

JR

中华人民共和国金融行业标准

JR/T 0265—2023

金融数据中心能力建设指引

Guidelines for financial data center capacity building

2023 - 07 - 25 发布

2023 - 07 - 25 实施

中国人民银行 发布

目 次

前言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 总则	2
6 数据中心治理	3
7 场地环境	8
8 网络通信	13
9 运行管理	16
10 风险管控	17
参考文献	20

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国人民银行科技司提出。

本文件由全国金融标准化技术委员会（SAC/TC 180）归口。

金融数据中心能力建设指引

1 范围

本文件规定了金融数据中心治理、场地环境、网络通信、运行管理和风险管控的能力要求。
本文件适用于金融数据中心建设与管理。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

- GB 50116 火灾自动报警系统设计规范
- GB 50140 建筑灭火器配置设计规范
- GB 50174 数据中心设计规范
- GB 50222 建筑内部装修设计防火规范
- GB 50223 建筑工程抗震设防分类标准
- GB 50370 气体灭火系统设计规范
- GB 50462 数据中心基础设施施工及验收规范
- GB 50981 建筑机电工程抗震设计规范
- GB/T 33136 信息技术服务 数据中心服务能力成熟度模型
- JGJ 339 非结构构件抗震设计规范
- JR/T 0071.2 金融行业网络安全等级保护实施指引 第2部分：基本要求
- JR/T 0166 云计算技术金融应用规范 技术架构
- JR/T 0167 云计算技术金融应用规范 安全技术要求
- JR/T 0168 云计算技术金融应用规范 容灾
- ISO/IEC 20000-2 信息技术 服务管理 第2部分：服务管理体系应用指南（Information technology—Service management—Part 2: Guidance on the application of service management systems）

3 术语和定义

下列术语和定义适用于本文件。

3.1

数据中心 data center

由计算机场地（机房）、机房基础设施、信息系统硬件（物理和虚拟资源）、信息系统软件、信息资源（数据）和人员以及相应的规章制度组成的组织。

[来源：GB/T 33136，3.1.1，有修改]

3.2

金融数据中心 financial data center

支持金融服务的数据中心。

3.3

治理域 governance domain

按照特定层次、功能划分的治理范围。

[来源：GB/T 34960.1, 3.4, 有修改]

3.4

建筑机电工程设施 building mechanical and electrical equipment engineering facilities

建筑中为建筑使用功能服务的附属机械、电气构件、部件和系统等。

[来源：GB 50981, 2.1.4, 有修改]

4 缩略语

下列缩略语适用于本文件。

ACL: 访问控制列表 (Access Control List)

CPU: 中央处理器 (Central Processing Unit)

IOPS: 每秒进行读写操作的次数 (Input/Output Operations Per Second)

IP: 互联网协议 (Internet Protocol)

IPv6: 互联网协议第6版 (Internet Protocol Version 6)

PDU: 电源分配单元 (Power Distribution Unit)

PCIe: 高速串行计算机扩展总线 (Peripheral Component Interconnect express)

RADIUS: 用户远程拨入认证服务 (Remote Authentication Dial In User Service)

UPS: 不间断电源系统 (Uninterruptible Power System)

VLAN: 虚拟局域网 (Virtual Local Area Network)

5 总则

5.1 概述

本文件以描述金融数据中心的治理域内容为基础,从金融数据中心建设、运营及安全保障的角度出发,逐一描述场地环境、网络通信、运行管理和风险管控等能力域的具体管理要求,金融数据中心能力域具体架构见图1。承载金融云的数据中心建设在满足本文件要求的基础上,也应满足JR/T 0166、JR/T 0167和JR/T 0168等系列标准的相关要求。

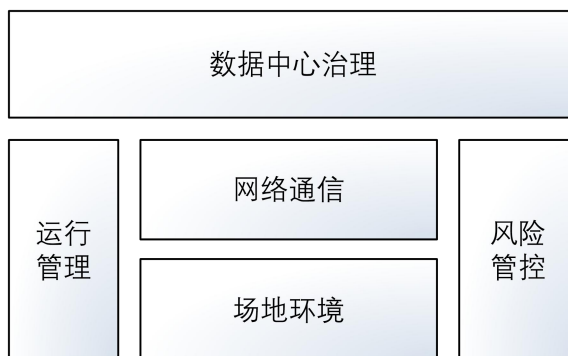


图1 金融数据中心能力域架构图

5.2 要求

金融数据中心能力建设的要求分为基本要求和增强要求。基本要求是在满足相关国家标准要求的前提下,根据金融行业的特性所提出的适应性要求;增强要求是为鼓励金融数据中心进一步提升安全稳定运行能力,在新技术应用、低碳环保、节能增效、业务连续性等方面提出的要求。

5.3 基本原则

金融数据中心能力建设在规划、建设、运行过程中的基本原则如下。

- a) 统一规划，安全可靠。各类金融机构在各级数据中心的生命周期内开展相关工作的能力建设，在提升金融机构自身管理水平的同时，提高金融数据中心的安全可靠性。
- b) 技术先进，平稳运行。汲取国际、国家相关标准经验，打造金融行业领域的特色标准，保障金融数据中心在全生命周期内质量可控、稳定运行。
- c) 经济适用，节能环保。根据金融机构自身情况和对数据中心的使用需求，合理控制各级数据中心的建设及运行成本，并努力达到节能环保的目标。

6 数据中心治理

6.1 概述

数据中心治理是金融数据中心能力建设的必要组成部分，其框架应包括治理的实施过程和治理域，金融数据中心治理框架见图2。金融数据中心组织应按照治理的实施过程，以治理域为对象，开展数据中心治理，应明确场地环境、网络通信等基础设施的管理要求，建立基础设施建设、采购、实施和运维机制，制定基础设施管理策略和方法，评估、指导、监督和改进基础设施相关的管理机制和服务能力。

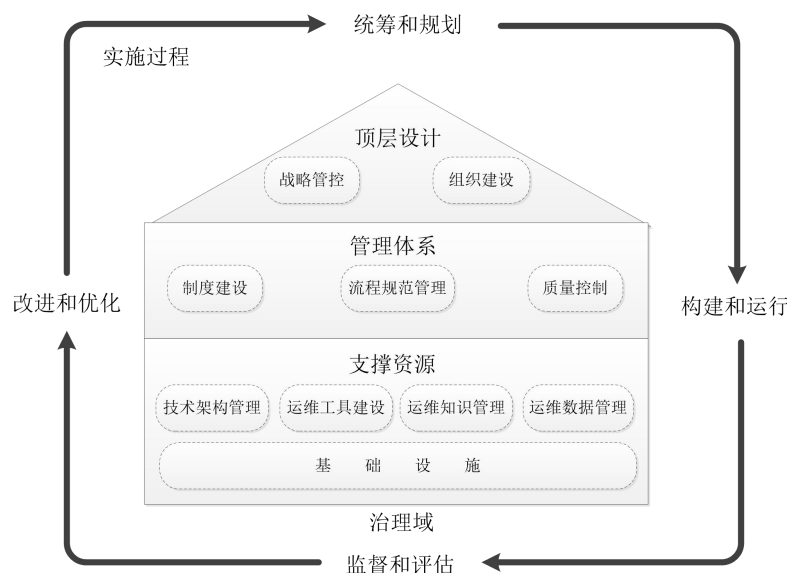


图2 金融数据中心治理框架

6.2 战略管控

6.2.1 战略规划

金融数据中心战略规划的基本要求包括以下内容。

- a) 应包括愿景陈述、规划范围、现状分析、战略相关方、发展规划、职责分工及风险分析等内容。
- b) 应结合行业管理要求、业务发展规划、金融科技发展趋势等，开展战略需求评估。
- c) 应识别金融数据中心战略的相关方，战略应与相关方达成一致。
- d) 应对当前和未来面临的内外部形势及技术发展趋势进行分析研究，体现创新理念。
- e) 当内外部环境发生重大变化时，应对战略规划进行评估，根据评估结果改进战略。

金融数据中心战略规划的增强要求包括以下内容。

- a) 宜规划战略执行评估及考核机制。
- b) 宜形成金融数据中心战略文档并经审批后正式发布，带动形成良好的组织文化。

6.2.2 战略实施

金融数据中心战略实施的基本要求包括以下内容。

- a) 应落实金融数据中心战略实施过程中的组织、资源、工具等保障措施。

- b) 应根据战略规划及业务目标，明确职责分工，做好工作任务的分解和阶段性工作计划的制定。
- c) 应持续监督战略实施状态，定期回顾总结并结合战略实施目标及时调整实施策略。

金融数据中心战略实施的增强要求包括宜对战略实施工作任务充分评估分析，包括成本分析、时间进度分析、风险分析、投入与收益分析等，依据分析结果确定任务优先级并合理配置资源。

6.2.3 战略评估

金融数据中心战略评估的基本要求包括应定期对金融数据中心战略实施情况进行评估并根据评估结果持续优化，指导战略实施工作的有效开展。评估内容应涵盖目标达成程度、实施效果、与规划的偏差分析等方面。

金融数据中心战略评估的增强要求包括以下内容。

- a) 宜针对金融数据中心战略实施建立系统完整的评估准则，明确评估方法。
- b) 宜采取量化分析、统计等方法，从成本、效益、时间、风险等角度对整体战略实施情况开展成本效益评估并根据评估结果及内外部环境变化，对中长期战略规划进行调整。

6.3 组织建设

6.3.1 组织架构

金融数据中心组织架构的基本要求包括以下内容。

- a) 应明确金融数据中心组织架构中各机构（部门）的职能、岗位和职责，确保责任、权利的一致。
- b) 应监督和评估组织架构中各机构（部门）的组织能力和运行绩效，并持续改进。

金融数据中心组织架构的增强要求包括宜根据发展战略目标、组织架构现状和内外部环境变化，对职能、岗位和职责等进行调整和优化。

6.3.2 人力资源管理

金融数据中心人力资源管理的基本要求包括以下内容。

- a) 应配备符合金融数据中心运行和发展需要的人员。
- b) 特定岗位专业技术人员应根据行业管理要求具备相应岗位执业资格证书或专业技术证书。
- c) 应根据岗位能力要求对人员实施培训和经验分享，不断提高金融数据中心人员能力。

金融数据中心人力资源管理的增强要求包括以下内容。

- a) 宜制定适合金融数据中心发展要求的人力资源战略规划，制定并执行人员职业发展规划。
- b) 宜建立覆盖管理、技术、安全、运营等方面的团队，建立绩效考核机制和薪酬福利管理体系。
- c) 宜建立人力资源风险管控机制，识别人员管理中的风险，采取适当措施预防风险发生，包括对涉密及敏感岗位加强风险监测、关键岗位实行备岗制、规范人员离岗（职）交接流程等。

6.3.3 组织文化管理

金融数据中心组织文化管理的基本要求包括以下内容。

- a) 应结合内外部环境及金融数据中心愿景与战略，明确组织文化建设的发展方向和期望目标。
- b) 应对组织文化建设效果进行回顾并持续改进，对组织文化建设提供必要的支持。

金融数据中心组织文化管理的增强要求包括宜构建系统的组织文化理念体系和行为规范体系，并进行内外部宣传和培训。

6.4 制度建设

6.4.1 制度体系规划

金融数据中心制度体系规划的3个层次包括以下内容。

- a) 基本制度与政策类：依据行政法规、行业主管部门规章所作的原则性、导向性、框架性的规范性文件。
- b) 管理办法与规定类：根据基本制度与政策，对管理职责、方法、流程等方面提出要求的制度。
- c) 操作规范与实施细则类：为落实管理办法与规定中的各项管理要求，所制定的详细说明、工具手册、操作模板、参考标准等。

金融数据中心制度体系规划的基本要求包括制度体系应覆盖场地环境管理、网络通信管理、运行管理、风险管控等领域。

6.4.2 制度制定

金融数据中心制度制定的基本要求包括以下内容。

- a) 应符合国家和行业主管部门的要求，保证制度的规范性和严肃性，并根据业务发展和金融数据中心的需要，制定、修订或废止相关制度。
- b) 应从金融数据中心建设实际出发，确保制度的前瞻性和可操作性。

6.4.3 制度实施

金融数据中心制度实施的基本要求包括以下内容。

- a) 应严格遵守审批制度、履行审批流程，审批完毕后予以发布实施。
- b) 应组织开展管理制度相关培训和宣传并检查管理制度的执行情况。

6.4.4 制度评估

金融数据中心制度评估的基本要求包括应结合内外部环境、合规要求、管理需要、实施情况等，对制度进行评估并持续修订，保障制度有效性。

金融数据中心制度评估的增强要求包括制度归口管理部门宜对其归口管理的制度进行定期评估，根据评估结论拟定相应制度的修订、废止或制定新制度的计划，以实现制度的持续优化。

6.5 流程规范管理

6.5.1 流程规范规划

金融数据中心流程规范规划的基本要求包括应结合实际情况，建立风险管理、信息安全管理、业务连续性管理、事件管理、问题管理、变更管理等流程规范，落实生产管理要求并在实践运行中及时优化调整。

金融数据中心流程规范规划的增强要求包括以下内容。

- a) 宜逐步建立服务目录，开展所辖资源的台账化管理。
- b) 宜建立服务请求管理、服务级别管理、配置管理、供应商管理、知识管理、创新管理等流程规范。

6.5.2 流程规范制定

金融数据中心流程规范制定的基本要求包括以下内容。

- a) 应明确组织架构、责任分工、执行管理、监督管理、持续改进等内容。
- b) 应包括各环节主要活动，形成可持续改进的管理闭环。

金融数据中心流程规范制定的增强要求包括宜设置衡量执行情况的管理指标，绘制流程图以辅助描述流程规范的主要活动。

6.5.3 流程规范实施

金融数据中心流程规范实施的基本要求包括以下内容。

- a) 应严格遵守审批制度、履行审批流程，审批完毕后予以发布实施。
- b) 应开展流程规范相关培训和宣传并评估各流程规范执行情况。

金融数据中心流程规范实施的增强要求包括以下内容。

- a) 宜建设电子化流程平台，辅助流程规范管理工作。
- b) 宜建立合适的监控、预测、优化调整等管理过程，回溯流程规范执行情况。

6.5.4 流程规范评估

金融数据中心流程规范评估的基本要求包括应结合内外部环境、合规要求、管理需要、实施情况等，对流程规范进行评估并持续修订，以保障流程规范的有效性。有内审、外审或权威机构验收检查机制的，可直接参考评审、验收结果进行评估。

金融数据中心流程规范评估的增强要求包括以下内容。

- a) 流程规范管理部门宜对其归口管理的流程规范进行定期评估, 并根据评估结果拟定流程规范的修订、废止或新流程规范的制定计划, 以实现流程规范的持续优化。
- b) 宜以达成业务目标、驱动业务创新、形成业务价值为导向, 进行定性与定量评估。

6.6 质量控制

6.6.1 质量目标制定

金融数据中心质量目标制定的基本要求包括应依据战略发展规划、服务水平要求, 科学合理制定质量控制目标。

6.6.2 质量监测检查

金融数据中心质量监测检查的基本要求包括应制定合理的监测检查频率, 分析和评估监测检查的结果并识别改进项。

金融数据中心质量监测检查的增强要求包括以下内容。

- a) 宜设置金融数据中心质量管理相关岗位并明确工作职责。
- b) 宜采用实时观测、测量、分析和评估方法并保留适当的文件信息作为结果证据。

6.6.3 持续改进

金融数据中心持续改进的基本要求包括以下内容。

- a) 应制定质量控制体系持续改进策略, 包括改进对象、目标及进度要求等, 开展改进策略回顾分析, 采取有效措施, 控制和维持改进对象的改进效果。
- b) 应明确改进目标, 设置优先级, 制定并实施改进计划。

6.7 技术架构管理

6.7.1 预研与引入

金融数据中心技术架构管理对象包括机房基础设施、IT(信息技术)基础设施建设与运维中所采用的核心技术路线及架构。金融数据中心技术架构预研与引入的基本要求包括应根据业务需求、行业管理要求、战略规划及发展趋势, 对新技术进行预研, 以评估其对金融数据中心的适用性和预期收益, 并制定技术架构引入策略。

金融数据中心技术架构预研与引入的增强要求包括宜针对计划引入的技术架构, 编写引入方案, 开展技术测试或行业应用调研, 根据测试结果或调研分析报告制定应用方案。

6.7.2 应用与推广

金融数据中心技术架构应用与推广的基本要求包括应根据引入策略, 在指定范围内应用并适时推广。

金融数据中心技术架构应用与推广的增强要求包括宜及时总结应用过程和结果, 制定技术规范。

6.7.3 运行与优化

金融数据中心技术架构运行与优化的基本要求包括应监测技术架构运行和发展情况并进行客观评估, 根据需要适时对技术架构进行优化更新。

6.8 运维工具建设

6.8.1 运维工具规划

金融数据中心运维工具包括监控工具、流程管理工具、自动化操作工具、配置管理工具、数据分析工具等在建设及运营过程中所使用的用于提升质量及效率的专用工具, 工具的形式可为脚本、系统、平台等。金融数据中心运维工具规划的基本要求包括以下内容。

- a) 应根据技术架构和组织架构, 针对性规划运维工具种类、技术路线和应用角色。
- b) 应结合内部运维需求和行业管理要求。
- c) 应评估运维工具可能对生产系统性能产生的影响。

金融数据中心运维工具规划的增强要求包括以下内容。

- a) 宜把握关键核心技术, 优先采用当前主流且具前瞻性的建设思路和技术路线。

- b) 宜考虑各种运维工具的适用范围，采取顶层设计，分领域、分阶段统筹短期、中期、长期的建设计划。
- c) 宜采用一体化、平台化设计。

6.8.2 运维工具研发

金融数据中心运维工具研发的基本要求包括应根据任务的复杂程度采用工程或项目的形式进行，具备监督和控制机制。

金融数据中心运维工具研发的增强要求包括一线运维人员宜主动从需求、开发、测试等环节参与研发任务，配套制度宜与研发同步编制。

6.8.3 运维工具应用推广

金融数据中心运维工具应用推广的基本要求包括以下内容。

- a) 应根据运维工具的适用范围，统一进行宣传和培训，包括功能、预期的效果和注意事项等内容。
- b) 应组织用户对运维工具的功能、性能、适宜性等进行评价与反馈。

金融数据中心运维工具应用推广的增强要求包括配套制度与运维工具宜同步试运行或同步发布，建设经验宜总结成知识成果并推广。

6.9 运维知识管理

6.9.1 运维知识管理策略确定

金融数据中心运维知识包括在建设及运营过程中经过积累、梳理、总结并被验证的信息或数据。金融数据中心运维知识管理策略确定的增强要求包括以下内容。

- a) 宜基于运维知识管理范围维护知识分类。敏感信息不宜作为知识发布。
- b) 宜按照管理制度、流程规范、操作手册、经验总结等维度对运维知识进行分类。
- c) 宜根据运维知识管理现状、需求和提升计划，制定运维知识管理的策略和原则，建立相应的激励机制。

6.9.2 运维知识创建与维护

金融数据中心运维知识创建与维护的增强要求包括宜基于运维知识分类，识别和创建运维知识，定期验证和持续更新。失效运维知识宜废止并根据需要归档。

6.9.3 运维知识使用

金融数据中心运维知识使用的增强要求包括以下内容。

- a) 宜开展运维知识使用情况分析，组织运维知识培训和考核。
- b) 宜建设信息化运维知识管理工具，实现运维知识自动归类、运维知识推荐等智能化功能。

6.10 运维数据管理

6.10.1 运维数据规范

金融数据中心运维数据包括监控数据、日志数据、流程管理数据和配置管理数据等在建设及运营过程中产生的相关数据。金融数据中心运维数据规范的基本要求包括以下内容。

- a) 应明确运维数据的纳入管理范围，建立运维数据采集、存储、加工和使用等基本管理机制。
- b) 应通过策略、流程和技术，对运维数据进行安全管理。

金融数据中心运维数据规范的增强要求包括以下内容。

- a) 宜制定明确的运维数据管理目标，建立数据权责机制，明确各类运维数据管理的优先级和质量要求。
- b) 宜定义和发布统一的运维数据标准，明确运维数据标准的管理部门和管理规则。

6.10.2 运维数据平台建设

金融数据中心运维数据平台建设的增强要求包括以下内容。

- a) 宜采取“场景驱动、以用促建”的策略分步建设。

- b) 宜采用分层架构设计，包括数据接入、数据存储、数据处理、数据应用等层级。
- c) 宜将运维数据平台建设纳入运维工具建设总体规划。

6.10.3 运维数据应用

金融数据中心运维数据应用的基本要求包括以下内容。

- a) 应进行宣传培训，培养运维数据应用意识，提升应用能力。
- b) 应选择适合的应用场景，安全合规提取相关的运维数据，进行数据统计与分析。

金融数据中心运维数据应用的增强要求包括应用场景宜包括运维数据服务、数据审计、智能运维、辅助业务运营等。

7 场地环境

7.1 概述

GB 50174将数据中心划分为A、B、C三级。在此基础上，本文件结合行业特点对不同等级的金融数据中心在场地环境方面提出以下适应性要求。

注：本文件中符合GB 50174 A级的金融数据中心简称A级金融数据中心，符合GB 50174 B级的金融数据中心简称B级金融数据中心，符合GB 50174 C级的金融数据中心简称C级金融数据中心。

7.2 规划及布局

7.2.1 规划选址

金融数据中心规划选址的基本要求符合GB 50174中选址的相关内容基础上，还应包括以下内容。

- a) 金融数据中心规划时应考虑多种条件和因素，包括容量、预算、升级要求、可用性级别、效率等；应在综合考量后根据建设需求，分析自然条件、电力条件、能耗指标、网络条件等因素，确定金融数据中心建设技术路线。
- b) 金融数据中心选址时应进行全面的风险评估，综合考虑地理位置、自然环境、资源配套、政策配套、成本效益及人力资源等各种因素对数据中心安全运营的影响，规避选址不当风险。
- c) 新建的A级金融数据中心、B级金融数据中心首层建筑完成面，应高出当地洪水百年重现期水位线1.0米以上，且高出室外地坪最少0.6米。同时应整体考虑园区和建筑物的排水措施，确保各类设施能够避免潮湿、水浸、淹没等情况影响其正常运行。

金融数据中心规划选址的增强要求包括以下内容。

- a) A级金融数据中心、B级金融数据中心不宜建在公共停车库的正上方。
- b) 同城灾备中心与生产数据中心直线距离宜大于10千米。异地灾备中心与生产数据中心不在同一个江河流域、地震带、台风等自然灾害隐患区，且直线距离宜大于300千米。

7.2.2 园区建筑布局

金融数据中心园区建筑布局的基本要求包括以下内容。

- a) 金融数据中心园区的总体布局应紧凑、合理并充分利用原有条件。
- b) 当金融数据中心与其他功能区域合用同一建筑时，金融数据中心的各个功能房间应集中布置，并且应综合考虑各种室外设备的位置。

金融数据中心园区建筑布局的增强要求包括以下内容。

- a) 园区内机房、办公、动力等建筑宜作为单体独立设置，宜进行合理连接。
- b) 建筑、设备布局宜有利于形成场地内良好的自然风环境并借助新技术及工具搭建数字仿真模型进行模拟分析，宜利用主导风向以便专用空调室外机等设备散热。

7.2.3 功能分区设置

金融数据中心功能分区设置的基本要求符合GB 50174中设备布置的相关内容基础上，还应包括以下内容。

- a) A级金融数据中心支持区的变配电室应单独设置。
- b) A级金融数据中心、B级金融数据中心支持区的发电机室应单独设置。
- c) A级金融数据中心、B级金融数据中心支持区的不间断电源系统室、电池室应物理划分。

金融数据中心功能分区设置的增强要求包括以下内容。

- a) A级金融数据中心、B级金融数据中心辅助区的消防安防控制室及行政管理区宜单独设置。
- b) A级金融数据中心支持区的空调室、辅助区的进线间宜物理划分。
- c) B级金融数据中心支持区的空调室、辅助区的进线间宜逻辑划分。

注：1. 支持区和辅助区未列出区块设置不做要求。

2. “单独设置”指功能空间物理上单独设立，不要求金融机构独立使用。

3. “逻辑划分”指在同一功能空间中，规划相对集中的不同使用区域，区域之间没有严格的物理分割标志。

4. “物理划分”指在同一功能空间中，规划相对集中的不同使用区域，区域之间有严格的物理分割标志。

7.3 基础环境

金融数据中心基础环境的基本要求应符合GB 50174中温度、露点温度、相对湿度、空气粒子浓度、噪声、电磁干扰、振动及静电等相关内容。

7.4 建筑结构与装饰装修

7.4.1 数据中心建筑设计

金融数据中心建筑设计的基本要求应符合GB 50174中建筑与结构的相关内容基础上，还应包括以下内容。

- a) 主体结构应具备耐火、抗震、防火、防止不均匀沉降等性能。变形缝不应穿过变配电室、不间断电源系统室及电池室等重要用房，避免对重要用房的环境条件产生影响和安全隐患。
- b) 运输通道设计应注意通道所运输设备类型的要求，特别是柴油发电机、变压器、水冷机组等大型设备的运输要求。运输通道应满足分期建设及故障维修时的运输要求，宽度应满足设备搬运条件并应满足当地消防要求。
- c) 对于UPS、电池、空调等重量较大的大型设备，应安装设备承重设施。

金融数据中心建筑设计布局的增强要求包括以下内容。

- a) 为便于IT设备的布置、后期维护及调整扩展，扩大操作人员、监控设备运行管理视野，主体结构宜采用大开间大跨度的柱网。
- b) 为便于机房再改造时灵活拆卸、移装，分室宜采用轻钢龙骨隔断。

7.4.2 数据中心结构设计

金融数据中心结构设计的基本要求应符合GB 50174中建筑与结构的相关内容基础上，还应包括以下内容。

- a) 金融数据中心结构荷载应包括地面荷载和吊挂荷载。地面荷载应视IT设备、变配电及动力设备的重量和受力面积确定，吊挂荷载应由吊挂载重量决定。金融数据中心荷载设计应考虑重型设备运输通道的地面荷载，应重点考虑大型设备的承重，尽量把重型设备放置在机房的承重梁上。
- b) A级金融数据中心抗震设防类别不应低于GB 50223关于乙类的相关要求，B级金融数据中心、C级金融数据中心抗震设防类别不应低于GB 50223关于丙类的相关要求。

金融数据中心结构设计的增强要求包括以下内容。

- a) 新建机房的主机房梁下净空高度应根据机柜高度、管线安装、通风及消防要求确定。主机房采用上走线时不宜小于3.2米。
- b) 大型机电设备（例如大功率柴油发电机、大功率水冷冷冻机组）间所在层梁下净空高度不宜小于6米。
- c) 气体灭火防护区围护结构承受内压不宜低于1200帕。

7.4.3 数据中心装修装饰要求

7.4.3.1 室内装修

金融数据中心室内装修的基本要求应符合GB 50174中室内装修的相关内容基础上，还应包括以下内容。

- a) 机房室内装修选用材料的燃烧性能应符合GB 50222的有关规定，机房顶棚和墙面装修材料的燃烧性能应达到GB 50222关于A级的相关要求。

- b) 应使用能节省自然资源的产品，避免产生有害物质或其他废物的排放，不应采用国家和地方限制使用的建筑材料及制品。

金融数据中心室内装修的增强要求包括以下内容。

- a) 宜采用可再利用建筑材料和可循环建筑材料。
- b) 宜考虑就近选材。
- c) 对于制造设备以及安装工程中所采用的各种材料，宜通过各种技术措施，防止二次污染。

7.4.3.2 非结构构件抗震

金融数据中心非结构构件抗震的基本要求包括气体灭火、给排水管线、排风风道、风机、水泵、发电机、变压器、蓄电池及承载架、配电柜、开关柜、UPS、空调等建筑机电工程设施应符合 GB 50981 和 JGJ 339 中非结构构件抗震相关内容。设计安装抗震支吊架、限位器、减隔震装置、伸缩节装置以增强抗震性能，降低地震情况下建筑机电工程设施功能失效的风险。

7.4.4 人流、物流及出入口

金融数据中心人流、物流及出入口的基本要求应符合 GB 50174 中人流、物流及出入口的相关内容。

7.4.5 围护结构热工设计和节能措施

金融数据中心围护结构热工设计和节能措施的基本要求应符合 GB 50174 中围护结构热工设计和节能措施的相关内容基础上，还应包括以下内容。

- a) 当主机房与外围护结构相邻时，对应部分外围护结构的热工性能应根据全年动态能耗分析情况确定最优值。
- b) 新建机房时应考虑电能利用效率（PUE）、水利用效率（WUE）等设计指标。

7.5 电气

7.5.1 供配电

7.5.1.1 设计架构

金融数据中心供配电设计架构的基本要求应符合 GB 50174 中供配电的相关内容基础上，还应包括以下内容。

- a) 供配电系统的设计方案应按各级金融数据中心的用电负荷等级、供电系统可靠性要求、近期和中远期供电容量需求及金融类用户的其他特殊使用要求确定。
- b) 照明插座用电、空调用电、动力用电、特殊用电等应根据其功能分回路供电。

7.5.1.2 供电电源

金融数据中心供电电源的基本要求包括 A 级金融数据中心、B 级金融数据中心应由双重电源供电并应设置备用电源，其中 A 级金融数据中心双重电源还应来自 2 个不同的变电站。

金融数据中心供电电源的增强要求包括 B 级金融数据中心双重电源宜来自 2 个不同的变电站。

7.5.1.3 备用电源

金融数据中心备用电源的基本要求应符合 GB 50174 中供配电的相关内容基础上，还应包括以下内容。

- a) 柴油在储存期间内，应定期对柴油品质进行检测，当柴油品质不能满足使用要求时，应对柴油进行更换和补充。
- b) A 级金融数据中心、B 级金融数据中心柴油发电机启动电池应冗余备份。
- c) C 级金融数据中心，当只有 1 路电源时，应设置柴油发电机组作为备用电源。

金融数据中心备用电源的增强要求包括以下内容。

- a) 大型金融数据中心发电机系统宜采用 10 千伏特等级发电机。

注：大型金融数据中心指以功率为 2.5kW 为一个标准机架，规模在 3000 个标准机架或总功率在 7500kW 及以上的数据中心。

- b) 当柴油发电机不能满足冗余时，宜设置外部电源应急接口。

7.5.1.4 不间断电源系统

金融数据中心不间断电源系统的基本要求应符合 GB 50174 中供配电的相关内容基础上，还应包括以下内容。

- a) 金融数据中心电子信息设备应由UPS供电，且UPS应有自动和手动旁路装置。
- b) 金融数据中心UPS所用电池组应每组配置直流断路器，且应采取漏液防护措施。
- c) A级金融数据中心、B级金融数据中心应监控每节电池的电压、内阻、故障和温度，C级金融数据中心应监控每组电池的电压、故障。

金融数据中心不间断电源系统的增强要求包括动力监控宜采用独立 UPS 供电。当使用第三方外置监控模块监控 UPS 主机时，宜为其选择其他的 UPS 供电。

7.5.1.5 机柜配电

金融数据中心机柜配电的基本要求包括以下内容。

- a) A级金融数据中心、B级金融数据中心机房机柜内应配置2路PDU，且2路PDU应由来自不同的UPS供电。
- b) 配电设备应按意义明确、简单易记的规则“自上而下、自左而右”的顺序编号。
- c) 配电柜内的空气开关、指示灯、按钮、旋转开关、控制及指示元器件应附有规范、清晰、牢固、准确的标签。
- d) A级金融数据中心、B级金融数据中心的单电源设备应加装静态转换开关。
- e) 机房负载应综合考虑主备设备、应用类别、业务种类和电源三相平衡，使负载合理分配于各机柜。

7.5.2 照明、静电防护、防雷与接地

金融数据中心照明、静电防护、防雷与接地的基本要求应符合 GB 50174 中照明、防雷与接地的相关内容。

7.6 线缆部署

7.6.1 电力线缆

金融数据中心电力线缆的基本要求应符合GB 50174中供配电的相关内容基础上，还应包括以下内容。

- a) 应选择符合国家供配电标准要求的电力线缆并根据末端负载大小、敷设环境，针对不同的功能分区确定电力线缆的需求。
- b) 当电力线缆沿桥架敷设时，电力线缆在桥架横断面的填充率不应大于40%。
- c) 封闭式母线水平敷设时，除电气房间外，与地面的距离不应小于2.2米；垂直敷设时，母线与地面垂直距离1.8米以下部分应采取防止母线机械损伤措施。母线终端无引出线和引入线时，端头应封闭。

金融数据中心电力线缆的增强要求包括以下内容。

- a) 不同电源的电力电缆宜在大楼内通过不同的竖井进行敷设。
- b) 在使用封闭式母线时，宜预留母线插接箱，便于后期扩容。
- c) 直线敷设长度超过制造厂给定的数值时，宜设置伸缩节，母线槽的连接处不宜设置在穿过楼板或墙壁处。

7.6.2 弱电线缆

金融数据中心弱电线缆的基本要求应符合 GB 50174 中布线系统和 GB 50462 中综合布线及网络系统的一般规定、线缆敷设的相关内容基础上，还应包括以下内容。

- a) 弱电线缆布放前应核对规格、长度、路由、位置。
- b) 弱电线缆在桥架横断面的填充率不应大于 50%。

7.7 电磁屏蔽

金融数据中心电磁屏蔽的基本要求包括对涉及国家秘密或企业对商业信息有保密要求的金融数据中心，应设置电磁屏蔽室或采取其他电磁泄漏防护措施。

7.8 空气调节

7.8.1 总体设计

金融数据中心空气调节总体设计的基本要求应符合 GB 50174 中空气调节一般规定的相关内容基础上，还应包括数据中心与其他功能用房共建于同一建筑内时，应设置独立的空调系统。

7.8.2 负荷计算

金融数据中心空气调节负荷计算的基本要求应符合 GB 50174 中空气调节负荷计算的相关内容基础上，还应包括以下内容。

- a) 电力设备的散热量应按效率损失转换为热能计算，机房内维护人员的人体散热量和散湿量按轻作业标准计算。
- b) 空调系统的冷负荷还应包括空气通过风机、风管等温升引起的附加冷负荷及冷冻水通过水泵、管道等温升引起的附加冷负荷。

7.8.3 气流组织

金融数据中心空气调节气流组织的基本要求应符合 GB 50174 中气流组织的相关内容基础上，还应包括以下内容。

- a) 当主机房设置冷热通道隔离时，冷热通道之间应避免孔洞缝隙，孔洞缝隙处应采取减少冷热气流混合的封堵措施。
- b) 采用地板下送风的机房，架空地板和作为空调回风道的吊顶内布放管道线缆时，应避免管道、线缆阻碍气流。

7.8.4 空调系统设计

金融数据中心空调系统设计的基本要求应符合 GB 50174 中空调系统设计的相关内容基础上，还应包括以下内容。

- a) 设置多种制冷模式的冷冻水空调系统，各模式之间应具备自动切换的功能，模式切换时应保证系统平稳、安全。
- b) A级金融数据中心冷冻水空调系统应设置蓄冷设施，蓄冷时间应满足电子信息设备的运行要求。冷冻水供水管路应采用环形管网或双供双回方式。

金融数据中心空调系统设计的增强要求包括采用风冷空调机组的数据中心，在条件具备时宜采用节能型风冷空调。

7.8.5 空调设备

金融数据中心空调设备的基本要求应符合 GB 50174 中空调设备选择的相关内容基础上，还应包括以下内容。

- a) 设有空调的供电房间，空调设施的冗余应与电力系统的可靠性要求一致。
- b) 机房专用空调应有来电自启动功能，具备现场监控及远程监控能力，且可以通过控制器实现多台机组的高级群控工作模式，保证机房整体的最佳性能；非机房专用空调应能来电自启动，可以是空调自带的，也可以是外加模块实现的。
- c) 主机房内的湿度应由机房空调或其他加湿设备、除湿设备进行控制。
- d) 在严寒地区及寒冷地区，机房专用空调应采取具备低温启动功能的措施。

7.8.6 新风系统

金融数据中心新风系统的基本要求应符合 GB 50174 中空调系统设计的相关内容基础上，还应包括以下内容。

- a) 进风口应设在空气较清洁的位置。
- b) 进风口与排风口应避免进风短路、排风短路。
- c) 寒冷和严寒地区，进风口处应设置防冻保温措施。

金融数据中心新风系统的增强要求包括新风机宜有温湿度调节功能。

7.9 消防与安全

7.9.1 一般规定、防火与疏散、安全措施

金融数据中心消防与安全的一般规定、防火与疏散、安全措施的基本要求应符合GB 50174中消防与安全的一般规定、防火与疏散、安全措施相关内容。

7.9.2 火灾报警及控制

金融数据中心火灾报警及控制的基本要求应符合GB 50116中气体灭火系统、泡沫灭火系统的联动控制设计及GB 50174中消防设施的相关内容基础上，还应包括主机房应同时设置2组独立的火灾探测器，且分别为感烟探测器和感温探测器。

金融数据中心火灾报警及控制的增强要求包括A级金融数据中心、B级金融数据中心火灾报警及控制宜部署极早期空气采样等灵敏度较高的报警系统。

7.9.3 灭火设施

金融数据中心灭火设施的基本要求应符合GB 50140中灭火器配置、GB 50174中消防设施、GB 50370中系统设置的相关内容基础上，还应包括以下内容。

- a) 2个或2个以上的防护区采用组合分配系统时，1个组合分配系统所保护的防护区不应超过8个。
- b) 组合分配系统的灭火剂储存量应按储存量最大的防护区确定。
- c) 消防水系统选型时应考虑环境温度，设计及施工过程中应根据需要增加相应的防冻措施。

7.10 给水排水

7.10.1 管道敷设

金融数据中心给水排水管道敷设的基本要求应符合GB 50174中管道敷设的相关内容基础上，还应包括以下内容。

- a) 金融数据中心不应有穿过与机房、变配电室、不间断电源系统室及电池室、发电机室等房间内设备无关的给排水管道。
- b) 相关给排水管道不应布置在电气设备的正上方。
- c) 机房室外管道应采取保温或防冻等措施。
- d) 安装有自动喷水灭火系统、机房专用空调和加湿器的房间，应结合设备设施情况设置挡水和排水设施并设置漏水报警装置。
- e) 进入主机房的给水管道应在进入房间前增设手动阀门或电动阀门，以便紧急情况下切断水源。

7.10.2 补水储水

金融数据中心补水储水的基本要求应符合GB 50174中补水储水的相关内容基础上，还应包括以下内容。

- a) 冷冻水系统、冷却水系统及加湿系统的水质均应满足使用要求。
- b) A级金融数据中心、B级金融数据中心冷却水补水储水量应满足冷却水系统12小时补水量。当外部供水时间有保障时，水存储量满足用水时间仅需大于外部供水时间。

金融数据中心补水储水的增强要求包括当不影响蓄冷装置供应冷冻水的时间时，冷却水补水储存装置可与蓄冷装置一体考虑。

7.11 智能化系统

金融数据中心智能化系统的基本要求应符合GB 50174中智能化系统的一般规定、环境和设备监控系统、安全防范系统、总控中心等相关内容。

8 网络通信

8.1 网络架构

8.1.1 概述

金融数据中心网络应根据用户需求和科技发展状况进行规划和设计，包括数据中心内部网络和跨数据中心网络。

8.1.2 数据中心内部网络

金融数据中心内部网络的基本要求包括以下内容。

- a) 应进行合理的 IP 地址规划。
- b) 应采用高冗余、高可靠、低时延、可扩展的网络架构。
- c) 应根据应用属性、安全要求等划分不同网络功能分区。
- d) 网络区域之间应采取可靠的技术隔离手段，例如部署防火墙或者 ACL 等，实现访问控制；应避免将重要网络区域部署在边界处。
- e) 应部署网管系统，实时监控网络状态。

金融数据中心内部网络的增强要求包括以下内容。

- a) 宜提供网络故障的快速分析能力；宜提供可量化的网络健康度评估，主动感知网络状态。
- b) 宜提供基于业务的运维能力，例如业务路径可视、业务流量质量感知。
- c) 宜构建满足未来网络发展的新一代通信网络，例如软件定义网络。

8.1.3 跨数据中心网络

金融数据中心跨数据中心网络的基本要求包括以下内容。

- a) 应支持多运营商线路，实现可靠互联。
- b) 应合理规划路由协议和安全策略，实现网络通信的高效性和安全性。

金融数据中心跨数据中心网络的增强要求包括以下内容。

- a) 宜能够主动感知网络状态，提供网络故障的快速分析能力。
- b) 宜支持流量分析和出口流量优化，并支持基于线路质量的智能选路。
- c) 网络边界宜采用多层异构防火墙或网闸等进行安全防护。
- d) 宜采用先进技术，提升跨数据中心网络智能化水平。

8.2 线路资源

8.2.1 概述

线路资源作为金融数据中心跨数据中心网络互联互通的基础，在数据中心建设中有着重要的地位。

8.2.2 线路资源冗余

金融数据中心线路资源冗余的基本要求包括以下内容。

- a) 金融数据中心应至少接入2家线路运营商。
- b) 线路运营商提供的重要网络线路应全链路路由冗余，确保任一局点或任一光缆故障，不影响数据中心通信。
- c) 每家线路运营商应至少提供2条路由，接入线路运营商的2个局端；线路运营商应提供双路由保护功能，当其中一条路由由故障时，自动切换到另一条路由，双路由保护切换时间应小于50毫秒。
- d) 承载互相隔离的不同网络时，应使用独立的线路、使用传输设备的不同板卡。

金融数据中心线路资源冗余的增强要求包括以下内容。

- a) 每家线路运营商直接接入2条不同物理路径的通信管道；在园区内外，2条通信管道无交叉、无重叠，间距大于20米。
- b) 在园区内，线路运营商的2条路由宜分别接入不同的进线间。
- c) 线路运营商宜部署多台传输设备，并采用双电源供电；每台传输设备接入2条路由。
- d) 承载互相隔离的不同网络时，宜使用不同的传输设备。

8.2.3 线路资源质量

金融数据中心线路资源质量的基本要求包括以下内容。

- a) 线路资源的网络可用性应大于等于99.99%。
- b) 线路资源的传输时延应小于等于 $(0.5N+0.005G)$ 毫秒，每加入一跳卫星电路，需另增加传输时间300毫秒。

注：1. N是线路中含交换机和交叉连接设备的数量。

2. G是线路长度（单位：公里）。

- c) 线路丢包率应小于等于0.01%。

8.3 网络设备

8.3.1 概述

金融业数据中心网络设备包括路由器、交换机等，是实现网络通信的基础设备。

8.3.2 性能及容量

金融数据中心网络设备性能及容量的基本要求包括以下内容。

- a) 应通过交换容量、转发性能等指标衡量网络设备的性能及容量。
- b) 网络设备的性能及容量指标均应高于业务峰值要求。

8.3.3 可用性

金融数据中心网络设备可用性的基本要求包括以下内容。

- a) 应支持异构品牌之间的组网。
- b) 应支持 IPv6。
- c) 应支持端口镜像功能。

金融数据中心网络设备可用性的增强要求包括以下内容。

- a) 宜支持板卡和接口的热插拔功能。
- b) 交换机设备宜支持多虚一、一虚多技术。

8.3.4 可靠性

金融数据中心网络设备可靠性的基本要求包括以下内容。

- a) 应支持部件冗余设计。
- b) 应支持冗余连接，发生单点故障时不应降低业务连续性。

金融数据中心网络设备可靠性的增强要求包括宜支持端口模块在线隔离或更换。

8.3.5 可管理性

金融数据中心网络设备可管理性的基本要求包括以下内容。

- a) 应支持远程维护管理、健康状况检查、性能监控、异常状态告警，并通过统一接口进行管理。
- b) 应具备重要部件的故障指示装置（例如故障指示灯），能够标识故障部件及位置，便于网络设备日常运维。
- c) 应支持查看、导出、清理设备操作日志。
- d) 应支持接受统一的时钟授时。
- e) 应具备独立的带外管理接口。
- f) 应支持基于控制台（Console）、安全外壳协议（SSH）、远程登录协议（telnet）、简单网络管理协议（SNMP）等方式进行配置管理。

金融数据中心网络设备可管理性的增强要求包括在软件定义网络中，宜支持通过控制器实现网络设备的自动化部署。

8.3.6 可扩展性

金融数据中心网络设备可扩展性的基本要求包括以下内容。

- a) 应支持模块化扩展方式扩充接口类型及数量（接入层网络设备除外）。
- b) 交换机设备应支持级联或堆叠等扩展方式。

金融数据中心网络设备可扩展性的增强要求包括宜支持通过软件更新实现功能扩展。

8.3.7 安全性

金融数据中心网络设备安全性的基本要求包括以下内容。

- a) 应支持RADIUS认证、用户分级管理和口令保护。
- b) 应支持基于端口和基于VLAN的标准ACL和扩展ACL。
- c) 应支持关闭非加密的管理方式。
- d) 应支持敏感数据加密存储功能。

e) 应支持鉴别失败处理、会话空闲超时处理等安全审计功能。

金融数据中心网络设备安全性的增强要求包括以下内容。

- a) 宜支持多因子认证登陆方式。
- b) 宜支持流量控制、资源耗尽防护等安全防护功能。
- c) 宜支持安全启动机制，在设备启动时对网络设备引导固件、初始化加载程序等进行完整性校验。

9 运行管理

9.1 资产管理

9.1.1 需求管理

金融数据中心资产需求管理的基本要求包括以下内容。

- a) 应定期评估已有资产使用年限、性能和容量，预估现有资产承载能力，合理提出资产调整需求。
- b) 应定期统计新增、更新的资产信息。
- c) 应根据资产需求编制资产采购计划，提出采购需求和采购申请。

9.1.2 采购管理

金融数据中心资产采购管理的基本要求包括以下内容。

- a) 应履行必要的资产采购立项申请流程，应对所购资产完成必要的安全评估。
- b) 应遵循采购政策制度相关要求，配合采购机构或采购实施部门开展采购实施和信息公开工作。
- c) 应会同采购部门或项目管理部门等做好采购项目的验收工作，验收报告应当包括每一项技术、服务、安全标准的履约情况。
- d) 验收通过后，应进行资产登记。

9.1.3 使用管理

金融数据中心资产使用管理的基本要求包括以下内容。

- a) 领用时应履行领用手续，保留必要的记录。
- b) 应指定专人负责资产管理，及时更新资产信息。
- c) 应建立资产台账并定期清点，做到账实相符。

9.1.4 报废管理

金融数据中心资产报废管理的基本要求包括以下内容。

- a) 应履行报废手续，保留必要的记录。记录内容包括资产名称、型号、数量等。
- b) 对于存储有敏感信息的资产报废前，应按照保密管理相关办法拆除其存储介质，并对存储介质进行消磁或物理销毁处理，确保原设备上信息具有不可恢复性。

金融数据中心资产报废管理的增强要求包括存储敏感信息的设备销毁时，宜专人在场监督销毁过程。

9.2 例行管理

9.2.1 监控管理

金融数据中心监控管理的基本要求应符合GB/T 33136、JR/T 0071.2中监控管理的相关内容基础上，还应包括监控范围涵盖金融数据中心建设涉及的场地环境、网络通信、IT设备等运行状态信息。

金融数据中心监控管理的增强要求包括以下内容。

- a) 宜对监控指标进行趋势分析并预警。
- b) 宜对多个监控指标进行关联分析，在指标达到阈值后发出告警。
- c) 宜对相似告警进行合并、过滤。
- d) 宜采用射频识别等物联网技术对进出数据中心的资产进行管理。

9.2.2 值班管理

金融数据中心值班管理的基本要求应符合GB/T 33136、JR/T 0071.2中值班管理的相关内容。

金融数据中心值班管理的增强要求包括宜配备专职人员负责数据中心日常值守,并指定专人负责值班工作的统一组织和协调。

9.2.3 作业管理

金融数据中心作业管理的基本要求应符合GB/T 33136中作业管理的相关内容。

金融数据中心作业管理的增强要求包括宜通过自动化平台完成定时和按需发起作业的调度,减少人工操作风险;作业执行出错时宜发出异常通知,并规定作业异常处理流程。

9.3 容量管理

金融数据中心容量管理的基本要求应符合GB/T 33136中容量管理的相关内容基础上,还应包括容量管理范围涵盖金融数据中心建设涉及的场地环境、网络通信、IT设备等。

金融数据中心容量管理的增强要求包括宜在投产前开展性能测试,有效评估当前容量上限;宜在投产后开展容量实时监控,掌握数据中心的性能和容量情况以及变化趋势,并及时开展优化调整;宜对特殊时期的容量进行重点监控。

9.4 事件管理

事件管理的目标是快速恢复受影响的业务或服务,将负面影响降到最低,进而确保能够保持服务质量与可用性级别。事件管理的主要活动包括事件记录、分类分级、事件升级、解决恢复、事件关闭。

金融数据中心事件管理的基本要求应符合GB/T 33136、ISO/IEC 20000-2、JR/T 0071.2中事件管理的相关内容基础上,还应包括对暂时无法查明原因的事件采取应急措施,并将事件转为问题管理流程进行处理。

金融数据中心事件管理的增强要求包括宜建立事件管理定期回顾和持续优化机制,定期对事件流程规则进行回顾更新,包括但不限于分类分级规则、优先级规则、升级规则、关闭规则;宜设置事件及时响应率等量化目标并跟踪量化目标的达成情况。

9.5 问题管理

问题管理的目标是通过采取措施消除事件的深层次原因,预防事件或问题再次发生,降低重复事件的影响,提高金融数据中心服务质量和稳定性。

金融数据中心问题管理的基本要求应符合GB/T 33136、ISO/IEC 20000-2、JR/T 0071.2中问题管理的相关内容基础上,还应包括问题来源包括但不限于尚未找到根本原因的事件、历史事件趋势分析、性能或容量数据分析、二线检查发现问题等;对未查明原因的问题,应增加监控和应急措施。

金融数据中心问题管理的增强要求包括宜建立问题管理定期回顾和持续优化机制,对问题流程规则进行回顾更新。

9.6 变更管理

金融数据中心变更管理的基本要求应符合GB/T 33136、ISO/IEC 20000-2中变更管理的相关内容基础上,还应包括设置合理的变更窗口减少对服务的影响。

金融数据中心变更管理的增强要求包括宜采用监控配置、自动化任务、批量处理等方式进行有效性检查;宜制定重要保障时期变更管理策略,明确启动机制、过程管理及风险控制等要求;宜对变更完成情况进行统计分析,包括失败变更数量及占比等。

10 风险管控

10.1 风险管理

金融数据中心风险管理的基本要求包括以下内容。

- a) 应确定金融数据中心风险管理对象、范围、要求、方针及策略。
- b) 发生重大安全事件或内外部环境重大变化时,应调整风险管理策略及措施。
- c) 应基于风险管理要求和策略,识别金融数据中心对环境管理、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、外包运维管理等管理对象的安全需求。

- d) 应根据识别的安全需求制定风险管理措施并予以落实，确保风险管理的持续有效性。
- e) 应建立风险评估机制，全面识别金融数据中心安全风险，将风险控制在可接受的范围内。
- f) 应定期对相关安全事件及风险进行分析，评估现有措施有效性并及时整改问题。
- g) 应每年至少开展1次风险评估，当内外部环境发生重大变化时，应重新开展风险评估。

10.2 物理安全

10.2.1 组织架构

金融数据中心组织架构的基本要求包括以下内容。

- a) 应明确负责安全保卫的部门，负责物理安全的组织、协调、推动与监督。
- b) 应设置专职安全保卫岗位，人员应具备物理安全专业素质与能力。

10.2.2 人员进出管理

金融数据中心人员进出管理的基本要求包括以下内容。

- a) 应根据实际情况对物理区域进行划分，明确人员、车辆和物品设备的进出管理策略。
- b) 应制定新增、变更、注销门禁权限的申请、审批相关流程。
- c) 应针对内部人员的工作需要，设置相应区域的门禁权限。
- d) 应针对外部人员的特征进行分类，制定相应的权限管理策略，必要时由内部人员进行陪同。

10.2.3 安全防范措施

金融数据中心安全防范措施的基本要求包括以下内容。

- a) 应设置围墙、栅栏等设施并安装脉冲电子围栏或周界入侵探测报警装置进行封闭管理，入口和园区内应进行机动车限速，车辆进入通道应设置防车辆冲撞装置。
- b) 应对进入主机房、支持区、主要通道等重要区域的人员携带物品进行检查。入口应安装出入口控制系统，记录出入人员情况，重要区域应安装视频监控装置，进行24小时连续监控，监控录像保存时间应不少于3个月，重要区域不应有监控盲区。
- c) 应及时响应和处理安防、消防系统故障、园区突发安全事件，做好记录报告、跟踪交接工作。
- d) 应建立巡检工作流程，合理规定每日巡检频率、巡检时间和巡检内容。

金融数据中心安全防范措施的增强要求包括金融数据中心重要区域的入口宜配备通过式金属探测门、手持式金属探测器、X射线安全检查设备等危险品探测装置。

10.2.4 安全教育与培训

金融数据中心安全教育与培训的基本要求包括以下内容。

- a) 应针对全体人员开展消防安全宣传教育，讲解防火与逃生自救知识与技能，提升消防安全意识与能力。
- b) 应针对新入职人员和外来人员进行园区安全管理要求宣讲教育。
- c) 应通过安全教育与培训提高安全管理人员的安全意识和技能。

10.3 支撑类系统安全

金融数据中心支撑类系统包括机房动力环境监控系统、网络监控系统、安防系统等支撑金融数据中心业务的系统。金融数据中心支撑类系统安全的基本要求包括以下内容。

- a) 应建立支撑类系统的身份鉴别和授权访问机制，防止未授权访问。
- b) 应对支撑类系统的监测和操作进行审计，审计记录的保存时间应满足故障诊断、事后审计的需要。
- c) 应采用安全技术和措施对支撑类系统运维终端的漏洞和病毒进行更新和防范。

金融数据中心支撑类系统安全的增强要求包括宜对支撑类系统的容量和性能需求进行前瞻性规划，通过监测、采集、分析和调优，提升业务系统运行的可靠性、稳定性和可用性。

10.4 应急管理

10.4.1 应急预案

金融数据中心应急预案的基本要求包括以下内容。

- 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。应急预案的编制工作应由相关部门共同完成，并经预案涉及的部门书面确认。
- b) 应针对金融数据中心各类突发事件制定相应的应急预案，包括但不限于基础设施故障事件应急预案、自然灾害事件应急预案、重大突发事件应急预案。

10.4.2 应急响应

金融数据中心应急响应的基本要求包括以下内容。

- a) 应按照可控性、严重性和影响程度，将安全事件进行分级。
- b) 应制定安全事件报告和处置管理制度，明确不同等级安全事件的报告、处置和响应流程。
- c) 应在安全事件发生后根据应急预案启动应急机制，响应安全事件，事后完善应急预案。
- d) 应及时向安全管理部门报告发现的安全弱点和可疑事件，对造成系统中断和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，根据要求及时向行业主管部门进行汇报。

10.4.3 应急演练

金融数据中心应急演练的基本要求包括以下内容。

- a) 应对金融数据中心相关人员每年至少开展1次应急预案培训并记录培训内容。
- b) 应每年至少进行1次全方位应急预案演练，记录应急预案演练的过程，编写应急演练总结报告，并根据演练结果完善应急预案。

参 考 文 献

- [1] GB 50606 智能建筑工程施工规范
 - [2] GB 50738 通风与空调工程施工规范
 - [3] GB/T 21050 信息安全技术 网络交换机安全技术要求
 - [4] GB/T 22080 信息技术 安全技术 信息安全管理体系 要求
 - [5] GB/T 22081 信息技术 安全技术 信息安全控制实践指南
 - [6] GB/T 22239 信息安全技术 网络安全等级保护基本要求
 - [7] GB/T 34960.1 信息技术服务 治理 第1部分：通用要求
 - [8] GB/T 34960.2 信息技术服务 治理 第2部分：实施指南
 - [9] GB/T 34960.3 信息技术服务 治理 第3部分：绩效评价
 - [10] GB/T 51314 数据中心基础设施运行维护标准
 - [11] DGJ 08—2068 公共建筑用能监测系统工程技术规范
 - [12] JGJ 242 住宅建筑电气设计规范
 - [13] JR/T 0011 银行集中式数据中心规范
 - [14] JR/T 0218 金融业数据能力建设指引
 - [15] YD/T 1097 路由器设备技术要求 核心路由器
 - [16] YD/T 1099 以太网交换机技术要求
 - [17] YD/T 1358 路由器设备安全技术要求—中低端路由器（基于IPv4）
 - [18] YD/T 1359 路由器设备安全技术要求—高端路由器（基于IPv4）
 - [19] YD/T 1454 IPv6网络设备技术要求 核心路由器
 - [20] YD/T 3096 数据中心接入以太网交换机设备技术要求
 - [21] T/CECS 485 数据中心网络布线技术规程
 - [22] ISO/IEC 20000-1 信息技术 服务管理 第1部分：服务管理体系要求（Information technology—Service management—Part 1: Service management system requirements）
 - [23] ISO/IEC 22237-2 信息技术 数据中心设施和基础设施 第2部分：建筑施工（Information technology—Data centre facilities and infrastructures—Part 2: Building construction）
 - [24] IETF RFC 4861 IPv6邻居发现（Neighbor Discovery for IP version 6）
 - [25] IETF RFC 5072 PPP协议上的IPv6连接（IP Version 6 over PPP）
 - [26] IETF RFC 5172 IPv6协议控制下的IPv6数据报压缩协议（Negotiation for IPv6 Datagram Compression Using IPv6 Control Protocol）
 - [27] TIA 942 数据中心电信基础设施标准（Telecommunications Infrastructure Standard for DataCenters）
-