**报告编号：33012199039-00002-21-0114-01-ZGJY**

**网络安全等级保护**

**私有云**

**整改建议书**

|  |  |
| --- | --- |
| **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** |

声 明

本方案是浙江省建设投资集团股份有限公司私有云的整改建议书。

本方案建议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。本方案中给出的整改建议仅对被测信息系统当时的安全状态有效。当测评工作完成后，由于信息系统发生变更而涉及到的系统构成组件（或子系统）都应重新进行等级测评，本方案不再适用。

在任何情况下，若需引用本方案中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

目 录

[声 明 I](#_Toc92798621)

[目 录 II](#_Toc92798622)

[1 项目概述 1](#_Toc92798623)

[1.1. 整改目标 1](#_Toc92798624)

[1.2. 整改依据 1](#_Toc92798625)

[2 整改建议 2](#_Toc92798626)

[2.1 安全物理环境 2](#_Toc92798627)

[2.2 安全通信网络 2](#_Toc92798628)

[2.3 安全区域边界 2](#_Toc92798629)

[2.4 安全计算环境 3](#_Toc92798630)

[2.5 安全管理中心 16](#_Toc92798631)

[2.6 安全管理制度 16](#_Toc92798632)

[2.7 安全管理机构 17](#_Toc92798633)

[2.8 安全管理人员 17](#_Toc92798634)

[2.9 安全建设管理 17](#_Toc92798635)

[2.10 安全运维管理 18](#_Toc92798636)

[3 软硬件设备增加建议 20](#_Toc92798637)

# 项目概述

通过本次网络安全等级保护测评能够全面、完整地了解浙江省建设投资集团股份有限公司私有云的现有安全状况，并了解其与《GB/T 22239-2019信息安全技术 网络安全等级保护基本要求》对应级别的差距，与相关网络安全等级保护管理规范之间的对比。根据测评结果，杭州中尔网络科技有限公司（以下简称“中尔网络”）提出相应的整改建议，达到以检查促整体安全的目的，实现重要信息系统的分等级保护与监管、信息安全事件分等级响应的目的，并且浙江省建设投资集团股份有限公司将信息系统的安全保护落实到点，实现信息系统的完整性、保密性和可用性。

## 整改目标

通过本次网络安全等级保护测评能够全面、完整地了解浙江省建设投资集团股份有限公司信息系统的现有安全状况，并了解其与《GB/T 22239-2019信息安全技术 网络安全等级保护基本要求》对应级别的差距，与相关网络安全等级保护管理规范之间的对比。根据测评结果，提出相应的整改建议，达到以检查促安全的目的，实现重要信息系统的分等级保护与监管、信息安全事件分等级响应的目的，并且帮助浙江省建设投资集团股份有限公司将信息系统的安全保护落实到点，实现信息系统的完整性、保密性和可用性，使信息系统安全管理水平明显提高，安全保护能力明显增强，安全隐患和安全事故明显减少，有效保障信息化健康发展。

## 整改依据

本次整改建议主要参考并遵守了以下标准和规范：

1. 《GB/T 22239-2019信息安全技术 网络安全等级保护基本要求》；

# 整改建议

## 安全物理环境

| **安全层面** | **测评对象** | **安全问题** | **整改建议** |
| --- | --- | --- | --- |
| 安全物理环境 | 物理机房 | 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。 | 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。 |

## 安全通信网络

| **安全层面** | **测评对象** | **安全问题** | **整改建议** |
| --- | --- | --- | --- |
| 安全通信网络 | 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。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。 | 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。 |

## 安全区域边界

| **安全层面** | **测评对象** | **安全问题** | **整改建议** |
| --- | --- | --- | --- |
| 安全区域边界 | 互联网边界、服务器边界 | 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。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。 | 建议部署准入控制系统防范非法内联行为。 |
| 安全区域边界 | 互联网边界、服务器边界 | 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。 | 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。 |
| 安全区域边界 | 互联网边界、服务器边界 | 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。 | 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。 |

## 安全计算环境

| **安全层面** | **测评对象** | **安全问题** | **整改建议** |
| --- | --- | --- | --- |
| 安全计算环境 | 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 | 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。 | 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。 |
| 安全计算环境 | 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 | 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。 | 建议重命名或删除默认账户。 |
| 安全计算环境 | 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 | 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。 | 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。 |
| 安全计算环境 | 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 | 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。 | 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。 |
| 安全计算环境 | 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 | 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。 | 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。 |
| 安全计算环境 | 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 | 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。 | 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。 |
| 安全计算环境 | 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 | 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。 | 建议利用通信网络将重要数据实时传送至备用场地。 |
| 安全计算环境 | 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 | 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。 | 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。 |
| 安全计算环境 | 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。 | 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。 |
| 安全计算环境 | 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 | 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。 | 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。 |
| 安全计算环境 | 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 | 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。 | 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。 |
| 安全计算环境 | 业务数据 | 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。 | 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。 |
| 安全计算环境 | 业务数据 | 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。 | 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。 |
| 安全计算环境 | CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02 | 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。 | 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。 |
| 安全计算环境 | CloudOS1、CloudOS2、CloudOS3 | 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。 | 建议配置登录连接超时策略，严格限制登录超时时间。 |
| 安全计算环境 | CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03、运维终端1、运维终端2 | 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。 | 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。 |
| 安全计算环境 | CloudOS1、CloudOS2、CloudOS3、CVK01、CVK02、CVK03、CVK04、CVK05、CVM01、CVM02、SDN01、SDN02、SDN03 | 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。 | 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。 |

## 安全管理中心

| **安全层面** | **测评对象** | **安全问题** | **整改建议** |
| --- | --- | --- | --- |
| 安全管理中心 | 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。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。 | 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。 |
| 安全管理中心 | 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。 | 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。 |
| 安全管理中心 | 安全管理中心 | 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。 | 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。 |

## 安全管理制度

| **安全层面** | **测评对象** | **安全问题** | **整改建议** |
| --- | --- | --- | --- |
| 安全管理制度 | 浙江省建设投资集团股份有限公司 | 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。 | 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。 |

## 安全管理机构

无。

## 安全管理人员

无。

## 安全建设管理

| **安全层面** | **测评对象** | **安全问题** | **整改建议** |
| --- | --- | --- | --- |
| 安全建设管理 | 浙江省建设投资集团股份有限公司 | 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。 | 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。 |
| 安全建设管理 | 浙江省建设投资集团股份有限公司 | 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。 | 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。 |
| 安全建设管理 | 浙江省建设投资集团股份有限公司 | 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。 | 建议对源代码进行审计并出具相关审计报告。 |
| 安全建设管理 | 浙江省建设投资集团股份有限公司 | 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。 | 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。 |
| 安全建设管理 | 浙江省建设投资集团股份有限公司 | 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。 | 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。 |

## 安全运维管理

| **安全层面** | **测评对象** | **安全问题** | **整改建议** |
| --- | --- | --- | --- |
| 安全运维管理 | 浙江省建设投资集团股份有限公司 | 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。 | 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。 |
| 安全运维管理 | 浙江省建设投资集团股份有限公司 | 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。 | 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。 |
| 安全运维管理 | 浙江省建设投资集团股份有限公司 | 未定期组织召开恶意代码宣传培训。 | 建议定期组织召开恶意代码宣传培训，提升员工的防恶意代码意识。 |
| 安全运维管理 | 浙江省建设投资集团股份有限公司 | 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。 | 建议使用的密码遵循密码相关的国家标准和行业标准。 |
| 安全运维管理 | 浙江省建设投资集团股份有限公司 | 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。 | 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。 |
| 安全运维管理 | 浙江省建设投资集团股份有限公司 | 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。 | 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。 |
| 安全运维管理 | 浙江省建设投资集团股份有限公司 | 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。 | 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。 |

# 软硬件设备增加建议

| **产品名称** | **功能描述** | **等级保护要求对应点** | **差距点** |
| --- | --- | --- | --- |
| 准入控制系统 | 入网准入控制 | 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。 |
| WAF | 应用层防护 | 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。 |
| 可信验证芯片 | 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 | a）可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未采用可信验证的设备或组件对操作系统的引导程序、系统程序、重要配置参数和应用程序等进行可信验证 |
| 集中管控设备 | 对安全策略、恶意代码防护、补丁升级等进行集中更新和管理 | 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； | 安全策略、恶意代码防护、补丁升级等操作在各设备上实现，未采取措施对相关事项进行集中管控。 |
| Linux主机入侵防护软件 | Linux主机入侵防护 | 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。 | 所有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。 |
| Linux主机防恶意代码软件 | Linux恶意代码检测和清除 | 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。 | 所有服务器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。 |

表格 3–1 软硬件设备建议清单