界、服务器边界 | 恶意攻击 | 无可信链和可信验证，无法通过主动免疫可信验证技术提高系统自身安全防护能力，无法实现积极主动防御。 | 低 |
| 6 | 安全计算环境 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 恶意攻击 | 用户名和口令安全强度有限，如果未采用双因素认证，一旦用户名和口令被嗅探和泄露，将再没有其它技术进行身份鉴别，存在非授权访问的风险。 | 中 |
| 7 | 未重命名或删除默认账户。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 恶意攻击 | 恶意人员可能利用默认账户对系统进行试探攻击，存在潜在的安全隐患。 | 中 |
| 8 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 越权或滥用 | 恶意用户可能通过修改用户权限等方法，非授权访问重要信息资源，存在潜在的安全隐患。 | 低 |
| 9 | 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。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 恶意攻击 | 无可信链和可信验证，不能通过主动免疫可信验证技术提高系统自身安全防护能力，不能实现积极主动防御。 | 低 |
| 10 | 未采用校验技术或密码技术保证重要审计数据和重要配置数据在存储过程中的完整性。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 篡改 | 可能导致重要数据在存储过程中被恶意篡改，影响信息系统的正常运行。 | 中 |
| 11 | 未使用备份文件进行过备份恢复测试。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、业务数据、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 软硬件故障 | 一旦出现故障，可能由于各种原因无法利用备份数据进行恢复，造成重要数据丢失。 | 中 |
| 12 | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、业务数据、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 物理环境影响 | 如机房遭受严重破坏，可能导致部分数据丢失。 | 中 |
| 13 | 未在远程管理云平台中设备时，在管理终端和云平台间建立双向身份验证机制。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、业务数据、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 恶意攻击 | 可能导致攻击者不可信管理终端接入，或者攻击者通过钓鱼或伪造云计算平台服务界面的形式诱骗管理员提供敏感数据，导致管理终端和云计算平台间通信被劫持或伪造。 | 中 |
| 14 | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、业务数据、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 恶意攻击 | 恶意用户可能通过获取虚拟机管理器权限或修改虚拟机管理权限等方式，非授权新建或重启虚拟机，存在潜在的安全隐患。 | 中 |
| 15 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、业务数据、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 越权或滥用 | 可能导致虚拟机镜像、快照中可能存在的敏感资源被攻击者非法访问，使敏感信息遭遇泄漏。 | 中 |
| 16 | 未采用校验技术或密码技术保证重要审计数据在传输过程中的完整性。 | H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、飞塔防火墙A、飞塔防火墙B、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 篡改 | 可能导致重要数据在传输过程中被攻击者劫持、篡改，使重要数据的完整性遭到破坏。 | 中 |
| 17 | 未采用校验技术或密码技术保证重要业务数据在存储过程中的完整性。 | 业务数据 | 篡改 | 可能导致重要数据在存储过程中被恶意篡改，影响信息系统的正常运行。 | 中 |
| 18 | 未采用密码技术保证重要业务数据在存储过程中的保密性。 | 业务数据 | 敏感信息泄露 | 可能导致重要数据在存储过程中被攻击者直接盗用，使私密信息遭遇泄漏。 | 中 |
| 19 | 未配置口令有效期策略。 | CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02 | 恶意攻击 | 账户口令可能被长时间使用，恶意人员可通过猜解或暴力破解的方式获取账户口令，存在非授权访问的风险。 | 中 |
| 20 | 未配置登录连接超时策略。 | CloudOS1、CloudOS2、CloudOS3 | 无作为或操作失误 | 设备易被非授权人员恶意操作，存在非授权访问的风险。 | 中 |
| 21 | 未部署主机入侵防护软件，无法对主机重要节点进行入侵行为进行检查、限制并报警。 | CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2 | 恶意攻击 | 无法及时发现入侵行为，不便于对入侵行为进行分析并迅速响应。 | 中 |
| 22 | 未安装防恶意代码软件，无法识别入侵和病毒行为，并将其有效阻断。 | CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03 | 恶意攻击 | 可能导致木马、病毒等恶意代码程序通过网络、存储介质对生产操作系统进行传染和破坏，对系统稳定和数据安全造成影响。 | 中 |
| 23 | 安全管理中心 | 未限制网络设备、安全设备、服务器等仅通过堡垒机进行运维管理，并对系统管理员的操作进行审计。 | 安全管理中心 | 管理不到位 | 无法对安全事件进行追溯，同时无法及时了解设备实际运行状况以及存在的安全隐患。 | 中 |
| 24 | 未限制网络设备、安全设备、服务器等仅通过堡垒机进行运维管理，并对安全管理员的操作进行审计。 | 安全管理中心 | 管理不到位 | 无法对安全事件进行追溯，同时无法及时了解设备实际运行状况以及存在的安全隐患。 | 中 |
| 25 | 未采取措施对安全策略、恶意代码、补丁升级等进行统一集中管理。 | 安全管理中心 | 管理不到位 | 无法对保护对象进行统一监视和控制，当安全事件发生时无法及时对威胁源进行阻断和干预。 | 中 |
| 26 | 安全管理制度 | 未定期对安全管理制度进行论证、审定以及修订。 | 制度或记录类文档 | 管理不到位 | 可能导致安全管理体系与现实情况不符，导致管理文档无法落地。 | 中 |
| 27 | 安全建设管理 | 未组织相关部分和有关专家对安全方案进行论证和审查。 | 制度或记录类文档 | 管理不到位 | 可能存在安全策略缺乏合理性和可行性，导致信息系统安全防御能力缺乏完整性、系统性，不足以满足业务发展需要。 | 中 |
| 28 | 该系统未使用密码产品，未采购和使用国家密码主管部门要求的密码产品。 | 制度或记录类文档 | 管理不到位 | 可能存在安全隐患，导致保护机制失效或恶意人员利用产品自身漏洞攻击信息系统。 | 中 |
| 29 | 未对源代码进行审计工作，并出具相关审计报告。 | 制度或记录类文档 | 管理不到位 | 可能存在后门未在上线前被发现及处理。 | 中 |
| 30 | 未聘请第三方工程监理控制项目的实施过程。 | 制度或记录类文档 | 管理不到位 | 可能导致工程实施缺少组织性，工程实施管理不到位。 | 中 |
| 31 | 安全测试未包含密码相关安全性测试内容。 | 制度或记录类文档 | 管理不到位 | 安全隐患可能在系统上线运行前未被发现并作出相应的处理。 | 中 |
| 32 | 安全运维管理 | 未建立介质管理制度对介质进行控制和保护，也未指定专人或专门的部门对介质进行管理并定期清算盘点。 | 制度或记录类文档 | 管理不到位 | 可能导致介质被未授权人员访问，导致系统敏感信息泄露等。 | 中 |
| 33 | 未对介质在物理传输过程中的人员选择、打包、交付等进行控制，也未对介质的归档和查询等进行登记记录。 | 制度或记录类文档 | 管理不到位 | 可能导致归档介质的丢失，而不能及时发现，使介质的安全管理不到位。 | 中 |
| 34 | 系统未使用密码产品，未遵循密码相关国家标准和行业标准。 | 制度或记录类文档 | 管理不到位 | 密码使用管理不到位，存在违反国家政策的风险。 | 中 |
| 35 | 未建立密码使用管理制度，未使用符合国家密码管理规定的密码技术和产品。 | 制度或记录类文档 | 管理不到位 | 导致信息系统所使用的密码密钥及密码设备等管理不到位，存在违反国家政策的风险。 | 中 |
| 36 | 未建立终止变更并从失败变更中恢复的程序。 | 制度或记录类文档 | 管理不到位 | 可能在变更过程中或变更后出现问题的情况下，存在无法回退的风险。 | 中 |
| 37 | 未定期对原有的应急预案重新评估并定期修订完善。 | 制度或记录类文档 | 管理不到位 | 未及时更新应急预案，导致使用时出现错误或导致无法在规定时间内完成应急工作。 | 中 |

# 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** |
| 私有云 | 0 | 33 | 4 | 76.59 |

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3级要求，经对私有云的安全保护状况进行综合分析评价后，等级测评结论如下：

私有云，本次等级测评的综合得分为76.59，但存在中等级安全风险，等级测评结论为中。

*…………………………本页结束，以下为空白…………………………*

# 安全问题整改建议

**表 7‑1安全问题整改建议**

| **序号** | **安全类** | **安全问题** | **关联资产** | **整改建议** |
| --- | --- | --- | --- | --- |
| 1 | 安全物理环境 | 未采取措施对关键设备实施电磁屏蔽防护。 | 物理机房 | 建议采取电磁屏蔽措施，如使用电磁屏蔽机房、电磁屏蔽机柜等，对关键设备进行电磁屏蔽防护，以保证关键设备的保密性。 |
| 2 | 安全通信网络 | 未基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 | 安全通信网络 | 建议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。 |
| 3 | 安全区域边界 | 未采取措施对非授权设备私自连入内部网络的行为进行检查和限制。 | 互联网边界、服务器边界 | 建议部署准入控制系统防范非法内联行为。 |
| 4 | 未采取措施针对网络访问的数据流量实现基于应用协议和应用内容的访问控制。 | 互联网边界、服务器边界 | 建议在网络边界处部署应用层防护设备，并开启内容过滤策略防范应用层面的攻击。 |
| 5 | 未采取措施基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 | 互联网边界、服务器边界 | 建议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。 |
| 6 | 安全计算环境 | 未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 建议采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，并且其中一种鉴别技术为密码技术，如：数字证书、动态口令等。 |
| 7 | 未重命名或删除默认账户。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 建议重命名或删除默认账户。 |
| 8 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 建议对资源进行严格划分，并对重要主体和客体进行分级标记，形成完整的资源分级和访问权限控制结构体系，依据安全标记控制主体对信息资源的访问。 |
| 9 | 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。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 建议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。 |
| 10 | 未采用校验技术或密码技术保证重要审计数据和重要配置数据在存储过程中的完整性。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 建议在重要审计数据和重要配置数据存储时，采用经国家密码主管部门认可的校验技术或密码技术，保证其在存储过程中数据的完整性。 |
| 11 | 未使用备份文件进行过备份恢复测试。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、业务数据、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 建议定期对备份的数据进行恢复测试，确保在出现数据破坏时，可利用备份数据进行恢复，并妥善保存相关记录。 |
| 12 | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、业务数据、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 建议利用通信网络将重要数据实时传送至备用场地。 |
| 13 | 未在远程管理云平台中设备时，在管理终端和云平台间建立双向身份验证机制。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、业务数据、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 建议在远程管理云平台中设备时，在管理终端和云平台间建立双向身份验证机制。 |
| 14 | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、业务数据、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 建议采取措施对非授权新建虚拟机或者重新启用虚拟机等进行检测并告警。 |
| 15 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | CAS平台、CloudOS平台、SNA平台、H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、综合日志审计系统、飞塔防火墙A、飞塔防火墙B、业务数据、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 建议采取密码技术或其他技术手段对虚拟机镜像、快照中敏感资源进行防护。 |
| 16 | 未采用校验技术或密码技术保证重要审计数据在传输过程中的完整性。 | H3C防火墙A、H3C防火墙B、威胁感知大数据平台、帕拉迪堡垒机A、帕拉迪堡垒机B、服务器防火墙、深信服上网行为管理A、深信服上网行为管理B、飞塔防火墙A、飞塔防火墙B、CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、亚信安全服务器深度安全防护系统、Leaf交换机A、Leaf交换机B、Spine交换机A、Spine交换机B、核心交换机A、核心交换机B | 建议采用校验码技术或密码技术保证重要审计数据在传输过程中的完整性。 |
| 17 | 未采用校验技术或密码技术保证重要业务数据在存储过程中的完整性。 | 业务数据 | 建议在重要业务数据存储时，采用经国家密码主管部门认可的校验技术或密码技术，保证其在存储过程中数据的完整性。 |
| 18 | 未采用密码技术保证重要业务数据在存储过程中的保密性。 | 业务数据 | 建议对重要业务数据采用经国家密码主管部门认可的密码技术，保证其在存储过程中数据的保密性。 |
| 19 | 未配置口令有效期策略。 | CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02 | 建议配置口令的有效期策略，定期更换口令，防止口令被轻易破解。 |
| 20 | 未配置登录连接超时策略。 | CloudOS1、CloudOS2、CloudOS3 | 建议配置登录连接超时策略，严格限制登录超时时间。 |
| 21 | 未部署主机入侵防护软件，无法对主机重要节点进行入侵行为进行检查、限制并报警。 | CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2 | 建议安装主机层入侵防护软件，对入侵的行为进行检测，并在发生严重入侵事件时提供报警。 |
| 22 | 未安装防恶意代码软件，无法识别入侵和病毒行为，并将其有效阻断。 | CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03 | 建议安装防恶意代码软件，抵御各类恶意程序的侵害，对操作系统安全形成技术保护，并保证防恶意代码软件的规则库能够及时更新。 |
| 23 | 安全管理中心 | 未限制网络设备、安全设备、服务器等仅通过堡垒机进行运维管理，并对系统管理员的操作进行审计。 | 安全管理中心 | 建议限制网络设备、安全设备、服务器仅通过堡垒机进行运维管理，并对系统管理员的操作进行审计。 |
| 24 | 未限制网络设备、安全设备、服务器等仅通过堡垒机进行运维管理，并对安全管理员的操作进行审计。 | 安全管理中心 | 建议限制网络设备、安全设备、服务器等仅通过堡垒机进行运维管理，并对安全管理员的操作进行审计。 |
| 25 | 未采取措施对安全策略、恶意代码、补丁升级等进行统一集中管理。 | 安全管理中心 | 建议采取措施对安全策略、恶意代码防范策略、系统或设备的补丁升级进行统一管理。 |
| 26 | 安全管理制度 | 未定期对安全管理制度进行论证、审定以及修订。 | 制度或记录类文档 | 建议定期对安全管理制度进行论和审定，并根据审查结果对安全管理制度进行修订。 |
| 27 | 安全建设管理 | 未组织相关部分和有关专家对安全方案进行论证和审查。 | 制度或记录类文档 | 建议组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。 |
| 28 | 该系统未使用密码产品，未采购和使用国家密码主管部门要求的密码产品。 | 制度或记录类文档 | 建议采购和使用符合国家密码主管部门的要求的密码产品。 |
| 29 | 未对源代码进行审计工作，并出具相关审计报告。 | 制度或记录类文档 | 建议对源代码进行审计并出具相关审计报告。 |
| 30 | 未聘请第三方工程监理控制项目的实施过程。 | 制度或记录类文档 | 建议聘请第三方工程监理的方式控制项目的实施过程，保障项目质量。 |
| 31 | 安全测试未包含密码相关安全性测试内容。 | 制度或记录类文档 | 建议对系统开展密码应用安全性测试或测评工作并遵照国家密码管理局印发的有关规定执行。 |
| 32 | 安全运维管理 | 未建立介质管理制度对介质进行控制和保护，也未指定专人或专门的部门对介质进行管理并定期清算盘点。 | 制度或记录类文档 | 建议建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定，并指定专人或专门的部分对介质进行管理并定期进行清算盘点。 |
| 33 | 未对介质在物理传输过程中的人员选择、打包、交付等进行控制，也未对介质的归档和查询等进行登记记录。 | 制度或记录类文档 | 建议对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，对介质归档和查询等进行登记记录。 |
| 34 | 系统未使用密码产品，未遵循密码相关国家标准和行业标准。 | 制度或记录类文档 | 建议使用的密码遵循密码相关的国家标准和行业标准。 |
| 35 | 未建立密码使用管理制度，未使用符合国家密码管理规定的密码技术和产品。 | 制度或记录类文档 | 建议建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。 |
| 36 | 未建立终止变更并从失败变更中恢复的程序。 | 制度或记录类文档 | 建议建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。 |
| 37 | 未定期对原有的应急预案重新评估并定期修订完善。 | 制度或记录类文档 | 建议定期对应急预案进行审查和根据实际情况更新的内容，并定期进行修订完善。 |

【正文结束】

1. 被测对象资产
   1. 物理机房

**附录A 表‑1物理机房**

| **序号** | **机房名称** | **物理位置** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- |
| 1 | 物理机房 | 浙江省杭州市西湖区古荡街道文三西路52号15楼 | 关键 | 1 |

* 1. 网络设备

**附录A 表‑2网络设备**

| **序号** | **设备名称** | **是否虚拟设备** | **系统及版本** | **品牌及型号** | **用途** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 核心交换机A | 否 | Version 7.1.045, Release 7184 | H3C S10506 | 核心数据交换 | 关键 | 1 |
| 2 | Spine交换机A | 否 | Version 7.1.070, Release 6607 | H3C S9850 | 数据交换 | 关键 | 1 |
| 3 | Leaf交换机A | 否 | Version 7.1.070, Release 2702 | H3C S6800 | 数据交换 | 关键 | 1 |
| 4 | 管理交换机 | 否 | Version 7.1.070, Release 1312 | H3C S5560-34C-EI | 数据交换 | 一般 | 纯二层交换机，不进行管理 |
| 5 | FC光纤交换机 | 否 | Version 5.20.99, Release 1022 | SN3000B | 存储数据交换 | 一般 | 纯二层交换机，不进行管理 |
| 6 | 外联线路接入交换机 | 否 | Version 5.20.13, Release 1112 | H3C S5110-28P | 外链线路接入 | 一般 | 纯二层交换机，不进行管理 |
| 7 | 核心交换机B | 否 | Version 7.1.045, Release 7184 | H3C S10506 | 核心数据交换 | 关键 | 1 |
| 8 | Spine交换机B | 否 | Version 7.1.070, Release 6607 | H3C S9850 | 数据交换 | 关键 | 1 |
| 9 | Leaf交换机B | 否 | Version 7.1.070, Release 2702 | H3C S6800 | 数据交换 | 关键 | 1 |

* 1. 安全设备

**附录A 表‑3安全设备**

| **序号** | **设备名称** | **是否虚拟设备** | **系统及版本** | **品牌及型号** | **用途** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 飞塔防火墙A | 否 | V6.4.3 build1778(GA) | 飞塔FG-600E | 访问控制、入侵防护、恶意代码防护 | 关键 | 1 |
| 2 | 飞塔防火墙B | 否 | V6.4.3 build1778(GA) | 飞塔FG-600E | 访问控制、入侵防护、恶意代码防护 | 关键 | 1 |
| 3 | 深信服上网行为管理A | 否 | AC11.9R1 | 深信服AC-3300-HY | 行为审计和外联控制 | 重要 | 1 |
| 4 | 深信服上网行为管理B | 否 | AC11.9R1 | 深信服AC-3300-HY | 行为审计和外联控制 | 重要 | 1 |
| 5 | 帕拉迪堡垒机A | 否 | ST00001B090 | 帕拉迪Core4A-UTM | 安全运维 | 重要 | 1 |
| 6 | 帕拉迪堡垒机B | 否 | ST00001B090 | 帕拉迪Core4A-UTM | 安全运维 | 重要 | 1 |
| 7 | H3C防火墙A | 否 | Vesion 7.1.064,Release 9608P30 | H3C F5030-D | 东西向流量访问控制 | 重要 | 1 |
| 8 | H3C防火墙B | 否 | Vesion 7.1.064,Release 9608P30 | H3C F5030-D | 东西向流量访问控制 | 重要 | 1 |
| 9 | 综合日志审计系统 | 否 | E1107 | H3C CSAP-SA | 日志审计 | 重要 | 1 |
| 10 | 服务器防火墙 | 否 | AF8.0.35 | 深信服AF-1000 | 访问控制、入侵防护、恶意代码防护 | 关键 | 1 |
| 11 | 威胁感知大数据平台 | 否 | V5.4.26 | 迪普 | 威胁集中分析和报警 | 重要 | 1 |

* 1. 服务器/存储设备

**附录A 表‑4服务器/存储设备**

| **序号** | **设备名称** | **所属业务应用系统/平台名称** | **是否虚拟设备** | **操作系统及版本** | **数据库管理系统及版本** | **中间件及版本** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | CVK01 | / | 否 | Centos7.6 | / | / | 关键 | 1 |
| 2 | CVK02 | / | 否 | Centos7.6 | / | / | 关键 | 1 |
| 3 | CVK03 | / | 否 | Centos7.6 | / | / | 关键 | 1 |
| 4 | CVK04 | / | 否 | Centos7.6 | / | / | 关键 | 1 |
| 5 | CVK05 | / | 否 | Centos7.6 | / | / | 关键 | 1 |
| 6 | CloudOS1 | CloudOS平台 | 否 | Centos7.6 | / | / | 重要 | 1 |
| 7 | CloudOS2 | CloudOS平台 | 否 | Centos7.6 | / | / | 重要 | 1 |
| 8 | CloudOS3 | CloudOS平台 | 否 | Centos7.6 | / | / | 重要 | 1 |
| 9 | CVM01 | CAS平台 | 否 | Centos7.6 | / | / | 重要 | 1 |
| 10 | CVM02 | CAS平台 | 否 | Centos7.6 | / | / | 重要 | 1 |
| 11 | SDN01 | SNA平台 | 否 | H3Linux Release 1.1.2 | / | / | 重要 | 1 |
| 12 | SDN02 | SNA平台 | 否 | H3Linux Release 1.1.2 | / | / | 重要 | 1 |
| 13 | SDN03 | SNA平台 | 否 | H3Linux Release 1.1.2 | / | / | 重要 | 1 |
| 14 | 核心存储HEP-01 | / | 否 | / | / | / | 一般 | 1 |
| 15 | 核心存储HEP-02 | / | 否 | / | / | / | 一般 | 1 |

* 1. 终端设备

**附录A 表‑5终端设备**

| **序号** | **设备名称** | **是否虚拟设备** | **操作系统/控制软件及版本** | **用途** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 运维终端1 | 否 | Windows 10 | 运维管控 | 一般 | 1 |
| 2 | 运维终端2 | 否 | Windows 10 | 运维管控 | 一般 | 1 |
| 3 | 运维终端 | 否 | Windows 10 | 运维管控 | 一般 | 4 |

* 1. 其他系统或设备

该系统不涉及其他系统或设备。

**附录A 表‑6其他设备**

| **序号** | **设备名称** | **是否虚拟设备** | **操作系统/控制软件及版本** | **设备类别/用途** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| / | / | / | / | / | / | / |

* 1. 系统管理软件/平台

**附录A 表‑7系统管理软件/平台**

| **序号** | **系统管理软件/平台名称** | **所在设备名称** | **版本** | **主要功能** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 亚信安全服务器深度安全防护系统 | / | 10.0.5129 | 主机层恶意代码防护 | 重要 | 1 |

该系统为浙江省建设投资集团股份有限公司提供云计算虚拟资源服务，且不提供租户侧的数据库服务，均由租户自行搭建和运维管理。

* 1. 业务应用系统/平台

**附录A 表‑8业务应用系统/平台**

| **序号** | **业务应用系统/平台名称** | **主要功能** | **业务应用软件及版本** | **开发厂商** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | CloudOS平台 | 用于私有云平台创建网络及虚拟机。 | / | 新华三技术有限公司 | 关键 | 1 |
| 2 | CAS平台 | 用于私有云平台底层资源创建和控制。 | / | 新华三技术有限公司 | 关键 | 1 |
| 3 | SNA平台 | 用于私有云平台控制网络虚拟化功能。 | / | 新华三技术有限公司 | 关键 | 1 |

* 1. 数据资源

**附录A 表‑9数据资源**

| **序号** | **数据类别** | **所属业务应用** | **安全防护需求** | **重要程度** |
| --- | --- | --- | --- | --- |
| 1 | 业务数据 | CloudOS平台、CAS平台、SNA平台 | 保密性、完整性、备份和恢复 | 重要 |

* 1. 密码产品

该系统不涉及密码产品。

**附录A 表‑10密码产品**

| **序号** | **产品/模块名称** | **生产厂商** | **商密型号** | **密码算法** | **用途** | **重要程度** |
| --- | --- | --- | --- | --- | --- | --- |
| / | / | / | / | / | / | / |

* 1. 安全相关人员

**附录A 表‑11安全相关人员**

| **序号** | **姓名** | **岗位/角色** | **联系方式** | **所属单位** |
| --- | --- | --- | --- | --- |
| 1 | 郑辉 | 安全管理员 | 0571-88260691 | 浙江省建设投资集团股份有限公司 |
| 2 | 李明明 | 系统管理员/审计管理员 | 13626815240 | 浙江省建设投资集团股份有限公司 |
| 3 | 关俭 | 系统管理员/应用管理员 | 13588759167 | 浙江省建设投资集团股份有限公司 |
| 4 | 张振 | 审计管理员 | 13454113928 | 浙江省建设投资集团股份有限公司 |
| 5 | 赖晋宝 | 网络管理员/机房管理员 | 13758191743 | 浙江省建设投资集团股份有限公司 |
| 6 | 李任华 | 安全管理员 | 19805812519 | 浙江省建设投资集团股份有限公司 |

* 1. 安全管理文档

**附录A 表‑12安全管理文档**

| **序号** | **文档名称** | **主要内容** |
| --- | --- | --- |
| 1 | 《ZJJT-XX-01-2020信息安全策略》 | 包含总体适用范围、信息安全职责等。 |
| 2 | 《ZJJT-XX-02-2020网络与信息安全管理制度》 | 包含人员管理、信息安全建设、信息安全事件严重程度级别划分等。 |
| 3 | 《ZJJT-XX-04-2020数据备份与恢复管理制度》 | 包含数据备份及恢复措施等。 |
| 4 | 《ZJJT-XX-05-2020机房管理制度》 | 包含机房进出管理、机房守则、机房建设等。 |
| 5 | 《ZJJT-XX-06-2020信息资产管理制度》 | 包含信息资产分类、处理管理办法。 |
| 6 | 《ZJJT-XX-10-2020信息安全员管理制度》 | 包含信息安全员聘用和管理、信息安全教育培训和考核等。 |
| 7 | 《ZJJT-XX-11-2020外部人员访问控制管理制度》 | 包含外部人员访问控制与管理等。 |
| 8 | 《ZJJT-XX-12-2020信息安全人员培训和教育管理制度》 | 包含培训要求、培训内容等。 |
| 9 | 《ZJJT-XX-16-2020信息系统安全补丁管理制度》 | 包含补丁更新、补丁测试等。 |
| 10 | 《ZJJT-XX-17-2020信息安全机构管理制度》 | 包含安全管理员、安全审计员等各岗位职责以及各岗位人员统计。 |
| 11 | 《ZJJT-XX-18-2020信息系统管理授权审批管理制度》 | 包含信息系统的授权审批流程。 |
| 12 | 《ZJJY-XX-21-2020信息安全产品采购管理制度》 | 包含设备采购、软件采购等采购管理制度。 |
| 13 | 《ZJJY-XX-22-2020信息安全外包运维管理制度》 | 包含外包服务合同管理要求、外包服务监控与评价等。 |
| 14 | 《ZJJY-XX-23-2020信息系统工程实施管理制度》 | 包含工程实施管理、实施人员行为准则等。 |
| 15 | 《aZJJT-XXBG-02-2020-B网络与信息系统安全运行月报》 | 网络与信息系统安全运行月报。 |
| 16 | 《ZJJT-XX-03-2020计算机病毒防治管理制度》 | 包含计算机病毒防治管理、指定计算机病毒防治工作的管理部门以及具体职责。 |
| 17 | 《ZJJT-XX-07-2020信息设备运维管理制度》 | 包含网络管理员具体职责、运维操作管理等。 |
| 18 | 《ZJJT-XX-08-2020信息系统巡检管理制度》 | 包含巡检的方式、过程等管理办法。 |
| 19 | 《ZJJT-XX-09-2020信息网络管理制度》 | 包含网络接入管理、网络运行管理等。 |
| 20 | 《ZJJT-XX-13-2020网络设备安全管理制度》 | 包含网络设备/安全设备安全管理、系统升级和补丁安全等。 |
| 21 | 《ZJJT-XX-14-2020业务应用系统软件安全管理制度》 | 包含业务应用系统软件的具体配置要求等。 |
| 22 | 《ZJJT-XX-15-2020计算机网络系统测试管理制度》 | 包含计算机网络系统测试要求、测试实施步骤、测试方案等。 |
| 23 | 《ZJJY-XX-19-2020系统安全管理制度》 | 包含用户账户管理、文件系统管理、系统安全管理、数据库管理、日志安全管理等。 |
| 24 | 《ZJJY-XX-20-2020软件开发管理制度》 | 包含外包软件开发管理、信息系统安全整体测试等。 |
| 25 | 《ZJJY-XX-24-2020信息系统数据质量管理制度》 | 包含数据质量管理职责、检查与考核等。 |
| 26 | 《aZJJT-XXBG-02-2020-A网络与信息安全事故情况报告表》 | 包含网络与信息安全事故的记录表单。 |
| 27 | 《aZJJT-XXBG-02-2020-C网络与重要信息系统敏感时期安全运行日报》 | 包含网络与重要信息系统敏感时期的运行日报记录内容。 |
| 28 | 《aZJJT-XXBG-02-2020-D离岗保密承诺书》 | 包含离岗保密协议相关内容。 |
| 29 | 《aZJJT-XXBG-02-2020-F保密协议(供应商)》 | 包含供应商保密协议相关内容。 |
| 30 | 《aZJJT-XXBG-03-2020-A恶意代码分析报告》 | 包含恶意代码分析相关内容。 |
| 31 | 《aZJJT-XXBG-03-2020-B恶意代码特征库更新记录表》 | 包含恶意代码规则库更新记录表单。 |
| 32 | 《aZJJT-XXBG-07-2020-A系统（设备）操作记录表》 | 包含系统和设备操作记录内容。 |
| 33 | 《aZJJT-XXBG-07-2020-C配置变更记录表》 | 包含系统变更相关记录内容。 |
| 34 | 《aZJJT-XXBG-08-2020-A巡视记录表》 | 包含巡检记录相关内容。 |
| 35 | 《aZJJT-XXBG-08-2020-B设备巡查记录表》 | 包含设备巡检记录表单内容。 |
| 36 | 《aZJJT-XXBG-10-2020-A人员离岗交接清单》 | 包含人员离岗时交接的内容清单。 |
| 37 | 《aZJJT-XXBG-10-2020-C保密协议》 | 包含建投集团保密协议内容。 |
| 38 | 《aZJJT-XXBG-11-2020-A外部人员访问申请授权表》 | 包含外部人员访问申请的相关记录内容。 |
| 39 | 《aZJJT-XXBG-12-2020-培训记录表》 | 包含培训有关记录表单。 |
| 40 | 《aZJJT-XXBG-16-2020系统补丁更新记录表》 | 包含系统补丁更新记录相关内容。 |
| 41 | 《a机房出入登记表》 | 包含机房出入登记相关内容。 |
| 42 | 《网络安全培训计划》 | 包含安全培训计划、方案、时间、地点等内容。 |
| 43 | 《03浙江省建设投资集团股份有限公司私有云系统应急预案》 | 包含私有云系统相关应急预案方案。 |
| 44 | 《04浙江省建设投资集团股份有限公司私有云系统应急演练记录》 | 包含私有云系统应急演练相关记录。 |
| 45 | 《关于成立信息安全管理工作领导小组的通知》 | 包含信息安全领导小组成立的红头文件的详细内容。 |
| 46 | 《私有云安全设计方案》 | 包含私有云安全方案设计的相关内容。 |
| 47 | 《产品选型测试记录表》 | 包含产品选型测试相关记录表单。 |
| 48 | 《私有云测试验收方案》 | 包含私有云系统验收测试方法、验收测试内容、验收测试预期结果。 |
| 49 | 《浙江省建设投资集团股份有限公司私有云风险评估报告》 | 包含私有云的风险评估过程、内容和结果。 |
| 50 | 《私有云系统实施方案》 | 包含私有云实施建设的全部流程，以及合理建议。 |
| 51 | 《技术培训记录》 | 包含运行维护人员相关培训情况，包括培训内容、培训时间、参与人员等。 |
| 52 | 《私有云操作手册》 | 包含私有云系统日常运行维护以及详细操作指导。 |
| 53 | 《浙江省建设投资集团股份有限公司安全整改报告》 | 包含私有云系统针对风评的结果，进行安全整改的记录过程。 |
| 54 | 《华三交换机操作手册》 | 包含华三交换机详细的操作流程及命令更能等。 |
| 55 | 《深信服防火墙操作手册》 | 包含深信服防火墙详细的操作流程及功能配置。 |
| 56 | 《运维审批记录》 | 包含运维开通，运维工具，运维权限分配、审核等相关记录。 |
| 57 | 《漏洞修补记录表》 | 包含系统和设备漏洞修补的维护记录内容。 |
| 58 | 《技能考核记录》 | 包含对不同岗位的人员技能考核记录。 |

1. 上次测评问题整改情况说明

浙江省建设投资集团股份有限公司私有云系统为首次进行网络安全等级保护测评。

*…………………………本页结束，以下为空白…………………………*

1. 单项测评结果汇总
   1. 安全物理环境

**附录C 表‑1安全物理环境单项测评结果汇总表（安全通用要求部分）**

| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **物理位置选择** | **物理访问控制** | **防盗窃和防破坏** | **防雷击** | **防火** | **防水和防潮** | **防静电** | **温湿度控制** | **电力供应** | **电磁防护** |
| 1 | 物理机房 | 符合 | 2 | 1 | 3 | 2 | 3 | 3 | 2 | 1 | 3 | 1 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**附录C 表‑2安全物理环境单项测评结果汇总表（安全扩展要求部分）**

| **序号** | **测评对象** | **符合情况** | **安全扩展要求** |
| --- | --- | --- | --- |
| **基础设施位置（云计算）** |
| 1 | 物理机房 | 符合 | 1 |
| 部分符合 | 0 |
| 不符合 | 0 |
| 不适用 | 0 |

* 1. 安全通信网络

**附录C 表‑3安全通信网络单项测评结果汇总表（安全通用要求部分）**

| **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 |

**附录C 表‑4安全通信网络单项测评结果汇总表（安全扩展要求部分）**

| **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 | 5 |
| 部分符合 | 0 |
| 不符合 | 0 |
| 不适用 | 0 |

* 1. 安全区域边界

**附录C 表‑5安全区域边界单项测评结果汇总表（安全通用要求部分）**

| **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 | 服务器边界 | 符合 | 2 | 4 | 4 | 1 | 4 | 0 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 |
| 不适用 | 1 | 0 | 0 | 1 | 0 | 0 |
| 2 | 互联网边界 | 符合 | 2 | 4 | 4 | 1 | 4 | 0 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 |
| 不适用 | 1 | 0 | 0 | 1 | 0 | 0 |

**附录C 表‑6安全区域边界单项测评结果汇总表（安全扩展要求部分）**

| **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 | 服务器边界 | 符合 | 2 | 4 | 2 |
| 部分符合 | 0 | 0 | 0 |
| 不符合 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 |
| 2 | 互联网边界 | 符合 | 2 | 4 | 2 |
| 部分符合 | 0 | 0 | 0 |
| 不符合 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 |

* 1. 安全计算环境
     1. 网络设备

**附录C 表‑7安全计算环境单项测评结果汇总表（安全通用要求部分）**

| **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 | Leaf交换机A | 符合 | 3 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 1 | 0 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 2 | 1 | 0 | 0 | 0 | 0 | 2 | 2 |
| 2 | Leaf交换机B | 符合 | 3 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 1 | 0 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 2 | 1 | 0 | 0 | 0 | 0 | 2 | 2 |
| 3 | Spine交换机A | 符合 | 3 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 1 | 0 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 2 | 1 | 0 | 0 | 0 | 0 | 2 | 2 |
| 4 | Spine交换机B | 符合 | 3 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 1 | 0 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 2 | 1 | 0 | 0 | 0 | 0 | 2 | 2 |
| 5 | 核心交换机A | 符合 | 3 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 1 | 0 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 2 | 1 | 0 | 0 | 0 | 0 | 2 | 2 |
| 6 | 核心交换机B | 符合 | 3 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 1 | 0 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 2 | 1 | 0 | 0 | 0 | 0 | 2 | 2 |

**附录C 表‑8安全计算环境单项测评结果汇总表（安全扩展要求部分）**

| **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 | 核心交换机A | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 2 | 核心交换机B | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 3 | Leaf交换机A | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 4 | Leaf交换机B | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 5 | Spine交换机A | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 6 | Spine交换机B | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |

* + 1. 安全设备

**附录C 表‑9安全计算环境单项测评结果汇总表（安全通用要求部分）**

| **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 | H3C防火墙A | 符合 | 3 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 1 | 0 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 2 | 1 | 0 | 0 | 0 | 0 | 2 | 2 |
| 2 | H3C防火墙B | 符合 | 3 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 1 | 0 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 2 | 1 | 0 | 0 | 0 | 0 | 2 | 2 |
| 3 | 威胁感知大数据平台 | 符合 | 3 | 5 | 4 | 5 | 0 | 0 | 0 | 2 | 0 | 0 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 2 | 2 |
| 4 | 帕拉迪堡垒机A | 符合 | 3 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 0 | 0 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 2 | 1 | 0 | 0 | 0 | 1 | 2 | 2 |
| 5 | 帕拉迪堡垒机B | 符合 | 3 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 0 | 0 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 2 | 1 | 0 | 0 | 0 | 1 | 2 | 2 |
| 6 | 服务器防火墙 | 符合 | 3 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 0 | 0 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 2 | 1 | 0 | 0 | 0 | 1 | 2 | 2 |
| 7 | 深信服上网行为管理A | 符合 | 3 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 1 | 0 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 2 | 1 | 0 | 0 | 0 | 0 | 2 | 2 |
| 8 | 深信服上网行为管理B | 符合 | 3 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 1 | 0 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 2 | 1 | 0 | 0 | 0 | 0 | 2 | 2 |
| 9 | 综合日志审计系统 | 符合 | 3 | 5 | 4 | 4 | 0 | 0 | 1 | 2 | 0 | 0 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 2 | 1 | 0 | 0 | 0 | 1 | 2 | 2 |
| 10 | 飞塔防火墙A | 符合 | 3 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 1 | 0 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 2 | 1 | 0 | 0 | 0 | 0 | 2 | 2 |
| 11 | 飞塔防火墙B | 符合 | 3 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 1 | 0 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 2 | 1 | 0 | 0 | 0 | 0 | 2 | 2 |

**附录C 表‑10安全计算环境单项测评结果汇总表（安全扩展要求部分）**

| **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 | H3C防火墙A | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 2 | H3C防火墙B | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 3 | 威胁感知大数据平台 | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 4 | 帕拉迪堡垒机A | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 5 | 帕拉迪堡垒机B | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 6 | 服务器防火墙 | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 7 | 深信服上网行为管理A | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 8 | 深信服上网行为管理B | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 9 | 综合日志审计系统 | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 10 | 飞塔防火墙A | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 11 | 飞塔防火墙B | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |

* + 1. 服务器和终端

**附录C 表‑11安全计算环境单项测评结果汇总表（安全通用要求部分）**

| **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 | CloudOS1 | 符合 | 1 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 2 | 2 | 0 |
| 部分符合 | 2 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |
| 2 | CloudOS2 | 符合 | 1 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 2 | 2 | 0 |
| 部分符合 | 2 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |
| 3 | CloudOS3 | 符合 | 1 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 2 | 2 | 0 |
| 部分符合 | 2 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |
| 4 | CVK01 | 符合 | 2 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 2 | 2 | 0 |
| 部分符合 | 1 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |
| 5 | CVK02 | 符合 | 2 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 2 | 2 | 0 |
| 部分符合 | 1 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |
| 6 | CVK03 | 符合 | 2 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 2 | 2 | 0 |
| 部分符合 | 1 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |
| 7 | CVK04 | 符合 | 2 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 2 | 2 | 0 |
| 部分符合 | 1 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |
| 8 | CVK05 | 符合 | 2 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 2 | 2 | 0 |
| 部分符合 | 1 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |
| 9 | CVM01 | 符合 | 2 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 2 | 2 | 0 |
| 部分符合 | 1 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |
| 10 | CVM02 | 符合 | 2 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 2 | 2 | 0 |
| 部分符合 | 1 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |
| 11 | SDN01 | 符合 | 3 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 2 | 2 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |
| 12 | SDN02 | 符合 | 3 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 2 | 2 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |
| 13 | SDN03 | 符合 | 3 | 5 | 4 | 4 | 0 | 0 | 0 | 2 | 2 | 2 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |
| 14 | 运维终端1 | 符合 | 2 | 2 | 4 | 3 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| 不符合 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 不适用 | 2 | 4 | 0 | 2 | 0 | 0 | 1 | 1 | 3 | 1 | 2 |
| 15 | 运维终端2 | 符合 | 2 | 2 | 4 | 3 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| 不符合 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 不适用 | 2 | 4 | 0 | 2 | 0 | 0 | 1 | 1 | 3 | 1 | 2 |

**附录C 表‑12安全计算环境单项测评结果汇总表（安全扩展要求部分）**

| **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 | CloudOS1 | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 2 | CloudOS2 | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 3 | CloudOS3 | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 4 | CVK01 | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 5 | CVK02 | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 6 | CVK03 | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 7 | CVK04 | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 8 | CVK05 | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 9 | CVM01 | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 10 | CVM02 | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 11 | SDN01 | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 12 | SDN02 | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 13 | SDN03 | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 14 | 运维终端1 | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 15 | 运维终端2 | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |

* + 1. 系统管理软件/平台

**附录C 表‑13安全计算环境单项测评结果汇总表（安全通用要求部分）**

| **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 | 亚信安全服务器深度安全防护系统 | 符合 | 3 | 6 | 4 | 4 | 0 | 0 | 0 | 2 | 0 | 1 | 0 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 2 | 1 | 0 | 0 | 0 | 1 | 1 | 2 |

**附录C 表‑14安全计算环境单项测评结果汇总表（安全扩展要求部分）**

| **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 | 亚信安全服务器深度安全防护系统 | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |

* + 1. 业务应用系统/平台

**附录C 表‑15安全计算环境单项测评结果汇总表（安全通用要求部分）**

| **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 | CAS平台 | 符合 | 3 | 5 | 4 | 3 | 0 | 0 | 1 | 2 | 0 | 1 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 3 | 1 | 0 | 0 | 0 | 1 | 1 | 2 |
| 2 | CloudOS平台 | 符合 | 3 | 5 | 4 | 3 | 0 | 0 | 1 | 2 | 0 | 1 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 3 | 1 | 0 | 0 | 0 | 1 | 1 | 2 |
| 3 | SNA平台 | 符合 | 3 | 5 | 4 | 3 | 0 | 0 | 1 | 2 | 0 | 1 | 0 |
| 部分符合 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| 不符合 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 3 | 1 | 0 | 0 | 0 | 1 | 1 | 2 |

**附录C 表‑16安全计算环境单项测评结果汇总表（安全扩展要求部分）**

| **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 | CAS平台 | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 2 | CloudOS平台 | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 3 | SNA平台 | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |

* + 1. 数据资源

**附录C 表‑17安全计算环境单项测评结果汇总表（安全通用要求部分）**

| **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 | 业务数据 | 符合 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| 不符合 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| 不适用 | 4 | 7 | 4 | 6 | 1 | 1 | 0 | 0 | 0 | 1 | 2 |

**附录C 表‑18安全计算环境单项测评结果汇总表（安全扩展要求部分）**

| **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 | 业务数据 | 符合 | 0 | 2 | 2 | 2 | 4 | 3 | 2 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |

* + 1. 其他系统或设备

本次测评不包含“安全计算环境单项测评结果汇总表（安全通用要求部分）”。

* 1. 安全管理中心

**附录C 表‑19安全管理中心单项测评结果汇总表**

| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | **安全扩展要求** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **系统管理** | **审计管理** | **安全管理** | **集中管控** | **集中管控（云计算）** |
| 1 | 安全管理中心 | 符合 | 1 | 2 | 1 | 5 | 4 |
| 部分符合 | 1 | 0 | 1 | 0 | 0 |
| 不符合 | 0 | 0 | 0 | 1 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 |

* 1. 安全管理制度

**附录C 表‑20安全管理制度单项测评结果汇总表**

| **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 | 制度或记录类文档 | 符合 | 1 | 3 | 2 | 0 |
| 部分符合 | 0 | 0 | 0 | 0 |
| 不符合 | 0 | 0 | 0 | 1 |
| 不适用 | 0 | 0 | 0 | 0 |

* 1. 安全管理机构

**附录C 表‑21安全管理机构单项测评结果汇总表**

| **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 | 制度或记录类文档 | 符合 | 3 | 2 | 3 | 3 | 3 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 0 | 0 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 |

* 1. 安全管理人员

**附录C 表‑22安全管理人员单项测评结果汇总表**

| **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 | 制度或记录类文档 | 符合 | 3 | 2 | 3 | 4 |
| 部分符合 | 0 | 0 | 0 | 0 |
| 不符合 | 0 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 0 |

* 1. 安全建设管理

**附录C 表‑23安全建设管理单项测评结果汇总表（安全通用要求部分）**

| **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 | 制度或记录类文档 | 符合 | 4 | 2 | 2 | 0 | 2 | 2 | 1 | 3 | 3 | 3 |
| 部分符合 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 |
| 不符合 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| 不适用 | 0 | 0 | 0 | 7 | 0 | 0 | 0 | 0 | 0 | 0 |

**附录C 表‑24安全建设管理单项测评结果汇总表（安全扩展要求部分）**

| **类或方面** | **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）** |
| 安全建设管理 | 符合 | 0 | 3 |
| 部分符合 | 0 | 0 |
| 不符合 | 0 | 0 |
| 不适用 | 5 | 0 |

* 1. 安全运维管理

**附录C 表‑25安全运维管理单项测评结果汇总表（安全通用要求部分）**

| **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 | 制度或记录类文档 | 符合 | 3 | 3 | 0 | 4 | 2 | 10 | 2 | 2 | 0 | 2 | 3 | 4 | 3 | 4 |
| 部分符合 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 不符合 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 1 | 0 | 0 | 1 | 0 |
| 不适用 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**附录C 表‑26安全运维管理单项测评结果汇总表（安全扩展要求部分）**

| **类或方面** | **符合情况** | **安全扩展要求** |
| --- | --- | --- |
| **云计算环境管理（云计算）** |
| 安全运维管理 | 符合 | 1 |
| 部分符合 | 0 |
| 不符合 | 0 |
| 不适用 | 0 |

* 1. 其他安全要求指标

本次检测不包含其他安全要求指标。

*…………………………本页结束，以下为空白…………………………*

1. 单项测评结果记录
   1. 安全物理环境
      1. 安全通用要求部分
         1. 物理机房

**附录D 表‑1安全物理环境结果记录表（物理机房）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 机房建设位于杭州市西湖区文三西路52号浙江建投大厦15层，该建筑具备防震验收文档，具备良好的防震、防雨和防风的能力，机房内不存在雨水渗漏、墙体开裂等情况。 | 符合 |
| b)机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。 | 机房建设在杭州市西湖区文三西路52号浙江建投大厦15楼，不处于楼顶和地下室，整体地板下方进行了防渗水、防潮措施，机房周围没有用水设备通过，精密空调底部水管采用防水层与防水棉，并设置有漏水检测措施。 | 符合 |
| 物理访问控制 | 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。 | 机房出入口已配备电子门禁系统，并配置电子门禁卡，能够控制、鉴别和记录进入的人员，记录保存时间长达6个月，且具备《机房出入登记表》，记录计入机房人员的姓名、进出时间、进出事由等相关信息。 | 符合 |
| 防盗窃和防破坏 | a)应将设备或主要部件进行固定，并设置明显的不易除去的标识； | 机房的主要部件均固定在机架当中，采用螺丝进行固定，且各设备上均粘贴有不易除去机打标签，标注为建投集团资产卡。 | 符合 |
| b)应将通信线缆铺设在隐蔽安全处； | 机房采用桥架方式，将通信线缆铺设于机柜上方的走线架中。 | 符合 |
| 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。 | 机房部署有7个海康威视的监控摄像头，覆盖整个机房视角，机房具有专人值守的视频监控区，海康威视的视频硬盘共8块，每块5个T的空间大小，能保存6个月以上的回放时间，且每个机柜门需要输入对应密码才能打开。 | 符合 |
| 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； | 机房当中所有机柜和设备均通过接地线接入静电地板底部的铜排，再连入整个大楼接地系统。 | 符合 |
| 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。 | 浙江建投大厦设置又避雷针。配电柜和列头柜已配备部署有施耐德防雷开关和LKX雷科星防雷器进行保护，可防止感应雷。 | 符合 |
| 防火 | a)机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火； | 机房已部署七氟丙烷自动灭火系统，安装有烟感探头，当前系统运行方式为手动，系统运转正常。当前有4个气罐，气压在正常范围内。可实现自动检测火情、自动报警、自动灭火。 | 符合 |
| b)机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料； | 机房大门采用防火门，工作室两面采用钢筋混凝土材质，另外两面采用DFB-08-C1.50防火玻璃，均为耐火等级材质。 | 符合 |
| 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。 | 机房划分有核心区域、动力区域、运营商区域等，各区域之间采用DFB-08-C1.50防火玻璃进行隔离，具备隔离防火措施。 | 符合 |
| 防水和防潮 | a)应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透； | 机房无窗户存在，屋顶和墙壁等位置未出现过漏水、渗透和返潮现象，且通过防水涂层进行防水处理。 | 符合 |
| b)应采取措施防止机房内水蒸气结露和地下积水的转移与渗透； | 机房使用Emerson艾默生精密空调进行温湿度调节防止水蒸气结露，精密空调下方的排水管采取密封防漏处理，且设置有排水管道防范地下积水。 | 符合 |
| 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。 | 精密空调下方部署有水浸绳与动环系统相连，如果发生漏水等异常情况，能够进行告警并及时通知管理员。 | 符合 |
| 防静电 | a)应采用防静电地板或地面并采用必要的接地防静电措施； | 机房地面已采用防静电地板进行铺设，且各区域机柜、配电柜、设备等均进行了接地，并与整个大楼的接地系统相连。 | 符合 |
| 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。 | 在机房出入口配置有静电消除器，可防止静电产生。 | 符合 |
| 温湿度控制 | 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。 | 机房使用3台Emerson艾默生精密空调进行温湿度控制，当前机房温度为23℃，湿度为45%，温湿度均在适宜可控范围内。 | 符合 |
| 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； | 机房配电柜的供电线路已配备施耐德稳压器和过压保护装置。 | 符合 |
| b)应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求； | 采用蓝代斯克UPS电池组作为备用电力供应，在外部电路切断的情况下，UPS电池组能至少提供2个小时的电力供应。 | 符合 |
| c)应设置冗余或并行的电力电缆线路为计算机系统供电。 | 机房电力供应通过双路市电接到UPS再双路加入配电柜中，再双路连接机柜两个PDU，能再断电后1秒的时候进行切换。 | 符合 |
| 电磁防护 | a)电源线和通信线缆应隔离铺设，避免互相干扰； | 机房电源线采用下走线方式，通信线缆采用上走线方式部署再桥架当中。 | 符合 |
| b)应对关键设备实施电磁屏蔽。 | 未采取措施对关键设备实施电磁屏蔽防护。 | 不符合 |

* + 1. 安全扩展要求部分
       1. 物理机房

**附录D 表‑2安全物理环境结果记录表（物理机房）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 基础设施位置 | 应保证云计算基础设施位于中国境内。 | 云计算服务器、存储设备及网络安全设备均部署于浙江省杭州市西湖区文三西路52号浙江建投大厦的物理机房内部，该云计算设施位于中国境内。 | 符合 |

* 1. 安全通信网络
     1. 安全通用要求部分
        1. 安全通信网络

**附录D 表‑3安全通信网络结果记录表（安全通信网络）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 当前接入交换机CPU2%，内存使用44%；核心交换机CPU15%，内存45%，Spine交换机CPU5%，内存25%；Leaf交换机CPU10%，内存42%，且通过CAS平台、CloudOS平台可查看各核心主要网络设备资源均占用较低，可满足业务高峰期使用需求。 | 符合 |
| b)应保证网络各个部分的带宽满足业务高峰期需要； | 外部线路采用两条电信两百兆带宽、一条联通一百兆专线，内部主干线路采用双线聚合互联，当前各主要线路带宽占用率低于30%，可满足业务高峰期使用需求。 | 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； | 已根据实际安全需求，依据工作职能、重要性、程度等通过核心交换机、Spine交换机、Leaf交换机划分不同的VLAN，例如按照楼层，服务器，有线，会议等原则，并合理分配网络地址。 | 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； | 网络拓扑图与实际运行环境一致，重要网段部署在网络边界内部区域，重要私有云服务器区域通过服务器防火墙，并配置访问控制策略进行逻辑隔离，网络出口边界采用飞塔防火墙进行逻辑隔离，可有效避免非授权访问。 | 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。 | 当前主干核心线路均采用双线聚合互联，关键核心交换、Spine交换机、Leaf交换机，关键出口安全设备，关键资源池服务器等均采用两台至多台进行热冗余部署，保证系统的高可用性。 | 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； | 网络设备、服务器采用SSH的方式进行远程连接管理，安全设备、应用系统采用HTTPS的方式进行远程管理，可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。 | 网络设备、服务器采用SSH的方式进行远程连接管理，安全设备、应用系统采用HTTPS的方式进行远程管理，可保证通信过程中数据的保密性。 | 符合 |
| 可信验证 | 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。 | 未基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。 | 不符合 |

* + 1. 安全扩展要求部分
       1. 安全通信网络

**附录D 表‑4安全通信网络结果记录表（安全通信网络）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 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； | 当前系统为浙江省建设投资集团股份有限公司自建私有云，该云平台的网络安全保护等级为第三级（S3A3G3），其私有云上没有承载高于其安全保护等级的业务系统。 | 符合 |
| b)应实现不同云服务客户虚拟网络之间的隔离； | 不同云服务客户之间均采用独立的VPC网络进行组网，由CloudOS平台创建不同的NetWork网络，通过配置服务链对虚拟网络进行隔离，不能互访。 | 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； | 私有云使用华三的云平台架构进行搭建，云平台部署有云安全组、边界防火墙并集成入侵防护和恶意代码防护功能以及威胁感知大数据平台等安全设备，可为云服务客户提供通信传输、边界防护、入侵防范等安全能力。 | 符合 |
| 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； | 云平台部署有CloudOS平台、SAN平台、CAS平台，支持云服务客户自主定义安全策略，并自主选择所需要的安全服务或组件。 | 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。 | 云平台开放第三方API接口，云服务客户可通过申请和工单的形式，在通过审批后可按照云服务客户的要求对接第三方安全服务或部署第三方安全产品。 | 符合 |

* 1. 安全区域边界
     1. 安全通用要求部分
        1. 服务器边界

**附录D 表‑5安全区域边界结果记录表（服务器边界）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 服务器边界部署服务器防火墙对进出网络的数据进行控制，数据在指定端口进行传输，通过访问控制策略对数据出入进行控制，仅允许指定端口跨越边界进行网络通信。 | 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； | 未采取措施对非授权设备私自连入内部网络的行为进行检查和限制。 | 不符合 |
| 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； | 部署有深信服上网行为管理，并配置权限策略拒绝采用远程软件远程服务器组，并配置上网认证，外联检查等功能，针对对非授权连接外部网络的行为进行检查或限制。 | 符合 |
| 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。 | 该系统未使用无线网络。 | 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； | 通过服务器防火墙配置策略对跨越边界的网络数据进行控制，且已配置启用访问控制规则，对不符合策略的数据采取拒绝操作，且最后一条策略为双向拒绝所有。 | 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； | 服务器防火墙当前无多余或无效的访问控制策略，不同的访问控制策略前后无包含关系，已使得访问控制列表最小化。 | 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； | 服务器防火墙配置策略对数据包的源地址、目标地址、协议等内容进行检查，根据防火墙安全策略对数据进行放行或拒绝。例如仅允许源地址（总部员工有线10.\*.1.\*/24，机房运维10.\*.2.\*/24）访问目的地址（内部服务器10.\*.58.\*/24网段），协议（22、443、3389）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； | 服务器防火墙配置对进出数据量提供明确的允许/拒绝访问的能力，可查询到详细的访问控制记录，并为进出数据流提供明确的允许或拒绝的能力，且策略有效。 | 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。 | 未采取措施针对网络访问的数据流量实现基于应用协议和应用内容的访问控制。 | 不符合 |
| 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； | 网络边界服务器防火墙已集成IPS功能，服务器防火墙已配置并配置入侵防护策略，策略范围覆盖所有IP网络节点，当前入侵防护规则库版本为2021.11.10，规则库策略：每天自动进行更新，其规则库已至最新版本，可针对外部网络攻击行为进行检测和限制。 | 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； | 网络边界服务器防火墙已集成IPS功能，且部署有威胁感知大数据平台，已配置对应入侵防护策略，策略范围覆盖所有IP网络节点，当前入侵防护规则库版本为2021.11.10，规则库策略：每天自动进行更新，其规则库已至最新版本可针对内部网络攻击行为进行检测和限制。 | 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； | 部署有威胁感知大数据平台，已配置并开启相关安全策略，策略合理有效，能够针对网络攻击及新型网络攻击行为进行检测分析。 | 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。 | 通过边界服务器防火墙、威胁感知大数据平台对攻击行为进行分析和记录，记录内容包含攻击者IP、攻击类型、目标IP、攻击时间等内容，且发生严重入侵事件时将通过邮件的方式及时告警管理员。 | 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； | 边界服务器防火墙已集成恶意代码防护功能，已配置并开启相应策略，策略范围覆盖所有重要网段，其恶意代码库已更新至最新，当前病毒库版本为2021-11-10，恶意代码库每天自动进行更新，其恶意代码库已至最新版本。 | 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。 | 该系统未涉及邮件系统。 | 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； | 服务器边界服务器防火墙、Spine交换机等设备均已开启审计功能，能够针对边界的访问流量，每个用户的访问行为以及重要安全事件等进行审计。 | 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； | 审计记录包含具体时间、登录用户、登录名称、登录IP、操作内容，漏洞名称、目标IP、结果等内容。 | 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； | 边界服务器防火墙、Spine交换机等设备审计记录通过SYSLOG的方式上传至综合日志审计系统，审计记录每季度备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达6个月。 | 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。 | 通过帕拉迪堡垒机针对远程访问的用户行为进行单独审计，通过深信服上网行为管理针对访问互联网的用户行为进行单独审计。 | 符合 |
| 可信验证 | 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。 | 未采取措施基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 | 不符合 |

* + - 1. 互联网边界

**附录D 表‑6安全区域边界结果记录表（互联网边界）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 互联网边界部署飞塔防火墙对进出网络的数据进行控制，数据在指定端口进行传输，通过访问控制策略对数据出入进行控制，仅允许指定端口跨越边界进行网络通信。 | 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； | 未采取措施对非授权设备私自连入内部网络的行为进行检查和限制。 | 不符合 |
| 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； | 部署有深信服上网行为管理，并配置权限策略拒绝采用远程软件远程服务器组，并配置上网认证，外联检查等功能，针对对非授权连接外部网络的行为进行检查或限制。 | 符合 |
| 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。 | 该系统未使用无线网络。 | 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； | 互联网边界通过飞塔防火墙配置策略对跨越边界的网络数据进行控制，且已配置并启用访问控制规则，对不符合策略的数据采取拒绝操作，最后一条策略为双向拒绝所有网络通信。 | 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； | 互联网边界飞塔防火墙当前无多余或无效的访问控制策略，不同的访问控制策略前后无包含关系，已使得访问控制列表最小化。 | 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； | 飞塔防火墙配置策略基于源目IP、源目端口和协议的访问控制规则，以此对数据包的进出进行检查和限制，例如仅允许策略名称（ZJJT-SSL\_VPN\_user），源地址（总部SSL拨号地址段），访问目的地址（总部部分内网IP地址段），只通外网地址段等。 | 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； | 通过飞塔防火墙对进出数据量提供明确的允许/拒绝访问的能力，可查询到详细的访问控制记录，并为进出数据流提供明确的允许或拒绝的能力，且策略有效。 | 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。 | 未采取措施针对网络访问的数据流量实现基于应用协议和应用内容的访问控制。 | 不符合 |
| 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； | 飞塔防火墙已集成IPS功能，边界飞塔防火墙已配置并开启入侵防护策略，策略范围覆盖所有IP网络节点，针对外部网络攻击行为进行检测和限制，当前IPS库版本为18.00039，更新时间为2021.11.15，规则库策略：每天自动进行更新，其规则库版本已至最新。 | 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； | 飞塔防火墙已集成IPS功能，已配置并开启内对外的策略，该策略覆盖所有IP，且部署有威胁感知大数据平台，针对内部网络攻击行为进行检测、限制；当前IPS库版本为18.00039，更新时间为2021.11.15，规则库策略：每天自动进行更新，其规则库版本已至最新。 | 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； | 部署有威胁感知大数据平台，已配置并开启相关安全策略，策略合理有效，能够针对网络攻击及新型网络攻击行为进行检测分析。 | 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。 | 网络层面部署有威胁感知大数据平台和飞塔防火墙，飞塔防火墙集成IPS功能模块，可记录攻击源IP、攻击类型、目的IP、具体时间、攻击名称、严重性、动作等信息，在发生严重入侵事件时通过邮件的方式及时告警管理员。 | 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； | 互联网部署有飞塔防火墙，已集成恶意代码防护功能，针对边界配置有恶意代码防护策略，当前恶意代码库版本为84.00787，杀毒引擎版本为6.00154，规则库更新时间：2021.11.15，规则库更新策略：每天自动进行更新，其恶意代码库已更新至最新版本，可对恶意代码进行检测和清除。 | 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。 | 该系统未涉及邮件系统。 | 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； | 互联网边界飞塔防火墙、深信服上网行为管理等设备均已启用审计功能，能够针对边界的访问流量，每个用户的访问行为以及重要安全事件等进行审计。 | 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； | 审计记录包含日期/时间、服务、源、文件名、病毒、详情、目的IP、结果、用户、消息、级别、日志描述等内容。 | 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； | 飞塔防火墙、深信服上网行为管理等设备审计记录已接入综合日志审计系统对审计记录进行保护，审计记录每季度进行备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达6个月。 | 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。 | 通过帕拉迪堡垒机针对远程访问的用户行为进行单独审计，通过深信服上网行为管理针对访问互联网的用户行为进行单独审计。 | 符合 |
| 可信验证 | 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。 | 未采取措施基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 | 不符合 |

* + 1. 安全扩展要求部分
       1. 服务器边界

**附录D 表‑7安全区域边界结果记录表（服务器边界）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 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； | 在虚拟化网络边界部署有访问控制机制，在云计算平台和云服务客户业务系统间部署云安全组，云计算平台网络边界处部署服务器防火墙，不同云服务客户之间通过VPC组进行隔离，各设备均已配置并启用访问控制策略，且策略有效。 | 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。 | 云平台网络安全保护等级为第三级（S3A3G3），云服务客户不同的等级区域通过VPC组进行隔离，云平台不同等级的网络区域通过CloudOS平台创建服务链配置不同NetWork网络进行隔离。 | 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； | 云平台部署有威胁感知大数据平台，云平台服务器边界服务器防火墙集成IPS功能，均已配置监控及报警策略，针对云服务客户发起的网络攻击行为进行记录，其设备规则库版本为20211110，均已升级至最新版本。 | 符合 |
| 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； | 云平台部署有威胁感知大数据平台，云平台服务器边界服务器防火墙集成IPS功能，已配置监控及报警策略，针对虚拟网络节点的攻击行为为进行记录，其设备规则库版本为20211110，均已升级至最新版本。 | 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； | 通过CAS平台针对虚拟机与宿主机、虚拟机与虚拟机之间的端口流量进行监控，当流量超出阈值时，会在平台进行告警。 | 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。 | 云平台部署有威胁感知大数据平台，已配置相应安全策略，对网络攻击行为，异常流量情况进行检测，其设备规则库版本为20211110，均已升级至最新版本，并通过邮件方式告警。 | 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； | 通过CloudOS平台记录云服务商和云租户的操作进行记录，内容包含登录日志、重启或删除虚拟机日志等。 | 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。 | 云服务商对云租户客户的操作日志会在CloudOS平台进行体现，云服务客户管理员可通过云平台查看系统和数据的审计记录，云服务商操作可备云服务客户审计。 | 符合 |

* + - 1. 互联网边界

**附录D 表‑8安全区域边界结果记录表（互联网边界）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 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； | 在虚拟化网络边界部署有访问控制机制，在云计算平台和云服务客户业务系统间部署云安全组，云计算平台网络边界处部署服务器防火墙，不同云服务客户之间通过VPC组进行隔离，各设备均已配置并启用访问控制策略，且策略有效。 | 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。 | 云平台网络安全保护等级为第三级（S3A3G3），云服务客户不同的等级区域通过VPC组进行隔离，云平台不同等级的网络区域通过CloudOS平台创建服务链配置不同NetWork网络进行隔离。 | 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； | 云平台部署有威胁感知大数据平台，云平台服务器边界服务器防火墙集成IPS功能，均已配置监控及报警策略，针对云服务客户发起的网络攻击行为进行记录，其设备规则库版本为20211110，均已升级至最新版本。 | 符合 |
| 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； | 云平台部署有威胁感知大数据平台，云平台服务器边界服务器防火墙集成IPS功能，已配置监控及报警策略，针对虚拟网络节点的攻击行为为进行记录，其设备规则库版本为20211110，均已升级至最新版本。 | 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； | 通过CAS平台针对虚拟机与宿主机、虚拟机与虚拟机之间的端口流量进行监控，当流量超出阈值时，会在平台进行告警。 | 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。 | 云平台部署有威胁感知大数据平台，已配置相应安全策略，对网络攻击行为，异常流量情况进行检测，其设备规则库版本为20211110，均已升级至最新版本，并通过邮件方式告警。 | 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； | 通过CloudOS平台记录云服务商和云租户的操作进行记录，内容包含登录日志、重启或删除虚拟机日志等。 | 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。 | 云服务商对云租户客户的操作日志会在CloudOS平台进行体现，云服务客户管理员可通过云平台查看系统和数据的审计记录，云服务商操作可备云服务客户审计。 | 符合 |

* 1. 安全计算环境
     1. 安全通用要求部分
        1. 网络设备
           1. 核心交换机A

**附录D 表‑9安全计算环境-网络设备结果记录表（核心交换机A）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 登录设备需要使用用户名加口令进行身份鉴别，身份标识唯一，当前口令长度8位以上，口令组成包含特殊字符，大小写字母和数字，已开启口令复杂度策略Password-control enable，要求口令长度至少8位，口令组成必须包含大小写字母、数字和特殊字符，每半年进行一次口令更换。 | 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； | 已开启登录失败处理功能，password-control login-attempt 5 exceed lock-time 10，口令尝试次数：5次，措施：锁定账户10分钟；登录连接超时自动退出时间为：idle-timeout＝5分钟。 | 符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 核心交换机通过SSH的方式对设备进行远程管理，在通信过程采用SSL协议传输数据，用户口令信息加密传输，防止鉴别信息在网络传输过程中呗窃听。 | 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。 | 仅使用用户名加口令进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员等账户进行登录，不存在匿名账户，并为其分配相关权限。 | 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； | 未重命名或删除默认admin账户，但已修改默认口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 当前使用admin、she\*\*\*、an\*\*\*、xi\*\*\*等账户，分别管理员、审计管理员、安全管理员security-admin、系统管理员network-operator等角色权限，各账户仅分配所需的最小权限，实现管理用户的权限分离。 | 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； | 由管理员依据具体业务划分情况对账户进行具体权限划分，未发现越权访问情况。 | 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； | 当前设备访问控制粒度达到主体为用户级，客体为命令级。 | 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。 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 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； | 核心交换机已开启info-center与logfile功能，可对每个用户的重要用户行为和重要事件进行记录。 | 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； | 审计记录包含具体时间、用户、OID、端口、MAC、IP地址、具体消息等内容。 | 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； | 核心交换机的审计记录已通过SYSLOG发送至综合日志审计系统当中进行保护，审计记录每季度备份至本地，管理员无法对审计记录进行删除、修改或覆盖，审计记录保存时间长达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。 | 由底层软件对审计进程进行保护，非授权用户无法中断审计。 | 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； | 底层OS及必要服务由设备厂商出厂前配置完成，用户无需登录底层操作系统并验证组件，系统遵循最小化安全原则，仅安装自身所需要的组件和程序。 | 符合 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 当前设备不存在默认共享，已关闭不必要的端口，仅开启业务所需端口。 | 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； | 通过配置策略限制仅允许总部员工有线、机房运维、网络监控平台等网段可远程登录管理。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 恶意代码防范 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 可信验证 | 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。 | 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。 | 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； | 核心交换机主要涉及鉴别数据、重要审计数据和重要配置数据，其中重要配置数据不进行传输，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的完整性。重要审计数据通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 核心交换机主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 核心交换机主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | 核心交换机主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 由管理员每月或在重大配置更新后对设备配置文件进行手工备份，备份地点本地运维终端，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | 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。 | 当前交换机使用两台设备采用IRF堆叠技术进行热冗余部署，保证系统高可用性。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |

* + - * 1. 核心交换机B

**附录D 表‑10安全计算环境-网络设备结果记录表（核心交换机B）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 登录设备需要使用用户名加口令进行身份鉴别，身份标识唯一，当前口令长度8位以上，口令组成包含特殊字符，大小写字母和数字，已开启口令复杂度策略Password-control enable，要求口令长度至少8位，口令组成必须包含大小写字母、数字和特殊字符，每半年进行一次口令更换。 | 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； | 已开启登录失败处理功能，password-control login-attempt 5 exceed lock-time 10，口令尝试次数：5次，措施：锁定账户10分钟；登录连接超时自动退出时间为：idle-timeout＝5分钟。 | 符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 核心交换机通过SSH的方式对设备进行远程管理，在通信过程采用SSL协议传输数据，用户口令信息加密传输，防止鉴别信息在网络传输过程中呗窃听。 | 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。 | 仅使用用户名加口令进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员等账户进行登录，不存在匿名账户，并为其分配相关权限。 | 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； | 未重命名或删除默认admin账户，但已修改默认口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 当前使用admin、she\*\*\*、an\*\*\*、xi\*\*\*等账户，分别管理员、审计管理员、安全管理员security-admin、系统管理员network-operator等角色权限，各账户仅分配所需的最小权限，实现管理用户的权限分离。 | 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； | 由管理员依据具体业务划分情况对账户进行具体权限划分，未发现越权访问情况。 | 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； | 当前设备访问控制粒度达到主体为用户级，客体为命令级。 | 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。 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 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； | 核心交换机已开启info-center与logfile功能，可对每个用户的重要用户行为和重要事件进行记录。 | 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； | 审计记录包含具体时间、用户、OID、端口、MAC、IP地址、具体消息等内容。 | 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； | 核心交换机的审计记录已通过SYSLOG发送至综合日志审计系统当中进行保护，审计记录每季度备份至本地，管理员无法对审计记录进行删除、修改或覆盖，审计记录保存时间长达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。 | 由底层软件对审计进程进行保护，非授权用户无法中断审计。 | 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； | 底层OS及必要服务由设备厂商出厂前配置完成，用户无需登录底层操作系统并验证组件，系统遵循最小化安全原则，仅安装自身所需要的组件和程序。 | 符合 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 当前设备不存在默认共享，已关闭不必要的端口，仅开启业务所需端口。 | 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； | 通过配置策略限制仅允许总部员工有线、机房运维、网络监控平台等网段可远程登录管理。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 恶意代码防范 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 可信验证 | 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。 | 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。 | 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； | 核心交换机主要涉及鉴别数据、重要审计数据和重要配置数据，其中重要配置数据不进行传输，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的完整性。重要审计数据通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 核心交换机主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 核心交换机主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | 核心交换机主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 由管理员每月或在重大配置更新后对设备配置文件进行手工备份，备份地点本地运维终端，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | 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。 | 当前交换机使用两台设备采用IRF堆叠技术进行热冗余部署，保证系统高可用性。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |

* + - * 1. Leaf交换机A

**附录D 表‑11安全计算环境-网络设备结果记录表（Leaf交换机A）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 登录设备需要使用用户名加口令进行身份鉴别，身份标识唯一，当前口令长度8位以上，口令组成包含特殊字符，大小写字母和数字，已开启口令复杂度策略Password-control enable，要求口令长度至少8位，口令组成必须包含大小写字母、数字和特殊字符，每半年进行一次口令更换。 | 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； | 已开启登录失败处理功能，password-control login-attempt 5 exceed lock-time 10，口令尝试次数：5次，措施：锁定账户10分钟；登录连接超时自动退出时间为：idle-timeout＝5分钟。 | 符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | Leaf交换机通过SSH的方式对设备进行远程管理，在通信过程采用SSL协议传输数据，用户口令信息加密传输，防止鉴别信息在网络传输过程中呗窃听。 | 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。 | 仅使用用户名加口令进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员等账户进行登录，不存在匿名账户，并为其分配相关权限。 | 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； | 未重命名或删除默认admin账户，但已修改默认口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 当前使用admin、she\*\*\*、an\*\*\*、xi\*\*\*等账户，分别管理员、审计管理员、安全管理员security-admin、系统管理员network-operator等角色权限，各账户仅分配所需的最小权限，实现管理用户的权限分离。 | 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； | 由管理员依据具体业务划分情况对账户进行具体权限划分，未发现越权访问情况。 | 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； | 当前设备访问控制粒度达到主体为用户级，客体为命令级。 | 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。 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 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； | Leaf交换机已开启info-center与logfile功能，可对每个用户的重要用户行为和重要事件进行记录。 | 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； | 审计记录包含具体时间、用户、OID、端口、MAC、IP地址、具体消息等内容。 | 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； | Leaf交换机的审计记录已通过SYSLOG发送至综合日志审计系统当中进行保护，审计记录每季度备份至本地，管理员无法对审计记录进行删除、修改或覆盖，审计记录保存时间长达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。 | 由底层软件对审计进程进行保护，非授权用户无法中断审计。 | 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； | 底层OS及必要服务由设备厂商出厂前配置完成，用户无需登录底层操作系统并验证组件，系统遵循最小化安全原则，仅安装自身所需要的组件和程序。 | 符合 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 当前设备不存在默认共享，已关闭不必要的端口，仅开启业务所需端口。 | 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； | 通过配置策略限制仅允许总部员工有线、机房运维、网络监控平台等网段可远程登录管理。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 恶意代码防范 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 可信验证 | 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。 | 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。 | 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； | Leaf交换机主要涉及鉴别数据、重要审计数据和重要配置数据，其中重要配置数据不进行传输，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的完整性。重要审计数据通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | Leaf交换机主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | Leaf交换机主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | Leaf交换机主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 由管理员每月或在重大配置更新后对设备配置文件进行手工备份，备份地点本地运维终端，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | 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。 | 当前交换机使用两台设备采用IRF堆叠技术进行热冗余部署，保证系统高可用性。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |

* + - * 1. Leaf交换机B

**附录D 表‑12安全计算环境-网络设备结果记录表（Leaf交换机B）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 登录设备需要使用用户名加口令进行身份鉴别，身份标识唯一，当前口令长度8位以上，口令组成包含特殊字符，大小写字母和数字，已开启口令复杂度策略Password-control enable，要求口令长度至少8位，口令组成必须包含大小写字母、数字和特殊字符，每半年进行一次口令更换。 | 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； | 已开启登录失败处理功能，password-control login-attempt 5 exceed lock-time 10，口令尝试次数：5次，措施：锁定账户10分钟；登录连接超时自动退出时间为：idle-timeout＝5分钟。 | 符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | Leaf交换机通过SSH的方式对设备进行远程管理，在通信过程采用SSL协议传输数据，用户口令信息加密传输，防止鉴别信息在网络传输过程中呗窃听。 | 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。 | 仅使用用户名加口令进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员等账户进行登录，不存在匿名账户，并为其分配相关权限。 | 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； | 未重命名或删除默认admin账户，但已修改默认口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 当前使用admin、she\*\*\*、an\*\*\*、xi\*\*\*等账户，分别管理员、审计管理员、安全管理员security-admin、系统管理员network-operator等角色权限，各账户仅分配所需的最小权限，实现管理用户的权限分离。 | 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； | 由管理员依据具体业务划分情况对账户进行具体权限划分，未发现越权访问情况。 | 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； | 当前设备访问控制粒度达到主体为用户级，客体为命令级。 | 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。 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 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； | Leaf交换机已开启info-center与logfile功能，可对每个用户的重要用户行为和重要事件进行记录。 | 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； | 审计记录包含具体时间、用户、OID、端口、MAC、IP地址、具体消息等内容。 | 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； | Leaf交换机的审计记录已通过SYSLOG发送至综合日志审计系统当中进行保护，审计记录每季度备份至本地，管理员无法对审计记录进行删除、修改或覆盖，审计记录保存时间长达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。 | 由底层软件对审计进程进行保护，非授权用户无法中断审计。 | 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； | 底层OS及必要服务由设备厂商出厂前配置完成，用户无需登录底层操作系统并验证组件，系统遵循最小化安全原则，仅安装自身所需要的组件和程序。 | 符合 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 当前设备不存在默认共享，已关闭不必要的端口，仅开启业务所需端口。 | 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； | 通过配置策略限制仅允许总部员工有线、机房运维、网络监控平台等网段可远程登录管理。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 恶意代码防范 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 可信验证 | 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。 | 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。 | 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； | Leaf交换机主要涉及鉴别数据、重要审计数据和重要配置数据，其中重要配置数据不进行传输，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的完整性。重要审计数据通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | Leaf交换机主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | Leaf交换机主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | Leaf交换机主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 由管理员每月或在重大配置更新后对设备配置文件进行手工备份，备份地点本地运维终端，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | 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。 | 当前交换机使用两台设备采用IRF堆叠技术进行热冗余部署，保证系统高可用性。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |

* + - * 1. Spine交换机A

**附录D 表‑13安全计算环境-网络设备结果记录表（Spine交换机A）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 登录设备需要使用用户名加口令进行身份鉴别，身份标识唯一，当前口令长度8位以上，口令组成包含特殊字符，大小写字母和数字，已开启口令复杂度策略Password-control enable，要求口令长度至少8位，口令组成必须包含大小写字母、数字和特殊字符，每半年进行一次口令更换。 | 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； | 已开启登录失败处理功能，password-control login-attempt 5 exceed lock-time 10，口令尝试次数：5次，措施：锁定账户10分钟；登录连接超时自动退出时间为：idle-timeout＝5分钟。 | 符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | Spine交换机通过SSH的方式对设备进行远程管理，在通信过程采用SSL协议传输数据，用户口令信息加密传输，防止鉴别信息在网络传输过程中呗窃听。 | 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。 | 仅使用用户名加口令进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员等账户进行登录，不存在匿名账户，并为其分配相关权限。 | 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； | 未重命名或删除默认admin账户，但已修改默认口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 当前使用admin、she\*\*\*、an\*\*\*、xi\*\*\*等账户，分别管理员、审计管理员、安全管理员security-admin、系统管理员network-operator等角色权限，各账户仅分配所需的最小权限，实现管理用户的权限分离。 | 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； | 由管理员依据具体业务划分情况对账户进行具体权限划分，未发现越权访问情况。 | 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； | 当前设备访问控制粒度达到主体为用户级，客体为命令级。 | 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。 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 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； | Spine交换机已开启info-center与logfile功能，可对每个用户的重要用户行为和重要事件进行记录。 | 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； | 审计记录包含具体时间、用户、OID、端口、MAC、IP地址、具体消息等内容。 | 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； | 核心交换机的审计记录已通过SYSLOG发送至综合日志审计系统当中进行保护，审计记录每季度备份至本地，管理员无法对审计记录进行删除、修改或覆盖，审计记录保存时间长达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。 | 由底层软件对审计进程进行保护，非授权用户无法中断审计。 | 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； | 底层OS及必要服务由设备厂商出厂前配置完成，用户无需登录底层操作系统并验证组件，系统遵循最小化安全原则，仅安装自身所需要的组件和程序。 | 符合 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 当前设备不存在默认共享，已关闭不必要的端口，仅开启业务所需端口。 | 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； | 通过配置策略限制仅允许总部员工有线、机房运维、网络监控平台等网段可远程登录管理。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 恶意代码防范 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 可信验证 | 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。 | 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。 | 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； | Spine交换机主要涉及鉴别数据、重要审计数据和重要配置数据，其中重要配置数据不进行传输，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的完整性。重要审计数据通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | Spine交换机主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | Spine交换机主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | Spine交换机主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 由管理员每月或在重大配置更新后对设备配置文件进行手工备份，备份地点本地运维终端，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | 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。 | 当前交换机使用两台设备采用IRF堆叠技术进行热冗余部署，保证系统高可用性。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |

* + - * 1. Spine交换机B

**附录D 表‑14安全计算环境-网络设备结果记录表（Spine交换机B）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 登录设备需要使用用户名加口令进行身份鉴别，身份标识唯一，当前口令长度8位以上，口令组成包含特殊字符，大小写字母和数字，已开启口令复杂度策略Password-control enable，要求口令长度至少8位，口令组成必须包含大小写字母、数字和特殊字符，每半年进行一次口令更换。 | 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； | 已开启登录失败处理功能，password-control login-attempt 5 exceed lock-time 10，口令尝试次数：5次，措施：锁定账户10分钟；登录连接超时自动退出时间为：idle-timeout＝5分钟。 | 符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | Spine交换机通过SSH的方式对设备进行远程管理，在通信过程采用SSL协议传输数据，用户口令信息加密传输，防止鉴别信息在网络传输过程中呗窃听。 | 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。 | 仅使用用户名加口令进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员等账户进行登录，不存在匿名账户，并为其分配相关权限。 | 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； | 未重命名或删除默认admin账户，但已修改默认口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 当前使用admin、she\*\*\*、an\*\*\*、xi\*\*\*等账户，分别管理员、审计管理员、安全管理员security-admin、系统管理员network-operator等角色权限，各账户仅分配所需的最小权限，实现管理用户的权限分离。 | 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； | 由管理员依据具体业务划分情况对账户进行具体权限划分，未发现越权访问情况。 | 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； | 当前设备访问控制粒度达到主体为用户级，客体为命令级。 | 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。 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 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； | Spine交换机已开启info-center与logfile功能，可对每个用户的重要用户行为和重要事件进行记录。 | 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； | 审计记录包含具体时间、用户、OID、端口、MAC、IP地址、具体消息等内容。 | 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； | 核心交换机的审计记录已通过SYSLOG发送至综合日志审计系统当中进行保护，审计记录每季度备份至本地，管理员无法对审计记录进行删除、修改或覆盖，审计记录保存时间长达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。 | 由底层软件对审计进程进行保护，非授权用户无法中断审计。 | 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； | 底层OS及必要服务由设备厂商出厂前配置完成，用户无需登录底层操作系统并验证组件，系统遵循最小化安全原则，仅安装自身所需要的组件和程序。 | 符合 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 当前设备不存在默认共享，已关闭不必要的端口，仅开启业务所需端口。 | 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； | 通过配置策略限制仅允许总部员工有线、机房运维、网络监控平台等网段可远程登录管理。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 恶意代码防范 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 可信验证 | 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。 | 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。 | 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； | Spine交换机主要涉及鉴别数据、重要审计数据和重要配置数据，其中重要配置数据不进行传输，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的完整性。重要审计数据通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | Spine交换机主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | Spine交换机主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | Spine交换机主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 由管理员每月或在重大配置更新后对设备配置文件进行手工备份，备份地点本地运维终端，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | 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。 | 当前交换机使用两台设备采用IRF堆叠技术进行热冗余部署，保证系统高可用性。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |

* + - 1. 安全设备
         1. H3C防火墙A

**附录D 表‑15安全计算环境-安全设备结果记录表（H3C防火墙A）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 登录设备需要使用用户名加口令进行身份鉴别，身份标识唯一，口令长度8位以上，口令组成包含特殊字符，大小写字母和数字，已开启口令复杂度策略，口令长度最小8位，口令组成不允许包含用户名或颠倒用户名，不允许包含连续三个或以上的相同字符，必须包含大小写字母、数字和特殊字符，每半年进行一次口令更换。 | 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； | 已开启登录失败处理功能，登录失败次数：3次，措施：锁定账户30分钟；登录连接超时自动退出时间为：10分钟。 | 符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | H3C防火墙采用HTTPS进行远程管理，用户口令信息加密传输，防止鉴别信息被窃取。 | 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。 | 仅使用用户名加口令进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员等账户进行登录，不存在匿名账户，并为其分配相关权限。 | 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； | 未重命名或删除默认admin账户，但已修改默认口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | H3C防火墙创建admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员等角色权限，各账户仅分配所需的最小权限，不同账户具备不同的访问权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 已配置访问控制功能，主体为用户级，客体为界面级。 | 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。 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 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； | 设备已开启审计功能，审计范围覆盖到每个用户，可对重要的用户行为和重要安全事件进行审计。 | 符合 |
| b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 审计记录包含具体时间、IP地址、操作内容、端口状态，是否成功等信息。 | 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； | 审计记录已通过SYSLOG方式上传综合日志审计系统进行保护，审计记录每季度备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达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。 | 由系统底层和综合日志审计系统对审计进程进行保护，非授权用户无法中断审计。 | 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； | 底层OS及必要服务由设备厂商出厂前配置完成，用户无需登录底层操作系统并验证组件，系统遵循最小化安全原则，仅安装自身所需要的组件和程序。 | 符合 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 当前设备不存在默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的系统服务。 | 符合 |
| c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 通过配置策略限制仅允许总部员工有线、机房运维、网络监控平台等网段可远程登录管理。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 恶意代码防范 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 可信验证 | 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。 | 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。 | 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； | H3C防火墙主要涉及鉴别数据、重要审计数据和重要配置数据，其中重要配置数据不进行传输，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的完整性。重要审计数据通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | H3C防火墙主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | H3C防火墙主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | H3C防火墙主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 由管理员每月或在重大配置更新后对设备配置文件进行手工备份，备份地点本地运维终端，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | 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。 | 当前设备使用两台设备配置主备双机的方式进行热冗余部署，保证系统高可用性。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |

* + - * 1. H3C防火墙B

**附录D 表‑16安全计算环境-安全设备结果记录表（H3C防火墙B）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 登录设备需要使用用户名加口令进行身份鉴别，身份标识唯一，口令长度8位以上，口令组成包含特殊字符，大小写字母和数字，已开启口令复杂度策略，口令长度最小8位，口令组成不允许包含用户名或颠倒用户名，不允许包含连续三个或以上的相同字符，必须包含大小写字母、数字和特殊字符，每半年进行一次口令更换。 | 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； | 已开启登录失败处理功能，登录失败次数：3次，措施：锁定账户30分钟；登录连接超时自动退出时间为：10分钟。 | 符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | H3C防火墙采用HTTPS进行远程管理，用户口令信息加密传输，防止鉴别信息被窃取。 | 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。 | 仅使用用户名加口令进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员等账户进行登录，不存在匿名账户，并为其分配相关权限。 | 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； | 未重命名或删除默认admin账户，但已修改默认口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | H3C防火墙创建admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员等角色权限，各账户仅分配所需的最小权限，不同账户具备不同的访问权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 已配置访问控制功能，主体为用户级，客体为界面级。 | 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。 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 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； | 设备已开启审计功能，审计范围覆盖到每个用户，可对重要的用户行为和重要安全事件进行审计。 | 符合 |
| b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 审计记录包含具体时间、IP地址、操作内容、端口状态，是否成功等信息。 | 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； | 审计记录已通过SYSLOG方式上传综合日志审计系统进行保护，审计记录每季度备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达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。 | 由系统底层和综合日志审计系统对审计进程进行保护，非授权用户无法中断审计。 | 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； | 底层OS及必要服务由设备厂商出厂前配置完成，用户无需登录底层操作系统并验证组件，系统遵循最小化安全原则，仅安装自身所需要的组件和程序。 | 符合 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 当前设备不存在默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的系统服务。 | 符合 |
| c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 通过配置策略限制仅允许总部员工有线、机房运维、网络监控平台等网段可远程登录管理。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 恶意代码防范 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 可信验证 | 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。 | 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。 | 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； | H3C防火墙主要涉及鉴别数据、重要审计数据和重要配置数据，其中重要配置数据不进行传输，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的完整性。重要审计数据通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | H3C防火墙主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | H3C防火墙主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | H3C防火墙主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 由管理员每月或在重大配置更新后对设备配置文件进行手工备份，备份地点本地运维终端，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | 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。 | 当前设备使用两台设备配置主备双机的方式进行热冗余部署，保证系统高可用性。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |

* + - * 1. 威胁感知大数据平台

**附录D 表‑17安全计算环境-安全设备结果记录表（威胁感知大数据平台）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 登录设备采用用户名加口令进行身份鉴别，身份标识唯一，当前口令长度8位以上，采用字母、 数字和特殊符号组成；已开启密码复杂度策略，要求口令长度6-12位，口令组成必须包含大小写字母、数字和特殊字符三种组成，设定策略每一个月对设备口令进行更换。 | 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； | 已开启登录失败处理功能，登录失败次数：10次，措施：锁定账户60分钟；登录连接超时自动退出时间为：30分钟。 | 符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 威胁感知大数据平台采用HTTPS的方式进行远程管理，用户口令信息加密传输，防止鉴别信息在网络传输过程中被窃取。 | 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。 | 仅使用用户名加口令进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员等账户进行登录，不存在匿名账户，并为其分配相关权限。 | 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； | 未重命名或删除默认admin账户，但已修改默认账户口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 当前使用admin、an\*\*\*、she\*\*\*、xi\*\*\*等账户，分别超级管理员、安全管理员、审计管理员、系统管理员等角色权限，各账户当前仅分配自身所需要的权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 当前设备访问控制粒度达到主体为用户级，客体为界面级。 | 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。 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 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； | 设备已开启审计功能，针对每个用户的重要操作行为，入侵行为、脆弱性感知等重要事件进行审计。 | 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； | 审计记录包含审计记录 用户名、操作地址、操作时间、操作、信息、告警、告警时间、告警类型、告警对象、告警级别、告警内容，告警状态。 | 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； | 审计记录通过SYSLOG的方式上传至综合日志审计系统对审计记录进行保护，审计记录每季度备份至本地，管理员无法对审计记录进行非预期删除、修改或覆盖，审计记录保存时间长达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。 | 系统已对审计进程进行保护，非授权用户不可被中断。 | 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； | 底层OS及必要服务由设备厂商出厂前配置完成，用户无需登录底层操作系统并验证组件，系统遵循最小化安全原则，仅安装自身所需要的组件和程序。 | 符合 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 当前设备不存在默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的系统服务。 | 符合 |
| c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 通过配置策略限制仅允许总部员工有线、机房运维、网络监控平台等网段可远程登录管理。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 威胁感知大数据平台可对重要节点入侵行为进行检查，已配置并开启对应安全策略，策略范围覆盖系统内部所有网络地址，在发生严重入侵事件时，将通过邮件方式进行告警。 | 符合 |
| 恶意代码防范 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 可信验证 | 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。 | 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。 | 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； | 威胁感知大数据平台主要涉及鉴别数据、重要审计数据和重要配置数据，其中重要配置数据不进行传输，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的完整性。重要审计数据通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 威胁感知大数据平台主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 威胁感知大数据平台主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | 威胁感知大数据平台主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 威胁感知大数据平台的配置数据每天凌晨自动进行一次备份，备份文件保存在设备本地，保存时间为1个月，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | 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。 | 当前设备采用旁路方式部署，仅作为网络威胁总体分析，设备宕机不影响业务系统的正常运行。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |

* + - * 1. 帕拉迪堡垒机A

**附录D 表‑18安全计算环境-安全设备结果记录表（帕拉迪堡垒机A）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 登录设备需要使用用户名加口令进行身份鉴别，身份标识唯一，口令长度8位以上，口令组成包含特殊字符，大小写字母和数字，已开启口令复杂度策略，口令长度至少8位，口令组成必须包含大小写字母、数字和特殊字符，每半年进行一次口令更换。 | 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； | 已开启登录失败处理功能，登录失败次数：10次，措施：锁定账户1分钟，网络登录连接空闲超时自动退出时间：30分钟。 | 符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 帕拉迪堡垒机采用HTTPS的方式进行远程管理，用户鉴别信息加密传输，防止鉴别信息在网络传输中被窃听。 | 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。 | 仅使用用户名加口令进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员，x\*\*、p\*\*\*、l\*\*\*、hu\*\*\*普通运维账户等，不存在匿名账户，并为其分配相关权限。 | 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； | 未重命名或删除默认admin账户，但已修改默认口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 当前使用admin、an\*\*\*、she\*\*\*、xi\*\*\*、li\*\*\*等账户，分别超级管理员、审计管理员、安全管理员、系统管理员以及普通用户等角色权限，各账户仅分配所需的最小权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 已配置访问控制功能，主体为用户级，客体为界面级。 | 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。 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 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； | 设备已开启审计功能，可对重要的用户行为和重要安全事件进行审计。 | 符合 |
| b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 审计记录包含具体时间、登录地址、登录用户、登录模式、登录状态。运维日志包含开始时间、结束时间、登录IP、用户名称、设备IP、账户名称、录像等内容。 | 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； | 审计记录已通过SYSLOG方式上传至综合日志审计系统对审计记录进行保护，审计记录每季度备份至本地，管理员账户无法对审计记录进行非预期的删除，修改或覆盖，审计记录保存时间长达6个月，最早能查询到2017-05-18的登录日志信息。 | 符合 |
| d)应对审计进程进行保护，防止未经授权的中断。 | 由系统底层对审计进程进行保护，非授权用户无法中断审计。 | 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； | 底层OS及必要服务由设备厂商出厂前配置完成，用户无需登录底层操作系统并验证组件，系统遵循最小化安全原则，仅安装自身所需要的组件和程序。 | 符合 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 当前设备不存在默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的系统服务。 | 符合 |
| c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 通过边界配置ACL3001，仅允许10.\*.1.\*，192.\*.9.\*远程管理设备。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 恶意代码防范 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 可信验证 | 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。 | 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。 | 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； | 帕拉迪堡垒机主要涉及鉴别数据、重要审计数据和重要配置数据，其中重要配置数据不进行传输，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的完整性。重要审计数据通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 帕拉迪堡垒机主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 帕拉迪堡垒机主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | 帕拉迪堡垒机主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 由管理员每月或在重大配置更新后对设备配置文件进行手工备份，备份地点本地运维终端，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | 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。 | 仅作为安全运维使用，非重要数据处理系统，设备宕机不影响业务系统正常运行。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |

* + - * 1. 帕拉迪堡垒机B

**附录D 表‑19安全计算环境-安全设备结果记录表（帕拉迪堡垒机B）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 登录设备需要使用用户名加口令进行身份鉴别，身份标识唯一，口令长度8位以上，口令组成包含特殊字符，大小写字母和数字，已开启口令复杂度策略，口令长度至少8位，口令组成必须包含大小写字母、数字和特殊字符，每半年进行一次口令更换。 | 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； | 已开启登录失败处理功能，登录失败次数：10次，措施：锁定账户1分钟，网络登录连接空闲超时自动退出时间：30分钟。 | 符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 帕拉迪堡垒机采用HTTPS的方式进行远程管理，用户鉴别信息加密传输，防止鉴别信息在网络传输中被窃听。 | 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。 | 仅使用用户名加口令进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员，x\*\*、p\*\*\*、l\*\*\*、hu\*\*\*普通运维账户等，不存在匿名账户，并为其分配相关权限。 | 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； | 未重命名或删除默认admin账户，但已修改默认口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 当前使用admin、an\*\*\*、she\*\*\*、xi\*\*\*、li\*\*\*等账户，分别超级管理员、审计管理员、安全管理员、系统管理员以及普通用户等角色权限，各账户仅分配所需的最小权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 已配置访问控制功能，主体为用户级，客体为界面级。 | 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。 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 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； | 设备已开启审计功能，可对重要的用户行为和重要安全事件进行审计。 | 符合 |
| b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 审计记录包含具体时间、登录地址、登录用户、登录模式、登录状态。运维日志包含开始时间、结束时间、登录IP、用户名称、设备IP、账户名称、录像等内容。 | 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； | 审计记录已通过SYSLOG方式上传至综合日志审计系统对审计记录进行保护，审计记录每季度备份至本地，管理员账户无法对审计记录进行非预期的删除，修改或覆盖，审计记录保存时间长达6个月，最早能查询到2017-05-18的登录日志信息。 | 符合 |
| d)应对审计进程进行保护，防止未经授权的中断。 | 由系统底层对审计进程进行保护，非授权用户无法中断审计。 | 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； | 底层OS及必要服务由设备厂商出厂前配置完成，用户无需登录底层操作系统并验证组件，系统遵循最小化安全原则，仅安装自身所需要的组件和程序。 | 符合 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 当前设备不存在默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的系统服务。 | 符合 |
| c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 通过边界配置ACL3001，仅允许10.\*.1.\*，192.\*.9.\*远程管理设备。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 恶意代码防范 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 可信验证 | 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。 | 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。 | 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； | 帕拉迪堡垒机主要涉及鉴别数据、重要审计数据和重要配置数据，其中重要配置数据不进行传输，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的完整性。重要审计数据通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 帕拉迪堡垒机主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 帕拉迪堡垒机主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | 帕拉迪堡垒机主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 由管理员每月或在重大配置更新后对设备配置文件进行手工备份，备份地点本地运维终端，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | 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。 | 仅作为安全运维使用，非重要数据处理系统，设备宕机不影响业务系统正常运行。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |

* + - * 1. 服务器防火墙

**附录D 表‑20安全计算环境-安全设备结果记录表（服务器防火墙）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 登录设备采用用户名加口令进行身份鉴别，身份标识唯一，当前口令长度8位以上，采用字母、 数字和特殊符号组成；已开启密码复杂度策略，要求口令长度8位以上，口令组成需包含数字、字母和特殊字符的两种及以上；每三个月对设备口令进行更换。 | 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； | 已开启登录失败处理功能，登录失败次数：10次，措施：锁定账户1分钟；登录连接超时自动退出时间为：10分钟。 | 符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 服务器防火墙采用HTTPS的方式进行远程管理，用户口令信息加密传输，防止鉴别信息在网络传输过程中被窃取。 | 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。 | 仅使用用户名加口令进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用admin管理员、aud\*\*\*审计管理员、sec\*\*\*安全管理员、sys\*\*\*系统管理员等账户，不存在匿名账户，并为各账户分配相关权限。 | 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； | 未重命名或删除默认admin账户，但已修改默认账户口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 当前使用admin管理员、aud\*\*\*审计管理员、sec\*\*\*安全管理员、sys\*\*\*系统管理员等角色权限，各账户仅分配所需的最小权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 当前设备访问控制粒度达到主体为用户级，客体为界面级。 | 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。 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 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； | 已开启审计功能，针对每个用户的重要操作行为，入侵行为、访问控制流量等重要事件进行审计。 | 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； | 审计记录包含具体时间、登录用户、登录名称、登录IP、操作内容，漏洞名称、目标IP、结果等内容。 | 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； | 审计记录已通过SYSLOG发送至综合日志审计系统中进行保存，审计记录每季度保存至本地，管理员无法对审计记录进行删除、修改或覆盖，审计记录保存时间长达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。 | 系统已对审计进程进行保护，非授权用户不可被中断。 | 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； | 底层OS及必要服务由设备厂商出厂前配置完成，用户无需登录底层操作系统并验证组件，系统遵循最小化安全原则，仅安装自身所需要的组件和程序。 | 符合 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 当前设备不存在默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的系统服务。 | 符合 |
| c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 已通过配置策略，仅允许10.\*.1.\*，10.\*.2.\*，10.\*.251.\*可远程管理设备。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 恶意代码防范 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 可信验证 | 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。 | 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。 | 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； | 服务器防火墙主要涉及鉴别数据、重要审计数据和重要配置数据，其中重要配置数据不进行传输，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的完整性。重要审计数据通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 服务器防火墙主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用RSA2048的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 服务器防火墙主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | 服务器防火墙主要涉及鉴别数据，鉴别数据采用RSA2048的方式，能够保证鉴别数据在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； | 服务器防火墙的配置数据每天凌晨自动进行一次备份，备份文件保存在设备本地，保存时间为1个月，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | 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。 | 设备仅作为服务器区边界安全防护，采用透明方式部署，设备宕机会触发bypass机制，不影响系统的正常运行。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |

* + - * 1. 深信服上网行为管理A

**附录D 表‑21安全计算环境-安全设备结果记录表（深信服上网行为管理A）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 登录设备需要使用用户名加口令进行身份鉴别，身份标识唯一，口令长度8位以上，口令组成包含特殊字符，大小写字母和数字，已开启密码复杂度校验功能，口令长度要求至少8位，口令组成必须包含大小写字母、数字和特殊字符，每半年进行一次口令更换。 | 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； | 已开启登录失败处理功能，登录失败次数：5次，措施：锁定账户1分钟，网络登录连接空闲超时自动退出时间：30分钟。 | 符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 深信服上网行为管理远程管理采用HTTPS，用户鉴别信息加密传输，防止鉴别信息在网络传输中被窃听。 | 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。 | 仅使用用户名加口令进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员等账户进行登录，不存在匿名账户，并为其分配相关权限。 | 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； | 未重命名或删除默认admin账户，但已修改默认口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 当前使用admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员等角色权限，各账户仅分配所需的最小权限，不同账户具备不同的访问权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 当前设备访问控制粒度达到主体为用户级，客体为界面级。 | 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。 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 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； | 设备已开启审计功能，可对重要的用户行为和重要安全事件进行审计。 | 符合 |
| b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 审计记录包含具体时间、用户名、组名、终端类型、网站分类、标题、URL地址、访问控制、登录用户、内容等信息。 | 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； | 审计记录已通过SYSLOG方式上传至综合日志审计系统对审计记录进行保护，审计记录每季度进行备份，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达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。 | 由系统底层对审计进程进行保护，非授权用户无法中断审计。 | 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； | 底层OS及必要服务由设备厂商出厂前配置完成，用户无需登录底层操作系统并验证组件，系统遵循最小化安全原则，仅安装自身所需要的组件和程序。 | 符合 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 当前设备不存在默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的系统服务。 | 符合 |
| c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 通过边界配置ACL3001，仅允许10.\*.1.\*，192.\*.9.\*远程管理设备。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 恶意代码防范 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 可信验证 | 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。 | 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。 | 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； | 深信服上网行为管理主要涉及鉴别数据、重要审计数据和重要配置数据，其中重要配置数据不进行传输，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的完整性。重要审计数据通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 深信服上网行为管理主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 深信服上网行为管理主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | 深信服上网行为管理主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 设备每天零点自动进行配置备份，备份至设备本地，备份文件保存时间为2个月，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | 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。 | 采用两台设备主备方式高可用部署实现热冗余，保证系统稳定运行。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |

* + - * 1. 深信服上网行为管理B

**附录D 表‑22安全计算环境-安全设备结果记录表（深信服上网行为管理B）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 登录设备需要使用用户名加口令进行身份鉴别，身份标识唯一，口令长度8位以上，口令组成包含特殊字符，大小写字母和数字，已开启密码复杂度校验功能，口令长度要求至少8位，口令组成必须包含大小写字母、数字和特殊字符，每半年进行一次口令更换。 | 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； | 已开启登录失败处理功能，登录失败次数：5次，措施：锁定账户1分钟，网络登录连接空闲超时自动退出时间：30分钟。 | 符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 深信服上网行为管理远程管理采用HTTPS，用户鉴别信息加密传输，防止鉴别信息在网络传输中被窃听。 | 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。 | 仅使用用户名加口令进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员等账户进行登录，不存在匿名账户，并为其分配相关权限。 | 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； | 未重命名或删除默认admin账户，但已修改默认口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 当前使用admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员等角色权限，各账户仅分配所需的最小权限，不同账户具备不同的访问权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 当前设备访问控制粒度达到主体为用户级，客体为界面级。 | 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。 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 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； | 设备已开启审计功能，可对重要的用户行为和重要安全事件进行审计。 | 符合 |
| b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 审计记录包含具体时间、用户名、组名、终端类型、网站分类、标题、URL地址、访问控制、登录用户、内容等信息。 | 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； | 审计记录已通过SYSLOG方式上传至综合日志审计系统对审计记录进行保护，审计记录每季度进行备份，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达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。 | 由系统底层对审计进程进行保护，非授权用户无法中断审计。 | 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； | 底层OS及必要服务由设备厂商出厂前配置完成，用户无需登录底层操作系统并验证组件，系统遵循最小化安全原则，仅安装自身所需要的组件和程序。 | 符合 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 当前设备不存在默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的系统服务。 | 符合 |
| c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 通过边界配置ACL3001，仅允许10.\*.1.\*，192.\*.9.\*远程管理设备。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 恶意代码防范 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 可信验证 | 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。 | 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。 | 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； | 深信服上网行为管理主要涉及鉴别数据、重要审计数据和重要配置数据，其中重要配置数据不进行传输，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的完整性。重要审计数据通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 深信服上网行为管理主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 深信服上网行为管理主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | 深信服上网行为管理主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 设备每天零点自动进行配置备份，备份至设备本地，备份文件保存时间为2个月，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | 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。 | 采用两台设备主备方式高可用部署实现热冗余，保证系统稳定运行。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |

* + - * 1. 综合日志审计系统

**附录D 表‑23安全计算环境-安全设备结果记录表（综合日志审计系统）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 登录设备需要使用用户名加口令进行身份鉴别，身份鉴别唯一，口令长度8位以上，口令组成包含特殊字符，大小写字母和数字，已开启密码复杂度校验功能，口令长度要求至少8位，口令组成包含大小写字母、数字和特殊字符，每半年进行一次口令更换。 | 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； | 已开启登录失败处理功能，登录失败次数：3次，措施：锁定账户10分钟，网络登录连接空闲超时自动退出时间：30分钟。 | 符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 综合日志审计系统采用HTTPS的远程管理方式，用户鉴别信息加密传输，防止鉴别信息在网络传输中被窃听。 | 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。 | 仅使用用户名加口令进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用admin管理员、buz\*\*\*安全管理员、sys\*\*\*系统管理员、aud\*\*\*审计管理员等账户进行登录，不存在匿名账户，并为其分配相关权限。 | 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； | 未重命名或删除默认admin账户，但已修改默认口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 当前使用admin管理员、buz\*\*\*安全管理员、sys\*\*\*系统管理员、aud\*\*\*审计管理员等账户角色，各账户仅分配所需的最小权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 当前设备访问控制粒度达到主体为用户级，客体为界面级。 | 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。 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 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； | 设备已开启审计功能，可对重要的用户行为和重要安全事件进行审计。 | 符合 |
| b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 审计记录包含操作时间、操作人、角色名称、登录IP、操作结果、操作内容等重要信息。 | 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； | 审计记录保存在设备本地仅授权用户可以访问，审计记录每季度备份至本地，管理员账户无法对审计记录进行非预期删除、修改或覆盖，审计记录保存时间长达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。 | 由系统底层对审计进程进行保护，非授权用户无法中断审计。 | 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； | 底层OS及必要服务由设备厂商出厂前配置完成，用户无需登录底层操作系统并验证组件，系统遵循最小化安全原则，仅安装自身所需要的组件和程序。 | 符合 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 当前设备不存在默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的系统服务。 | 符合 |
| c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 通过配置策略限制仅允许总部员工有线、机房运维、网络监控平台等网段可远程登录管理。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 恶意代码防范 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 可信验证 | 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。 | 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。 | 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； | 综合日志审计系统主要涉及鉴别数据、重要审计数据和重要配置数据，其中重要审计数据和重要配置数据不进行传输，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | 综合日志审计系统主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 综合日志审计系统主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | 综合日志审计系统主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 由管理员定期或在重大配置更新后对设备配置文件进行手工备份，备份地点本地运维终端，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | 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。 | 该设备仅作为日志审计，非重要数据处理系统，采用旁路部署，设备宕机不影响业务系统正常运行。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |

* + - * 1. 飞塔防火墙A

**附录D 表‑24安全计算环境-安全设备结果记录表（飞塔防火墙A）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 登录设备需要使用用户名加口令进行身份鉴别，身份标识唯一，口令长度8位以上，口令组成包含特殊字符，大小写字母和数字，已开启口令复杂度策略，口令长度至少8位，口令组成必须包含大小写字母、数字和特殊字符，每半年进行一次口令更换。 | 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； | 已开启登录失败处理功能，登录失败次数：5次，登录失败措施：锁定账户1800秒；网络登录连接空闲超时自动退出时间：30分钟。 | 符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 飞塔防火墙远程管理采用HTTPS，用户鉴别信息加密传输，保证鉴别信息在网络传输中被窃听。 | 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。 | 仅使用用户名加口令进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员等账户进行登录，不存在匿名账户，并为其分配相关权限。 | 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； | 未重命名或删除默认admin账户，但已修改默认口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 当前使用admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员等角色权限，各账户仅分配所需的最小权限，不同账户具备不同的访问权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 当前设备访问控制粒度达到主体为用户级，客体为界面级。 | 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。 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 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； | 设备已开启审计功能，可对重要的用户行为和重要安全事件进行审计。 | 符合 |
| b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 审计记录包含日期/时间、服务、源、文件名、病毒、详情、目的IP、结果、用户、消息、级别、日志描述等内容。 | 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； | 飞塔防火墙已配置SYSLOG日志上传至综合日志审计系统进行收集和保护，审计记录每季度备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达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。 | 由系统底层和综合日志审计系统对审计进程进行保护，非授权用户无法中断审计。 | 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； | 底层OS及必要服务由设备厂商出厂前配置完成，用户无需登录底层操作系统并验证组件，系统遵循最小化安全原则，仅安装自身所需要的组件和程序。 | 符合 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 当前设备不存在默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的系统服务。 | 符合 |
| c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 通过边界配置ACL3001，仅允许10.\*.1.\*，192.\*.9.\*远程管理设备。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 恶意代码防范 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 可信验证 | 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。 | 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。 | 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； | 飞塔防火墙主要涉及鉴别数据、重要审计数据和重要配置数据，其中重要配置数据不进行传输，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的完整性。重要审计数据通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 飞塔防火墙主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+9位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 飞塔防火墙主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | 飞塔防火墙主要涉及鉴别数据，鉴别数据采用SHA512+9位salt的方式，能够保证鉴别数据在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； | 由管理员每月或在重大配置更新后对设备配置文件进行手工备份，备份地点本地运维终端，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | 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。 | 当前设备采用两台设备虚拟化热冗余部署，并已配置主备模式，保证系统稳定运行。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |

* + - * 1. 飞塔防火墙B

**附录D 表‑25安全计算环境-安全设备结果记录表（飞塔防火墙B）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 登录设备需要使用用户名加口令进行身份鉴别，身份标识唯一，口令长度8位以上，口令组成包含特殊字符，大小写字母和数字，已开启口令复杂度策略，口令长度至少8位，口令组成必须包含大小写字母、数字和特殊字符，每半年进行一次口令更换。 | 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； | 已开启登录失败处理功能，登录失败次数：5次，登录失败措施：锁定账户1800秒；网络登录连接空闲超时自动退出时间：30分钟。 | 符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 飞塔防火墙远程管理采用HTTPS，用户鉴别信息加密传输，保证鉴别信息在网络传输中被窃听。 | 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。 | 仅使用用户名加口令进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员等账户进行登录，不存在匿名账户，并为其分配相关权限。 | 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； | 未重命名或删除默认admin账户，但已修改默认口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 当前使用admin管理员、xi\*\*\*系统管理员、an\*\*\*安全管理员、she\*\*\*审计管理员等角色权限，各账户仅分配所需的最小权限，不同账户具备不同的访问权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 当前设备访问控制粒度达到主体为用户级，客体为界面级。 | 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。 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 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； | 设备已开启审计功能，可对重要的用户行为和重要安全事件进行审计。 | 符合 |
| b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 审计记录包含日期/时间、服务、源、文件名、病毒、详情、目的IP、结果、用户、消息、级别、日志描述等内容。 | 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； | 飞塔防火墙已配置SYSLOG日志上传至综合日志审计系统进行收集和保护，审计记录每季度备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达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。 | 由系统底层和综合日志审计系统对审计进程进行保护，非授权用户无法中断审计。 | 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； | 底层OS及必要服务由设备厂商出厂前配置完成，用户无需登录底层操作系统并验证组件，系统遵循最小化安全原则，仅安装自身所需要的组件和程序。 | 符合 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 当前设备不存在默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的系统服务。 | 符合 |
| c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 通过边界配置ACL3001，仅允许10.\*.1.\*，192.\*.9.\*远程管理设备。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 恶意代码防范 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 可信验证 | 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。 | 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。 | 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； | 飞塔防火墙主要涉及鉴别数据、重要审计数据和重要配置数据，其中重要配置数据不进行传输，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的完整性。重要审计数据通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 飞塔防火墙主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+9位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 飞塔防火墙主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | 飞塔防火墙主要涉及鉴别数据，鉴别数据采用SHA512+9位salt的方式，能够保证鉴别数据在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； | 由管理员每月或在重大配置更新后对设备配置文件进行手工备份，备份地点本地运维终端，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | 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。 | 当前设备采用两台设备虚拟化热冗余部署，并已配置主备模式，保证系统稳定运行。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |

* + - 1. 服务器和终端
         1. CloudOS1

**附录D 表‑26安全计算环境-服务器和终端结果记录表（CloudOS1）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 使用用户名加口令身份验证方式对用户进行鉴别；用户名作为用户唯一身份标识；无空口令账户；当前口令复杂度包含数字、大小写、特殊字符；口令长度8位以上；已开启口令复杂度策略lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1；定期更换口令时间为0， 口令策略： PASS\_MAX\_DAYS 99999 PASS\_MIN\_DAYS 0 PASS\_MIN\_LEN 8 PASS\_WARN\_AGE 7。 | 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； | 已启用登录失败处理功能，登录失败3次，锁定30分钟，未启用登录连接超时自动退出功能。 | 部分符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 服务器采用SSH方式进行远程管理，通信过程中基于SSL协议传输数据，用户口令信息加密传输，可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。 | 服务器设备仅采用用户名+口令方式进行登录管理，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等账户，不存在匿名账户，并为其分配了相关权限。 | 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； | 未重命名或删除默认账户root，但已修改默认账户口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 服务器使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等角色权限，各账户仅分配所需的最小权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 已配置访问控制功能，主体为用户级，客体为文件级。 | 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。 | 服务器SELinux设置为Permissive，不能实现通过安全标记强制控制主体对客体的访问。 | 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； | rsyslog日志进程和auditd日志审计进程均已开启，审计范围覆盖到每个用户重要安全事件、重要用户行为等，日志文件存放在/var/log文件夹下，包括/var/log/messages等日志文件。 | 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； | 审计记录包括事件的日期（年月日等），时间、类型、成功与否、事件内容、IP地址等。 | 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； | 审计记录已通过SYSLOG的方式上传综合日志审计系统进行保护，审计记录每季度进行备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达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。 | 通过综合日志审计系统对审计记录进行保护对审计进程进行保护，非授权用户无法中断审计。 | 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； | 系统遵循最小安装原则，未安装不必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； | 服务器未开启非必要的端口，不存在默认共享和高危端口的使用。 | 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； | 通过服务器防火墙配置策略仅允许地址范围总部有线网段，机房运维网段可进行远程管理。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 服务器未部署主机入侵防护软件，无法对主机重要节点进行入侵行为进行检查、限制并报警。 | 不符合 |
| 恶意代码防范 | 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。 | 服务器未安装防恶意代码软件，无法识别入侵和病毒行为，无法将其有效阻断。 | 不符合 |
| 可信验证 | 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。 | 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。 | 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； | 服务器主要涉及鉴别数据、重要配置数据和重要审计数据，其中重要配置数据不进行传输，服务器通过SSH的方式进行远程管理，其鉴别数据传输是基于SSL协议实现，能够保证鉴别数据在传输过程中的完整性。重要审计记录通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 服务器主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 服务器主要涉及鉴别数据，鉴别数据采用SSH的方式，能够保证鉴别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。 | 服务器主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 服务器数据通过数腾备份软件备份；备份策略：增量备份；备份频率：每天；备份地点：本地服务器，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 通过数腾软件对重要服务器数据每天进行增量备份，然后通过软件介质实时同步，将重要数据备份至宁波建投子公司。 | 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。 | 服务器采用多台设备热备方式部署，可实现热冗余，保证系统高可用性。 | 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； | linux系统退出时自动对鉴别信息所在的存储空间进行完全的清除。 | 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。 | HISTSIZE=1000，history无法查询上次登录的命令，可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。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |

* + - * 1. CloudOS2

**附录D 表‑27安全计算环境-服务器和终端结果记录表（CloudOS2）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 使用用户名加口令身份验证方式对用户进行鉴别；用户名作为用户唯一身份标识；无空口令账户；当前口令复杂度包含数字、大小写、特殊字符；口令长度8位以上；已开启口令复杂度策略lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1；定期更换口令时间为0， 口令策略： PASS\_MAX\_DAYS 99999 PASS\_MIN\_DAYS 0 PASS\_MIN\_LEN 8 PASS\_WARN\_AGE 7。 | 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； | 已启用登录失败处理功能，登录失败3次，锁定30分钟，未启用登录连接超时自动退出功能。 | 部分符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 服务器采用SSH方式进行远程管理，通信过程中基于SSL协议传输数据，用户口令信息加密传输，可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。 | 服务器设备仅采用用户名+口令方式进行登录管理，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等账户，不存在匿名账户，并为其分配了相关权限。 | 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； | 未重命名或删除默认账户root，但已修改默认账户口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 服务器使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等角色权限，各账户仅分配所需的最小权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 已配置访问控制功能，主体为用户级，客体为文件级。 | 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。 | 服务器SELinux设置为Permissive，不能实现通过安全标记强制控制主体对客体的访问。 | 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； | rsyslog日志进程和auditd日志审计进程均已开启，审计范围覆盖到每个用户重要安全事件、重要用户行为等，日志文件存放在/var/log文件夹下，包括/var/log/messages等日志文件。 | 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； | 审计记录包括事件的日期（年月日等），时间、类型、成功与否、事件内容、IP地址等。 | 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； | 审计记录已通过SYSLOG的方式上传综合日志审计系统进行保护，审计记录每季度进行备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达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。 | 通过综合日志审计系统对审计记录进行保护对审计进程进行保护，非授权用户无法中断审计。 | 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； | 系统遵循最小安装原则，未安装不必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； | 服务器未开启非必要的端口，不存在默认共享和高危端口的使用。 | 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； | 通过服务器防火墙配置策略仅允许地址范围总部有线网段，机房运维网段可进行远程管理。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 服务器未部署主机入侵防护软件，无法对主机重要节点进行入侵行为进行检查、限制并报警。 | 不符合 |
| 恶意代码防范 | 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。 | 服务器未安装防恶意代码软件，无法识别入侵和病毒行为，无法将其有效阻断。 | 不符合 |
| 可信验证 | 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。 | 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。 | 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； | 服务器主要涉及鉴别数据、重要配置数据和重要审计数据，其中重要配置数据不进行传输，服务器通过SSH的方式进行远程管理，其鉴别数据传输是基于SSL协议实现，能够保证鉴别数据在传输过程中的完整性。重要审计记录通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 服务器主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 服务器主要涉及鉴别数据，鉴别数据采用SSH的方式，能够保证鉴别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。 | 服务器主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 服务器数据通过数腾备份软件备份；备份策略：增量备份；备份频率：每天；备份地点：本地服务器，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 通过数腾软件对重要服务器数据每天进行增量备份，然后通过软件介质实时同步，将重要数据备份至宁波建投子公司。 | 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。 | 服务器采用多台设备热备方式部署，可实现热冗余，保证系统高可用性。 | 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； | linux系统退出时自动对鉴别信息所在的存储空间进行完全的清除。 | 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。 | HISTSIZE=1000，history无法查询上次登录的命令，可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。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |

* + - * 1. CloudOS3

**附录D 表‑28安全计算环境-服务器和终端结果记录表（CloudOS3）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 使用用户名加口令身份验证方式对用户进行鉴别；用户名作为用户唯一身份标识；无空口令账户；当前口令复杂度包含数字、大小写、特殊字符；口令长度8位以上；已开启口令复杂度策略lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1；定期更换口令时间为0， 口令策略： PASS\_MAX\_DAYS 99999 PASS\_MIN\_DAYS 0 PASS\_MIN\_LEN 8 PASS\_WARN\_AGE 7。 | 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； | 已启用登录失败处理功能，登录失败3次，锁定30分钟，未启用登录连接超时自动退出功能。 | 部分符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 服务器采用SSH方式进行远程管理，通信过程中基于SSL协议传输数据，用户口令信息加密传输，可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。 | 服务器设备仅采用用户名+口令方式进行登录管理，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等账户，不存在匿名账户，并为其分配了相关权限。 | 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； | 未重命名或删除默认账户root，但已修改默认账户口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 服务器使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等角色权限，各账户仅分配所需的最小权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 已配置访问控制功能，主体为用户级，客体为文件级。 | 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。 | 服务器SELinux设置为Permissive，不能实现通过安全标记强制控制主体对客体的访问。 | 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； | rsyslog日志进程和auditd日志审计进程均已开启，审计范围覆盖到每个用户重要安全事件、重要用户行为等，日志文件存放在/var/log文件夹下，包括/var/log/messages等日志文件。 | 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； | 审计记录包括事件的日期（年月日等），时间、类型、成功与否、事件内容、IP地址等。 | 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； | 审计记录已通过SYSLOG的方式上传综合日志审计系统进行保护，审计记录每季度进行备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达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。 | 通过综合日志审计系统对审计记录进行保护对审计进程进行保护，非授权用户无法中断审计。 | 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； | 系统遵循最小安装原则，未安装不必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； | 服务器未开启非必要的端口，不存在默认共享和高危端口的使用。 | 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； | 通过服务器防火墙配置策略仅允许地址范围总部有线网段，机房运维网段可进行远程管理。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 服务器未部署主机入侵防护软件，无法对主机重要节点进行入侵行为进行检查、限制并报警。 | 不符合 |
| 恶意代码防范 | 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。 | 服务器未安装防恶意代码软件，无法识别入侵和病毒行为，无法将其有效阻断。 | 不符合 |
| 可信验证 | 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。 | 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。 | 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； | 服务器主要涉及鉴别数据、重要配置数据和重要审计数据，其中重要配置数据不进行传输，服务器通过SSH的方式进行远程管理，其鉴别数据传输是基于SSL协议实现，能够保证鉴别数据在传输过程中的完整性。重要审计记录通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 服务器主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 服务器主要涉及鉴别数据，鉴别数据采用SSH的方式，能够保证鉴别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。 | 服务器主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 服务器数据通过数腾备份软件备份；备份策略：增量备份；备份频率：每天；备份地点：本地服务器，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 通过数腾软件对重要服务器数据每天进行增量备份，然后通过软件介质实时同步，将重要数据备份至宁波建投子公司。 | 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。 | 服务器采用多台设备热备方式部署，可实现热冗余，保证系统高可用性。 | 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； | linux系统退出时自动对鉴别信息所在的存储空间进行完全的清除。 | 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。 | HISTSIZE=1000，history无法查询上次登录的命令，可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。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |

* + - * 1. CVK01

**附录D 表‑29安全计算环境-服务器和终端结果记录表（CVK01）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 使用用户名加口令身份验证方式对用户进行鉴别； 用户名作为用户唯一身份标识； 无空口令账户；已配置口令复杂度策略； lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1； 口令复杂度包含数字、大小写、特殊字符； 口令长度8位以上； 定期更换口令时间为0； 口令策略： PASS\_MAX\_DAYS 99999 PASS\_MIN\_DAYS 0 PASS\_MIN\_LEN 8 PASS\_WARN\_AGE 7。 | 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； | 已启用登录失败处理功能，登录失败3次，锁定30分钟，超时断开连接已开启：TMOUT=300，已开启登录连接超时自动退出功能。 | 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； | 服务器采用SSH方式进行远程管理，通信过程中基于SSL协议传输数据，用户口令信息加密传输，可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。 | 服务器设备仅采用用户名+口令方式进行登录管理，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等账户，不存在匿名账户，并为其分配了相关权限。 | 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； | 未重命名或删除默认账户root，但已修改默认账户口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 服务器使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等角色权限，各账户仅分配所需的最小权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 已配置访问控制功能，主体为用户级，客体为文件级。 | 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。 | 服务器SELinux设置为Permissive，不能实现通过安全标记强制控制主体对客体的访问。 | 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； | rsyslog日志进程和auditd日志审计进程均已开启，审计范围覆盖到每个用户重要安全事件、重要用户行为等，日志文件存放在/var/log文件夹下，包括/var/log/messages等日志文件。 | 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； | 审计记录包括事件的日期（年月日等），时间、类型、成功与否、事件内容、IP地址等。 | 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； | 审计记录已通过SYSLOG的方式上传综合日志审计系统进行保护，审计记录每季度进行备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达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。 | 通过综合日志审计系统对审计记录进行保护对审计进程进行保护，非授权用户无法中断审计。 | 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； | 系统遵循最小安装原则，未安装不必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； | 服务器未开启非必要的端口，不存在默认共享和高危端口的使用。 | 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； | 通过服务器防火墙配置策略仅允许地址范围总部有线网段，机房运维网段可进行远程管理。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 服务器未部署主机入侵防护软件，无法对主机重要节点进行入侵行为进行检查、限制并报警。 | 不符合 |
| 恶意代码防范 | 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。 | 服务器未安装防恶意代码软件，无法识别入侵和病毒行为，无法将其有效阻断。 | 不符合 |
| 可信验证 | 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。 | 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。 | 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； | 服务器主要涉及鉴别数据、重要配置数据和重要审计数据，其中重要配置数据不进行传输，服务器通过SSH的方式进行远程管理，其鉴别数据传输是基于SSL协议实现，能够保证鉴别数据在传输过程中的完整性。重要审计记录通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 服务器主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 服务器主要涉及鉴别数据，鉴别数据采用SSH的方式，能够保证鉴别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。 | 服务器主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 服务器数据通过数腾备份软件备份；备份策略：增量备份；备份频率：每天；备份地点：本地服务器，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 通过数腾软件对重要服务器数据每天进行增量备份，然后通过软件介质实时同步，将重要数据备份至宁波建投子公司。 | 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。 | 该服务器为云平台提供最基础的系统资源，服务器采用多设备集群方式进行部署，可实现热冗余，保证系统高可用性。 | 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； | linux系统退出时自动对鉴别信息所在的存储空间进行完全的清除。 | 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。 | HISTSIZE=5，history无法查询上次登录的命令，可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。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |

* + - * 1. CVK02

**附录D 表‑30安全计算环境-服务器和终端结果记录表（CVK02）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 使用用户名加口令身份验证方式对用户进行鉴别； 用户名作为用户唯一身份标识； 无空口令账户；已配置口令复杂度策略； lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1； 口令复杂度包含数字、大小写、特殊字符； 口令长度8位以上； 定期更换口令时间为0； 口令策略： PASS\_MAX\_DAYS 99999 PASS\_MIN\_DAYS 0 PASS\_MIN\_LEN 8 PASS\_WARN\_AGE 7。 | 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； | 已启用登录失败处理功能，登录失败3次，锁定30分钟，超时断开连接已开启：TMOUT=300，已开启登录连接超时自动退出功能。 | 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； | 服务器采用SSH方式进行远程管理，通信过程中基于SSL协议传输数据，用户口令信息加密传输，可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。 | 服务器设备仅采用用户名+口令方式进行登录管理，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等账户，不存在匿名账户，并为其分配了相关权限。 | 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； | 未重命名或删除默认账户root，但已修改默认账户口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 服务器使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等角色权限，各账户仅分配所需的最小权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 已配置访问控制功能，主体为用户级，客体为文件级。 | 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。 | 服务器SELinux设置为Permissive，不能实现通过安全标记强制控制主体对客体的访问。 | 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； | rsyslog日志进程和auditd日志审计进程均已开启，审计范围覆盖到每个用户重要安全事件、重要用户行为等，日志文件存放在/var/log文件夹下，包括/var/log/messages等日志文件。 | 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； | 审计记录包括事件的日期（年月日等），时间、类型、成功与否、事件内容、IP地址等。 | 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； | 审计记录已通过SYSLOG的方式上传综合日志审计系统进行保护，审计记录每季度进行备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达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。 | 通过综合日志审计系统对审计记录进行保护对审计进程进行保护，非授权用户无法中断审计。 | 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； | 系统遵循最小安装原则，未安装不必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； | 服务器未开启非必要的端口，不存在默认共享和高危端口的使用。 | 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； | 通过服务器防火墙配置策略仅允许地址范围总部有线网段，机房运维网段可进行远程管理。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 服务器未部署主机入侵防护软件，无法对主机重要节点进行入侵行为进行检查、限制并报警。 | 不符合 |
| 恶意代码防范 | 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。 | 服务器未安装防恶意代码软件，无法识别入侵和病毒行为，无法将其有效阻断。 | 不符合 |
| 可信验证 | 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。 | 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。 | 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； | 服务器主要涉及鉴别数据、重要配置数据和重要审计数据，其中重要配置数据不进行传输，服务器通过SSH的方式进行远程管理，其鉴别数据传输是基于SSL协议实现，能够保证鉴别数据在传输过程中的完整性。重要审计记录通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 服务器主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 服务器主要涉及鉴别数据，鉴别数据采用SSH的方式，能够保证鉴别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。 | 服务器主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 服务器数据通过数腾备份软件备份；备份策略：增量备份；备份频率：每天；备份地点：本地服务器，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 通过数腾软件对重要服务器数据每天进行增量备份，然后通过软件介质实时同步，将重要数据备份至宁波建投子公司。 | 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。 | 该服务器为云平台提供最基础的系统资源，服务器采用多设备集群方式进行部署，可实现热冗余，保证系统高可用性。 | 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； | linux系统退出时自动对鉴别信息所在的存储空间进行完全的清除。 | 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。 | HISTSIZE=5，history无法查询上次登录的命令，可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。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |

* + - * 1. CVK03

**附录D 表‑31安全计算环境-服务器和终端结果记录表（CVK03）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 使用用户名加口令身份验证方式对用户进行鉴别； 用户名作为用户唯一身份标识； 无空口令账户；已配置口令复杂度策略； lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1； 口令复杂度包含数字、大小写、特殊字符； 口令长度8位以上； 定期更换口令时间为0； 口令策略： PASS\_MAX\_DAYS 99999 PASS\_MIN\_DAYS 0 PASS\_MIN\_LEN 8 PASS\_WARN\_AGE 7。 | 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； | 已启用登录失败处理功能，登录失败3次，锁定30分钟，超时断开连接已开启：TMOUT=300，已开启登录连接超时自动退出功能。 | 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； | 服务器采用SSH方式进行远程管理，通信过程中基于SSL协议传输数据，用户口令信息加密传输，可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。 | 服务器设备仅采用用户名+口令方式进行登录管理，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等账户，不存在匿名账户，并为其分配了相关权限。 | 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； | 未重命名或删除默认账户root，但已修改默认账户口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 服务器使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等角色权限，各账户仅分配所需的最小权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 已配置访问控制功能，主体为用户级，客体为文件级。 | 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。 | 服务器SELinux设置为Permissive，不能实现通过安全标记强制控制主体对客体的访问。 | 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； | rsyslog日志进程和auditd日志审计进程均已开启，审计范围覆盖到每个用户重要安全事件、重要用户行为等，日志文件存放在/var/log文件夹下，包括/var/log/messages等日志文件。 | 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； | 审计记录包括事件的日期（年月日等），时间、类型、成功与否、事件内容、IP地址等。 | 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； | 审计记录已通过SYSLOG的方式上传综合日志审计系统进行保护，审计记录每季度进行备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达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。 | 通过综合日志审计系统对审计记录进行保护对审计进程进行保护，非授权用户无法中断审计。 | 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； | 系统遵循最小安装原则，未安装不必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； | 服务器未开启非必要的端口，不存在默认共享和高危端口的使用。 | 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； | 通过服务器防火墙配置策略仅允许地址范围总部有线网段，机房运维网段可进行远程管理。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 服务器未部署主机入侵防护软件，无法对主机重要节点进行入侵行为进行检查、限制并报警。 | 不符合 |
| 恶意代码防范 | 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。 | 服务器未安装防恶意代码软件，无法识别入侵和病毒行为，无法将其有效阻断。 | 不符合 |
| 可信验证 | 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。 | 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。 | 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； | 服务器主要涉及鉴别数据、重要配置数据和重要审计数据，其中重要配置数据不进行传输，服务器通过SSH的方式进行远程管理，其鉴别数据传输是基于SSL协议实现，能够保证鉴别数据在传输过程中的完整性。重要审计记录通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 服务器主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 服务器主要涉及鉴别数据，鉴别数据采用SSH的方式，能够保证鉴别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。 | 服务器主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 服务器数据通过数腾备份软件备份；备份策略：增量备份；备份频率：每天；备份地点：本地服务器，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 通过数腾软件对重要服务器数据每天进行增量备份，然后通过软件介质实时同步，将重要数据备份至宁波建投子公司。 | 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。 | 该服务器为云平台提供最基础的系统资源，服务器采用多设备集群方式进行部署，可实现热冗余，保证系统高可用性。 | 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； | linux系统退出时自动对鉴别信息所在的存储空间进行完全的清除。 | 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。 | HISTSIZE=5，history无法查询上次登录的命令，可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。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |

* + - * 1. CVK04

**附录D 表‑32安全计算环境-服务器和终端结果记录表（CVK04）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 使用用户名加口令身份验证方式对用户进行鉴别； 用户名作为用户唯一身份标识； 无空口令账户；已配置口令复杂度策略； lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1； 口令复杂度包含数字、大小写、特殊字符； 口令长度8位以上； 定期更换口令时间为0； 口令策略： PASS\_MAX\_DAYS 99999 PASS\_MIN\_DAYS 0 PASS\_MIN\_LEN 8 PASS\_WARN\_AGE 7。 | 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； | 已启用登录失败处理功能，登录失败3次，锁定30分钟，超时断开连接已开启：TMOUT=300，已开启登录连接超时自动退出功能。 | 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； | 服务器采用SSH方式进行远程管理，通信过程中基于SSL协议传输数据，用户口令信息加密传输，可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。 | 服务器设备仅采用用户名+口令方式进行登录管理，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等账户，不存在匿名账户，并为其分配了相关权限。 | 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； | 未重命名或删除默认账户root，但已修改默认账户口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 服务器使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等角色权限，各账户仅分配所需的最小权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 已配置访问控制功能，主体为用户级，客体为文件级。 | 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。 | 服务器SELinux设置为Permissive，不能实现通过安全标记强制控制主体对客体的访问。 | 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； | rsyslog日志进程和auditd日志审计进程均已开启，审计范围覆盖到每个用户重要安全事件、重要用户行为等，日志文件存放在/var/log文件夹下，包括/var/log/messages等日志文件。 | 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； | 审计记录包括事件的日期（年月日等），时间、类型、成功与否、事件内容、IP地址等。 | 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； | 审计记录已通过SYSLOG的方式上传综合日志审计系统进行保护，审计记录每季度进行备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达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。 | 通过综合日志审计系统对审计记录进行保护对审计进程进行保护，非授权用户无法中断审计。 | 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； | 系统遵循最小安装原则，未安装不必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； | 服务器未开启非必要的端口，不存在默认共享和高危端口的使用。 | 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； | 通过服务器防火墙配置策略仅允许地址范围总部有线网段，机房运维网段可进行远程管理。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 服务器未部署主机入侵防护软件，无法对主机重要节点进行入侵行为进行检查、限制并报警。 | 不符合 |
| 恶意代码防范 | 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。 | 服务器未安装防恶意代码软件，无法识别入侵和病毒行为，无法将其有效阻断。 | 不符合 |
| 可信验证 | 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。 | 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。 | 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； | 服务器主要涉及鉴别数据、重要配置数据和重要审计数据，其中重要配置数据不进行传输，服务器通过SSH的方式进行远程管理，其鉴别数据传输是基于SSL协议实现，能够保证鉴别数据在传输过程中的完整性。重要审计记录通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 服务器主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 服务器主要涉及鉴别数据，鉴别数据采用SSH的方式，能够保证鉴别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。 | 服务器主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 服务器数据通过数腾备份软件备份；备份策略：增量备份；备份频率：每天；备份地点：本地服务器，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 通过数腾软件对重要服务器数据每天进行增量备份，然后通过软件介质实时同步，将重要数据备份至宁波建投子公司。 | 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。 | 该服务器为云平台提供最基础的系统资源，服务器采用多设备集群方式进行部署，可实现热冗余，保证系统高可用性。 | 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； | linux系统退出时自动对鉴别信息所在的存储空间进行完全的清除。 | 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。 | HISTSIZE=5，history无法查询上次登录的命令，可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。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |

* + - * 1. CVK05

**附录D 表‑33安全计算环境-服务器和终端结果记录表（CVK05）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 使用用户名加口令身份验证方式对用户进行鉴别； 用户名作为用户唯一身份标识； 无空口令账户；已配置口令复杂度策略； lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1； 口令复杂度包含数字、大小写、特殊字符； 口令长度8位以上； 定期更换口令时间为0； 口令策略： PASS\_MAX\_DAYS 99999 PASS\_MIN\_DAYS 0 PASS\_MIN\_LEN 8 PASS\_WARN\_AGE 7。 | 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； | 已启用登录失败处理功能，登录失败3次，锁定30分钟，超时断开连接已开启：TMOUT=300，已开启登录连接超时自动退出功能。 | 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； | 服务器采用SSH方式进行远程管理，通信过程中基于SSL协议传输数据，用户口令信息加密传输，可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。 | 服务器设备仅采用用户名+口令方式进行登录管理，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等账户，不存在匿名账户，并为其分配了相关权限。 | 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； | 未重命名或删除默认账户root，但已修改默认账户口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 服务器使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等角色权限，各账户仅分配所需的最小权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 已配置访问控制功能，主体为用户级，客体为文件级。 | 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。 | 服务器SELinux设置为Permissive，不能实现通过安全标记强制控制主体对客体的访问。 | 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； | rsyslog日志进程和auditd日志审计进程均已开启，审计范围覆盖到每个用户重要安全事件、重要用户行为等，日志文件存放在/var/log文件夹下，包括/var/log/messages等日志文件。 | 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； | 审计记录包括事件的日期（年月日等），时间、类型、成功与否、事件内容、IP地址等。 | 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； | 审计记录已通过SYSLOG的方式上传综合日志审计系统进行保护，审计记录每季度进行备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达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。 | 通过综合日志审计系统对审计记录进行保护对审计进程进行保护，非授权用户无法中断审计。 | 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； | 系统遵循最小安装原则，未安装不必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； | 服务器未开启非必要的端口，不存在默认共享和高危端口的使用。 | 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； | 通过服务器防火墙配置策略仅允许地址范围总部有线网段，机房运维网段可进行远程管理。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 服务器未部署主机入侵防护软件，无法对主机重要节点进行入侵行为进行检查、限制并报警。 | 不符合 |
| 恶意代码防范 | 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。 | 服务器未安装防恶意代码软件，无法识别入侵和病毒行为，无法将其有效阻断。 | 不符合 |
| 可信验证 | 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。 | 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。 | 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； | 服务器主要涉及鉴别数据、重要配置数据和重要审计数据，其中重要配置数据不进行传输，服务器通过SSH的方式进行远程管理，其鉴别数据传输是基于SSL协议实现，能够保证鉴别数据在传输过程中的完整性。重要审计记录通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 服务器主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 服务器主要涉及鉴别数据，鉴别数据采用SSH的方式，能够保证鉴别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。 | 服务器主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 服务器数据通过数腾备份软件备份；备份策略：增量备份；备份频率：每天；备份地点：本地服务器，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 通过数腾软件对重要服务器数据每天进行增量备份，然后通过软件介质实时同步，将重要数据备份至宁波建投子公司。 | 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。 | 该服务器为云平台提供最基础的系统资源，服务器采用多设备集群方式进行部署，可实现热冗余，保证系统高可用性。 | 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； | linux系统退出时自动对鉴别信息所在的存储空间进行完全的清除。 | 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。 | HISTSIZE=5，history无法查询上次登录的命令，可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。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |

* + - * 1. CVM01

**附录D 表‑34安全计算环境-服务器和终端结果记录表（CVM01）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 使用用户名加口令身份验证方式对用户进行鉴别； 用户名作为用户唯一身份标识； 无空口令账户；已配置口令复杂度策略； lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1； 口令复杂度包含数字、大小写、特殊字符； 口令长度8位以上； 定期更换口令时间为0； 口令策略： PASS\_MAX\_DAYS 99999 PASS\_MIN\_DAYS 0 PASS\_MIN\_LEN 8 PASS\_WARN\_AGE 7。 | 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； | 已启用登录失败处理功能，登录失败3次，锁定30分钟，超时断开连接已开启：TMOUT=300，已开启登录连接超时自动退出功能。 | 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； | 服务器采用SSH方式进行远程管理，通信过程中基于SSL协议传输数据，用户口令信息加密传输，可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。 | 服务器设备仅采用用户名+口令方式进行登录管理，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等账户，不存在匿名账户，并为其分配了相关权限。 | 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； | 未重命名或删除默认账户root，但已修改默认账户口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 服务器使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等角色权限，各账户仅分配所需的最小权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 已配置访问控制功能，主体为用户级，客体为文件级。 | 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。 | 服务器SELinux设置为Permissive，不能实现通过安全标记强制控制主体对客体的访问。 | 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； | rsyslog日志进程和auditd日志审计进程均已开启，审计范围覆盖到每个用户重要安全事件、重要用户行为等，日志文件存放在/var/log文件夹下，包括/var/log/messages等日志文件。 | 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； | 审计记录包括事件的日期（年月日等），时间、类型、成功与否、事件内容、IP地址等。 | 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； | 审计记录已通过SYSLOG的方式上传综合日志审计系统进行保护，审计记录每季度进行备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达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。 | 通过综合日志审计系统对审计记录进行保护对审计进程进行保护，非授权用户无法中断审计。 | 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； | 系统遵循最小安装原则，未安装不必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； | 服务器未开启非必要的端口，不存在默认共享和高危端口的使用。 | 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； | 通过服务器防火墙配置策略仅允许地址范围总部有线网段，机房运维网段可进行远程管理。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 服务器未部署主机入侵防护软件，无法对主机重要节点进行入侵行为进行检查、限制并报警。 | 不符合 |
| 恶意代码防范 | 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。 | 服务器未安装防恶意代码软件，无法识别入侵和病毒行为，无法将其有效阻断。 | 不符合 |
| 可信验证 | 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。 | 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。 | 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； | 服务器主要涉及鉴别数据、重要配置数据和重要审计数据，其中重要配置数据不进行传输，服务器通过SSH的方式进行远程管理，其鉴别数据传输是基于SSL协议实现，能够保证鉴别数据在传输过程中的完整性。重要审计记录通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 服务器主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 服务器主要涉及鉴别数据，鉴别数据采用SSH的方式，能够保证鉴别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。 | 服务器主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 服务器数据通过数腾备份软件备份；备份策略：增量备份；备份频率：每天；备份地点：本地服务器，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 通过数腾软件对重要服务器数据每天进行增量备份，然后通过软件介质实时同步，将重要数据备份至宁波建投子公司。 | 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。 | 该服务器为云平台提供最基础的系统资源，服务器采用多设备集群方式进行部署，可实现热冗余，保证系统高可用性。 | 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； | linux系统退出时自动对鉴别信息所在的存储空间进行完全的清除。 | 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。 | HISTSIZE=5，history无法查询上次登录的命令，可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。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |

* + - * 1. CVM02

**附录D 表‑35安全计算环境-服务器和终端结果记录表（CVM02）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 使用用户名加口令身份验证方式对用户进行鉴别； 用户名作为用户唯一身份标识； 无空口令账户；已配置口令复杂度策略； lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1； 口令复杂度包含数字、大小写、特殊字符； 口令长度8位以上； 定期更换口令时间为0； 口令策略： PASS\_MAX\_DAYS 99999 PASS\_MIN\_DAYS 0 PASS\_MIN\_LEN 8 PASS\_WARN\_AGE 7。 | 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； | 已启用登录失败处理功能，登录失败3次，锁定30分钟，超时断开连接已开启：TMOUT=300，已开启登录连接超时自动退出功能。 | 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； | 服务器采用SSH方式进行远程管理，通信过程中基于SSL协议传输数据，用户口令信息加密传输，可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。 | 服务器设备仅采用用户名+口令方式进行登录管理，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等账户，不存在匿名账户，并为其分配了相关权限。 | 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； | 未重命名或删除默认账户root，但已修改默认账户口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 服务器使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等角色权限，各账户仅分配所需的最小权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 已配置访问控制功能，主体为用户级，客体为文件级。 | 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。 | 服务器SELinux设置为Permissive，不能实现通过安全标记强制控制主体对客体的访问。 | 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； | rsyslog日志进程和auditd日志审计进程均已开启，审计范围覆盖到每个用户重要安全事件、重要用户行为等，日志文件存放在/var/log文件夹下，包括/var/log/messages等日志文件。 | 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； | 审计记录包括事件的日期（年月日等），时间、类型、成功与否、事件内容、IP地址等。 | 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； | 审计记录已通过SYSLOG的方式上传综合日志审计系统进行保护，审计记录每季度进行备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达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。 | 通过综合日志审计系统对审计记录进行保护对审计进程进行保护，非授权用户无法中断审计。 | 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； | 系统遵循最小安装原则，未安装不必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； | 服务器未开启非必要的端口，不存在默认共享和高危端口的使用。 | 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； | 通过服务器防火墙配置策略仅允许地址范围总部有线网段，机房运维网段可进行远程管理。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 服务器未部署主机入侵防护软件，无法对主机重要节点进行入侵行为进行检查、限制并报警。 | 不符合 |
| 恶意代码防范 | 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。 | 服务器未安装防恶意代码软件，无法识别入侵和病毒行为，无法将其有效阻断。 | 不符合 |
| 可信验证 | 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。 | 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。 | 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； | 服务器主要涉及鉴别数据、重要配置数据和重要审计数据，其中重要配置数据不进行传输，服务器通过SSH的方式进行远程管理，其鉴别数据传输是基于SSL协议实现，能够保证鉴别数据在传输过程中的完整性。重要审计记录通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 服务器主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 服务器主要涉及鉴别数据，鉴别数据采用SSH的方式，能够保证鉴别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。 | 服务器主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 服务器数据通过数腾备份软件备份；备份策略：增量备份；备份频率：每天；备份地点：本地服务器，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 通过数腾软件对重要服务器数据每天进行增量备份，然后通过软件介质实时同步，将重要数据备份至宁波建投子公司。 | 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。 | 该服务器为云平台提供最基础的系统资源，服务器采用多设备集群方式进行部署，可实现热冗余，保证系统高可用性。 | 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； | linux系统退出时自动对鉴别信息所在的存储空间进行完全的清除。 | 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。 | HISTSIZE=5，history无法查询上次登录的命令，可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。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |

* + - * 1. SDN01

**附录D 表‑36安全计算环境-服务器和终端结果记录表（SDN01）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 使用用户名加口令身份验证方式对用户进行鉴别； 用户名作为用户唯一身份标识； 无空口令账户； 口令复杂度包含数字、大小写、特殊字符； 口令长度8位以上； 定期更换口令时间为90； 已配置口令复杂度策略： lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1； 口令策略： PASS\_MAX\_DAYS 90 PASS\_MIN\_DAYS 0 PASS\_MIN\_LEN 8 PASS\_WARN\_AGE 7 已配置口令复杂度策略及口令有限期策略。 | 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； | 已启用登录失败处理功能，登录失败3次，锁定30分钟，，超时断开连接已开启：TMOUT=300，已开启登录连接超时自动退出功能。 | 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； | 服务器采用SSH方式进行远程管理，通信过程中基于SSL协议传输数据，用户口令信息加密传输，可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。 | 服务器设备仅采用用户名+口令方式进行登录管理，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等账户，不存在匿名账户，并为其分配了相关权限。 | 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； | 未重命名或删除默认账户root，但已修改默认账户口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 服务器使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等角色权限，各账户仅分配所需的最小权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 已配置访问控制功能，主体为用户级，客体为文件级。 | 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。 | 服务器SELinux设置为Permissive，不能实现通过安全标记强制控制主体对客体的访问。 | 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； | rsyslog日志进程和auditd日志审计进程均已开启，审计范围覆盖到每个用户重要安全事件、重要用户行为等，日志文件存放在/var/log文件夹下，包括/var/log/messages等日志文件。 | 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； | 审计记录包括事件的日期（年月日等），时间、类型、成功与否、事件内容、IP地址等。 | 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； | 审计记录已通过SYSLOG的方式上传综合日志审计系统进行保护，审计记录每季度进行备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达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。 | 通过综合日志审计系统对审计记录进行保护对审计进程进行保护，非授权用户无法中断审计。 | 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； | 系统遵循最小安装原则，未安装不必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； | 服务器未开启非必要的端口，不存在默认共享和高危端口的使用。 | 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； | 通过服务器防火墙配置策略仅允许地址范围总部有线网段，机房运维网段可进行远程管理。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 服务器未部署主机入侵防护软件，无法对主机重要节点进行入侵行为进行检查、限制并报警。 | 不符合 |
| 恶意代码防范 | 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。 | 服务器未安装防恶意代码软件，无法识别入侵和病毒行为，无法将其有效阻断。 | 不符合 |
| 可信验证 | 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。 | 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。 | 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； | 服务器主要涉及鉴别数据、重要配置数据和重要审计数据，其中重要配置数据不进行传输，服务器通过SSH的方式进行远程管理，其鉴别数据传输是基于SSL协议实现，能够保证鉴别数据在传输过程中的完整性。重要审计记录通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 服务器主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 服务器主要涉及鉴别数据，鉴别数据采用SSH的方式，能够保证鉴别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。 | 服务器主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 服务器数据通过数腾备份软件备份；备份策略：增量备份；备份频率：每天；备份地点：本地服务器，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 通过数腾软件对重要服务器数据每天进行增量备份，然后通过软件介质实时同步，将重要数据备份至宁波建投子公司。 | 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。 | 服务器采用多设备热备方式部署，可实现热冗余，保证系统高可用性。 | 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； | linux系统退出时自动对鉴别信息所在的存储空间进行完全的清除。 | 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。 | HISTSIZE=1000，history无法查询上次登录的命令，可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。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |

* + - * 1. SDN02

**附录D 表‑37安全计算环境-服务器和终端结果记录表（SDN02）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 使用用户名加口令身份验证方式对用户进行鉴别； 用户名作为用户唯一身份标识； 无空口令账户； 口令复杂度包含数字、大小写、特殊字符； 口令长度8位以上； 定期更换口令时间为90； 已配置口令复杂度策略： lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1； 口令策略： PASS\_MAX\_DAYS 90 PASS\_MIN\_DAYS 0 PASS\_MIN\_LEN 8 PASS\_WARN\_AGE 7 已配置口令复杂度策略及口令有限期策略。 | 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； | 已启用登录失败处理功能，登录失败3次，锁定30分钟，，超时断开连接已开启：TMOUT=300，已开启登录连接超时自动退出功能。 | 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； | 服务器采用SSH方式进行远程管理，通信过程中基于SSL协议传输数据，用户口令信息加密传输，可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。 | 服务器设备仅采用用户名+口令方式进行登录管理，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等账户，不存在匿名账户，并为其分配了相关权限。 | 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； | 未重命名或删除默认账户root，但已修改默认账户口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 服务器使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等角色权限，各账户仅分配所需的最小权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 已配置访问控制功能，主体为用户级，客体为文件级。 | 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。 | 服务器SELinux设置为Permissive，不能实现通过安全标记强制控制主体对客体的访问。 | 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； | rsyslog日志进程和auditd日志审计进程均已开启，审计范围覆盖到每个用户重要安全事件、重要用户行为等，日志文件存放在/var/log文件夹下，包括/var/log/messages等日志文件。 | 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； | 审计记录包括事件的日期（年月日等），时间、类型、成功与否、事件内容、IP地址等。 | 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； | 审计记录已通过SYSLOG的方式上传综合日志审计系统进行保护，审计记录每季度进行备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达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。 | 通过综合日志审计系统对审计记录进行保护对审计进程进行保护，非授权用户无法中断审计。 | 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； | 系统遵循最小安装原则，未安装不必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； | 服务器未开启非必要的端口，不存在默认共享和高危端口的使用。 | 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； | 通过服务器防火墙配置策略仅允许地址范围总部有线网段，机房运维网段可进行远程管理。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 服务器未部署主机入侵防护软件，无法对主机重要节点进行入侵行为进行检查、限制并报警。 | 不符合 |
| 恶意代码防范 | 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。 | 服务器未安装防恶意代码软件，无法识别入侵和病毒行为，无法将其有效阻断。 | 不符合 |
| 可信验证 | 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。 | 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。 | 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； | 服务器主要涉及鉴别数据、重要配置数据和重要审计数据，其中重要配置数据不进行传输，服务器通过SSH的方式进行远程管理，其鉴别数据传输是基于SSL协议实现，能够保证鉴别数据在传输过程中的完整性。重要审计记录通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 服务器主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 服务器主要涉及鉴别数据，鉴别数据采用SSH的方式，能够保证鉴别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。 | 服务器主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 服务器数据通过数腾备份软件备份；备份策略：增量备份；备份频率：每天；备份地点：本地服务器，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 通过数腾软件对重要服务器数据每天进行增量备份，然后通过软件介质实时同步，将重要数据备份至宁波建投子公司。 | 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。 | 服务器采用多设备热备方式部署，可实现热冗余，保证系统高可用性。 | 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； | linux系统退出时自动对鉴别信息所在的存储空间进行完全的清除。 | 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。 | HISTSIZE=1000，history无法查询上次登录的命令，可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。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |

* + - * 1. SDN03

**附录D 表‑38安全计算环境-服务器和终端结果记录表（SDN03）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 使用用户名加口令身份验证方式对用户进行鉴别； 用户名作为用户唯一身份标识； 无空口令账户； 口令复杂度包含数字、大小写、特殊字符； 口令长度8位以上； 定期更换口令时间为90； 已配置口令复杂度策略： lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1； 口令策略： PASS\_MAX\_DAYS 90 PASS\_MIN\_DAYS 0 PASS\_MIN\_LEN 8 PASS\_WARN\_AGE 7 已配置口令复杂度策略及口令有限期策略。 | 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； | 已启用登录失败处理功能，登录失败3次，锁定30分钟，，超时断开连接已开启：TMOUT=300，已开启登录连接超时自动退出功能。 | 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； | 服务器采用SSH方式进行远程管理，通信过程中基于SSL协议传输数据，用户口令信息加密传输，可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。 | 服务器设备仅采用用户名+口令方式进行登录管理，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等账户，不存在匿名账户，并为其分配了相关权限。 | 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； | 未重命名或删除默认账户root，但已修改默认账户口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 服务器使用root管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等角色权限，各账户仅分配所需的最小权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 已配置访问控制功能，主体为用户级，客体为文件级。 | 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。 | 服务器SELinux设置为Permissive，不能实现通过安全标记强制控制主体对客体的访问。 | 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； | rsyslog日志进程和auditd日志审计进程均已开启，审计范围覆盖到每个用户重要安全事件、重要用户行为等，日志文件存放在/var/log文件夹下，包括/var/log/messages等日志文件。 | 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； | 审计记录包括事件的日期（年月日等），时间、类型、成功与否、事件内容、IP地址等。 | 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； | 审计记录已通过SYSLOG的方式上传综合日志审计系统进行保护，审计记录每季度进行备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达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。 | 通过综合日志审计系统对审计记录进行保护对审计进程进行保护，非授权用户无法中断审计。 | 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； | 系统遵循最小安装原则，未安装不必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； | 服务器未开启非必要的端口，不存在默认共享和高危端口的使用。 | 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； | 通过服务器防火墙配置策略仅允许地址范围总部有线网段，机房运维网段可进行远程管理。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 服务器未部署主机入侵防护软件，无法对主机重要节点进行入侵行为进行检查、限制并报警。 | 不符合 |
| 恶意代码防范 | 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。 | 服务器未安装防恶意代码软件，无法识别入侵和病毒行为，无法将其有效阻断。 | 不符合 |
| 可信验证 | 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。 | 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。 | 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； | 服务器主要涉及鉴别数据、重要配置数据和重要审计数据，其中重要配置数据不进行传输，服务器通过SSH的方式进行远程管理，其鉴别数据传输是基于SSL协议实现，能够保证鉴别数据在传输过程中的完整性。重要审计记录通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 服务器主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 服务器主要涉及鉴别数据，鉴别数据采用SSH的方式，能够保证鉴别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。 | 服务器主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 服务器数据通过数腾备份软件备份；备份策略：增量备份；备份频率：每天；备份地点：本地服务器，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 通过数腾软件对重要服务器数据每天进行增量备份，然后通过软件介质实时同步，将重要数据备份至宁波建投子公司。 | 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。 | 服务器采用多设备热备方式部署，可实现热冗余，保证系统高可用性。 | 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； | linux系统退出时自动对鉴别信息所在的存储空间进行完全的清除。 | 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。 | HISTSIZE=1000，history无法查询上次登录的命令，可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。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，服务器未在该条款测评对象内。 | 不适用 |

* + - * 1. 运维终端1

**附录D 表‑39安全计算环境-服务器和终端结果记录表（运维终端1）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 运维终端采用用户名加口令的方式进行登录，当前身份标识唯一，当前口令复杂度采用八位以上，口令由字母大小写、数字和特殊符号组成，系统设定密码长度最小值:8； 密码最短使用期限:0； 密码最长使用期限:90。 | 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； | 在本地安全策略中已配置账户锁定时间:30分钟； 账户锁定阀值:5次无效登录； 复位账户锁定计数器:30分钟之后。 | 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； | 运维终端仅本地登录，不能远程管理。 | 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。 | 终端对象不涉及该项要求检查，不适用。 | 不适用 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 为登录的用户分配了administrator等不同的账户，并为其分配相关权限。 | 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； | 未重命名administrator账户，但已修改administrator账户默认口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 当前运维终端设备不存在多余、过期账户，无共享账户存在。 | 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； | 终端对象不涉及该项要求检查，不适用。 | 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； | 终端对象不涉及该项要求检查，不适用。 | 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； | 终端对象不涉及该项要求检查，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。 | 终端对象不涉及该项要求检查，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； | 已在组策略中开启审计功能，可对所有重要的用户行为和重要安全事件进行审计，审计范围覆盖系统内所有用户。 | 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； | windows事件查看器的查看记录默认包括事件的日期、时间、类型、主体标识、客体标识和结果等。 | 符合 |
| 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； | 能够查看到半年的日志，且管理员会定期对日志进行备份至移动硬盘，能够有效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。 | Windows系统具备在审计进程自我保护的功能，系统已对审计进程进行保护，非授权用户不可被中断。 | 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； | 运维终端已遵循最小化安装原则，仅安装必要的组件和程序。 | 符合 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 运维终端不存在不必要的默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的服务。 | 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； | 运维终端仅通过本地方式进行管理。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，终端未在该条款测评对象内，该项不适用。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 终端未部署主机入侵防护软件，无法对主机重要节点进行入侵行为进行检查、限制并报警。 | 不符合 |
| 恶意代码防范 | 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。 | 运维终端已安装了360杀毒软件，当前软件版本为12.0.0.2131，恶意代码库版本为2021-11-17，当前规则库已更新至最新，规则库更新频率：每天自动进行更新。 | 符合 |
| 可信验证 | 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。 | 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。 | 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； | 当前运维终端主要涉及鉴别数据、重要配置数据、重要审计数据，其中重要配置数据、鉴别数据、重要审计数据不进行传输。 | 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。 | 当前运维终端主要涉及鉴别数据、重要配置数据、重要审计数据，鉴别数据采用SHA512+12位SALT算法，能够保证鉴别数据在存储过程中的完整性。未采用校验技术或密码技术保证重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 当前运维终端主要涉及鉴别数据、重要配置数据、重要审计数据，其中重要配置数据、鉴别数据、重要审计数据不进行传输。 | 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。 | 当前运维终端主要涉及鉴别数据，鉴别数据采用SHA512+12位SALT算法进行存储，能够保障鉴别数据在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； | 该终端为运维终端，仅用于系统运维，不涉及重要数据的本地备份和恢复。 | 不适用 |
| 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； | 该终端为运维终端，仅用于系统运维，不涉及重要数据的异地备份。 | 不适用 |
| 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。 | 该终端为运维终端，仅用于系统运维，不涉及重要数据处理系统的热冗余部署。 | 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； | 身份鉴别未记录历史口令，虚拟内存空间存储的数据在释放后能得以完全清除。 | 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。 | 该终端为运维终端，仅用于系统运维，不涉及敏感数据。 | 不适用 |
| 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，终端未在该条款测评对象内，该项不适用。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，终端未在该条款测评对象内，该项不适用。 | 不适用 |

* + - * 1. 运维终端2

**附录D 表‑40安全计算环境-服务器和终端结果记录表（运维终端2）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 运维终端采用用户名加口令的方式进行登录，当前身份标识唯一，当前口令复杂度采用八位以上，口令由字母大小写、数字和特殊符号组成，系统设定密码长度最小值:8； 密码最短使用期限:0； 密码最长使用期限:90。 | 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； | 在本地安全策略中已配置账户锁定时间:30分钟； 账户锁定阀值:5次无效登录； 复位账户锁定计数器:30分钟之后。 | 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； | 运维终端仅本地登录，不能远程管理。 | 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。 | 终端对象不涉及该项要求检查，不适用。 | 不适用 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 为登录的用户分配了administrator等不同的账户，并为其分配相关权限。 | 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； | 未重命名administrator账户，但已修改administrator账户默认口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 当前运维终端设备不存在多余、过期账户，无共享账户存在。 | 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； | 终端对象不涉及该项要求检查，不适用。 | 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； | 终端对象不涉及该项要求检查，不适用。 | 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； | 终端对象不涉及该项要求检查，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。 | 终端对象不涉及该项要求检查，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； | 已在组策略中开启审计功能，可对所有重要的用户行为和重要安全事件进行审计，审计范围覆盖系统内所有用户。 | 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； | windows事件查看器的查看记录默认包括事件的日期、时间、类型、主体标识、客体标识和结果等。 | 符合 |
| 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； | 能够查看到半年的日志，且管理员会定期对日志进行备份至移动硬盘，能够有效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。 | Windows系统具备在审计进程自我保护的功能，系统已对审计进程进行保护，非授权用户不可被中断。 | 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； | 运维终端已遵循最小化安装原则，仅安装必要的组件和程序。 | 符合 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 运维终端不存在不必要的默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的服务。 | 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； | 运维终端仅通过本地方式进行管理。 | 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，终端未在该条款测评对象内，该项不适用。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 终端未部署主机入侵防护软件，无法对主机重要节点进行入侵行为进行检查、限制并报警。 | 不符合 |
| 恶意代码防范 | 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。 | 运维终端已安装了360杀毒软件，当前软件版本为12.0.0.2131，恶意代码库版本为2021-11-17，当前规则库已更新至最新，规则库更新频率：每天自动进行更新。 | 符合 |
| 可信验证 | 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。 | 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。 | 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； | 当前运维终端主要涉及鉴别数据、重要配置数据、重要审计数据，其中重要配置数据、鉴别数据、重要审计数据不进行传输。 | 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。 | 当前运维终端主要涉及鉴别数据、重要配置数据、重要审计数据，鉴别数据采用SHA512+12位SALT算法，能够保证鉴别数据在存储过程中的完整性。未采用校验技术或密码技术保证重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 当前运维终端主要涉及鉴别数据、重要配置数据、重要审计数据，其中重要配置数据、鉴别数据、重要审计数据不进行传输。 | 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。 | 当前运维终端主要涉及鉴别数据，鉴别数据采用SHA512+12位SALT算法进行存储，能够保障鉴别数据在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； | 该终端为运维终端，仅用于系统运维，不涉及重要数据的本地备份和恢复。 | 不适用 |
| 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； | 该终端为运维终端，仅用于系统运维，不涉及重要数据的异地备份。 | 不适用 |
| 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。 | 该终端为运维终端，仅用于系统运维，不涉及重要数据处理系统的热冗余部署。 | 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； | 身份鉴别未记录历史口令，虚拟内存空间存储的数据在释放后能得以完全清除。 | 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。 | 该终端为运维终端，仅用于系统运维，不涉及敏感数据。 | 不适用 |
| 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； | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，终端未在该条款测评对象内，该项不适用。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GB∕T 28448-2019 信息安全技术网络安全等级保护测评要求》，终端未在该条款测评对象内，该项不适用。 | 不适用 |

* + - 1. 其他设备

本次测评不包含本安全层面检测项。

* + - 1. 系统管理软件/平台
         1. 亚信安全服务器深度安全防护系统

**附录D 表‑41安全计算环境-系统管理软件平台结果记录表（亚信安全服务器深度安全防护系统）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 登录设备需要使用用户名加口令进行身份鉴别，身份标识唯一，口令长度8位以上，口令组成包含特殊字符，大小写字母和数字，已开启密码复杂度校验功能，口令长度至少8位，口令组成必须包含大小写字母、数字和特殊字符，每半年进行一次口令更换。 | 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； | 已开启登录失败处理功能，登录失败次数：5次，措施：永久锁定账户，网络登录连接空闲超时自动退出时间：30分钟。 | 符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 当前设备远程管理采用HTTPS，用户口令信息加密传输，防止鉴别信息在网络传输中被窃听。 | 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。 | 仅采用用户名加口令的方式进行身份鉴别，未采用两种或两种以上的组合鉴别方式。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用MasterAdmin管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员等账户，不存在匿名账户，并为其分配了相关权限。 | 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； | 已重命名默认账户为MasterAdmin，已修改默认口令为复杂口令。 | 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； | 未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 当前使用MasterAdmin管理员、an\*\*\*安全管理员、she\*\*\*审计管理员、xi\*\*\*系统管理员，各账户仅分配所需的最小权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 当前设备访问控制粒度达到主体为用户级，客体为界面级。 | 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。 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 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； | 设备已开启审计功能，可对重要的用户行为和重要安全事件进行审计。 | 符合 |
| b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 审计记录包含具体时间、计算机、原因、操作、排序、方向、接口、源目IP、源目MAC等重要信息。 | 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； | 审计记录已通过SYSLOG的方式上传至综合日志审计系统当中进行保护，审计每季度备份至本地，审计记录无法受到非预期的删除、修改或覆盖，审计记录保存时间长达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。 | 由系统底层对审计进程进行保护，非授权用户无法中断审计。 | 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； | 底层OS及必要服务由设备厂商出厂前配置完成，用户无需登录底层操作系统并验证组件，系统遵循最小化安全原则，仅安装自身所需要的组件和程序。 | 符合 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 当前设备不存在默认共享，已关闭不必要的端口，仅开启业务所需端口，已禁用不必要的系统服务。 | 符合 |
| c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 通过配置策略限制仅允许总部员工有线、机房运维、网络监控平台等网段可远程登录管理。 | 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 恶意代码防范 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 可信验证 | 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。 | 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。 | 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； | 亚信安全服务器深度安全防护系统主要涉及鉴别数据、重要审计数据和重要配置数据，其中重要配置数据不进行传输，鉴别数据采用HTTPS的方式，能够保证鉴别数据在传输过程中的完整性。重要审计数据通过SYSLOG的方式明文传输，无法保证重要审计数据在传输过程中的完整性。 | 部分符合 |
| 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。 | 亚信安全服务器深度安全防护系统主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | 亚信安全服务器深度安全防护系统主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | 亚信安全服务器深度安全防护系统主要涉及鉴别数据，鉴别数据采用SHA512+8位salt的方式，能够保证鉴别数据在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； | 由管理员每月或在重大配置更新后对设备配置文件进行手工备份，备份地点本地运维终端，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | 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。 | 该设备为非重要数据处理系统，采用旁路方式进行部署，设备宕机不影响业务系统正常运行。 | 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； | 系统登录时不自动保存和显示历史账号和口令，在用户退出后及时清空cookie和会话session，无法通过回退操作访问退出前界面，用户的鉴别信息所在的存储空间被释放或重新分配前能够得到完全清除。 | 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。 | 该设备仅作为主机恶意代码防护，不存在敏感数据。 | 不适用 |
| 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； | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |

* + - 1. 业务应用系统/平台
         1. CAS平台

**附录D 表‑42安全计算环境-业务应用系统平台结果记录表（CAS平台）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 登录系统采用用户名和口令的方式进行身份鉴别，身份标识具有唯一性，当前口令8位以上，采用大小写字符、数字和特殊字符组成，已开启口令复杂度策略，要求口令最小长度8位，口令组成必须包含字母、数字和特殊字符，每半年人为进行一次口令更换。 | 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； | 已开启登录失败处理功能，登录失败次数：3次，措施：锁定账户30分钟；登录连接超时自动退出时间为：30分钟。 | 符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | CAS平台采用HTTPS的方式进行远程管理，用户鉴别信息加密传输，防止鉴别信息在网络传输过程中被窃取。 | 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。 | CAS平台仅使用用户名加口令进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用admin管理员、xitong系统管理员、anquan安全管理员、shenji审计管理员等账户，不存在匿名账户，并为其分配了不同权限。 | 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； | 未重命名或删除默认账户admin，但已修改默认账户的默认口令为复杂口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | CAS平台未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | CAS平台当前使用admin管理员、xitong系统管理员、anquan安全管理员、shenji审计管理员等角色权限账户，各账户仅分配所需的最小权限，不同账户具备不同的访问权限，实现管理员用户权限分离。 | 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； | 已由授权主体配置访问控制策略，管理员具有概览、一键、云资源、主机池管理、集群管理、主机管理、虚拟机管理、云业务管理、云安全、系统管理、虚拟化、拓扑、自定义菜单、监控管理、告警管理等权限，普通用户仅有部分权限，审计管理员仅有日志查看权限。 | 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； | 当前设备访问控制粒度达到主体为用户级，客体为界面级。 | 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。 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 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； | CAS平台已开启审计功能，审计范围覆盖到每个操作用户，审计内容覆盖到每个用户、对重要用户的行为和重要安全事件进行审计。 | 符合 |
| b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 操作日志审计记录包括登录名、操作员姓名、完成时间、登录地址、操作分类、操作对象、操作描述、执行结果、失败原因等内容。 | 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； | CAS平台审计记录保存在本地，通过CVM每季度进行备份，管理员无法对审计记录进行非预期的删除、修改或覆盖，最早审计记录可查看到2020/09/03日，审计记录保存时间长达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。 | 系统底层已对审计进程进行保护，非授权用户不可被中断。 | 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； | 该测评对象为应用系统，该条款在服务器层面实现。 | 不适用 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 该测评对象为应用系统，该条款在服务器层面实现。 | 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； | 通过配置策略限制仅允许总部员工有线、机房运维、网络监控平台等网段可远程登录管理CAS平台。 | 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； | 应用系统已对数据有效性进行校验，针对改动的数据格式，配置等要求进行校验，不满足要求无法生效，对于不符合的相关链接内容会弹出403的错误界面。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 恶意代码防范 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 可信验证 | 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。 | 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。 | 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； | CAS平台主要涉及鉴别数据、重要审计数据和重要配置数据，其中重要审计数据和重要配置数据不进行传输，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | CAS平台主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA256+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | CAS平台主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | CAS平台主要涉及鉴别数据，鉴别数据采用SHA256+8位salt的方式进行保存，能够保证鉴别数据在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； | 重要数据通过CVM备份配置，包含文件名、创建时间、版本号、MD5摘要、备份目的地、IP地址、链接方式、备份位置。每周增量进行备份至本地，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | 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。 | 该测评对象为应用系统，重要数据处理系统的热冗余部署，在服务器层面实现。 | 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； | 系统登录时不自动保存和显示历史账号和口令，在用户退出后及时清空cookie和会话session，无法通过回退操作访问退出前界面，用户的鉴别信息所在的存储空间被释放或重新分配前能够得到完全清除。 | 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。 | 该系统仅作为私有云的管理控制平台，不涉及敏感数据内容。 | 不适用 |
| 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； | 该系统仅作为私有云的管理控制平台，不涉及用户个人信息。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 该系统仅作为私有云的管理控制平台，不涉及用户个人信息。 | 不适用 |

* + - * 1. CloudOS平台

**附录D 表‑43安全计算环境-业务应用系统平台结果记录表（CloudOS平台）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 登录系统采用用户名和口令的方式进行身份鉴别，身份标识具有唯一性，当前口令8位以上，采用大小写字符、数字和特殊字符组成，已开启口令复杂度策略，口令最小长度8位，口令组成必须包含字母、数字和特殊字符，每半年人为进行一次口令更换。 | 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； | 已开启登录失败处理功能，登录失败次数：5次，措施：锁定账户30分钟；登录连接超时自动退出时间为：30分钟。 | 符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | CloudOS平台采用HTTPS的方式进行远程管理，用户鉴别信息加密传输，防止鉴别信息在网络传输过程中被窃取。 | 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。 | CloudOS平台仅使用用户名加口令进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用系统管理员admin、组织管理员用户ZJJT00008、zjjt、审计管理员shenji账户，不存在匿名账户，并已为其分配了相关权限。 | 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； | 未重命名或删除默认admin账户，但已修改默认口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | CloudOS平台未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | 当前使用系统管理员admin、组织管理员用户ZJJT00008、zjjt、审计管理员shenji账户等角色权限，各账户仅分配所需的最小权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 当前设备访问控制粒度达到主体为用户级，客体为界面级。 | 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。 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 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； | CloudOS平台已开启安全审计功能，审计范围覆盖到每个操作用户，审计内容覆盖到每个用户、对重要用户的行为和重要安全事件进行审计。 | 符合 |
| b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 审计记录包括用户名称、IP地址、操作、资源对象、操作时间、级别、结果等内容。 | 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； | CloudOS平台审计记录保存在本地，审计记录每季度进行备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录最早可查看到2020.09.04，审计记录保存时间长达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。 | 系统底层已对审计进程进行保护，非授权用户不可被中断。 | 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； | 该测评对象为应用系统，该条款在服务器层面实现。 | 不适用 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 该测评对象为应用系统，该条款在服务器层面实现。 | 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； | 通过配置策略限制仅允许总部员工有线、机房运维、网络监控平台等网段可远程登录管理CloudOS平台。 | 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； | 应用系统已对数据有效性进行校验，针对改动的数据格式，配置等要求进行校验，不满足要求无法生效，对于不符合的相关链接内容会弹出403的错误界面。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 恶意代码防范 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 可信验证 | 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。 | 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。 | 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； | CloudOS平台主要涉及鉴别数据、重要审计数据和重要配置数据，其中重要审计数据和重要配置数据不进行传输，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | CloudOS主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA256+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | CloudOS平台主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | CloudOS平台主要涉及鉴别数据，鉴别数据采用SHA256+8位salt的方式进行保存，能够保证鉴别数据在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； | 重要数据采用三台服务器实时进行互备，且每周以增量的方式备份至本地，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | 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。 | 该测评对象为应用系统，重要数据处理系统的热冗余部署，在服务器层面实现。 | 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； | 系统登录时不自动保存和显示历史账号和口令，在用户退出后及时清空cookie和会话session，无法通过回退操作访问退出前界面，用户的鉴别信息所在的存储空间被释放或重新分配前能够得到完全清除。 | 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。 | 该系统仅作为私有云的管理控制平台，不涉及敏感数据内容。 | 不适用 |
| 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； | 该系统仅作为私有云的管理控制平台，不涉及用户个人信息。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 该系统仅作为私有云的管理控制平台，不涉及用户个人信息。 | 不适用 |

* + - * 1. SNA平台

**附录D 表‑44安全计算环境-业务应用系统平台结果记录表（SNA平台）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 登录系统采用用户名和口令的方式进行身份鉴别，身份标识具有唯一性，当前口令8位以上，采用大小写字符、数字和特殊字符组成，已开启口令复杂度策略，口令最小长度8位，口令组成必须包含字母、数字和特殊字符，每半年人为进行一次口令更换。 | 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； | 已开启登录失败处理功能，登录失败次数：5次，措施：锁定账户30分钟；登录连接超时自动退出时间为：30分钟。 | 符合 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | SNA平台采用HTTPS的方式进行远程管理，用户鉴别信息加密传输，防止鉴别信息在网络传输过程中被窃取。 | 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。 | SNA平台仅使用用户名加口令进行身份鉴别，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 当前使用admin管理员、sna、xitong系统管理员、shenji审计管理员、anquan安全管理员等账户进行登录，不存在匿名账户，并已为其分配相关权限。 | 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； | 未重命名或删除默认账户admin，已修改默认账户的默认口令。 | 部分符合 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | SNA平台未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况。 | 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； | SNA平台创建xitong系统管理员、anquan安全管理员、shenji审计管理员等账户角色权限，各账户仅分配所需的最小权限，不同账户具备不同的访问权限，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； | 依据具体业务划分情况对账户进行具体权限划分，不同账户具有不同访问权限，未发现越权访问情况。 | 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； | 当前设备访问控制粒度达到主体为用户级，客体为界面级。 | 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。 | 未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 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； | SNA平台已启用安全审计功能，审计包括操作日志、系统日志、诊断日志，审计内容覆盖到每个用户、对重要用户的行为和重要安全事件进行审计。 | 符合 |
| b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 操作审计记录包括时间、组件名称、用户名称、用户ip、节点名称、服务名称、操作结果、操作描述，系统日志审计记录包含日期、组件名称、节点名称、服务名称、描述信息。 | 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； | SNA平台审计记录保存在本地，操作日志、系统日志最早可查看到2020/09/03，审计记录每季度进行备份至本地，管理员无法对审计记录进行非预期的删除、修改或覆盖，审计记录保存时间长达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。 | 系统底层已对审计进程进行保护，非授权用户不可被中断。 | 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； | 该测评对象为应用系统，该条款在服务器层面实现。 | 不适用 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 该测评对象为应用系统，该条款在服务器层面实现。 | 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； | 通过配置策略限制仅允许总部员工有线、机房运维、网络监控平台等网段可远程登录管理SNA平台。 | 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； | 应用系统已对数据有效性进行校验，针对改动的数据格式，配置等要求进行校验，不满足要求无法生效，对于不符合的相关链接内容会弹出403的错误界面。 | 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； | 建投集团与联通签署有漏扫服务，每半年进行一次漏洞扫描服务，对于发现的漏洞通过测试评估后及时进行修补。本次漏洞扫描结果中，未发现高风险漏洞存在。相关修补记录保存在《漏洞修补记录表》当中。 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 恶意代码防范 | 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。 | 根据《GBT 28448-2019 信息安全技术 网络安全等级保护测评要求》可知，该条款不适用与此测评对象。 | 不适用 |
| 可信验证 | 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。 | 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。 | 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； | SNA平台主要涉及鉴别数据、重要审计数据和重要配置数据，其中重要审计数据和重要配置数据不进行传输，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | SNA平台主要涉及鉴别数据、重要审计数据和重要配置数据，鉴别数据采用SHA256+8位salt的方式，能够保证鉴别数据在存储过程中的完整性。未采取措施保障重要审计数据和重要配置数据在存储过程中的完整性。 | 部分符合 |
| 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； | SNA平台主要涉及鉴别数据，鉴别数据采用HTTPS的方式，能够保证鉴别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。 | SNA平台主要涉及鉴别数据，鉴别数据采用SHA256+8位salt的方式进行保存，能够保证鉴别数据在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； | 重要数据采用三台服务器实时进行互备，且每周以增量的方式备份至本地，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | 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。 | 该测评对象为应用系统，重要数据处理系统的热冗余部署，在服务器层面实现。 | 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； | 系统登录时不自动保存和显示历史账号和口令，在用户退出后及时清空cookie和会话session，无法通过回退操作访问退出前界面，用户的鉴别信息所在的存储空间被释放或重新分配前能够得到完全清除。 | 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。 | 该系统仅作为私有云的管理控制平台，不涉及敏感数据内容。 | 不适用 |
| 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； | 该系统仅作为私有云的管理控制平台，不涉及用户个人信息。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 该系统仅作为私有云的管理控制平台，不涉及用户个人信息。 | 不适用 |

* + - 1. 数据资源
         1. 业务数据

**附录D 表‑45安全计算环境-数据资源结果记录表（业务数据）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 数据资源不涉及该项要求检测，不适用。 | 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； | 数据资源不涉及该项要求检测，不适用。 | 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； | 数据资源不涉及该项要求检测，不适用。 | 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。 | 数据资源不涉及该项要求检测，不适用。 | 不适用 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 数据资源不涉及该项要求检测，不适用。 | 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； | 数据资源不涉及该项要求检测，不适用。 | 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； | 数据资源不涉及该项要求检测，不适用。 | 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； | 数据资源不涉及该项要求检测，不适用。 | 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； | 数据资源不涉及该项要求检测，不适用。 | 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； | 数据资源不涉及该项要求检测，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。 | 数据资源不涉及该项要求检测，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； | 数据资源不涉及该项要求检测，不适用。 | 不适用 |
| 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； | 数据资源不涉及该项要求检测，不适用。 | 不适用 |
| 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； | 数据资源不涉及该项要求检测，不适用。 | 不适用 |
| d)应对审计进程进行保护，防止未经授权的中断。 | 数据资源不涉及该项要求检测，不适用。 | 不适用 |
| 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； | 数据资源不涉及该项要求检测，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； | 数据资源不涉及该项要求检测，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； | 数据资源不涉及该项要求检测，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； | 数据资源不涉及该项要求检测，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； | 数据资源不涉及该项要求检测，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。 | 数据资源不涉及该项要求检测，不适用。 | 不适用 |
| 恶意代码防范 | 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。 | 数据资源不涉及该项要求检测，不适用。 | 不适用 |
| 可信验证 | 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。 | 数据资源不涉及该项要求检测，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； | CloudOS平台、CAS平台、SNA平台主要涉及重要业务数据，重要业务数据采用HTTPS的方式，能够保证重要业务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。 | CloudOS平台、CAS平台、SNA平台主要涉及重要业务数据，未采取措施保障重要业务数据在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； | CloudOS平台、CAS平台、SNA平台主要涉及重要业务数据，重要业务数据采用HTTPS的方式，能够保证中亚业务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。 | CloudOS平台、CAS平台、SNA平台主要涉及重要业务数据，未采取措施保障重要业务数据在存储过程中的保密性。 | 不符合 |
| 数据备份恢复 | a)应提供重要数据的本地数据备份与恢复功能； | 重要业务数据每天实时全量同步至两台服务器、三台服务器之中，但未使用备份文件进行过备份恢复测试。 | 部分符合 |
| 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； | 系统备份数据仅在本地保存，未利用通信网络将关键数据实时传送至备用场地。 | 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。 | CloudOS平台、CAS平台、SNA平台均采用的多台服务器高可用集群方式进行部署，可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； | CloudOS平台、CAS平台、SNA平台系统登录时不自动保存和显示历史账号和口令，在用户退出后及时清空cookie和会话session，无法通过回退操作访问退出前界面，用户的鉴别信息所在的存储空间被释放或重新分配前能够得到完全清除。 | 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。 | CloudOS平台、CAS平台、SNA平台仅作为私有云的管理控制平台，不涉及敏感数据内容。 | 不适用 |
| 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； | CloudOS平台、CAS平台、SNA平台仅作为私有云的管理控制平台，不涉及用户个人信息。 | 不适用 |
| b)应禁止未授权访问和非法使用用户个人信息。 | CloudOS平台、CAS平台、SNA平台仅作为私有云的管理控制平台，不涉及用户个人信息。 | 不适用 |

* + 1. 安全扩展要求部分
       1. 网络设备
          1. 核心交换机A

**附录D 表‑46安全计算环境-网络设备结果记录表（核心交换机A）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. 核心交换机B

**附录D 表‑47安全计算环境-网络设备结果记录表（核心交换机B）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. Leaf交换机A

**附录D 表‑48安全计算环境-网络设备结果记录表（Leaf交换机A）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. Leaf交换机B

**附录D 表‑49安全计算环境-网络设备结果记录表（Leaf交换机B）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. Spine交换机A

**附录D 表‑50安全计算环境-网络设备结果记录表（Spine交换机A）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. Spine交换机B

**附录D 表‑51安全计算环境-网络设备结果记录表（Spine交换机B）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - 1. 安全设备
         1. H3C防火墙A

**附录D 表‑52安全计算环境-安全设备结果记录表（H3C防火墙A）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. H3C防火墙B

**附录D 表‑53安全计算环境-安全设备结果记录表（H3C防火墙B）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. 威胁感知大数据平台

**附录D 表‑54安全计算环境-安全设备结果记录表（威胁感知大数据平台）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. 帕拉迪堡垒机A

**附录D 表‑55安全计算环境-安全设备结果记录表（帕拉迪堡垒机A）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. 帕拉迪堡垒机B

**附录D 表‑56安全计算环境-安全设备结果记录表（帕拉迪堡垒机B）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. 服务器防火墙

**附录D 表‑57安全计算环境-安全设备结果记录表（服务器防火墙）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. 深信服上网行为管理A

**附录D 表‑58安全计算环境-安全设备结果记录表（深信服上网行为管理A）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. 深信服上网行为管理B

**附录D 表‑59安全计算环境-安全设备结果记录表（深信服上网行为管理B）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. 综合日志审计系统

**附录D 表‑60安全计算环境-安全设备结果记录表（综合日志审计系统）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. 飞塔防火墙A

**附录D 表‑61安全计算环境-安全设备结果记录表（飞塔防火墙A）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. 飞塔防火墙B

**附录D 表‑62安全计算环境-安全设备结果记录表（飞塔防火墙B）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - 1. 服务器和终端
         1. CloudOS1

**附录D 表‑63安全计算环境-服务器和终端结果记录表（CloudOS1）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. CloudOS2

**附录D 表‑64安全计算环境-服务器和终端结果记录表（CloudOS2）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. CloudOS3

**附录D 表‑65安全计算环境-服务器和终端结果记录表（CloudOS3）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. CVK01

**附录D 表‑66安全计算环境-服务器和终端结果记录表（CVK01）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. CVK02

**附录D 表‑67安全计算环境-服务器和终端结果记录表（CVK02）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. CVK03

**附录D 表‑68安全计算环境-服务器和终端结果记录表（CVK03）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. CVK04

**附录D 表‑69安全计算环境-服务器和终端结果记录表（CVK04）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. CVK05

**附录D 表‑70安全计算环境-服务器和终端结果记录表（CVK05）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. CVM01

**附录D 表‑71安全计算环境-服务器和终端结果记录表（CVM01）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. CVM02

**附录D 表‑72安全计算环境-服务器和终端结果记录表（CVM02）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. SDN01

**附录D 表‑73安全计算环境-服务器和终端结果记录表（SDN01）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. SDN02

**附录D 表‑74安全计算环境-服务器和终端结果记录表（SDN02）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. SDN03

**附录D 表‑75安全计算环境-服务器和终端结果记录表（SDN03）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. 运维终端1

**附录D 表‑76安全计算环境-服务器和终端结果记录表（运维终端1）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. 运维终端2

**附录D 表‑77安全计算环境-服务器和终端结果记录表（运维终端2）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - 1. 系统管理软件/平台
         1. 亚信安全服务器深度安全防护系统

**附录D 表‑78安全计算环境-系统管理软件平台结果记录表（亚信安全服务器深度安全防护系统）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - 1. 业务应用系统/平台
         1. CAS平台

**附录D 表‑79安全计算环境-业务应用系统平台结果记录表（CAS平台）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. CloudOS平台

**附录D 表‑80安全计算环境-业务应用系统平台结果记录表（CloudOS平台）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - * 1. SNA平台

**附录D 表‑81安全计算环境-业务应用系统平台结果记录表（SNA平台）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* + - 1. 数据资源
         1. 业务数据

**附录D 表‑82安全计算环境-数据资源结果记录表（业务数据）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 身份鉴别 | 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。 | 对云平台进行远程管理时，管理终端和平台之间采用的是单向认证方式。 | 不符合 |
| 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； | 通过云安全组和云防火墙配置虚拟机访问控制策略，在虚拟机迁移时，其云安全组和云防火墙的访问控制策略也将随着一起迁移，始终绑定。 | 符合 |
| 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。 | 云服务客户可通过云安全组和云防火墙设置不同虚拟机之间的访问控制策略进行隔离，云服务客户可自行配置其访问控制策略。 | 符合 |
| 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； | 通过CloudOS平台，配置服务链策略进行隔离，若隔离策略失效，平台将显示为非活跃状态，并在平台进行告警。 | 符合 |
| 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； | 云平台无法检测非授权新建虚拟机或者重新启用虚拟机，也无法进行告警。 | 不符合 |
| 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。 | 当前私有云已对接亚信安全服务器深度安全防护系统，每一个虚拟机必须安装，且通过平台进行统一管理，用于检测和清除主机层面的恶意代码，并会在平台进行告警。 | 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； | 云服务客户可自定义操作系统镜像或云服务商提供模板给云服务客户，云服务商可根据客户需求手动为客户虚拟进行操作系统安全加固。 | 符合 |
| 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； | 云平台的虚拟机镜像、快照完整性校验等采用MD5校验算法，保证虚拟机镜像、快照完整性校验等，防止虚拟机镜像被恶意篡改。 | 符合 |
| 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。 | 未采取措施防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 不符合 |
| 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； | 云平台和云服务客户的数据均在中国境内，地点为浙江省杭州市西湖区文三西路52号，数据不需要出境。 | 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； | 云平台无云服务客户数据的管理权限，虚拟机和其中存储的数据由云服务客户自行管理。 | 符合 |
| 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； | 在虚拟机迁移过程中，采用MD5算法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迁移会失败，并要求重新进行迁移操作。 | 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。 | 云服务客户可通过API接口来部署密钥管理解决方案，云服务客户可自行选择第三方加密软件、设备、平台等，申请获批后可自行对租户自身的业务数据进行加解密操作。 | 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； | 本系统属于云平台系统，云租户业务数据的本地保存，由云服务客户自行负责。 | 不适用 |
| b)应提供查询云服务客户数据及备份存储位置的能力； | 云服务商提供云服务客户数据及备份存储位置查询功能，云服务客户可通过CAS平台查看其数据及备份存储位置。 | 符合 |
| 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； | 云平台采用外置存储的方式，外置存储采用raid 5存储机制，存在3个可用副本，各副本之间内容一致，保证原数据的可用性。 | 符合 |
| 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。 | 云平台侧在租户提交申请后可为云服务客户提供将其业务系统迁移至其他云平台或本地系统的技术支持。 | 符合 |
| 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； | 当虚拟机回收后所使用的内存、存储空间的数据进行擦除操作，保证数据得到完全清楚并释放对应内存和存储空间。 | 符合 |
| 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中所有副本删除。 | 当云服务客户删除业务应用数据时，云存储中所有副本也将同步进行删除。 | 符合 |

* 1. 安全管理中心
     1. 安全通用要求部分

**附录D 表‑83安全管理中心结果记录表（安全管理中心）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 部署有帕拉迪堡垒机，通过帕拉迪堡垒机对系统管理员的身份进行鉴别，但未限制网络设备、安全设备、服务器等仅通过堡垒机进行运维管理，并对系统管理员的操作进行审计。 | 部分符合 |
| 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。 | 所有测评对象已进行三权分立，仅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。 | 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； | 部署有综合日志审计系统，通过用户名加口令的方式对审计管理员进行身份鉴别，并在所有设备上均单独创建有审计管理员账户she\*\*\*，对这些操作进行审计。 | 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。 | 部署有综合日志审计系统，仅通过审计管理员对审计记录进行分析，并根据分析结果进行处理。 | 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； | 部署有帕拉迪堡垒机，通过帕拉迪堡垒机对安全管理员的身份进行鉴别，但未限制网络设备、安全设备、服务器等仅通过堡垒机进行运维管理，并对安全管理员的操作进行审计。 | 部分符合 |
| 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。 | 所有测评对象已进行三权分立，仅通过安全管理员对系统中的安全策略进行配置。 | 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； | 网络中已划分出单独的安全管理区用于部署安全设备及安全组件，网络安全设备及安全组件均部署在该区域。 | 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； | 网络中的安全设备和安全组件均采用HTTPS的方式进行远程管理。 | 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； | 通过CAS平台、CloudOS平台对云平台各服务器运行状况，网络设备、网络链路等进行集中监控，并可依据其工作状态及设定阈值实时报警。 | 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； | 部署有综合日志审计系统对各个设备的日志进行统一收集管理，且各个设备均已开启安全审计功能，审计记录保存时间长达6个月。 | 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； | 未采取措施对安全策略、恶意代码、补丁升级等进行统一集中管理。 | 不符合 |
| 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。 | 当前部署有威胁感知大数据平台，能够对网络当中各类安全事件进行识别、分析，监测范围覆盖系统网络所有关键路径，在发生重要安全事件时通过邮件的方式告警管理员。 | 符合 |

* + 1. 安全扩展要求部分

**附录D 表‑84安全管理中心结果记录表（安全管理中心）**

| **测评指标** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 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； | 云平台通过CAS平台、SNA平台和CloudOS平台对物理资源和虚拟资源按照管理员策略意愿做统一管理调度与分配。 | 符合 |
| 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； | 平台本身物理流量和租户的业务流量分离，云计算平台的管理流量通过各管理平台进行管控和监测，云租户的流量通过安装CasTools，并通过CAS平台进行管控。 | 符合 |
| 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； | 云服务商和云服务客户的审计记录通过综合日志审计平台和控制台进行收集，并创建不同的管理账户，各管理账户仅能查看自建所拥有的设备相关权限。 | 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。 | 云服务商和云租户客户可通过账户划分，对各虚拟网络设备、虚拟机、虚拟安全设备等进行自主控制管理。 | 符合 |

* 1. 安全管理制度

**附录D 表‑85安全管理制度结果记录表（制度或记录类文档）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 安全策略 | 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。 | 《ZJJT-XX-01-2020信息安全策略》对安全工作的总体方针和安全策略做了相关说明，对机构安全工作的总体目标、范围、原则和安全框架等进行了阐明，包括组织机构及岗位职责，人员安全管理、环境和资产安全管理、系统安全建设管理 系统安全运行管理、事件处置和应急响应等。 | 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； | 已制定《ZJJT-XX-02-2020网络与信息安全管理制度》、《ZJJT-XX-05-2020机房管理制度 》、《ZJJT-XX-06-2020信息资产管理制度》、《ZJJT-XX-07-2020信息设备运维管理制度》、《ZJJT-XX-08-2020信息系统巡检管理制度》、《ZJJT-XX-09-2020信息网络管理制度》、《ZJJT-XX-14-2020业务应用系统软件安全管理制度》、《ZJJT-XX-18-2020信息系统管理授权审批管理制度》、《ZJJY-XX-19-2020系统安全管理制度》、《ZJJY-XX-24-2020信息系统数据质量管理制度》等制度，相关制度中包含服务运维、系统运维、系统数据安全等管理内容。 | 符合 |
| b)应对管理人员或操作人员执行的日常管理操作建立操作规程； | 已制定《ZJJT-XX-17-2020信息安全机构管理制度》、《ZJJT-XX-03-2020计算机病毒防治管理制度》、《ZJJT-XX-04-2020数据备份与恢复管理制度》、《ZJJT-XX-08-2020信息系统巡检管理制度》、《ZJJT-XX-11-2020外部人员访问控制管理制度》、《ZJJT-XX-16-2020信息系统安全补丁管理制度》等制度，相关制度中包含对系统维护、系统配置、用户操作等访问的规定。 | 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。 | 已制定《ZJJT-XX-02-2020网络与信息安全管理制度》、《ZJJT-XX-05-2020机房管理制度 》、《ZJJT-XX-06-2020信息资产管理制度》、《ZJJT-XX-07-2020信息设备运维管理制度》、《ZJJT-XX-08-2020信息系统巡检管理制度》、《ZJJT-XX-09-2020信息网络管理制度》、《ZJJT-XX-14-2020业务应用系统软件安全管理制度》、《ZJJT-XX-18-2020信息系统管理授权审批管理制度》、《ZJJY-XX-19-2020系统安全管理制度》、《ZJJY-XX-24-2020信息系统数据质量管理制度》、《ZJJT-XX-17-2020信息安全机构管理制度》、《ZJJT-XX-03-2020计算机病毒防治管理制度》、《ZJJT-XX-04-2020数据备份与恢复管理制度》、《ZJJT-XX-08-2020信息系统巡检管理制度》、《ZJJT-XX-11-2020外部人员访问控制管理制度》、《ZJJT-XX-16-2020信息系统安全补丁管理制度》等制度，并留存相关记录表单，形成全面的安全管理制度体系。 | 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； | 指定科技信息科负责安全管理制度的制定。 | 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。 | 浙江省建设投资集团股份有限公司的安全管理制度通过红头文件的形式进行发布，其管理制度文件通过内部办公OA系统进行正式发布，且进行了版本控制。 | 符合 |
| 评审和修订 | 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。 | 未定期对安全管理制度进行论证、审定以及修订。 | 不符合 |

* 1. 安全管理机构

**附录D 表‑86安全管理机构结果记录表（制度或记录类文档）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 《ZJJT-XX-01-2020信息安全策略》中已明确成立网络安全工作领导小组，并通过红头文件发布有《关于成立信息安全管理工作领导小组的通知》，明确了人员构成情况和相关职责。 | 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； | 设立网络安全管理工作的职能部门科技信息部，设立安全主管岗位，《ZJJT-XX-17-2020信息安全机构管理制度》说明部门职责及各个工作岗位的职责。 | 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。 | 浙江省建设投资集团股份有限公司已对安全管理岗位进行划分，在《ZJJT-XX-17-2020信息安全机构管理制度》中明确设立了系统管理员、安全审计员、安全管理员、网络管理员、应用管理员等岗位，并明确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； | 当前配备有系统管理员3名，审计管理员2名、安全管理员2名，网络管理员1名、机房管理员1名、应用管理员1名，其中李明明兼任系统管理员和审计管理员，关俭兼任系统管理员和应用管理员，赖晋宝兼容网络管理员和机房管理员。 | 符合 |
| b)应配备专职安全管理员，不可兼任。 | 当前已配置两名安全管理员：李任华、郑辉，不存在兼任的情况。 | 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； | 已制定《ZJJT-XX-18-2020信息系统管理授权审批管理制度》，明确各个部门岗位的具体职责划分以及授权审批事项、审批部门和批准人等内容。 | 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； | 已制定《ZJJT-XX-18-2020信息系统管理授权审批管理制度》、《ZJJY-XX-19-2020系统安全管理制度》、《ZJJY-XX-20-2020软件开发管理制度》等制度，对系统变更，重要操作、物理访问和系统接入等事项执行过程进行了审批和流程规定，具体工作在内部OA办公系统中审批。 | 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。 | 每年对各类审批项目、审批部门和审批人进行更新，记录表单类文档中具有更新需授权和审批的项目、审批部门和审批人等信息，记录日期与审查周期一致。 | 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； | 已建立各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通机制，每年组织一次工作会议进行沟通合作，共同协调处理信息安全相关问题，具备相关会议记录。 | 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； | 与中国电信股份有限公司、杭州西湖区网警、外包供应商：新华三技术有限公司、业界专家、安全公司、安全组织等，定期进行沟通、合作，通过会议、电话、邮件等方式进行交流沟通，具备沟通合作记录。 | 符合 |
| c)应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。 | 已建立浙江省建设投资集团股份有限公司的《外联单位联系表》，内容包括外联单位名称、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； | 查看到具有《aZJJT-XXBG-02-2020-B网络与信息系统安全运行月报2021年2月》，相关记录表单为《a定期全面信息系统安全检查表》，每季度进行安全检测，报告内容包括系统日常运维、文档、数据备份、系统漏洞等情况。 | 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； | 每年进行一次全面的安全检查，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，且具备检查记录《a定期全面信息系统安全检查表》。 | 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。 | 具备安全检查表格、安全检查记录、安全检查报告、安全检查结果通报记录等；安全检查表记录包含常规检查、全面检查的相关数据，每年形成安全检查报告，通过邮件、会议等方式对安全检查结果进行通报。 | 符合 |

* 1. 安全管理人员

**附录D 表‑87安全管理人员结果记录表（制度或记录类文档）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 人员录用 | a)应指定或授权专门的部门或人员负责人员录用； | 已指定人事部专门负责对人员录用。 | 符合 |
| 人员录用 | b)应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核； | 已制定《ZJJT-XX-10-2020信息安全员管理制度》规定在人员录用时对被录用人身份、安全背景、专业资格或资质等进行了审查，对其技术能力进行了考核，且具备相关审查记录及考核记录。 | 符合 |
| 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。 | 已制定《ZJJT-XX-10-2020信息安全员管理制度》，与正式员工签署有保密协议，与关键岗位人员签署有岗位责任协议；保密协议中包含保密范围、保密责任、违约责任、协议的有效期限和责任人签字等内容；岗位责任协议中包含岗位安全责任定义、协议的有效期限和责任人签字等内容。 | 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； | 在《ZJJT-XX-10-2020信息安全员管理制度》规定所有人员离职时的操作流程：删除该人员的信息系统访问账号和权限；明确保密事项，不得泄露原单位信息秘密，不得使用原单位的知识产权。 | 符合 |
| 人员离岗 | 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。 | 《ZJJT-XX-10-2020信息安全员管理制度》中规定了人员调离手续和离岗要求等，《aZJJT-XXBG-10-2020-A人员离岗交接清单》中按照人员管理文档中的离岗程序办理人员调离手续。。 | 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； | 《ZJJT-XX-12-2020信息安全人员培训和教育管理制度》规定了各类人员的安全意识教育和岗位技能培训，并明确了相关安全责任和惩戒措施，具备《aZJJT-XXBG-12-2020-培训记录表》。 | 符合 |
| 安全意识教育和培训 | 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； | 《ZJJT-XX-12-2020信息安全人员培训和教育管理制度》，具有不同岗位的培训计划，培训计划包含了培训目的、培训方式、培训对象、培训内容，对不同岗位指定了不同的培训计划，对安全基础知识、岗位操作等进行培训，具备《aZJJT-XXBG-12-2020-培训记录表》。 | 符合 |
| 安全意识教育和培训 | c)应定期对不同岗位的人员进行技能考核。 | 信息安全内部培训与考核。培训应长期进行开展，并覆盖公司全员。针对公司安全管理员、安全审计员、系统管理员、网络管理员、数据库管理员、应用管理员、机房管理员应根据岗位不同，对员工进行相关的信息安全培训，并在培训后实行书面信息安全考核，具备《技能考核记录》。 | 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； | 已制定《ZJJT-XX-11-2020外部人员访问控制管理制度》规定了外部人员的访问情况，在外部人员物理访问受控区域前先提出书面申请，填写《aZJJT-XXBG-11-2020-A外部人员访问申请授权表》，由系统管理员批准，通过审批后由专人全程陪同，并登记备案。 | 符合 |
| 外部人员访问管理 | 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； | 已制定《ZJJT-XX-11-2020外部人员访问控制管理制度》规定了在外部人员接入受控网络访问系统前先提出书面申请，填写《aZJJT-XXBG-11-2020-A外部人员访问申请授权表》，批准后由专人开设账户、分配权限，并登记备案。 | 符合 |
| 外部人员访问管理 | c)外部人员离场后应及时清除其所有的访问权限； | 在《ZJJT-XX-11-2020外部人员访问控制管理制度》中已规定外部人员离场后须及时清除其所有的访问权限，具备外部人员访问系统登记记录，记录中包含访问权限的清除时间等内容。 | 符合 |
| 外部人员访问管理 | 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。 | 《ZJJT-XX-11-2020外部人员访问控制管理制度》对系统访问情况进行了规定，获得系统访问授权的外部人员应签署保密协议，协议中明确了外部人员的保密义务，包含不得进行非授权操作，不得复制信息等内容。 | 符合 |

* 1. 安全建设管理
     1. 安全通用要求部分

**附录D 表‑88安全建设管理结果记录表（制度或记录类文档）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 已在浙江省建设投资集团股份有限公司私有云定级报告中明确了该系统的网络安全保护等级为第三级（S3A3G3），在报告中详细描述了网络安全保护等级的确定方法和理由。 | 符合 |
| b)应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定； | 浙江省建设投资集团股份有限公司私有云的定级结果已经通过了专家评审，由安全技术专家对系统定级结果的合理性和正确性进行论证，具备专家定级评审反馈意见表。 | 符合 |
| c)应保证定级结果经过相关部门的批准； | 定级结果已通过杭州西湖区网安批准及信息安全部门的批准，具备私有云定级情况审批意见。 | 符合 |
| d)应将备案材料报主管部门和相应公安机关备案。 | 浙江省建设投资集团股份有限公司私有云的定级材料已提交杭州西湖区网安进行备案，具有公安出具的备案证明。 | 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； | 该系统具备《浙江省建设投资集团股份有限公司私有云风险评估报告》，报告中已明确根据等级保护第三级（S3A3G3）的要求对系统进行分析，并依据风险分析的结果补充和调整系统的安全性措施。 | 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； | 《私有云安全设计方案》中包含与其他系统交互的整体规划设计部分，其中包括不同级别系统间如何进行数据传输以及采用何种密码算法等内容，且整体规划设计详细实施方案具备配套执行文件。 | 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。 | 未组织相关部分和有关专家对安全方案进行论证和审查。 | 不符合 |
| 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； | 该系统相关网络安全产品均采用公开招投标、邀请招标、单一来源等方式开展采购，招投标文件、流程符合国家《中华人民共和国招投标法》的有关要求，且网络安全产品均具备销售许可证。 | 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； | 该系统未使用密码产品，未采购和使用国家密码主管部门要求的密码产品。 | 不符合 |
| 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。 | 由科技信息部负责产品的选型测试，形成了产品候选范围，并根据安全需求及市场变动，调整并更新了候选产品，留存有《产品选择测试记录表》。 | 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； | 不涉及自行软件开发。 | 不适用 |
| 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； | 不涉及自行软件开发。 | 不适用 |
| 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； | 不涉及自行软件开发。 | 不适用 |
| 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； | 不涉及自行软件开发。 | 不适用 |
| 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； | 不涉及自行软件开发。 | 不适用 |
| 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； | 不涉及自行软件开发。 | 不适用 |
| 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。 | 不涉及自行软件开发。 | 不适用 |
| 外包软件开发 | a)应在软件交付前检测其中可能存在的恶意代码； | 在《ZJJT-XX-17-2020信息安全机构管理制度》中包含外包软件开发，在系统上线前，需由软件开发商对软件包中可能存在的恶意代码进行检测，具备《aZJJT-XXBG-03-2020-A恶意代码分析报告》。 | 符合 |
| b)应保证开发单位提供软件设计文档和使用指南； | 在《ZJJT-XX-17-2020信息安全机构管理制度》中包含外包软件开发，规定开发单位需提供软件涉及文档和使用指南。具体包含系统设计流程图、需求说明文档、系统概要设计文档等。 | 符合 |
| 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。 | 在《ZJJT-XX-17-2020信息安全机构管理制度》中包含外包软件开发，指出开发单位必须提供软件源代码，但未聘请专门的机构或者自己公司对系统交付进行源代码审计工作，并出具相关审计报告。 | 部分符合 |
| 工程实施 | a)应指定或授权专门的部门或人员负责工程实施过程的管理； | 科技信息部负责信息系统工程实施过程的管理工作。 | 符合 |
| b)应制定安全工程实施方案控制工程实施过程； | 已制定《ZJJY-XX-23-2020信息系统工程实施管理制度》在工程实施之前，由工程实施单位制定详细的工程实施方案《私有云系统实施方案》对实施过程进行控制，该方案需要经信息安全管理工作领导小组批准认可后方可实施。 | 符合 |
| c)应通过第三方工程监理控制项目的实施过程。 | 未聘请第三方工程监理控制项目的实施过程。 | 不符合 |
| 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； | 在测试验收前制订《私有云测试验收方案》，《私有云测试验收方案》详细记录了时间、人员、现场操作过程、测试验收结果等方面内容，并形成《私有云系统测试验收报告》。 | 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。 | 该系统上线前测试中包含安全性测试，具备相关安全测试报告，但该报告中未包含密码应用安全性测试相关内容。 | 部分符合 |
| 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； | 制定有交付清单，系统交付清单包括系统设计流程图、效果图、需求说明文档、概要设计、详细设计、开发过程文档及系统操作手册等。 | 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； | 由科技信息部人员进行系统的运行维护；在系统正式运行前对运行维护人员进行培训；主要针对的方面：操作、问题处理、功能介绍等；具备相关《技术培训记录》，内容包括培训内容、培训时间、参与人员等。 | 符合 |
| c)应提供建设过程文档和运行维护文档。 | 已提供系统建设过程中的文档和指导用户进行系统运行维护的文档，包括系统建设文档、指导用户进行系统运维的文档、系统培训手册《私有云操作手册》。 | 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； | 该系统定级为第三级（S3A3G3），本次为首次测评。 | 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； | 在确定该信息系统的安全保护等级后，并未发生较大变更，未调整安全保护级别，系统发生重大变更或级别发生变化时及时进行等级测评。 | 符合 |
| c)应确保测评机构的选择符合国家有关规定。 | 等级测评单位名称：杭州中尔网络科技有限公司；该单位具有相关技术资质、安全资质。 | 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； | 信息系统选择的安全服务商：新华三技术有限公司、浙江乾冠信息安全研究院有限公司，均具备相应服务资质，且资质在有效期内，符合国家有关规定。 | 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； | 已和新华三技术有限公司、浙江乾冠信息安全研究院有限公司签订相关服务合同，服务合同中明确了甲乙双方的责任和义务。 | 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。 | 新华三技术有限公司、浙江乾冠信息安全研究院有限公司具备每年的安全服务报告交付物，目前安全服务商未发起服务变更申请，无需对变更进行审核，在合同中明确了评价指标、考核内容、进入及退出机制等。 | 符合 |

* + 1. 安全扩展要求部分

**附录D 表‑89安全建设管理结果记录表（制度或记录类文档）**

| **扩展类型** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 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； | 该系统为云计算平台，故该条款不适用。 | 不适用 |
| 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； | 该系统为云计算平台，故该条款不适用。 | 不适用 |
| 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； | 该系统为云计算平台，故该条款不适用。 | 不适用 |
| 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； | 该系统为云计算平台，故该条款不适用。 | 不适用 |
| 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。 | 该系统为云计算平台，故该条款不适用。 | 不适用 |
| 供应链管理 | a)应确保供应商的选择符合国家有关规定； | 云服务商选择的供应商为：新华三技术有限公司，具备销售许可证、服务资质等，符合国家规定。 | 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； | 在发生安全事件时，云服务商通过邮件或电话方式通知云服务客户，并向云服务客户提交安全事件报告或威胁报告，报告内容包括响应流程响应和处理的范围、程度及处理方法等。 | 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。 | 云服务商对每次供应商的重要变更均进行风险评估并采取控制措施，在供应商发生重要变更后云服务商通过邮件或电话方式通知云服务客户。 | 符合 |

* 1. 安全运维管理
     1. 安全通用要求部分

**附录D 表‑90安全运维管理结果记录表（制度或记录类文档）**

| **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- |
| 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； | 已制定《ZJJT-XX-05-2020机房管理制度》，机房管理员由信息科技部指定专人担任，具备《a机房出入登记表》，机房供配电、空调、温湿度设备等的定期巡检和维护记录。 | 符合 |
| 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； | 已制定《ZJJT-XX-05-2020机房管理制度》，制度中已明确对机房人员进出、物品的带进带出和日常安全环境管理等进行规定，具备《机房出入登录表》、《aZJJT-XXBG-08-2020-A巡视记录表》等记录表单。 | 符合 |
| 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。 | 已在《ZJJT-XX-11-2020外部人员访问控制管理制度》中规定，来访人员在会议室接待，敏感机制不得随意存放，避免外部人员接触，含有敏感信息的纸质文件和移动介质不得随意放置在办公桌面等位置。 | 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； | 已制定《ZJJT-XX-06-2020信息资产管理制度》，相关制度中已对信息资产分类进行规定，并留存有资产清单表，包括资产责任部门、重要程度和所处位置等内容。 | 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； | 已制定《ZJJT-XX-06-2020信息资产管理制度》，相关制度中已明确了资产的标识方法，以及对不同资产的管理措施要求，同时资产清单中设备具有相应标识，符合相应制度要求。 | 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。 | 在《ZJJT-XX-06-2020信息资产管理制度》中，所有信息资产都应指定资产责任人，并由资产责任人负责进行相关资产的识别、统计、分类、分级，以便相关人员采取相应的保护措施。 | 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； | 未建立介质管理制度对介质进行控制和保护，也未指定专人或专门的部门对介质进行管理并定期清算盘点。 | 不符合 |
| 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。 | 未对介质在物理传输过程中的人员选择、打包、交付等进行控制，也未对介质的归档和查询等进行登记记录。 | 不符合 |
| 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； | 机房内的各类线路及设备指定信息科负责运行维护，具备《ZJJT-XX-07-2020信息设备运维管理制度》，文档中明确了设备维护管理的责任部门为科技信息部，每天进行一次维护管理工作。 | 符合 |
| 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； | 已制定《ZJJT-XX-07-2020信息设备运维管理制度》，信息资产日常使用管理过程中涉及维修的，原则上要求服务商现场维修，确需送外单位维修时，应彻底清除所存的工作相关信息，并与设备维修厂商签订保密协议，具备《aZJJT-XXBG-07-2020-A系统（设备）操作记录表》。 | 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； | 含有重要数据的设备带出机房/工作环境要进行加密处理，并进行申请，经过本部门经理签字后方可带离，且留存有审批记录表。 | 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。 | 已制定《ZJJT-XX-07-2020信息设备运维管理制度》，制度中要求含有存储介质的设备在报废或重用前，须对数据进行加密，以确保其所存储信息完全清除或被安全覆盖，不可恢复，且具备详细的清除记录。 | 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； | 已制定《ZJJT-XX-07-2020信息设备运维管理制度》，中规定由信息科技部，定期对私有云系统进行漏洞扫描，且与联通签订由协议，每半年进行一次漏洞扫描和渗透测试工作，具有漏洞扫描报告及渗透测试报告，报告描述了存在的漏洞、严重等级、原因分析和改进意见等方面，具备《aZJJT-XXBG-16-2020系统补丁更新记录表》。 | 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。 | 每年对私有云进行安全测评，并出具《浙江省建设投资集团股份有限公司私有云风险评估报告》，中报告日期符合每年开展安全测评的要求，具备《浙江省建设投资集团股份有限公司安全整改报告》，且依据上述风险分析报告所发现的问题进行了分析和整改。 | 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； | 在《ZJJT-XX-17-2020信息安全机构管理制度》中已划分有系统管理员、网络管理员和安全管理员等角色，具备人员职责划分文档，文档中明确了各个角色的具体责任和权限。 | 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； | 指定信息科技部负责账户管理，创建账户、修改账户权限、删除账户等操作，经过审批后方可执行；具备相关审批记录。 | 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； | 已制定《ZJJT-XX-02-2020网络与信息安全管理制度》、《ZJJT-XX-07-2020信息设备运维管理制度》、《ZJJT-XX-08-2020信息系统巡检管理制度》等制定，明确了在日常运维工作中的安全策略、账户管理、配置管理、日志管理等的操作规程。 | 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； | 具有《华三交换机操作手册》、《深信服防火墙操作手册》等重要设备的配置操作手册，包含了设备的操作步骤，参数配置等内容。 | 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； | 具备《aZJJT-XXBG-08-2020-A巡视记录表》，包括日常巡检记录、运行维护记录、参数的设置和修改等内容。 | 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； | 指定审计管理员每周对系统进行巡检，对日志、监测和报警数据等进行分析、统计，并出《aZJJT-XXBG-08-2020-A巡视记录表》，表中包含对日志、监测和报警数据等进行分析、统计的内容。 | 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； | 该系统具备配置信息库，调整配置参数后立即同步更新配置信息库，配置库版本为最新；运维管理员需填写《aZJJT-XXBG-07-2020-C配置变更记录表》，通过审批后方可进行系统连接、安装系统组件或调整配置参数等活动。 | 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； | 运维人员使用帕拉迪堡垒机对系统进行运维，使用运维工具接入系统时，须提交审批申请，经部门领导签字确认后方可接入系统，所有操作日志留存在堡垒机当中。 | 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； | 系统在日常运维过程中存在远程运维，远程运维使用帕拉迪堡垒机进行，远程运维的开通须填写审批单，留存有《运维审批记录》；远程运维的帕拉迪堡垒机开启了审计日志功能，审计内容有时间、操作人员、操作内容等内容，审计日志不可更改。 | 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。 | 应用系统以及终端所有需与外部链接的端口和IP需经过上级信息部门的批准。 | 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； | 《ZJJT-XX-16-2020信息系统安全补丁管理制度》中规定，所有联网和非联网计算机，要按照要求统一安装办法的防恶意代码软件，并定期更新（升级）计算机病毒防范产品的版本，具备《aZJJT-XXBG-03-2020-B恶意代码特征库更新记录表》。 | 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。 | 已制定《ZJJT-XX-03-2020计算机病毒防治管理制度》，制度中已规定须在服务器及终端均安装企业版防恶意代码软件，并定期对恶意代码库进行更新，并进行检测分析，且具备《aZJJT-XXBG-03-2020-B恶意代码特征库更新记录表》、《aZJJT-XXBG-03-2020-A恶意代码分析报告》等。 | 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； | 已记录和保存系统基本配置信息；配置信息文档包含网络拓扑结构、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信息。 | 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。 | 基本配置信息变更后已及时更新配置信息库；制定有配置信息变更相应的申报审批程序，相关审批内容须经部门领导签字确认。 | 符合 |
| 密码管理 | a)应遵循密码相关国家标准和行业标准； | 系统未使用密码产品，未遵循密码相关国家标准和行业标准。 | 不符合 |
| 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。 | 未建立密码使用管理制度，未使用符合国家密码管理规定的密码技术和产品。 | 不符合 |
| 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； | 已制定《ZJJT-XX-18-2020信息系统管理授权审批管理制度》，制度中已明确变更前需根据变更需求制定变更方案，方案内容须包括变更类型，变更原因，变更过程、变更前评估等内容，具有《aZJJT-XXBG-07-2020-C配置变更记录表》。 | 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； | 已制定《ZJJT-XX-18-2020信息系统管理授权审批管理制度》，制度中已规定变更控制的申报和审批程序，具有《aZJJT-XXBG-07-2020-C配置变更记录表》，审批记录包含变更类型、申报流程、审批部门、批准人等方面内容。 | 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。 | 未建立终止变更并从失败变更中恢复的程序。 | 不符合 |
| 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； | 在《ZJJT-XX-04-2020数据备份与恢复管理制度》中已明确需要定期备份的信息为系统重要业务数据、系统软件配置信，具备备份记录。 | 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； | 已制定《ZJJT-XX-04-2020数据备份与恢复管理制度》，制定中已对备份方式、备份频率、备份介质、备份保存时长等内容进行了规定。 | 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。 | 《ZJJT-XX-04-2020数据备份与恢复管理制度》规定对重要数据制定数据恢复策略、备份程序和恢复程序，并定期对策略、程序等进行实用性验证。 | 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； | 《ZJJT-XX-02-2020网络与信息安全管理制度》明确系统运维人员在发现安全弱点和可疑事件时及时向安全管理部及时报告。 | 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； | 《ZJJT-XX-02-2020网络与信息安全管理制度》已明确针对计算机病毒、网络攻击事件的威胁隔离、信息的收集、消除隐患等方面的内容。 | 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； | 《ZJJT-XX-02-2020网络与信息安全管理制度》明确如发生安全事件，事后应详细分析事件发生的原因，记录处理过程，总结经验教训等。 | 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。 | 已制定《ZJJT-XX-02-2020网络与信息安全管理制度》，制度中规定了对造成系统中断和造成信息泄密的安全事件采用不同的处理程序和报告程序，且实际工作中对造成系统中断和造成信息泄漏的重大安全事件制定了不同的处理程序和报告程序。 | 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； | 《03浙江省建设投资集团股份有限公司私有云系统应急预案》，制度中明确了应急预案工作小组由组长、副组长及组员组成，并对职责进行了详细描述；具有统一的应急预案框架描述，包括启动应急预案的条件、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； | 《03浙江省建设投资集团股份有限公司私有云系统应急预案》，中对应急事件的处置流程、恢复流程等进行了说明。 | 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； | 已根据《03浙江省建设投资集团股份有限公司私有云系统应急预案》要求，每年进行一次应急培训，培训记录包含培训对象、培训内容、培训结果等内容；每半年组织一次系统相关人员进行预案的演练，《04浙江省建设投资集团股份有限公司私有云系统应急演练记录》包含演练时间、主要操作内容、演练结果等内容。 | 符合 |
| d)应定期对原有的应急预案重新评估，修订完善。 | 未定期对原有的应急预案重新评估并定期修订完善。 | 不符合 |
| 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； | 选择新华三技术有限公司作为系统运维服务商，符合国家相关规定。 | 符合 |
| 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； | 已和新华三技术有限公司签订相关的协议，对运维内容、范围等进行确定，并签订相关协议。 | 符合 |
| 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； | 浙江省建设投资集团股份有限公司与外包运维服务商签订的外包运维合同中有乙方应具备依据等级保护标准要求提供服务的能力以及相关要求。 | 符合 |
| 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。 | 浙江省建设投资集团股份有限公司与外包运维服务商签订的外包运维服务商签署的合同中明确了敏感信息及应急保障方面安全要求。 | 符合 |

* + 1. 安全扩展要求部分

**附录D 表‑91安全运维管理结果记录表（制度或记录类文档）**

| **扩展类型** | **控制点** | **测评项** | **结果记录** | **符合情况** |
| --- | --- | --- | --- | --- |
| 云计算安全扩展要求 | 云计算环境管理 | 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。 | 云平台运维地点位于浙江省杭州市西湖区古荡街道文三西路52号15楼，属于中国境内，云平台无境外远程运维操作。 | 符合 |

* 1. 其他安全要求

本次检测不包含其他安全要求。

*…………………………本页结束，以下为空白…………………………*

1. 漏洞扫描结果记录

**附录E 表‑1漏洞扫描主要安全漏洞**

| **序号** | **危险程度** | **漏洞名称** | **影响IP** |
| --- | --- | --- | --- |
| 1 | 中危 | RC4 加密问题漏洞 | 10.\*.\*.254、10.\*.\*.13、10.\*.\*.11 |
| 2 | 中危 | TLS/SSL协议 RC4算法安全漏洞(CVE-2013-2566) | 10.\*.\*.254、10.\*.\*.13、10.\*.\*.11 |
| 3 | 低危 | 支持SSH弱MAC算法 | 10.\*.\*.254、10.\*.\*.13、10.\*.\*.11 |
| 4 | 低危 | SSH版本信息可被获取 | 10.\*.\*.254、10.\*.\*.13、10.\*.\*.11、10.\*.\*.131、10.\*.\*.132、10.\*.\*.133、10.\*.\*.134、10.\*.\*.135、10.\*.\*.101、10.\*.\*.102、10.\*.\*.103、10.\*.\*.107、10.\*.\*.108、10.\*.\*.104、10.\*.\*.105、10.\*.\*.106 |
| 5 | 低危 | SSH协议支持的算法 | 10.\*.\*.254、10.\*.\*.13、10.\*.\*.11、10.\*.\*.131、10.\*.\*.132、10.\*.\*.133、10.\*.\*.134、10.\*.\*.135、10.\*.\*.101、10.\*.\*.102、10.\*.\*.103、10.\*.\*.107、10.\*.\*.108、10.\*.\*.104、10.\*.\*.105、10.\*.\*.106 |
| 6 | 低危 | 服务器加密通信支持的SSL加密算法（原理扫描） | 10.\*.\*.254、10.\*.\*.13、10.\*.\*.11 |
| 7 | 低危 | 服务器支持的SSL加密协议（原理扫描） | 10.\*.\*.254、10.\*.\*.13、10.\*.\*.11 |
| 8 | 低危 | HTTP Server类型和版本号 | 10.\*.\*.254、10.\*.\*.13、10.\*.\*.11、10.\*.\*.222 |
| 9 | 低危 | 错误页面Web应用服务器版本泄露 | 10.\*.\*.121 |
| 10 | 低危 | E-Mail地址 | 10.\*.\*.123 |
| 11 | 低危 | 内网IP | 10.\*.\*.123 |
| 12 | 低危 | 电话号码 | 10.\*.\*.123 |

*…………………………本页结束，以下为空白…………………………*

1. 渗透测试结果记录
   1. CloudOS平台存在Docker Engine API信息泄露

|  |  |
| --- | --- |
| 漏洞名称 | CloudOS平台Docker Engine API信息泄露 |
| 测试日期 | 2021年12月01日 |
| 漏洞位置 | https://10.0.58.121:2375/info |
| 风险等级 | 中危 |
| 漏洞说明 | 系统仅能通过内部网络访问  访问https://10.0.58.121:2375/info，泄露了docker相关的信息。 |
| 漏洞危害 | 泄露了docker系统信息。 |
| 安全建议 | 限制对Docker Engine API的访问。 |
| 整改情况 | / |
| 整改结果 | 未整改 |

* 1. CAS平台存在点击劫持

|  |  |
| --- | --- |
| 漏洞名称 | CloudOS平台Docker Engine API信息泄露 |
| 测试日期 | 2021年12月01日 |
| 漏洞位置 | https://10.0.58.123:8080/ |
| 风险等级 | 低危 |
| 漏洞说明 | 系统仅能通过内部网络访问  用Burpsuite发包，查看Response发现服务器未返回 X-Frame-Options报头 |
| 漏洞危害 | 存在诱使 Web 用户点击与用户认为其单击的内容不同的内容，从而在单击看似无害的网页时有可能导致机密信息泄露或计算机被控制。 |
| 安全建议 | 配置服务器，使其包含X-Frame-Options报头和带有frame-ancestors指令的 CSP报头。 |
| 整改情况 | / |
| 整改结果 | 未整改 |

*…………………………本页结束，以下为空白…………………………*

1. 威胁列表

**附录G 表‑1威胁列表**

| **序号** | **威胁分（子）类** | **威胁描述** |
| --- | --- | --- |
| 1 | 恶意攻击 | 利用工具和技术对信息系统进行攻击和入侵。 |
| 2 | 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造等问题。 |
| 3 | 管理不到位 | 由于制度缺失、不完善等原因导致安全管理无法落实或者不到位。 |
| 4 | 无作为或操作失误 | 应该执行而没有执行相应的操作，或者无意执行了错误的操作。 |
| 5 | 敏感信息泄露 | 敏感信息泄露给不应了解的他人。 |
| 6 | 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。 |
| 7 | 越权或滥用 | 越权访问本来无权访问的资源，或者滥用自己的权限破坏信息系统。 |
| 8 | 物理攻击 | 通过物理的接触造成对软件、硬件和数据的破坏。 |
| 9 | 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。 |
| 10 | 抵赖 | 否认所做的操作。 |

1. 云计算平台测评及整改情况

该系统为云计算平台。

*…………………………本页结束，以下为空白…………………………*

1. 大数据平台测评及整改情况

该系统不涉及大数据平台。

*…………………………本页结束，以下为空白…………………………*