黑龙江省城市信息模型基础平台
运行维护标准
（征求意见稿）

Operation and maintenance specifications for basic platform of city information model/modeling in Heilongjiang province

目　次

前 言

为推动城市治理体系和治理能力现代化建设，贯彻落实《住房和城乡建设部 工业和信息化部 中央网信办关于开展城市信息模型（CIM）基础平台建设的指导意见》（建科〔2020〕59 号），按照《住房和城乡建设部、中央网信办、科技部、工业和信息化部、人力资源社会保障部、商务部、银保监会关于加快推进新型城市基础设施建设的指导意见》（建改发〔2020〕73 号）、黑龙江省住房和城乡建设厅、中共黑龙江省委网信办、省科技厅、省工业和信息化厅、省人社厅、省商务厅、银保监会黑龙江监管局、省通信局《关于加快基于 CIM 基础平台的新型城市基础设施建设的实施意见》(黑建城管〔2020〕15 号)等文件政策要求，标准编制组经广泛调查研究，认真总结实践经验，参考相关国内外先进标准，并在广泛征求意见的基础上，编制了本标准。

本标准的主要技术内容是：1.总则；2.术语和符号；3.基本规定；4.运维服务对象；5.运维工作内容；6.运维过程管理；7.运维组织体系；8.运维保障资源。

本标准由黑龙江省住房和城乡建设厅负责管理，奥格科技股份有限公司负责具体技术内容的解释。执行过程中如有意见或建议，请寄送 XXX（地址：XXX；邮政编码：XXX）。

1 总则

1.0.1 为保障平台安全、稳定的运行，规范黑龙江省各级城市信息模型（CIM）基础平台运维服务对象、工作组成、过程管理、运维组织体系、运维保障资源等方面的要求，制定本标准。

1.0.2 本标准适用于黑龙江省各级城市信息模型（CIM）基础平台的运行维护。

1.0.3 黑龙江省城市信息模型（CIM）基础平台的运行维护，除应符合本标准外，尚应符合国家、行业和本省现行有关标准的规定。

2 术语和符号

2.1 术语

2.1.1 运维服务 operation and maintenance service

运维服务是结合用户实际需求通过信息技术手段及方法，综合利用日常运维、响应式运维、应急式运维等多种手段和方法，为 CIM 基础平台运行环境、功能应用等健康稳定运行提供技术支持和维护服务，包括信息化基础设施运维、CIM 数据更新与运维、CIM 基础平台功能与服务运维、安全运维等。

2.1.2 运维活动 operation and maintenance activities

为满足事先约定的服务要求而对 CIM 基础平台运维对象开展的维护动作。

2.1.3 自行运维 self operation and maintenance

指由运维管理机构作为运维服务机构，承担 CIM 基础平台的运维服务工作。

2.1.4 外包运维 outsourced operation and maintenance

指由运维管理机构以外的专业信息技术服务单位作为运维服务机构，承担 CIM 基础平台的运维服务工作。

2.2 缩略语

CAB——变更咨询委员会 Change Advisory Board

CI——配置项 Configuration Item

CIM——城市信息模型 City Information Model/Modeling

CMDB——配置管理数据库 Configuration Management Database

ECAB——紧急变更咨询委员会 Emergency Change Advisory Board

OLA——操作级别协议 Operational Level Agreements

RFC——变更请求 Request for Change

SLA——服务级别协议 Service Level Agreements

UC——支撑合同 Underpinning Contracts

UPS——不间断电源 Uninterrupted Power Supply

3 基本规定

3.1 一般规定

3.1.1 CIM 基础平台运维应由运维主管机构、运维管理机构和运维服务机构分工负责组成，应满足以下要求：

a) 运维主管机构应负责运维工作的整体协调；

b) 运维管理机构应负责运维工作的组织、管理、监督、检查，负责运维经费的申请、管理；

c) 运维服务机构应依照运维模式选定，负责承担具体运维工作。

3.1.2 CIM 基础平台运维应依照实际情况选用自行运维、外包运维、混合运维等模式。

3.1.3 自行运维或混合运维中自行维护宜由运维管理机构作为运维服务机构，承担黑龙江省 CIM 基础平台的运维服务工作。

3.1.4 外包运维或混合运维中外包运维部分宜由运维管理机构以外的专业信息技术服务单位作为运维服务机构，承担黑龙江省 CIM 基础平台的运维服务工作。

3.1.5 外包运维应建立外包服务管理机制，运维管理机构宜根据《信息技术服务 运行维护 第 1 部分：通用要求》GB/T28827.1、《信息技术服务 运行维护 第 2 部分：交付规范》GB/T 28827.2、5《信息技术服务 运行维护 第 3 部分：应急响应规范》GB/T 28827.3 等系列标准选择外包服务单位，并进行管理和评估。

3.1.6 CIM 基础平台运维生命周期应满足以下要求：

a) CIM 基础平台设计阶段（包括初步设计、实施方案等），运维管理机构应在工程投资中考虑运维费用；

b) CIM 基础平台建设期，运维管理机构应参与 CIM 基础平台建设过程，并配合建设管理单位开展运维管理工作，承建单位承担建设期运维服务工作；

c) CIM 基础平台或其部分要素竣工验收后，运维管理机构应全面负责运维管理工作，并选定 CIM 基础平台运维服务机构开展运维服务工作。

3.1.7 运维服务要求应包括 CIM 基础平台可用率、服务受理时间、服务响应时

间、故障恢复时间等四方面控制指标组成，并应符合表 3.1.7 要求。

表3.1.7 运维服务控制指标

控制指标	平台可用率	服务受理时间	服务响应时间	故障恢复时间
要求	≥99.5%	7×24h	≤0.5h	一般故障≤ 2h 重大故障≤ 8h
平台可用率=1-全年异常宕机小时数/全年小时数×100%				

3.1.8 运维管理机构应定期考核运维服务机构的服务质量，运维服务机构应根据运维管理机构考核评估要求或参考已建 CIM 基础平台的省市自治区，定期开展 CIM 基础平台运维服务质量自评估或绩效自评估，考核评估宜包括服务指标完成情况、重大故障处理情况、平台使用满意度情况等内容。

3.2 运维保障体系构成

3.2.1 CIM 基础平台运维保障体系由运维服务对象、运维工作内容、运维过程管理、运维组织体系、运维保障资源组成，组成如图 3.2.1 所示：

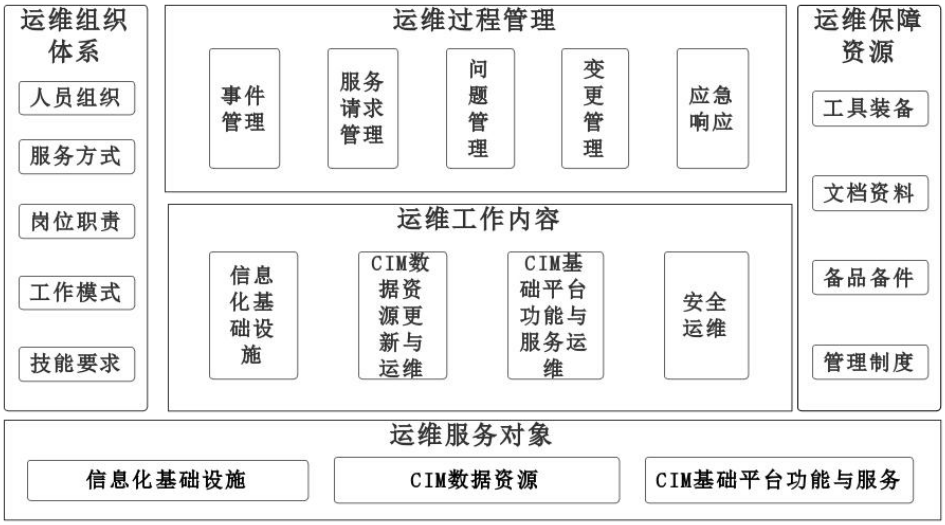


图 3.2.1 CIM 基础平台运维保障体系总体框架

3.2.2 运维服务可将 CIM 基础平台整体视为一个对象，也可将 CIM 基础平台一个或多个组成要素视为一个对象，宜符合如下要求：

a) 运维服务对象宜包括信息化基础设施、CIM 数据资源和 CIM 基础平台功能与服务；

b) 运维工作宜分为信息化基础设施运维、CIM 数据更新与运维、CIM 基础平台功能与服务运维、安全运维；

c) 运维过程管理宜包括事件管理、服务请求管理、问题管理、变更管理、应急响应；

d) 运维组织体系宜包括人员组织、服务方式、工作模式、岗位职责、技能要求五方面；

e) 运维保障资源宜包括工具装备、文档资料、备品备件、管理制度四方面。

3.3 运维服务能力管理

3.3.1 运维服务能力管理宜采用规划、实施、检查、改进模型，如图 3.3.1 所示 PDCA 模型，CIM 基础平台运维组织应按照服务能力管理模型，不断提升运维服务能力。

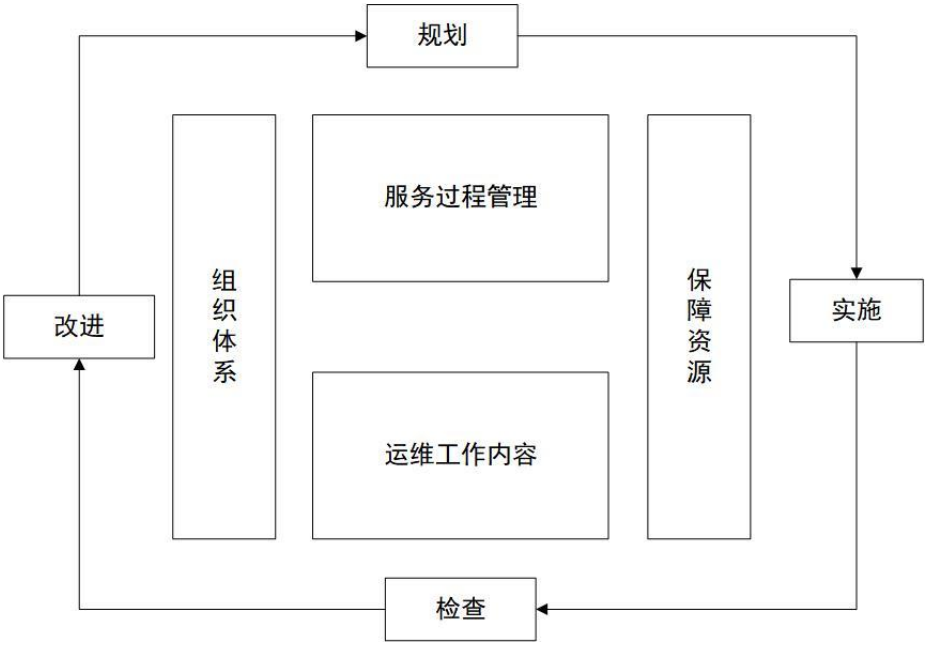


图 3.3.1 CIM 基础平台运维服务能力管理模型

3.3.2 运维服务机构应按照 PDCA 模型进行运维能力管理，并执行下列具体规定：

a) 依据 CIM 基础平台运维服务要求制定每月每周的运维服务规划，服务规划至少应包括运维服务内容、运维服务组织体系设计、运维服务保障资源计划、服务过程管理流程与管理指标等；
b) 根据运维服务规划组织运行维护实施，包括制定实施计划、完成实施工作、记录实施活动、提交实施成果等；
c) 监控服务过程和结果，对比服务要求和服务规划，分析存在的不足；
d) 对运维服务中存在的不足进行改进，持续提升运行维护服务能力。

4 运维服务对象

4.1 一般规定

4.1.1 为保障 CIM 基础平台的高效稳定运行，应完成包括构成黑龙江省 CIM 基础平台的信息化基础设施、CIM 数据资源、CIM 基础平台功能与服务等运维服务对象的运维工作内容。

4.1.2 应每周、每月定期对运维服务对象进行盘点、更新，应进行每日硬拷贝。

4.2 信息化基础设施

4.2.1 信息化基础设施（数据存储、计算、传输、服务等基础软硬件资源）包括物理环境、网络、主机、存储备份、安全设施、基础软件等。

4.2.2 信息化基础设施宜符合表 4.2.2 的规定。

表 4.2.2 信息化基础设施

名称	主要内容	示例
物理环境	黑龙江省 CIM 基础平台以及集成整合的政务服务、工程建设项目管理和“多规合一”相关系统等运行的机房环境及机房辅助设施	机房、配线间、空调、UPS、供电系统、换气系统、除湿/加湿设备、防雷接地、消防、门禁、环境监控等
网络	系统运行的网络环境，宜采用黑龙江省电子政务外网	政务云平台
主机	各类服务器及终端	服务器、虚拟服务器、台式计算机、移动终端、数据可视化大屏、VR/AR 设备、便民服务一体机、打印/复印机等
存储备份	存储、备份 CIM 基础平台信息的各类硬件设备及管理软件等	存储网络设备、磁盘阵列、磁带库等硬件设备、存储管理系统、备份管理系统等
安全设施	CIM 基础平台安全防护的硬件设备及软件系统	安全防控设备、安全检测设备、用户认证设备等硬件设备、安全防控软件、安全监测软件、用户认证系统等

名称	主要内容	示例
基础软件	支撑 CIM 基础平台运行的支撑软件	数据库软件、中间件软件等

4.3 CIM 数据资源

数据资源应包括时空基础数据、业务系统数据、资源调查数据、规划管控数据、工程建设项目数据、公共专题数据、物联感知数据等，应符合《黑龙江省城市信息模型（CIM）信息入库标准》的规定。

4.4 CIM 基础平台功能与服务

4.4.1 省级 CIM 基础平台应具备重要数据汇聚与管理、场景配置、数据查询与可视化、统计分析、数据共享与交换、监测监督、运行管理、分析应用、开发接口等功能。市级 CIM 基础平台应具备数据汇聚与管理、场景配置、数据查询与可视化、数据共享与交换、分析应用、运行与服务、开发接口等功能。

4.4.2 CIM 基础平台服务应符合《黑龙江省城市信息模型（CIM）基础平台服务规范》的规定。

5 运维工作内容

5.1 一般规定

5.1.1 为保障 CIM 基础平台的高效稳定运行，黑龙江省 CIM 基础平台的运维工作应包括信息化基础设施运维、CIM 数据更新与运维、CIM 基础平台功能与服务运维、安全运维等。

5.1.2 应每周、每月定期对运维工作进行盘点、总结。

5.2 信息化基础设施运维

5.2.1 信息化基础设施运维工作内容应包括监控巡检、例行维护、响应式维护、故障处置、分析总结、整理资料等。

5.2.2 信息化基础设施运维服务对象运维活动周期宜符合表 5.2.2 的规定：

表5.2.2 运维活动周期表

运维服务对象	工作内容							
	巡检/清查	监控	例行维护	响应性维护	故障处置	分析总结	资料整理	运维报告
物理环境	每日	实时自动	每月	/	按需要确定	每月	每月	每周
网络	每日	实时自动	每月	即时响应	按需要确定	每月	每月	每周
服务器	每日	实时自动	每月	现场响应	按需要确定	每月	每月	每周
终端	每年	实时自动	每年	即时响应	按需要确定	每月	每月	每周
存储	每日	实时自动	每月	即时响应	按需要确定	每月	每月	每周
备份	每日	每小时	每月	即时响应	按需要确定	每月	每月	每周
安全设备	每日	实时自动	每月	现场响应	按需要确定	每月	每月	每周
数据库管理系统	每日	实时自动	每月	即时响应	按需要确定	每月	每月	每周
中间件及其他基础软件	每日	实时自动	每月	即时响应	按需要确定	每月	每月	每周

5.2.3 监控巡检应符合下列规定：

a) 运维服务机构应提供监控巡检服务，应实时或定期对 CIM 基础平台运行状态进行监控，并定期对物理环境、主机、用于存储备份的硬件设备、安全设施中的硬件设备等进行人工巡检。网络、用于存储备份的管理软件、用于平台安全防护的软件系统和基础软件应进行实时自动的监控，并定期进行人工监控；

b) 运维服务机构应根据服务要求制定监控及巡检服务计划，应做好监控巡检记录，对于监控巡检中发现的问题应根据事先制定的工作流程进行通知、通告及处置；

c) 监控巡检内容宜符合 5.2.3 的规定。

表5.2.3 监控巡检内容

运维服务对象	巡检内容	监控内容
物理环境	CIM基础平台所处机房辅助设施的运行状况、参数变化及告警信息，空调、UPS等关键设施	机房超温、超湿、漏水、火情、非法入侵等异常情况。
网络	设备运行状况及告警信息	a) 网络设备运行状态； b) 网络设备 CPU、内存占用率情况； c) 网络设备日志检查分析； d) 主要网络节点之间的丢包、延迟等情况； e) 网络链路通断情况； f) 网络链路带宽占用情况； g) 网络流量情况。
服务器	设备运行状况及告警信息	a) 服务器运行状态； b) 服务器 CPU、内存占用率情况； c) 服务器日志检查分析； d) 服务器磁盘利用率。
终端	a) 终端基本信息、硬件信息、网	a) 终端感染病毒、木马以及未完成的漏洞

运维服务对象	巡检内容	监控内容
	络信息等； b) 终端安全隐患状况； c) 终端防病毒软件的有效性； d) 终端安全管理软件的有效性； e) 终端信息（使用人、IP 地址等）的一致性。	修补等信息； b) 分析终端安全日志。
存储	设备运行状况及告警信息	a) 存储系统运行状态； b) 存储系统占用率情况； c) 存储系统日志检查分析； d) 存储空间利用率。
备份	设备运行状况及告警信息	a) 备份系统运行状态； b) 备份作业情况； c) 备份系统日志检查分析； d) 备份空间利用率。
安全设备	设备运行状况及告警信息	a) 安全设施运行状态； b) 安全设施系统日志分析。
数据库管理系统	/	a) 数据库运行状态； b) 数据库表空间占用率； c) 数据库系统日志的异常分析。
中间件及其他基础软件	/	a) 中间件及其他基础软件运行状态； b) 中间件及其他基础软件日志异常分析。

5.2.4 例行维护应符合下列规定：

a) 运维服务机构应提供例行维护服务，定期对 CIM 基础平台进行保养、健康检查、系统更新等周期性维护；

b) 运维服务机构应根据服务要求制定例行维护的服务计划，应做好例行维护工作记录，发现问题可根据事先制定的工作流程进行通知、通告及处

置；

c) 例行维护内容宜符合表 5.2.4 的规定。

表5.2.4 例行维护内容

运维服务对象	例行维护内容
物理环境	定期对空调、UPS等机房辅助设施进行保养
网络	a) 网络设备健康检查，主要设备应定期进行包括性能分析、安全审计的全面健康检查； b) 设备登录口令定期修改，网络设备固件和软件升级； c) 网络设备配置文件应定期备份，设备配置变化后应及时备份。
服务器	a) 服务器健康检查，主要设备应定期进行包括性能分析、安全审计的全面健康检查； b) 服务器登录口令定期修改； c) 服务器固件及系统软件升级； d) 备份策略审核。
终端	a) 终端的定期清洗和保养； b) 按需对终端的软件升级。
存储	a) 存储系统健康检查，主要设备应定期进行包括容量分析、容量预警、性能分析的全面健康检查； b) 存储系统登录口令定期修改； c) 存储系统固件及系统软件升级。
备份	a) 备份系统健康检查，主要设备应定期进行全面健康检查，包括容量分析； b) 备份系统登录口令定期检查、修改； c) 备份系统固件及系统软件升级； d) 备份系统的数据资源定期进行恢复测试。
安全设备	a) 安全设施健康检查，主要设备应定期进行全面健康检查； b) 安全设施登录口令定期修改； c) 安全设施配置文件备份；

运维服务对象	例行维护内容
	d) 安全设施固件及系统软件升级； e) 安全策略审核。
数据库管理系统	a) 数据库健康检查，关键数据库应定期进行包括性能分析、安全审计的全面健康检查； b) 数据库系统登录口令定期修改； c) 数据库系统软件补丁升级。
中间件及其他基础软件	a) 中间件及其他基础软件健康检查，关键系统应定期进行全面健康检查； b) 中间件及其他基础软件登录口令定期修改； c) 中间件及其他基础软件补丁升级。

5.2.5 响应式维护应符合下列规定：

a) 运维服务机构应根据业务需要进行配置变更、平台优化、信息更新等响应式维护，应做好响应式维护工作记录；

b) 响应式维护开展前宜根据事先制定的工作流程进行申请审批、通知、通告；

c) 响应式维护实施前应制定实施方案，重点是应急恢复方案，保证 CIM 基础平台的安全可靠及可恢复性；

d) 响应式维护内容宜符合表 5.2.5 的规定。

表5.2.5 响应式维护内容

运维服务对象	响应式维护内容
物理环境	更换物理环境设备时与厂商的沟通、安装、调试。
网络	a) 网络规划调整； b) 网络资源分配； c) 网络设备配置变更。
服务器	a) 服务器配置变更； b) 服务器备份策略调整。
终端	a) 终端入网、离网和变更；

运维服务对象	响应式维护内容
	b) 端操作系统、办公软件等软件安装、配置、问题解答； c) 终端病毒查杀； d) 打印机等外联设备的安装、配置。
存储	a) 存储空间划分、调整等配置变更； b) 存储系统数据迁移、同步、复制等。
备份	a) 备份策略调整等配置变更； b) 备份客户端的安装、卸载等。
安全设备	a) 安全策略调整等配置变更； b) 配合完成 CIM 基础平台安全等级保护测评相关工作； c) 安全预警信息发布。
数据库管理系统	a) 数据库用户权限管理； b) 数据库表空间分配等资源规划及分配； c) 数据迁移等； d) 配合功能应用进行数据库性能监控和优化等。
中间件及其他基础软件	a) 配合功能应用进行中间件及其他基础软件配置变更； b) 配合功能应用进行中间件及其他基础软件性能监控和优化等。
功能应用	a) 功能应用权限变更、业务流程调整等配置变更； b) 功能应用数据的添加、修改、删除及导入、导出； c) 功能应用系统补丁升级。

5.2.6 故障处置应符合下列规定：

a) 运维服务机构应提供故障处置服务，在 CIM 基础平台发生故障时，根据服务要求，在规定的时间内消除故障影响，并最终清除故障；

b) 依据《信息技术服务 运行维护 第 3 部分：应急响应规范》GB/T 28827.3 分类分级标准，CIM 基础平台故障根据故障严重性和受影响系统的重要性分为：重大故障和一般故障两个等级。重大故障应启动应急预案，按预先制定的应急预案进行处置；

c) 故障处置宜先修复安全功能，再遵循“先抢通、后修复，先核心、后边缘”的原则，优先保证重要业务的恢复，特殊情况酌情处理；

d) 故障处置应根据预设工作流程开展，根据故障情况适时启动应急响应机制；

e) 故障处置完成后应及时记录故障处理方法、做好故障总结，并定期进行统计分析，对发生频次较多的故障现象应进行重点分析，采取相应措施，降低故障发生率；

f) 故障处理应根据服务要求按时修复发生的设施、网络、服务器、终端系统、存储系统、备份系统、安全设施、数据库系统、中间件及其他基础软件、功能应用故障。

5.2.7 分析总结应符合下列规定：

a) 运维服务机构应定期进行分析总结；

b) 分析总结应包括 CIM 基础平台运行状况的分析总结、运维工作的分析总结及安全状况分析总结，提出优化完善建议，并优化改进运维工作；

c) 应定期进行总结评估，对物理环境、计算机网络、服务器、终端系统、存储系统、备份系统、安全设施、数据库系统、中间件及其他基础软件、功能应用运行状况及运维工作情况进行分析，提出改进意见。

5.2.8 整理资料应符合下列规定：

a) 应做好相关技术文档的收集、整理及保管，宜明确文档的使用范围并严格控制。应做好运维工作过程的记录；

b) 应制定运维操作规程，规范各项维护工作。应定期对运维对象、备品备件进行盘点。

5.3 CIM 数据更新与运维

5.3.1 CIM 数据资源宜通过 CIM 基础平台定期或根据业务需求频次分专题、分区域对各类数据进行更新维护。

5.3.2 CIM 数据更新与维护应包括 CIM 数据更新、处理、发布及存档等。

5.3.3 CIM 数据的更新应符合下列规定：

a) CIM 数据的更新方式宜包括在线更新和离线拷贝；

b) CIM 数据更新方式和更新频次宜符合表 5.3.3 的规定；

表5.3.3 CIM数据更新

序号	一级名称	二级名称	更新方式	更新频次
1	时空基础数据	行政区	在线更新	实时
		测绘遥感数据	在线更新或离线拷贝	定期
		三维模型	在线更新或离线文件	定期
2	业务系统数据	建筑行业企业/人员资质审批、房地产市场监管、建筑市场监管、工程勘察设计统计信息和大型公建能耗管理等数据	在线更新或离线文件	定期
3	资源调查数据	地质调查、国土调查、耕地资源、水资源、房屋建筑普查和市政设施普查数据	在线更新	实时
4	规划管控数据	开发评价、重要控制线、国土空间规划、专项规划	在线更新	实时
5	工程建设项目数据	立项用地规划许可数据、建设工程规划许可数据、施工许可数据、竣工验收数据	在线更新	实时
		规划设计模型、施工图模型、竣工验收模型	在线提交/离线拷贝	定期
6	公共专题数据	社会数据、实有单位、宏观经济数据、实有人口、兴趣点数据、地名地址数据	在线更新	实时
7	物联感知数据	建筑监测数据、市政设施监测数据、气象监测数据、交通监测数据、生态环境监测数据及城市运行与安防数据	在线更新	实时

c) 与其他平台（系统）对接共享的数据资源宜实时访问系统中最新数据。

5.3.4 CIM 数据处理应包括坐标及投影变换、数据的切割和拼接、空间数据格式转换、属性数据格式转换以及影像数据的对比度、灰度、饱和度一致性调整。

5.3.5 数据资源的发布应符合以下要求：

a) 时空基础数据和规划管控数据应进行统一更新维护，并对外提供（政务版、公众版）在线服务，符合保密要求的原始数据（25 平方公里内）授

权后可在线下载；

b) 工程建设项目数据、资源调查、公共专题及物联感知数据应由各市动态更新维护并自动同步汇交至省平台。

5.3.6 CIM 数据存档应满足国家有关档案管理和保密的规定，基本要求如下：

a) 存档数据中的文档应填写完整、正确、整洁、清晰，并保存为模拟和电子两种形式，存档数据中的图件，图面应整洁、无损；

b) 存档数据应以数据、文档、图件的清单及必要的说明为包装标签，至少复制两份，异地存放，确保数据安全；

c) 数据文件和电子文档应选用高品质磁盘、光盘或磁带等作为存储介质。

5.4 CIM 基础平台功能与服务运维

5.4.1 宜实时或定期通过系统后台监控 CIM 基础平台功能运行情况、调用情况、出错情况，形成相应的运维报告。

5.4.2 宜结合业务需求变化（如流程改造、政策适应性改造等），对 CIM 基础平台功能与服务进行修改、完善和新增开发。

5.4.3 应明确 CIM 基础平台功能应用及服务调用权限，登录口令应定期修改。

5.4.4 宜根据需要对平台功能应用进行响应性维护，包括权限变更、业务流程调整、配置变更等。

5.4.5 宜对平台功能和服务技术资料进行收集、整理，并做好运行维护工作过程文档的收集和存档。

5.5 网络运维

黑龙江省 CIM 基础平台网络运维应符合《电子政务云监管平台运维管理规范》（DB23/T3338-2022）的规定。

5.6 安全运维

5.6.1 应建立数据安全、平台安全和网络安全等安全运维体系。

5.6.2 数据安全运维应包括数据传输安全、存储安全、共享安全、备份恢复安全和安全隔离等，应符合表 5.5.2 的规定。

表5.5.2 数据安全要求

安全措施		满足要求
数据传输安全	传输介质安全	a) 应确保数据传输介质（如电缆、光纤等）的物理环境安全，有效防雷击、防鼠害、防盗、防水、防人为破坏； b) 应选择电磁辐射低的数据传输介质，或者采用有效的措施防止数据传输介质的电磁泄漏； c) 应确保信息设备接入可靠的无线网络或传感网络。
	传输通道安全	a) 应采取有效措施保障敏感信息和重要数据的传输过程的机密性； b) 应对采取有效措施保障敏感信息和重要数据传输过程的完整性； c) 数据管理存储系统应采用安全协议连接，防范非授权访问和管理信息泄露。
存储安全	数据存储访问控制	a) 应对数据文件进行访问控制，严格控制不同权限的用户对不同文件的访问和操作，对文件系统、数据库管理系统、操作系统等分别采取访问控制措施； b) 数据库管理系统和操作系统依据最小授权原则设计安全访问控制策略，依据业务要求实现不同用户对不同数据的访问权限； c) 数据库管理系统和操作系统不得使用相同的用户名和密码，防范入侵操作系统的攻击者直接入侵数据库。
	数据存储安全审计	a) 应对数据文件的操作行为进行安全审计，至少对用户操作、存储事件和文件变更信息进行记录； b) 应对虚拟化组件的活动进行监控，至少对虚拟网络、虚拟主机、虚拟桌面、虚拟 CU、虚拟存储的活动进行监控； c) 应对虚拟资源使用情况进行记录，至少对 CPU、内存、存储的容量、可用空间、使用比例信息进行记录，并设置报警阈值，提供报警功能； d) 应使用内容发现机制扫描存储数据，识别已泄漏的敏感数据； e) 应对平台系统管理员的操作和系统管理员的权限进行审计； f) 应定期提供平台运行报告，报告内容包括平台运行状态、安全情况、事

安全措施		满足要求
		故情况、变更情况等； g) 应引入第三方审计机构，对 CIM 基础平台定期进行审计，评估是否实现了合理的安全控制措施； h) 应采取有效措施保障日志不会被非授权的访问、修改和覆盖，确保审计措施不会带来新的安全问题。
	数据存储设备与介质安全	a) 存储设备和介质保存环境必须保持清洁，且需要防盗、防震、防火、防雷、防高温、防潮湿、防静电、防电磁干扰； b) 制定存储设备和介质资产清单，清单内容包括存储设备和介质名称、责任人、用途、采购时间等，并定期更新存储设备和介质资产清单信息； c) 正确移动存储设备和介质，存储设备和介质移动时避免碰撞和大幅度震荡； d) 严格规范存储设备和介质数据读写操作，避免对存储设备和介质超频使用，保障读写数据时的持续供电； e) 存储设备和介质维修时，必须安排陪同人员对维修过程进行监控，严格控制数据知悉范围，对于重要数据，要求维修人员到指定地点进行维修； f) 制定存储设备和介质使用管理制度，规范存储设备和介质使用人员权限、使用审批流程、使用操作规范、故障处理流程等。
	数据存储加密	a) 应对敏感数据提供数据加密功能，可以对不同安全要求数据进行不同强度的加密； b) 应制定和实施密码控制策略，并符合 GB/T 22081-2008 中 12.3.1 的相关要求； c) 应采用成熟的密钥管理方案，对密钥的生命周期进行有效的管理，密钥管理应符合 GB/T22081-2008 中 12.3.2 的要求。
	数据离散存储	a) 应选择数据离散存储，对数据离散存储的敏感数据片进行加密； b) 应对数据离散存储的数据进行完整性校验，确保有效的数据重构恢复。
数据共享安全		a) 应提供严格的共享数据访问权限控制功能，访问控制粒度细化到用户的具体操作；

安全措施	满足要求
	b) 应采用有效的措施控制共享数据，确保已授权的用户才能对共享数据进行增加、删除、查看、修改、上传和下载; c) 应采用有效措施，保障存储的敏感信息和重要数据的机密性和完整性; d) 在数据共享的过程中使用切片后的数据发布服务进行使用的，前端通过请求调用相关级别、范围的瓦片数据进行业务应用搭建，禁止使用矢量数据服务格式，确保源数据安全和保密。
数据备份恢复安全	a) CIM 基础平台数据备份应采用磁带，有容错能力的磁盘阵列(RAID)，光学存储设备等介质； b) CIM 基础平台应采取增进物理安全、实施密码及策略、正确分配备份人员的权限等措施进行数据库备份； c) 应强化本地与异地的物理安全与制度管理，减少人员与备份设备和介质接触的机会，对操作维护人员的操作过程进行审核。应打印并异地保存备份操作的文档，经常整理并归档备份，把备份和操作手册的副本与介质共同异地保存。应对介质的废弃处理有明确的规定，对介质安全低级格式化处理； d) 备份内容的安全应采用密码保护，应包括备份前的数据加密与备份时对备份集的加密两种； e) 密码应具有一定的复杂性。密码必须为大写字母、小写字母、数字、特殊字符的组合，而且不能少于 8 位； f) 备份工作应由三人完成：高层管理人员，备份操纵员和备份日志管理员。备份密码分为两部分，由高层管理人员和备份日志管理人员分别保管其中的一部分。高层管理人员负责保存密码的前一部分，并审核数据恢复的日志。备份操作员完成每日的备份工作，完成介质异地存储，查看备份日志，不保存备份密码，与其他人完成备份策略的设定。备份日志管理员审核与管理每日备份与恢复操作日志，保存后一部分的备份密码； g) 应依据 GB/T 20988 的要求制定灾难恢复策略，建立灾备中心； h) 应设计数据备份与恢复方案，确定数据备份的范围、策略、方法和流程，确定数据恢复的目标、流程；

安全措施	满足要求
	i) 应依据业务安全目标要求，制定数据备份措施，并及时根据业务需求更新备份措施； j) 应定期组织数据恢复测试； k) 异地备份中心建设选址，应符合国家政策要求和业务安全要求。
数据安全隔离	a) 采用有效措施隔离 CIM 基础平台不同用户的数据和备份数据； b) 应依据终端、物理主机和虚拟主机的业务类别、地理位置、部门属性和安全级别划分不同的安全域； c) 应规划合理的虚拟化网络安全控制措施，划分虚拟化网络子网，对 CIM 基础平台流入数据和流出数据设置访问控制策略； d) 应对不同安全级别的业务数据进行物理隔离或强逻辑隔离，即必须部署在不同的物理主机、不同子网、不同集群或者不同虚拟机上； e) 相同安全级别的业务数据之间，管理终端与业务系统之间的不同安全域需要实现逻辑隔离，需要采用物理防火墙技术、划分子网等方式进行隔离、虚拟化系统实现集群隔离、多租户隔离、资源池隔离、操作系统隔离和数据隔离。

5.6.3 平台安全应符合下列规定：

a) CIM 基础平台应对所有数据进行严格的控制，应根据用户身份和现实工作中的角色和职责，确定访问数据资源的权限，对用户对业务数据的访问权限进行配置。数据分类分范围（行政区）进行授权控制；

b) 应对系统的所有用户进行分级管理，设置不同的角色，对每个角色分配不同的数据权限；

c) CIM 基础平台应采用三权分立的安全管理体制：分为数据库管理员（DBA）、数据库安全管理员（SSO）和数据库审计员（Auditor）三类。DBA 负责自主存取控制及系统维护与管理方面的工作，SSO 负责强制存取控制，Auditor 负责系统的审计；

d) 用户管理应包括标识和鉴别，应对授权用户进行识别。

5.6.4 网络安全应符合以下规定：

a) 采用防火墙、入侵检测、漏洞扫描、病毒防治等网络安全技术，实现对各种不同的安全防御设备的统一管理、配置、监控、分析等，提供全面的、基于统一安全策略的网络安全防御，避免来自各个不同目的的攻击、干扰和非法访问等。

b) 省政务云按照网络安全等级保护第三级实施安全防护。云服务商按照信息安全相关法律规定和政策要求，制定安全管理制度，落实安全管理和防护措施,按规定开展省政务云网络安全等级保护工作。

6 运维过程管理

6.1 一般规定

6.1.1 应依据运维管理环节、管理内容、管理要求等制定统一的运维工作流程，实现运维工作的标准化、规范化和自动化。

6.1.2 宜根据《信息技术 服务管理 第 1 部分：规范》GB/T 24405.1 的相关规定加强运维服务过程管理，过程管理至少应包括事件管理、服务请求管理、问题管理和变更管理。

6.2 事件管理

6.2.1 事件管理负责对事件处理过程进行监控，并根据事件影响程度决定服务等级或应急响应等级的升降。事件管理涉及控制的范围应包括日常巡检、日常运维与监控、配置管理、备份与恢复、应急响应等运维活动。事件管理记录包含的信息如表 6.2.1 所示。

表6.2.1 事件管理记录信息

序号	信息项	描述
1	用户信息	与事件关联的用户信息，例如姓名、部门、联系方式、联系地址、通知方法等
2	事件类型	事件类型的描述，如信息类、告警类、异常类等
3	响应结果	对事件响应结果的描述
4	记录时间	事件记录的时间
5	记录人员	记录事件的人员
6	事件描述	对事件及其基础信息的描述

6.2.2 事件管理过程应包括事件的发生和通告、事件检测和录入、过滤判定、事件分类判定、事件关联、响应选择、人为干预、自动响应、问题/变更管理判定、事件关闭、评估行动等，其流程可参考图 6.2.2，各步骤说明如表 6.2.2-1，

参与角色及职责如表 6.2.2-2，实际应用中可根据自身情况进行调整相应管理。

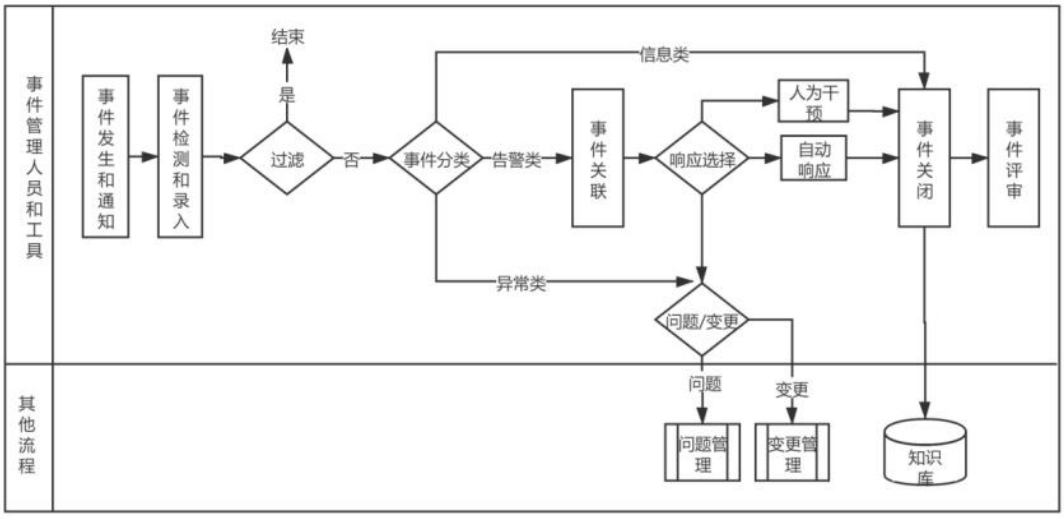


图 6.2.2 事件管理流程

表6.2.2-1 事件管理流程说明

序号	步骤名称	描述
1	事件的发生和通告	事件发生后，配置项通过轮询或通知的方式生成通告消息。
2	事件检测和录入	a) 通过运行在同一系统上的代理或管理工具本身，检测和解析通告信息； b) 将检测到的事件信息录入日志。
3	过滤判定	a) 对检测出的事件进行必要的过滤； b) 将过滤掉的事件录入到日志文件中。
4	事件分类判定	a) 对过滤后的事件按照其重要性进行必要的分类，类型包括信息类、告警类以及异常类； b) 信息类事件则直接结束； c) 告警类事件进行事件关联分析； d) 异常类事件进行进一步升级，启动问题/变更管理中必要的流程来处理。
5	事件关联	通过特定的管理工具将告警类事件与一组事先规定的标准和规则进行比较，从而识别事件的意义并确定相应的事件处理行

序号	步骤名称	描述
		动。
6	响应选择	依据事件关联的分析结果，触发相应的处理方式。
7	人为干预	a) 如果告警类事件处理需要人为干预，则应该发出报警信息通知相关人员或团队。 b) 相关人员或团队接到告警信息后对事件进行处理。
8	自动响应	如果告警类事件已有自动响应方式，则依据该方式自动处理。
9	问题/变更管理判定	对于异常类以及被升级为异常类的其他类事件，需启动问题/变更管理来处理。
10	事件关闭	a) 自动响应的告警类事件在处理成功后自动关闭； b) 人为干预的告警类事件处理完毕评估后关闭； c) 异常类事件在成功启动问题或变更管理流程后评估关闭； d) 发送事件处理报告，相关人员以此用来更新知识库。
11	评估行动	a) 如果事件触发了问题或变更管理，评估重点应当关注事件是否被正确移交，并是否得到了所期待的处理； b) 对于其他事件，则进行抽样评估。

表 6.2.2-2 事件管理参与角色及职责

角色	职责
事件管理人员和工具	事件管理不为其分配特定的管理者，流程的执行依赖于相关管理人员和必要的工具。相关人员具体包括服务台、技术管理人员、应用管理人员以及 IT 运营管理人员。

6.3 服务请求管理

6.3.1 服务请求管理是对服务请求过程进行监控，其涉及控制的范围应包括应急响应机制与执行活动。

6.3.2 服务请求管理过程应包括接收服务请求、提供菜单供用户选择、财务审批、判定是否通过财务审批请求、其他审批、判定是否通过其他审批请求、实现、关闭等，其流程可参考图 6.3.2，各步骤说明如表 6.3.2-1，参与角色及职责如表

6.3.2-2，实际应用中可根据自身情况进行调整相应管理。

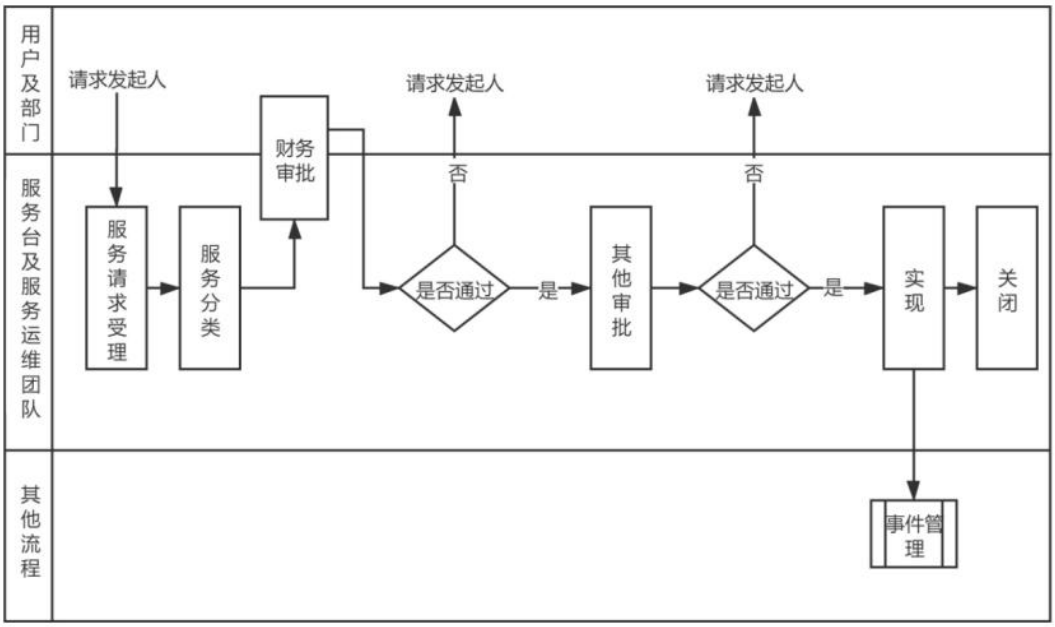


图 6.3.2 服务请求管理流程

表 6.3.2 -1 服务请求管理流程说明

序号	步骤名称	说明
1	接收服务请求	服务请求大多来自服务台。用户可通过电话呼叫或 Web 等方式将服务请求提交到服务台。
2	提供菜单供用户选择	提供标准的服务请求清单供用户选择，用户确认服务请求的细节，并订下符合 SLA 的请求实现目标。
3	财务审批	a) 对于成本确定的标准请求，通常作为组织每年财务管理的一部分来审批； b) 其他情况下，则先要评估实现请求的成本，再将评估结果提交给用户审批。
4	判定是否通过请求	a) 根据财务审批，决定是否通过服务请求； b) 如果通过，进入下一步； c) 如果不通过退还给服务请求发起人。
5	其他审批	在某些情况下需要进一步的审批，比如一致性相关的或业务相关的审批。

序号	步骤名称	说明
6	判定是否通过请求	a) 根据其他审批，决定是否通过服务请求： b) 如果通过，进入下一步； c) 如果不通过，退还给服务请求发起人。
7	实现	a) 某些简单的服务请求可能直接由服务台一线支持人员执行； b) 某些服务可能需要进一步交给专家团队或者供应商来处理和满足。
8	关闭	用户的服务请求实现后，必须反馈给服务台来关闭。服务台在关闭前可能发起客户回访和满意度调查并输出。

表 6.3.2 - 2 服务请求管理参与角色及职责

角色	职责
服务台和服务运营团队	服务请求通常由服务台和服务运营团队来实现。请求实现的职责由相应的事件管理相关角色承担。设备管理，采购和其他业务领域常常协助实现服务请求。

6.4 问题管理

6.4.1 问题是指导致事件产生的原因，问题管理涉及控制的范围应包括日常巡检、日常运维与监控、配置管理、备份与恢复、应急响应等运维活动，应按照不同领域的问题（如网络、主机、中间件、数据库、应用等）由相关领域的技术支持专家来处理。问题管理记录的信息如表 6.4.1 所示。

表6.4.1 问题管理记录信息

序号	信息项	描述
1	用户信息	与问题关联的用户信息，例如姓名、部门、联系方式、联系地址、通知方法等。
2	服务信息	与问题关联的服务信息，例如 SLA、OLA、UC、服务质量等。
3	设备信息	与问题关联的设备信息，例如设备的 CI、IT 基础设施等。
4	记录时间	问题记录的时间。

序号	信息项	描述
5	优先级和分类信息	问题定义的优先级和问题归属类别。
6	问题描述	详细描述问题的内容。
7	问题状态	问题所处的状态，如新建、已接受、已计划、已分配、激活状态、已暂停、已解决、已关闭等。
8	所有诊断信息或实施过的解决方案信息	已有的对问题的诊断信息以及为解决问题而实施过的解决方案和措施等信息。

6.4.2 问题管理过程应包括问题检测和记录、问题归类和优先级处理、问题调查和诊断、创建已知错误记录、解决问题、问题关闭、重大问题评估等，其流程可参考图 6.4.2，各步骤说明如表 6.4.2-1，参与角色及职责如表 6.4.2-2，实际应用中可根据自身情况进行调整相应管理。

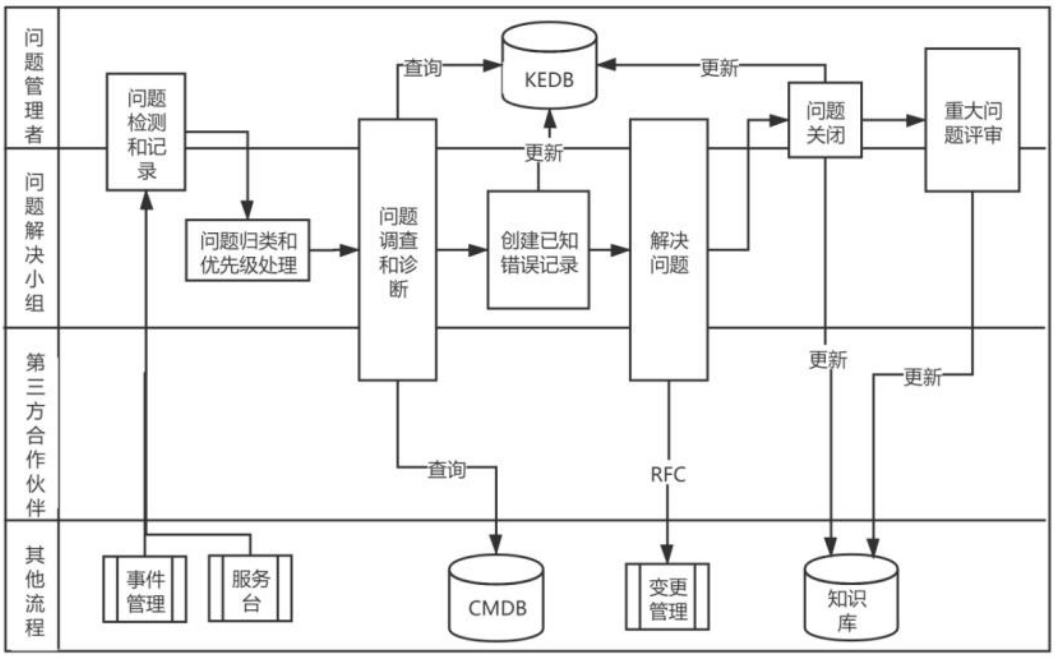


图 6.4.2 问题管理流程

表 6.4.2 - 1 问题管理流程说明

序号	步骤名称	说明
1	问题检测和	a) 问题管理者接收来自服务台，事件管理以及合作伙伴等提交

序号	步骤名称	说明
	记录	的事故报告或潜在问题报告； b) 问题解决小组通过主动问题管理发现潜在的问题并提交报告； c) 问题管理者收集相关报告并创建问题记录； d) 问题管理者将记录的问题分配给指定的问题处理小组或人员处理。
2	问题归类和优先级处理	问题解决小组对问题进行归类和优先级处理。
3	问题调查和诊断	a) 问题管理者组织问题解决小组成员对问题进行调查和诊断； b) 如果调查和诊断需要第三方合作伙伴的协助，则由问题管理者负责联络和沟通； c) 如果问题所造成的事故频繁复发或紧急度非常高，则需要制定并实施临时措施，暂时性的 恢复服务水平；临时措施实施之后，问题处理小组必须继续寻求并制定一套永久性的解决方案； d) 如果问题的影响度非常低而解决的成本非常高，这时组织需要考虑是否有必要实施解决方案。如果决定暂不实施，则需要制定并实施一套临时措施，以降低问题对服务的影响； e) 问题管理者负责收集和整理问题调查和诊断相关记录，并为服务台和事故管理提供临时措施等方面的建议； f) 临时措施的制定和实施需要第三方合作伙伴协助时，由问题管理者负责联络和沟通。
4	创建已知错误记录	问题解决小组根据调查和诊断的结果以及临时修复方案创建已知错误记录，并将其存放在已知错误库中。
5	解决问题	a) 根据调查和诊断的结果实施解决方案； b) 如果解决方案需要对基础设施进行变更，则由问题管理者提交变更请求，启动变更管理流程； c) 解决方案需要第三方合作伙伴协助时，由问题管理者负责联

序号	步骤名称	说明
		络和沟通。
6	问题关闭	a) 问题管理者审核已解决的问题记录，正式批准关闭问题记录； b) 整理问题解决相关知识，更新知识库。
7	重大问题评估	a) 重大问题处理之后，问题管理者应组织和召开重大问题评估会议，探讨和学习相关经验和教训； b) 会后整理相关知识，更新知识库。

表 6.4.2 - 2 问题管理参与角色及职责

角色	职责
问题管理者	a) 定期组织相关人员对事故记录进行分析，发现潜在问题； b) 联络所有的问题解决小组确保在 SLA 目标内迅速解决问题； c) 开发并负责维护已知错误数据库； d) 负责维护已知错误以及管理已知错误的检索算法； e) 联络供应商、承包商等第三方合作伙伴，确保其履行合同内的职责，特别是有关问题解决以及问题相关信息和数据的提供的职责； f) 正式关闭问题记录； g) 负责定期安排和执行重大问题评估的一系列相关活动。
问题解决小组	a) 根据事故处理和日常维护要求创建问题，启动问题管理流程； b) 对问题实施分类和优先级处理； c) 自行调查和诊断问题,制定解决方案； d) 和第三方合作伙伴一同调查和诊断问题、制定解决方案； e) 提交变更请求； f) 回顾问题、整理解决方案并提交知识库。

6.4.3 问题分类和优先级

问题的分类通常采用多层次结构，一个类别包括多个子类。分类时将问题归入某一类别或某一子类中。分类方法可以按问题发生的可能原因分类，也可按相关支持小组进行分类。

问题的优先级通常由服务台通过与用户进行协商，并根据 SLA 确定。优先级通常用数字来表示，根据紧急度和影响度确定，如表 6.4.3 所示。

表 6.4.3 优先级与紧急度和影响度的关系

优先级代码	描述	目标解决时间
1	高影响度高紧急度	＜1 小时
2	高影响度中紧急度/ 中影响度高紧急度	＜8 小时
3	高影响度低紧急度/ 中影响度中紧急度/ 低影响度高紧急度	＜24 小时
4	中影响度低紧急度/ 低影响度中紧急度	＜48 小时
5	低影响度低紧急度	/

6.5 变更管理

6.5.1 变更管理是对变更过程进行监控，变更管理涉及控制的范围应包括日常巡检、日常运维与监控、配置管理、备份与恢复、应急响应等运维活动。

6.5.2 变更管理过程应包括创建 RFC、记录和过滤 RFC、判断是否过滤、评估变更、判定是否授权变更、评估变更、判定能否授权、评估变更、判定是否授权变更、变更规划、协调变更实施、实施变更、回顾变更、关闭变更、紧急变更子流程等，其流程可参考图 6.5.2，各步骤说明如表 6.5.2-1，参与角色及职责如表 6.5.2-2，实际应用中可根据自身情况进行调整相应管理。

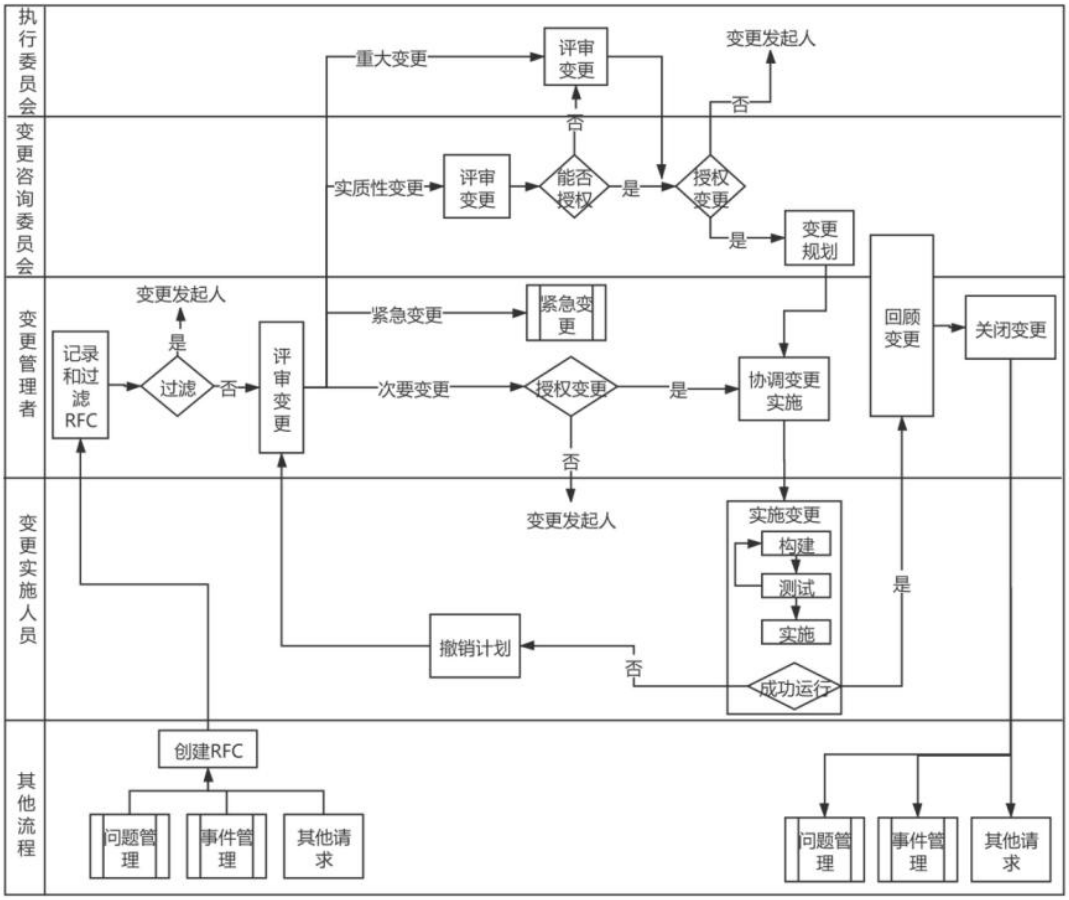


图 6.5.2 变更管理流程

表 6.5.2 - 1 变更管理流程说明

序号	步骤名称	说明
1	创建 RFC	a) 变更发起人根据来自维护人员或其他 IT 人员、项目建设、事件、问题等管理流程提出的需求，收集信息并与相关部门或用户确认； b) 创建变更请求记录； c) 初步为变更分配类型、优先级、风险等级等； d) 接收来自被变更管理者或 CAB 拒绝的 RFC 及反馈意见； e) 如需再次重新发起该 RFC，变更发起人需根据反馈意见在 RFC 中追加必要的增补信息，保证变更信息项的完整性和正确性，并再次提交 RFC。
2	记录和过滤 RFC	a) 变更管理者接收并记录变更发起人提交的 RFC； b) 对 RFC 进行初步评估，过滤不切实际的、重复提交的、

序号	步骤名称	说明
		已拒绝以及不完善的 RFC。
3	判断是否过滤	a) 判断是否过滤该 RFC； b) 如果过滤则将 RFC 退还给变更发起人并关闭变更，同时将过滤理由和相关反馈意见记入变更日志中； c) 如果不过滤，则进入下一步。
4	评估变更	a) 变更管理者召集变更管理小组成员，对变更风险、优先级以及类型等进行划分和确认： b) 对于确认的紧急变更应该立即启动“紧急变更子流程”； c) 接收来自“紧急变更子流程”拒绝的紧急变更请求，评估相关意见，并通知变更发起人； d) 对于重大变更应先提交 IT 执行委员会审批； e) 对于实质性变更，变更管理者应协调资源，初步制定变更计划，包括创建、测试、回退以及补救计划，在下一次 CAB 会议提交审批； f) 对于影响度低的次要变更，变更管理者可以直接判断是否授权。
5	判定是否授权变更	a) 针对次要性变更，变更管理者可直接判断是否授权； b) 如果授权则直接进入下一步； c) 如果拒绝，则将 RFC 退还给变更发起人并关闭变更，同时将拒绝理由和相关反馈意见记入变更日志中。
6	评估变更	a) 针对实质性变更，变更管理者召开 CAB 会议评估变更； b) 会议上，CAB 成员对变更进行评估，包括判定变更分类、优先级划分、风险评估等是否正确。
7	判定能否授权	a) 如果无法就此变更授权达成一致或变更被重新认定为重大变更，CAB 则应提交至 IT 执行委员会进行最后审批； b) 对于无争议的变更，进入下一步。
8	评估变更	a) 对变更管理者提交的重大变更，或 CAB 会议上争议的变更进行评估并判定是否授权变更；

序号	步骤名称	说明
		b) 将评估结果以及授权或拒绝意见反馈给 CAB。
9	判定是否授权变更	a) 如果会议拒绝授权的变更，或是得到 IT 执行委员会的拒绝指示，则应将 RFC 退还给变更 发起人并关闭变更，同时将拒绝理由和相关反馈意见记入变更日志中； b) 如果会议通过变更授权，或是得到 IT 执行委员会的授权指示，则正式授权变更管理者实施变更，进入下一步进行变更规划。
10	变更规划	a) 由 CAB 成员对实质性变更进行相关规划，商讨详细的变更实施方案和计划，包括创建、测试、回退以及补救计划，并制定变更计划进度表； b) 接收来自 IT 执行委员会授权的变更（包括重大变更、存在争议变更）以及相关反馈意见， 为其进行规划，商讨详细的变更实施方案和计划，包括创建、测试、回退以及补救计划，并制定变更计划进度表。
11	协调变更实施	a) 变更管理者将 RFC 送往变更实施人员处进行变更； b) 负责协调各方资源，确保整个变更按照变更计划进度表实施； c) 负责全程监控变更的实施； d) 变更管理者也可以委托变更主管全程监控变更。
12	实施变更	a) 变更实施人员根据变更实施进度计划进行变更； b) 变更的实施过程包括构建、测试和实施； c) 如果变更成功实施，则进入下一步； d) 如果不成功，则实施撤销计划回滚变更。
13	回顾变更	a) 变更完成后，变更管理者负责准备回顾资料，召集 CAB 成员及其他相关部门人员参加会议，对成功实施的变更，重大变更、失败而执行过撤销计划的变更以及被拒绝的变更进行回顾和评估。 b) 变更管理者负责将回顾结果更新到变更记录中。

序号	步骤名称	说明
14	关闭变更	a) 如果变更是问题等其他流程发起，则提交变更结果给相关处理人； b) 对于重大的变更，需提交总结报告至高层； c) 整理信息、更新变更记录，正式关闭变更。
15	紧急变更子流程	参见“ 紧急变更子流程”。

表 6.5.2-2 变更管理参与角色及职责

角色	职责
IT 执行委员会	a) 负责对提交的重大变更实施授权； b) 审批 CAB 无法达成的最后决议。
变更管理者	a) 负责与 RFC 发起人联络，接收和登记 RFC，拒绝任何不切实际的 RFC； b) 组织评估变更，为其分配优先级； c) 组织召升 CAB 会议； d) 决定会议的组成，根据 RFC 的不同确定与会人员和人员职责； e) 为紧急变更召开紧急 CAB 会议或 ECAB 会议； f) 就任 CAB 和 ECAB 主席职务； g) 通过服务台，分发变更进度计划表； h) 负责与所有的主要合作伙伴联络和沟通，协调变更构建、测试和实施，确保其与进度计划表一致； i) 负责更新变更日志； j) 评估所有已实施的变更，确保它们满足目标；回顾所有失败或回滚的变更； k) 分析变更记录以确定任何可能发生的趋势或明显的问题； l) 正式关闭 RFC； m) 生成正规的、准确的管理报告。
变更咨询委员会	a) 参加变更委员会会议或紧急变更委员会；

角色	职责
(CAB) /紧急变更咨询委员会(ECAB)	b) 协助变更管理者对变更进行评估； c) 参与制定变更计划进度表和日程安排； d) 回顾失败的或补救过的变更，确保今后不再发生类似的情况； e) 同顾已实施的变更，确保其满足目标； f) 对流程提出修改意见和建议。
变更实施人员/紧急变更实施 人员	根据变更相关规划和变更计划进度表实施变更，包括构建、测试以及实施等步骤。

6.5.3 紧急变更管理过程应包括召集紧急变更咨询委员会 ECAB、快速评估和审批、确认是否为紧急变更、判定能否授权、评估变更、判定是否授权变更、快速制定实施、测试、回退以及补救计划、协调紧急变更实施、回顾紧急变更、关闭紧急变更等，其流程可参考图 6.5.3，各步骤说明如表 6.5.3，参与角色及职责如表 6.5.2-2，紧急变更在重大灾害等需求时，应有一键切入机制，实际应用中可根据自身情况进行调整相应管理。

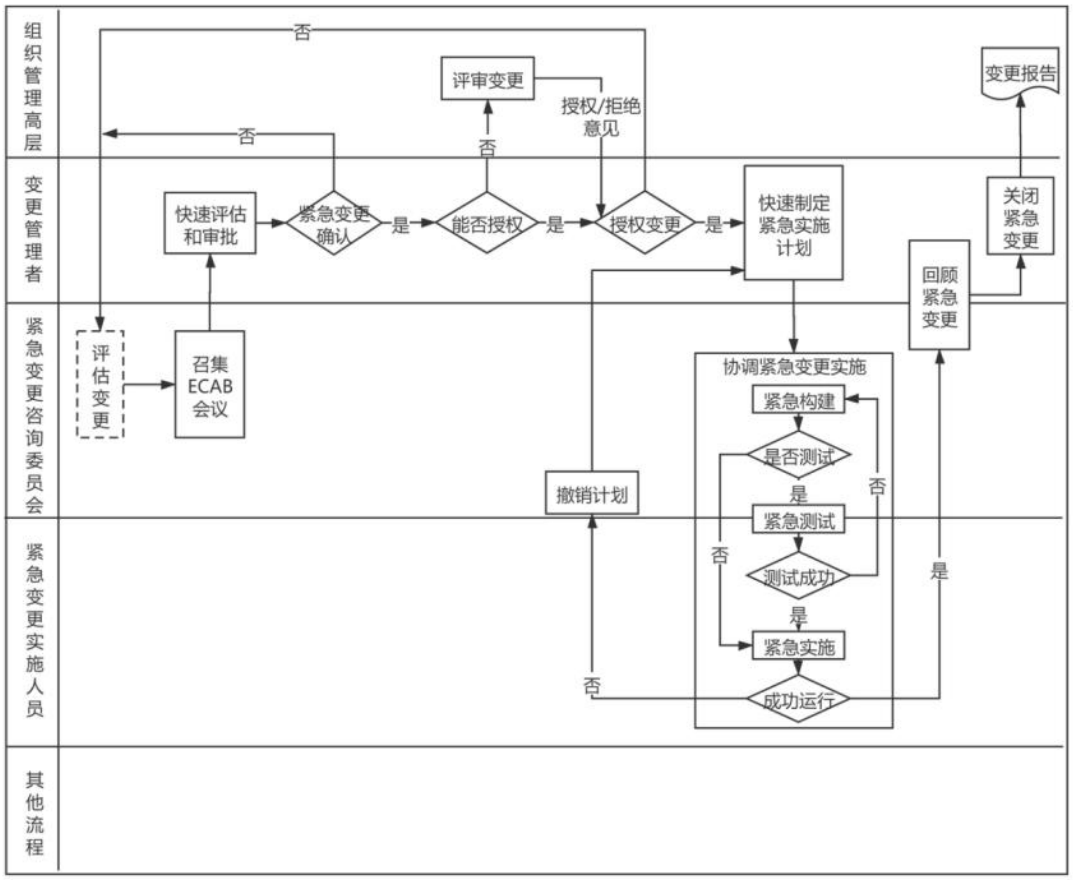


图 6.5.3 紧急变更管理流程

表 6.5.3 紧急变更管理流程说明

序号	步骤名称	说明
1	召集紧急变更咨询委员会 ECAB	变更管理者组织召开 ECAB 会议。
2	快速评估和审批	a) ECAB 成员检查和审阅需要讨论的紧急变更请求； b) 如果变更委员会发现 RFC 的信息不足以作出决定，应当立即要求变更请求若提供更多信息，而变更请求者在紧急变更处理过程中应当随时准备配合； c) ECAB 成员评估变更，对该变更做出批准或驳回的意见； d) 如不同意该紧急变更，则返回原流程。
3	确认是否为紧急变更	a) 确认此变更请求是否为紧急变更请求； b) 如果是，则进入下一步； c) 如果不是，则转退回，变更管理者需重新判定变更类型。
4	判定能否授权	a) ECAB 成员如果无法就此变更授权达成一致， 或变更

序号	步骤名称	说明
		被认定为重大变更，则应提交组织管理高层进行定夺； b) 对于无争议的紧急变更，进入下一步。
5	评估变更	对 ECAB 提交的紧急变更，高层人员应当立刻尽快做出评估意见，并将其转交 ECAB。
6	判定是否授权变更	a) 如果 ECAB 拒绝授权变更，或得到组织管理高层的拒绝指示，则转入判定能否授权，并同时将拒绝理由和相关反馈意见记入变更日志中； b) 如果 ECAB 通过变更授权，或是得到组织管理高层的授权指示，则正式授权变更管理者实施紧急变更，进入变更规划。
7	快速制定实施、测试、回退以及补救计划	ECAB 快速制定紧急变更计划，包括实施计划、测试计划、撤销计划以及补救计划等并制定紧急变更计划进度表。
8	协调紧急变更实施	a) 变更管理者协调一切可使用的资源，组织相关专业人员，对被批准的紧急变更进行紧急创建； b) 判断是否有充分时间进行测试。如果有则进行紧急测试，紧急测试应当尽量缩短测试程序，保留对关键对象的测试； c) 如果时间不允许，则按照方案执行紧急变更实施； d) 如果测试成功，则按照方案执行紧急变更实施； e) 如果不成功，执行撤销计划重新进行紧急构建； f) 变更管理者组织变更实施人员，按照实施计划在生产环境实施变更。实施的同时也可以并行测试； g) 实施变更后判断服务是否运行正常； h) 如果正常则进入下一步； i) 如果不正常，应该立刻实施补救计划，并转向步骤 7 新商讨制定计划； j) 变更管理者可以委托变更主管全程监控变更。

序号	步骤名称	说明
9	回顾紧急变更	a) 变更管理者确定参加回顾的人员，并将相关信息发给与会人员； b) 变更管理者主持回顾会议，回顾该紧急变更的根源，变更的业务或技术目的，给出建议或意见。
10	关闭紧急变更	a) 提交变更总结报告至管理高层； b) 整理资料，更新变更记录，通知变更请求者，关闭变更。

6.6 应急响应

6.6.1 运维服务机构应提供应急响应服务，包括实施应急响应流程、应急响应预案流程、保障措施等。

6.6.2 运维服务机构应按应急响应流程响应 CIM 基础平台的突发事件。响应流程应包括事先预防、事发通报、事中处理、事后总结等，详见附录 A。

6.6.3 运维服务机构应实施应急响应预案流程并不断更新完善，应急事件类型及预案流程见附录 B。

6.6.4 运维服务机构应实施应急演练、人员培训、硬件资源保障、文档资料准备、技术支持保障等相关保障措施，应满足表 6.6.4 的规定。

表6.6.4 应急保障措施

保障措施	满足要求
应急演练	a) 应定期或不定期组织应急预案演练，提高平台突发事件应急响应水平； b) 应检验应急预案各环节之间的通信、协调、指挥等是否符合快速、高效的要求； c) 应通过演习，进一步明确应急响应各岗位责任，并对预案中存在的问题和不足及时补充、完善。
人员培训	应定期或不定期地举办不同层次、不同类型的技术讲座或研讨会。
硬件资源保障	a) 应为相应的核心业务平台提供必要的备份设备与线缆等硬件资源，并配备与现有设备兼容的设备； b) 硬件资源应预先采购并保存在专门位置。
文档资料准备	文档资料准备应包括平台工维护手册、操作手册、设备配置参数、拓扑图以及 IP 地址规范及分布情况等。
技术支持保障	应建立预警与应急处理的技术平台，从技术上逐步实现应急环节、专项业务系统及相关部门之间应急处理的联动机制。

7 运维组织体系

7.1 人员组织

7.1.1 运维队伍应由运维服务机构成立，专职负责运维工作。

7.1.2 运维队伍宜由技术人员和管理人员组成，并根据工作内容配备相应专业技术人员。

7.1.3 运维队伍宜根据运维工作对象类别分成多个专业服务组，各专业组分工协作，共同完成运维工作。

7.2 服务方式

7.2.1 运维服务方式宜包括远程服务、现场驻点服务、电话支持服务、全天候在线咨询等。

7.2.2 远程服务宜支持通过远程软件保障现场系统平稳运行。

7.2.3 现场驻点服务宜支持短期或长期现场驻守，负责软件系统功能运维、服务器运维。

7.2.4 电话支持服务宜支持通过电话支持的方式与运维工程师联系进行问题诊断。

7.2.5 宜支持 7×24 小时在线支持，提供包含电子邮件支持在内的综合性在线支持。

7.3 工作模式

7.3.1 运维队伍应根据运维实际建立高效的工作模式，合理利用资源。

7.3.2 运维工作应建立由热线（服务台）、一线（运维工程师）、二线（运维专家）、专业机构组成的多级技术支持体系。热线不能解决的问题提交一线；一线负责监控巡检、一般性的问题处理，并配合二线进行复杂问题处置，一线不能处理的问题提交二线；二线负责解决复杂问题，并进行深度的运行状况分析、评估，二线不能解决的问题提交设备生产厂商、软件开发商或第三方服务单位等专业机构。

7.4 岗位职责

7.4.1 运维工作应进行岗位设计，明确运维岗位，规定岗位职责，岗位职责规定至少应包括维护对象范围、工作内容及工作要求等。

7.4.2 根据实际情况，每名运维人员可以任职多个岗位，重要岗位应有两人或两人以上任职。

7.5 技能要求

7.5.1 运维人员应具备信息技术基础知识、运维岗位所需的专业知识及 CIM 基础平台所支撑业务的相关业务知识，宜具有专业技能资质证书。

7.5.2 运维队伍应加强人才队伍的建设和培养，定期组织各类培训，运维人员每年参加专业技术培训时间宜不少于 48 学时。

8 运维保障资源

8.1 工具装备

8.1.1 运维保障装备应配备必要的专用仪器、仪表，仪器、仪表应专人专管、定期测检校正。

8.1.2 运维保障装备应配备必要的维护工具，维护工具领用应登记，并妥善保管。

8.2 文档资料

8.2.1 运维工作应建立运维对象清单、平台详细说明、操作手册、应急预案等文档，且技术资料应整理成册。

8.2.2 开展运维工作应对平台运行状况、运维服务过程进行记录，并整理形成平台运行资料。宜建立运维知识库，并建立更新维护机制。

8.3 备品备件

8.3.1 运维保障应总结分析常见故障设备，预先储备相应的备品备件，以便在发生故障时能及时更换受损部件。

8.3.2 运维保障应加强备品备件管理，定期对备品备件进行盘点，做好备件入库、领用登记；备品备件应分类妥善保管，并定期检查抽测，以保证其性能良好。

8.4 管理制度

8.4.1 制度体系内容应涵盖网络管理、系统及应用管理、安全管理、存储和备份管理、技术服务管理、人员管理以及质量考核等类别。具体如下所示：

a) 网络管理制度：包括网络的准入管理制度、网络的配置管理制度、网络的运行/监控管理制度等；

b) 系统及应用管理制度：包括对主机、数据库、中间件、应用系统的配置

管理制度、运行/监控管理制度、数据管理制度等；

c) 安全管理制度：包括网络、主机、数据库、中间件、应用软件、数据的安全管理制度及安全事故应急处理制度；

d) 存储备份管理制度：包括备份数据的管理制度和备份设备的管理制度；

e) 故障管理制度：包括对故障处理过程的管理制度、故障处理流程的变更管理制度、故障信息利用的管理制度及重大故障的应急管理制度等；

f) 技术支持工具管理制度：指对运维管理平台、运维知识库等的使用、维护的有关制度；

g) 人员管理制度：包括对运维人员的能级管理制度、奖惩制度、考核制度等；

h) 质量考核制度：制定相关制度，对以上各类制度的执行情况进行考核。

8.4.2 运维工作应定期和不定期开展检查，促进各项制度规范的贯彻落实，实现各项工作的规范化管理，并确保各项制度随着 CIM 基础平台的不断发展及时更新。

附录 A（资料性附录）应急响应流程

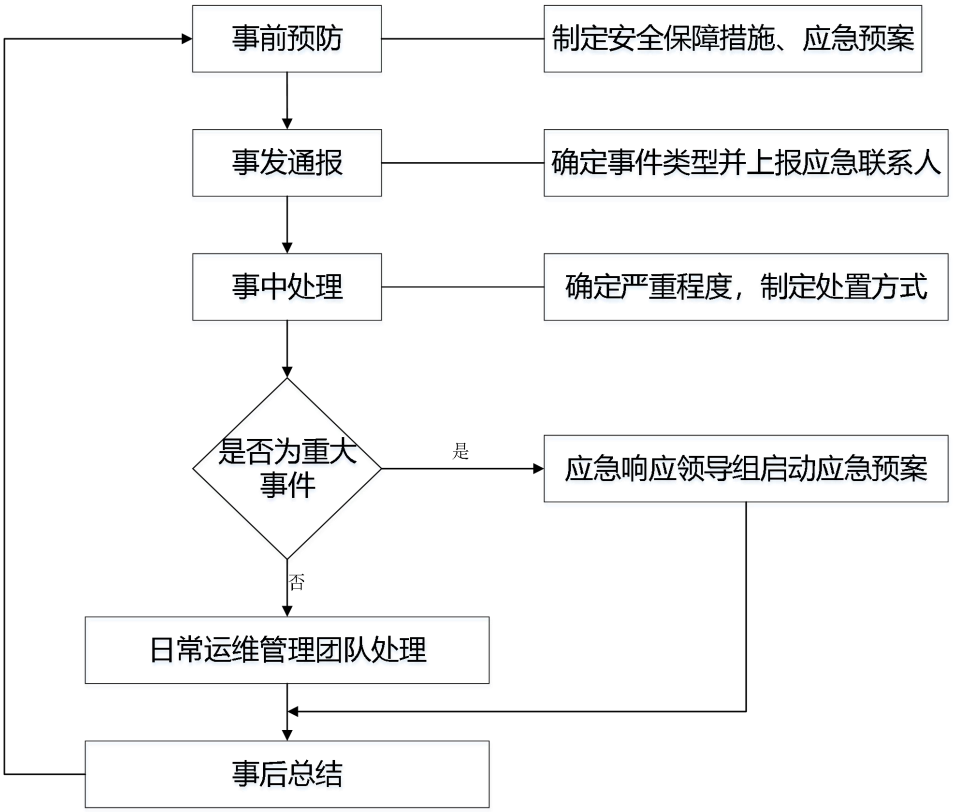


图 A 应急响应流程

表 A 应急响应流程说明

响应步骤	说明
事先预防	a) 应参照国家信息安全等级保护三级的相关要求采取相应的安全保障措施； b) 应对网络基础设施和相关平台进行全面的安全监测，识别平台的资产价值及脆弱性，分析各种威胁发生的可能性并针对各种威胁制定相关应急预案。
事发通报	a) 在突发事件发生后，发现人应当立即向 CIM 基础平台应急联系人报告。同时，发现人应当对发现的事件进行调查核实、保存相关证据，并在事件被发现时将证据报至应急联系人； b) 应急联系人接到信息安全突发事件报告后，经初步核实后，应将有关情况及时向应急领导组报告，进一步进行情况综合，研究分析可能造成损害的程度，提出初步行动对策，并及时报应急领导组； c) 领导小组应视情况召集协调会，决策行动方案，发布指示和命令。

响应步骤	说明
事中处置	a) 预案启动 **1** 对于特别重大以及重大事件，应按照快速有序的原则启动应急预案，并由应急响应领导组发布应急响应启动命令； **2** 应由运维管理团队处理日常运维事件管理流程即可解决的一般事件，不需要启动应急预案。 b) 应急处置 **1** 应急预案启动后，应急实施组应立即采取相关措施抑制信息安全事件的影响，避免造成更大损失； **2** 应根据应急事件的分类，初步确定应急处置方式，区别对待； **3** 灾害事件：应根据实际情况，在保障人身安全的前提下，保障数据安全和设备安全；具体方法包括硬盘的拔出与保存、设备的断电与拆卸、搬迁等； **4** 故障或攻击事件：判断故障或攻击的来源与性质，关闭影响安全与稳定的网络设备和服务器设备，断开平台与攻击来源的网络物理连接，跟踪并锁定攻击来源的IP地址或其他网络用户信息，修复被破坏的信息，恢复平台。具体处置措施应按照对应的应急预案严格执行。 c) 灾难恢复 **1** 在应急处置工作结束后，应迅速采取有效措施，抢修受损的基础设施，减少损失，尽快恢复正常工作； **2** 应通过统计各种数据，查明原因，对安全事件造成的损失和影响以及恢复重建能力进行分析评估，认真制定恢复重建计划，迅速组织实施灾难恢复工作，把受到影响的系统和网络设备彻底还原到它们正常的任务状态； **3** 恢复工作应避免出现误操作导致数据的丢失； **4** 恢复工作中如涉及到机密数据，应额外遵照机密系统的恢复要求。
事后总结	a) 应急事件处置完毕后，应急处置各组应回顾并整理已发生信息安全事件的各种相关信息，尽可能地把所有情况记录到文档中； b) 发生重大信息安全事件时，应急响应各组应在事件处理完毕后一个工

响应步骤	说明
	作日内，将处理结果上报到领导组备案； c) 应对信息安全事件进行统计、汇总以及任务完成情况总结，不断改进信息安全应急预案。

附录 B（资料性附录）应急响应预案流程

表 B　CIM 基础平台应急响应事件类型清单

事件类别		事件表述	流程
有害程序事件	计算机病毒事件	指蓄意制造、传播有害程序，或是因受到有害程序的影响而导致的信息安全事件。	详见图 B.1
	蠕虫事件		
	特洛伊木马事件		
	僵尸网络事件		
	混合攻击程序事件		
	网页内嵌恶意代码事件		
	其他		
网络攻击事件	拒绝服务攻击事件	指通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷、或使用暴力攻击对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的信息安全事件。	详见图 B.2
	后门攻击事件		
	漏洞攻击事件		
	网络扫描窃听事件		
	网络钓鱼事件		
	干扰事件		
	其他		
信息破坏事件	信息篡改事件	指通过网络或其他技术手段，造成信息系统中的信息被篡改、假冒、泄露、窃取等而导致的信息安全事件。	详见图 B.3
	信息假冒事件		
	信息泄露事件		
	信息窃取事件		
	信息丢失事件		
	其他		
信息内容安全事件	违反宪法和法律、行政法规的信息安全事件	指利用信息网络发布、传播危害国家安全、社会稳定和公共利益的安全事件。	详见图 B.4
	针对社会事项进行讨论、评论形成网上敏感的舆论热点，出现一定规模炒作的信息安全事件		
	组织串联，煽动机会游行的信息安全事件		
	其他		

事件类别		事件表述	流程
设备设施故障事件	软硬件自身故障	指由于信息系统自身故障或外围保障设施故障而导致的信息安全事件，以及人为的使用非技术手段有意或无意的造成信息系统破坏而导致的信息安全事件。	详见图 B.5
	外围保障设施故障		
	人为破坏事故		
	其他		

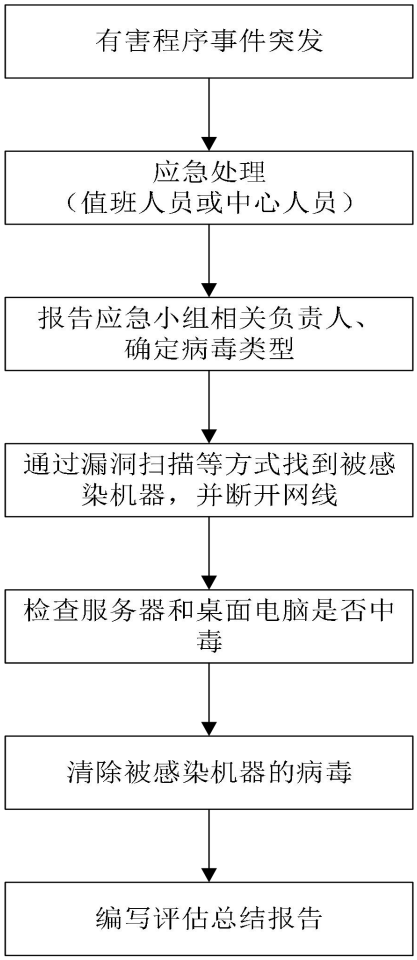


图 B.1 有害程序事件应急预案流程

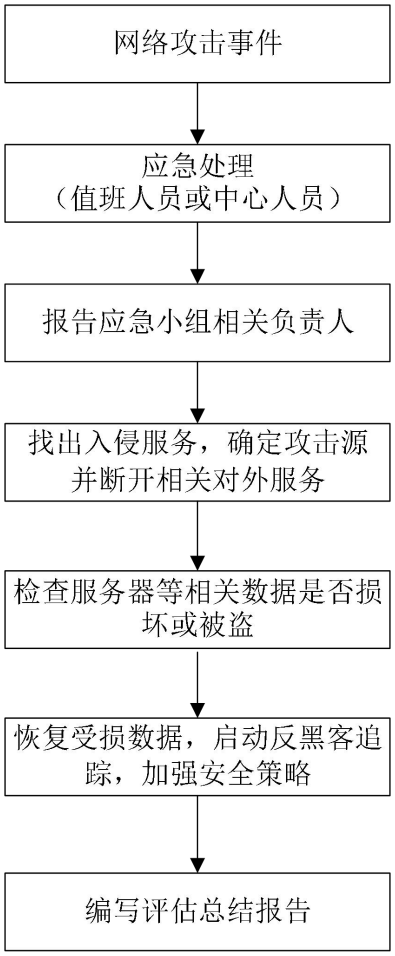
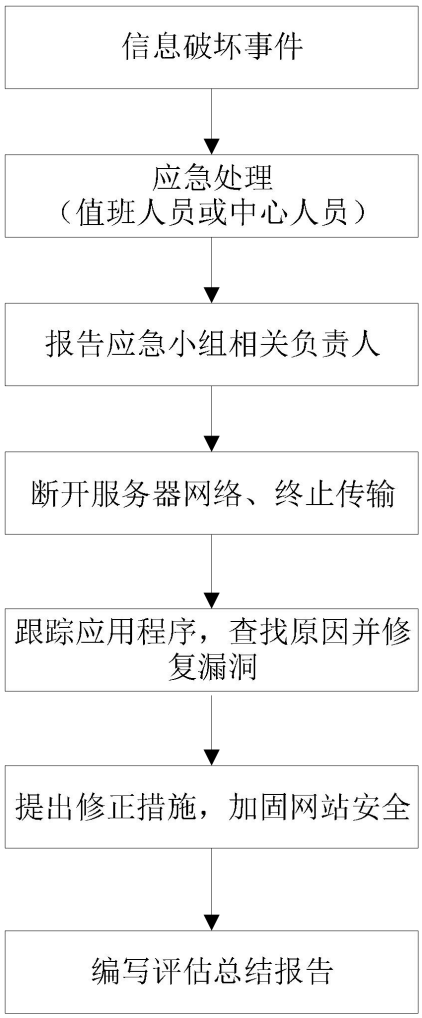
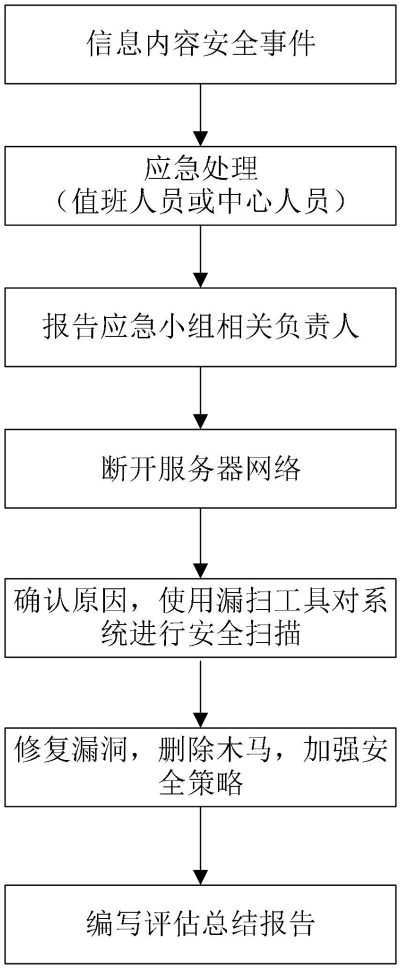


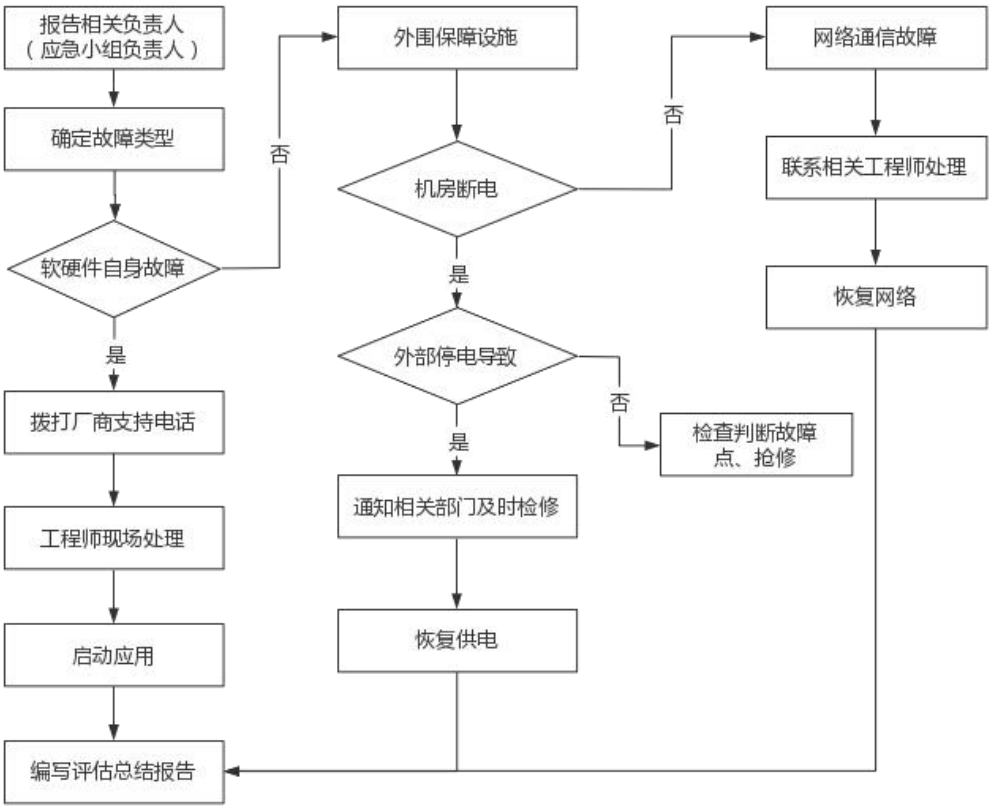
图 B.2 网络攻击事件应急预案流程



图B.3 信息破坏事件应急预案流程



图B.4 信息内容安全事件应急预案程



附图B.5 设备设施故障事件预案流程

本标准用词说明

1. 为便于在执行本标准条文时区别对待,对要求严格程度不同的用词说明如下：

表示很严格，非这样做不可的用词：

正面词采用“必须”，反面词采用“严禁”；

表示严格，在正常情况均应这样做的用词：

正面词采用“应”，反面词采用“不应”或“不得”；

表示允许稍有选择，在条件许可时首先应这样做的用词：

正面词采用“宜”，反面词采用“不宜”；

表示有选择，在一定条件下可以这样做的用词，采用“可”。

2. 条文中指明应按其他有关标准或规范执行的写法为：“应符合……的规定”或“应按……执行”。

引用标准名录

1 《信息安全技术 信息系统灾难恢复规范》GB/T 20988

2 《信息技术 服务管理 第 1 部分：规范》GB/T 24405.1

3 《信息技术服务 运行维护 第 1 部分：通用要求》GB/T28827.1

4 《信息技术服务 运行维护 第 2 部分：交付规范》GB/T 28827.2

5 《信息技术服务 运行维护 第 3 部分：应急响应规范》GB/T 28827.3

6 《信息技术 安全技术 信息安全管理实用规则》GB/T 22081-2008