ICS 35.240.40
A11
备案号：

JR

中华人民共和国金融行业标准

JR/T 0011—2004

银行集中式数据中心规范

Systematic specification of centralized bank data center

2004-12-01 发布　　2004-12-01 实施

中国人民银行　发布

目　次

前　言

本标准由中国工商银行提出。

本标准由全国金融标准化技术委员会归口。

本标准起草单位：中国工商银行、中国人民银行、中国农业银行、中国银行、中国建设银行、中国标准研究中心。

本标准主要起草人：林晓轩、吕仲涛、张艳、张宏、张颖、张轶、姚红玲、赵博、朱铭烜、童杰、陈树文、王益清、顾骏、陆书春、谢凯、朱宇、朱玉红、魏宏。

引　言

银行集中式数据中心是银行信息的管理中心和业务的处理中心，是银行各项业务开展的重要基础。银行集中式数据处理中心能够减少银行信息技术基础设施和信息技术人员成本，改善银行对外服务水平和形象，通过科学的统计数据和量化的模型分析，有助于银行提高决策和管理水平，促进银行集约化经营水平的提高。

本标准的制定用于规范、指导银行集中式数据中心的建设以及集中式数据中心的日常安全生产运行。

银行集中式数据中心规范

1 范围

本标准规定了银行集中式数据中心的定义、目标、范围、技术规范、管理规范和应具有的职能，是建设和管理银行集中式数据中心的指导。

本标准适用于中华人民共和国境内银行及金融机构。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准：

GB/T 9361 计算机场地安全要求

GB/T 2887 电子计算机场地通用规范

GB 50174 电子计算机机房设计规范

ISO/IEC 17799 信息安全管理

3 术语与定义

下列术语和定义适用于本标准。

3.1

银行集中式数据中心 centralized bank data center

以集中的数据存储和统一的信息处理平台为依托，在相应的系统支撑下，通过集中的运行、监控、管理手段，承担银行区域或全辖范围内信息存储、处理和传输的机构。

3.2

银行集中式数据中心下辖机构 institution administered by centralized bank data center

指各项业务及管理数据由银行集中式数据中心进行存储、处理的机构，在本标准内所指的下辖机构不涉及行政隶属关系。

3.3

开放系统 open system

开放系统是这样一些功能部件的集合：它们使正确执行的应用程序能在多个厂商提供的不同的平台上运行，和其他应用程序互操作，并且为用户相互作用提供一个统一风格的界面。

3.4

灾难 disaster

指造成数据中心部分或全部的计算机软硬件设备、附属设备、资料档案或机房环境损坏以致于严重影响数据中心正常运行的事件，它可能由于自然灾害、突发事件、设备故障及人为因素等所造成。

3.5

灾难备份 disaster backup

指利用技术、管理手段以及相关资源确保既定的银行关键数据、关键数据处理系统和关键业务在灾难发生后可以恢复的过程。

3.6

软件安全 software security

指系统软件、应用软件、工具软件、数据库和中间件软件等获取渠道的合法性、安全性和运行的稳定性。

3.7

企业总控中心 enterprise command center

指对银行集中式数据中心实施集中监测、集中操作和集中管理的场所，是大型数据中心必备的信息技术基础机构。

4 职能

4.1 职能概述

银行集中式数据中心正常运行应具备的基本职能应包括：日常运行职能、系统维护职能、网络维护职能、应用维护职能、安全管理职能、设备维护职能、数据档案管理职能、应急处理职能、服务质量管理职能、对外联系职能、日常行政人力资源等管理职能。

本部分并不规定银行集中式数据中心的机构设置，但在附录A中给出了银行集中式数据中心职能及相应机构设置的举例。

4.2 日常运行职能

负责银行集中式数据中心的生产管理工作，保证银行集中式数据中心生产工作的顺利、高效进行。包括：

a) 运行协调管理：负责银行集中式数据中心内部生产运行工作的协调；

b) 作业调度管理：负责作业流程的编写、审核、修改，制定生产作业计划，检查作业执行情况，安排非常规计划操作的具体内容；

c) 运行制度管理：负责建立健全运行管理有关规章制度并督促检查落实执行情况；

d) 运行操作管理：负责组织实施主机生产系统的运行操作，人员调度，督促操作人员按照规范，完成操作任务，控制操作质量。对重大操作进行监督、指导；

e) 运行监控管理：负责环境、系统、网络、应用等运行情况的监控，负责监控管理生产系统的运行情况。通过监控及时发现、处理、转发、登记运行问题。

4.3 系统维护职能

负责维护银行集中式数据中心的生产、测试系统，保证系统的正常运行。包括：

a) 系统软件维护：按照技术规范，对主机、开放平台及外设的资源配置进行维护，对系统软件、工具软件及各类补丁进行维护，采集、分析系统软件的性能数据和服务水平，进行系统健康检查，制定系统软件应急预案和操作流程，编写资源使用情况报告、性能分析报告和健康状况评估报告；

b) 数据库系统维护：负责主机及开放平台数据库管理系统、辅助工具软件及参数的维护，编制数据整理、数据备份、数据恢复和应急处理的技术方案和操作流程；采集、分析数据库数据并适时调整和优化，监控和预测数据库的运行状态；负责数据库的故障处理和数据的应急恢复；协助进行应用版本的升级变更和应用软件的问题处理；

c) 存储管理：负责规划主机及开放平台磁盘和磁带库的物理连接、容量分布和相关配置，利用辅助工具实施存储管理和备份管理，制定数据存储、分布、备份和恢复的策略，编写相关的技术方案和应急操作流程并定期进行演练；采集和分析存储系统的吞吐性能和发展趋势，发现I/O瓶颈，并适时进行改进和优化。

4.4 网络维护职能

负责维护和建设银行集中式数据中心内部通讯系统和计算机网络系统，保障银行集中式数据中心通讯系统和计算机网络系统的正常运行。包括：

a) 通讯系统维护：负责程控交换机、电话总机和办公电话的安装和维护，确保中心电话系统的通讯畅通；

注：如银行集中式数据中心没有单独的电话系统，则没有维护电话系统的职能。

b) 通信线路维护：负责通讯系统和计算机网络系统所需各种电信线路的申请、开通、维护和撤销，线路资源的管理和协调联络，受理全网的通讯故障申告，判断并排除故障等；

c) 计算机网络系统维护：银行集中式数据中心计算机网络系统包括局域网、城域网、广域网、网络管理系统和网络安全系统五个部分。负责按照技术规范和业务需求，维护网络架构和网络设备配置，定期编写配置图和配置手册，管理网络设备资源，利用网络管理系统等工具定期监控、分析网络的运行状态，解决各类突发性网络故障，分析网络系统性能，优化网络运行效率，积极预防网络故障发生；负责网络安全设备的技术维护，配合制定安全策略，预防和解决各类网络安全问题。

4.5 应用维护职能

负责银行集中式数据中心应用系统的维护、支持、测试和监控。包括：

a) 日常管理：负责银行集中式数据中心生产应用系统的日常维护工作和技术支持工作，负责应用系统在生产运行过程中应用问题的收集、提出并跟踪问题的解决；

b) 测试投产管理：负责应用系统在银行集中式数据中心投产前的适应性测试工作，包括系统环境的搭建、相关软件系统的安装和参数设置、整理测试中发现的问题并协调各方解决，完成应用系统投产前的环境清理和数据移行工作；

c) 性能管理：负责银行集中式数据中心生产应用系统性能监控，提出并牵头实施应用系统性能优化方案，保证银行集中式数据中心生产应用系统的高可靠性和高可用性。

4.6 安全管理职能

负责银行集中式数据中心内部系统、网络以及生产等方面的安全工作的实施以及组织、协助并督促、检查下辖机构安全工作的实施。包括：

a) 制度实施管理：负责银行集中式数据中心的安全制度、机房安全保卫及消防等制度的实施和检查；落实主管部门规定的安全制度，根据银行集中式数据中心自身的特点制定并实施安全措施，定期检查银行集中式数据中心的安全状况，编制安全状况报告；

b) 运行环境管理：负责计算机系统运行环境、供电、网络、设备、空调、操作系统等的安全管理；

c) 应用系统安全管理：负责计算机应用系统、应用程序版本、应用系统密钥等的安全管理；

d) 系统安全控制管理：负责主机系统安全控制管理，设计主机系统安全控制实施方案，查找系统安全漏洞并编制检查报告；

e) 网络监测管理：负责银行集中式数据中心网络安全的监测和漏洞检测管理工作，运用最新技术手段分析和评估全行在网设备的安全运行状况，定期提交网络安全检测报告；

f) 防病毒防黑客安全管理：及时掌握计算机病毒和黑客对银行集中式数据中心系统的侵犯情况，提供解决病毒侵犯、防病毒、防黑客等方面的技术支持，软件安装前及使用中进行病毒检测及定期发布防病毒软件的适用版本；

g) 实体安全管理：负责银行集中式数据中心园区的实体安全管理；

h) 数据及档案的安全管理：业务数据、机密部件、本地和异地备份等的安全管理；

i) 操作规范管理：负责审核对集中式数据中心内计算机系统操作，包括应用维护、系统维护、日常操作、数据操作、档案维护等的规范性审核。

4.7 设备维护职能

负责银行集中式数据中心内设备的日常维护和检修，保证设备的正常运行。包括：

a) 主机及外围设备管理：负责主机、磁盘机的安装和调试，光纤通道适配器、外部时钟、磁带机、磁带库、终端控制器、前置机、打印机等设备的维护、保养、管理；

b) 网络通讯设备管理：负责对主机与外界通讯的设备进行维护、保养、调整及维修，负责银行集中式数据中心辖内通讯干线、骨干网络通信设备的管理和维护；

c) 服务器与办公设备管理：负责服务器和办公设备的维护与修理，以及与产品供应商的协调工作，根据需要进行设备升级及板卡更换工作；

d) 电力与动力设备管理：负责不间断电源、内部电源、电路、电器的维护、保养和检测，高低压配送电和发电机设备的维护、管理。对发电机进行定时、有效的功能测试，在突发事件发生时应做到稳定切换；

e) 机房场地设备管理：负责中心大型空调的维护、保养、检测及维修，定期进行空调主要指标的测试，银行集中式数据中心各个场所应控制在符合规定的温湿度指标范围内；

f) 仪器与备件管理：负责各类专用的仪器的管理，对各类关键部件的备件的管理。

4.8 数据及档案管理职能

进行生产系统的数据备份及管理，负责银行集中式数据中心档案的归档及管理。包括：

a) 生产数据管理：负责生产数据的备份恢复管理，自动带库的备份策略制定，带库分配和管理，异地备份数据的迁移和保存，数据存储介质的管理，过期数据的清理，数据档案的查询，开发环境使用生产数据的审批管理；

b) 运行档案管理：负责生产运行档案的收集、汇总、整理和保存；

c) 设备出入库及档案管理：负责设备档案的建立、查询，提供设备更新计划、设备报废计划和设备供求信息；

d) 公文档案管理：负责收集整理收发文、内部文件、图表、照片（含底片）、簿册、录音、录像等资料。督促各部门及时清退办理完毕的文件，根据组卷原则进行立卷，并依次编案卷号。

4.9 应急处理职能

负责制定银行集中式数据中心生产系统应急方案，定期组织应急演练，紧急情况发生时按照应急处理流程进行处理。包括：

a) 制定、修改银行集中式数据中心生产系统应急方案，制定启动应急处理流程的标准；

b) 定期组织相关部门进行应急演练；

c) 在紧急情况发生时启动应急处理流程并协调银行集中式数据中心和业务部门按照应急处理流程进行处理。

4.10 服务质量管理职能

面向数据中心的服务对象制定相应的服务标准，并依据此标准进行服务质量的考核。包括：

a) 服务标准：负责根据数据中心提供的业务制定统一的服务标准，形成量化的服务指标，以及这些服务指标的衡量方法；

b) 服务协议：负责与服务对象签订服务质量协议，经银行审批后执行；

c) 服务考核：负责定期根据服务协议提供各类服务指标的实际值，然后根据服务协议组织考核和评比；

d) 服务质量管理工具：负责采用统一的软件工具对服务质量进行管理、衡量和考核。

4.11 日常行政管理职能

负责银行集中式数据中心日常的行政管理、人力资源管理、后勤保障、对外联系等工作。

5 技术规范

5.1 基础设施

5.1.1 园区基础设施

银行集中式数据中心园区基础设施的设计和建设应严格执行国家有关各类设计和建设标准，并至少达到以下管理要求：

a) 园区基础设施的设计、建设方案和管理措施应通过主管部门的评估和检查；

b) 园区实行封闭式管理，设置一个主出入口和一个备用出入口，正常情况下使用主出入口，关闭备用出入口；

c) 园区应与居民楼分隔，除必要的办公和后勤服务设施外，园区内不能建有居民生活楼；

d) 主出入口应设置门卫值班室，外单位人员一律在值班室登记并换取通行证件后方可进入园区；

e) 园区出入口和周边围墙应设置闭路电视监控装置，实行 24 小时录像，录像资料应妥善保存；

f) 园区应由专业的物业管理机构管理，严格执行国家有关物业管理的法规和标准；

g) 应建立园区管理的规章制度，在园区显著位置给予明示，由指定的部门负责定期组织检查和审计；

h) 园区的管理应得到当地政府和公安机关的支持，接受监督和检查。

5.1.2 机房基础设施

银行集中式数据中心机房基础设施的设计和建设应严格执行计算机机房的设计和建设标准，并至少达到以下管理要求：

a) 机房基础设施的设计、建设方案和管理措施应通过主管部门的评估和审查；

b) 机房选址应尽量避开地震多发地带；建于地震多发地带的机房，其建筑设计应按当地地震裂度等级提高一级；机房应采取防水、防雷、防鼠装置并定期进行检查；机房应具备防电磁干扰和泄漏的能力，达到国家有关计算机机房的级别标准和要求；机房动力应提供双路供电、不间断电源和自备发电设施（发电机的位置、燃料的存放应符合相关标准规定）并装有电力自动报警装置，动力电源应定期进行切换演练；

c) 要建立机房动力管理规定：机房动力供、配电系统由专人负责管理，由合格的持证电工对机房实行 24 小时值班，定时检测，并作好记录；机房内各类固定设备的电源插座不应放在地板表面，临时设备使用电源要经过审批；机房内不应使用各类电热器具，因工作特殊需要应使用时，应由专人按技术规范操作，使用完毕后应立即做好善后安全处理；

d) 要建立机房消防管理规定：机房应安装火灾传感（烟感、温感）报警系统和自动灭火装置，并配备规定数量的手动消防器材，所有消防设施和器材，应经过消防部门的检查验收；机房的地板、隔墙、天花吊顶等室内装修应采用阻燃材料；要建立消防预案，指定消防管理员和义务消防员，定期检查消防设施，每季度至少组织一次消防演练；

e) 要建立机房空调管理规定：指定专人负责机房空调的维护和管理，每天定时检查记录空调的运转情况和机房温湿度数值，并安装机房空调的自动报警装置；

f) 要建立机房出入管理规定：机房所在区域应安装 24 小时视频监控录像装置，重要机房区域实行 24 小时警卫值班；机房实行封闭式管理，设置一个主出入口和一个或多个备用出入口，正常情况下使用主出入口；机房应配置电子门禁系统，实行分区管理，通过配发门禁卡限定出入机房人员及其允许进入的区域。所有工作区域门禁系统日常处于常闭状态，所有人员进出应验卡并严格登记。经批准并办妥有关手续的非本单位人员进入机房，应由相关人员全程陪同；严格执行人员和物品的出入检查制度，与工作无关的物品不得带入机房，携带计算机及相关设备出入机房应办理有关手续，由机房主管批准后，方可带进或带出；电子门禁系统、视频监控录像系统的信息资料应妥善保管，所有机房出入记录信息应至少保存 1 年，视频监控录像资料应至少保存 1 个月，更新、销毁保存介质应严格按照销毁秘密文件的规定执行；

g) 机房设施应分类存放，分类标准可以是：按功能划分生产、开发、测试、备用，或者按设备类型划分主机、服务器、网络、存储等；机房内不应存放易燃、易爆、易碎、易污染、强磁场、腐蚀性物品；机房内重要数据资料应按照保密制度，由专人保管，并存放在固定位置。需要废弃、销毁的资料，严格按规定销毁；任何食物、饮料不得带入机房，机房内应保持整洁，操作台面、常用设备要定期清理，保持机房的洁净度；

h) 机房管理的规章制度应在机房显著位置给予明示，由指定的部门负责定期组织检查和审计。

5.1.3 办公和服务基础设施

银行集中式数据中心的办公和服务基础设施应与机房分开，设计和建设应严格执行国家各类设计和建设标准，并至少达到以下管理要求：

a) 办公和服务区域应独立于机房设施之外，办公和服务基础设施的设计、建设方案和管理措施应通过主管部门的评估和检查；

b) 办公和服务设施应具备良好的空调和新风设施，并定期消毒，保证工作人员有良好的工作环境；

c) 数据中心应制定和完善办公和服务设施的管理制度，为工作人员提供良好的办公和后勤服务；

d) 办公和服务设施可以由专业的物业管理机构管理，但是要严格执行国家有关物业管理的法规和标准。

5.2 系统环境的建设和维护

5.2.1 硬件系统环境的建设和维护

硬件系统环境是银行集中式数据中心的关键性基础设施，主要包括：处理器、通道连接设备、存储设备、输出设备及其它外设等。硬件系统环境的建设和维护应符合以下规范和要求：

a) 银行集中式数据中心应建立并不断完善硬件系统环境建设和维护的规章制度和管理办法，有关文字材料应妥善保存并接受主管部门的检查；

b) 银行集中式数据中心硬件系统环境的建设、升级、扩充等工程应经过科学的规划、充分的论证和严格的技术审查，有关文字材料应妥善保存并接受主管部门的检查；

c) 银行集中式数据中心硬件系统环境的功能、性能和容量要满足银行业务处理的需求，处理器和存储设备的平均使用率宜控制在75%以内，计算机系统的时钟与标准时间的误差不宜超过30秒；

d) 银行集中式数据中心应建立硬件系统环境的可用性保障机制，主要处理器、通道、存储设备及关键外设应采用具有冗余技术的设备；

e) 银行集中式数据中心硬件系统环境要适当采用冗余备份、负载均衡、并行处理和集群等技术，充分保证系统的可靠性和处理效率；要尽量减少硬件系统的计划性停机时间，尽量避免硬件系统的非计划性停机；

f) 硬件设备应科学分类和摆放，并按规定的格式给予明显标识，建立设备台账，指定专门的部门和岗位负责统一管理；

g) 硬件系统环境应采取定时巡检、定期检修和阶段性评估的措施，银行业务高峰时段和业务高峰日要加强巡检频度和力度，确保硬件可靠、运转正常；

h) 银行集中式数据中心硬件系统环境的方案和配置应视同秘密，不得向无关单位和个人透露；银行集中式数据中心应与本单位员工和经常有机会直接接触银行集中式数据中心硬件系统环境的其他单位签订保密协议。

5.2.2 软件系统环境的建设和维护

银行集中式数据中心的软件系统环境主要包括：操作系统、数据库管理系统、中间件、工具软件、应用软件等。软件系统环境的建设和维护应符合以下规范和要求：

a) 银行集中式数据中心应建立并不断完善软件系统环境建设和维护的规章制度和管理办法，有关文字材料应妥善保存并接受主管部门的检查；

b) 银行集中式数据中心软件系统环境的建设、升级、改造、推广等工程应经过科学的规划、充分的论证、严格的技术审查和业务测试，有关文字材料应妥善保存并接受主管部门的检查；

c) 银行集中式数据中心软件系统环境的功能、性能和容量要满足银行业务需求，并与银行集中式数据中心的运行环境相配套；

d) 银行集中式数据中心应保证软件来源、安装、使用的正当性、合法性和安全性，软件能够持续、稳定的提供服务，软件问题的及时有效解决，对软件可能受到的外部攻击进行防护。保障银行集中式数据中心各类操作系统、数据库系统和应用系统安全、有效地运行；

e) 银行集中式数据中心应建立软件系统环境的可用性保障机制，关键的程序、参数和数据要定期备份，银行分户账和交易日志等重要数据的备份介质应实行本地、异地同时存放，使用备份介质要经过严格的授权；

f) 银行集中式数据中心软件系统环境要适当采用冗余备份、负载均衡、并行处理和集群等技术，

充分保证系统的可靠性和处理效率；要尽量减少软件系统的计划性停机时间，尽量避免软件系统的非计划性停机；

g) 软件应科学分类和管理，并按规定的格式给予标识和登记，建立软件台账，指定专门的部门和岗位负责统一管理；

h) 软件系统环境应采取定时巡检、定期维护和阶段性评估的措施，银行业务高峰时段和业务高峰日要加强巡检频度和力度，确保软件可靠、运行正常；

i) 银行集中式数据中心应适当采用具有自动化处理功能的软件系统来提高系统维护和管理、运行操作和监控、故障诊断和报告的自动化水平；

j) 银行集中式数据中心软件系统环境的方案和配置应视同秘密，加密、认证、密码、密钥等核心技术和信息应由银行内部专职人员掌握，使用这些技术和信息要经过严格的授权，不得向无关单位和个人透露；银行集中式数据中心应与本单位员工和经常有机会直接接触银行集中式数据中心软件系统环境的其他单位签订保密协议。

5.2.3 其它

5.2.3.1 数据的备份

银行集中式数据中心应采用灾难备份技术在同城、异地建立备份中心，备份中心应至少保存有银行前一个营业日终了的分户账数据和交易日志，并按相关业务管理规定的时限保存相应的数据，同时确保数据的可用性和完整性。

5.2.3.2 银行集中式数据中心的灾难备份

银行集中式数据中心的灾难备份中心可以由银行自行建设和管理，也可以采用外包方式，通过签订服务协议，委托其他企业建设和管理；采用外包方式建设和管理灾难备份中心，其方案和服务协议应报主管部门审批，并接受主管部门的监管（银行集中式数据中心灾难备份环境的建设和维护规范，见 5.5）。

5.2.3.3 企业总控中心

银行集中式数据中心应建立集中式的企业总控中心和技术人员值班制度，负责 24 小时监控生产系统软硬件和通讯网络的运行状态，集中进行银行集中式数据中心生产运行的操作。企业总控中心的物理位置应与主要机房相对隔离，最大程度地减少机房人员的出入。

5.2.3.4 技术支持

银行集中式数据中心应建立完善的系统技术支持体系，技术支持队伍主要包括：数据中心内部技术人员，本银行内但不属于数据中心的其他技术人员（例如软件开发中心），以及与数据中心或银行签订合同的产品供应商和技术服务商；要制定并不断完善技术支持的规章制度和工作流程。

5.3 应用软件系统的建设和维护

银行集中式数据中心的应用软件系统是银行集中式数据中心下辖机构各种业务运作和内部管理的处理平台，应用软件系统的建设和维护应符合以下规范和要求：

a) 应用软件系统在银行集中式数据中心投入运行前，应安排在银行集中式数据中心测试环境上进行功能测试和压力测试，在确认系统运行稳定并且实现了全部设计功能后，才能在数据中心投入生产运行；

b) 银行集中式数据中心各个应用软件系统的日常操作和监控，应有专人负责，严格按照各个应用软件系统的操作手册和监控手册进行，按照银行集中式数据中心生产运行管理制度处理运行中出现的各种问题；

c) 银行集中式数据中心应建立所有应用软件系统版本的管理台账，制定应用软件系统版本更新计划，根据主管部门的统一安排，进行应用软件系统版本的安装、测试和投产；

d) 银行集中式数据中心所有应用软件系统的技术维护工作应明确具体的负责人，应用软件系统的维护人员应掌握所负责系统的结构和功能，应具有分析定位应用软件系统生产问题的技能，能够迅速解决应用软件系统运行中出现的各种问题；

e) 银行集中式数据中心投产应用软件系统前，应对具体的维护人员进行必要的技术培训，提供应

用软件系统的安装手册、维护手册、系统设计说明书、系统功能说明书等技术资料，保证数据中心应用维护人员掌握必要的应用软件系统的维护技能；

f）银行集中式数据中心所有应用软件系统应取得系统开发单位的技术支持保证，包括自行开发的应用软件系统和外购的第三方的应用软件系统，保证数据中心应用软件系统出现复杂问题时能够得到顺利解决。

5.4 网络通信设施的建设和维护

5.4.1 通信系统的建设和维护

银行集中式数据中心的通信系统主要包括：数据通信系统、语音通信系统等，通信系统的建设和维护应符合以下规范和要求：

a）为确保银行集中式数据中心的数据通信安全，应采用多于一家电信运营商互相备份的模式，要求每家电信运营商提供双路接入保护；

b）为确保银行集中式数据中心的数据通信容量能够根据需要快速升级，要求电信运营商为银行集中式数据中心配备的用户端设备应有足够的富裕容量和良好的扩展性；

c）银行集中式数据中心采用的电信线路应具有良好的带宽扩展性；

d）银行集中式数据中心应为每位员工提供便捷、园区可移动的固定电话通信系统；

e）银行集中式数据中心应为主要员工配备移动通信系统，与固定电话通信系统形成互为备份。

5.4.2 计算机网络系统的建设和维护

银行集中式数据中心计算机网络系统主要包括：局域网、城域网、广域网、网管系统、网络安全等，计算机网络系统的建设和维护应符合以下规范和要求：

a）银行集中式数据中心应建立并不断完善网络系统建设和维护的规章制度和管理办法，有关文字材料应妥善保存并接受主管部门的检查；

b）银行集中式数据中心网络系统的建设、升级、扩充等工程应经过科学的规划、充分的论证和严格的技术审查，有关材料应妥善保存并接受主管部门的检查；

c）银行集中式数据中心网络系统的方案和配置应视同秘密，不得向无关单位和个人透露；银行集中式数据中心应与本单位员工和经常有机会直接接触银行集中式数据中心网络系统的其他单位签订保密协议。银行集中式数据中心网络系统的建设应采用业界成熟的技术，设备应具有良好的扩展性；

d）银行集中式数据中心应为核心网络设备划定独立的功能区域，不得与其他功能区域混用；

e）网络设备应科学分类和摆放，并按规定的格式给予明显标识，建立设备台账，指定专门的部门和岗位负责统一管理；

f）新建的网络在投入使用前，应制订相对应的网络安全防范措施，并对新建的网络实施安全检验，未经检验的新建网络不允许投产使用；

g）网络系统进行结构性改造后，应及时调整网络安全防范措施，并重新对调整后的网络进行安全检查；

h）银行集中式数据中心网络系统的功能、性能和容量要满足银行业务处理的需求，处理器和内存系统的平均使用率应控制在75%以内；

i）银行集中式数据中心应建立网络系统的可用性保障机制，核心网络设备应采用冗余热备份；

j）银行集中式数据中心网络系统要适当采用冗余备份、负载均衡等技术，充分保证系统的可靠性和处理效率；

k）网络系统应采取定时巡检、定期检修和阶段性评估的措施，银行业务高峰时段和业务高峰日要加强巡检频度和力度，确保硬件可靠、运转正常；

l）网络设备配置和核心网络设备的系统日志应定期保存；

m）银行集中式数据中心应建立网络设备的时钟同步机制；

n）银行集中式数据中心网络系统与外单位的接口必须依据集中式数据中心安全规范确定的安全等级，并进行严格的网络安全防护；

o) 银行集中式数据中心网络设备的访问应是授权的，责认明确的及可追溯的；

p) 银行集中式数据中心采用的网络安全技术应定期回顾，确保安全技术的及时更新及漏洞堵塞；

q) 银行集中式数据中心应建立网络安全风险分析机制，利用各种技术及工具检测网络的漏洞和弱点并及时改正；

r) 应采用有效监测工具，及时掌握网络安全运行状况，提高通信网络可用性，提高网络抗攻击能力，对网络安全风险事件进行紧急响应处理，并对网络安全事故、网络破坏进行取证、举证，以通过法律的手段保护自己同时打击攻击者。

5.5 灾难备份环境的建设和维护

银行集中式数据中心由于处理能力的高度集中，一旦发生风险，将会造成较大范围的影响，因此，对于银行集中式数据中心应建立相应的灾难备份环境和应急处理机制保持业务的连续性。灾难备份环境的建立和维护应至少达到以下要求：

a) 要对银行集中式数据中心可能面临的灾难事件等级进行详细划分，对不同等级的灾难事件进行风险评估，并分别制定有效的保持业务连续性运作方案；

b) 银行集中式数据中心建立灾难备份环境的首要任务是确保银行业务数据的安全、完整和可用，保证银行业务的连续性，保护银行和客户的利益。要采取科学、有效的技术措施建立灾难备份环境，确保当灾难事件发生时，银行集中式数据中心的核心业务数据丢失在规定的时间范围内，从而保证事后数据完全恢复；

c) 银行应根据不同的实时性要求建立不同等级的灾难备份环境，可以采取同步技术或异步技术，建立同城、异地备份。对于有条件的银行集中式数据中心，应考虑建立异地的灾难备份中心；

d) 要针对不同等级的灾难事件分别制定应急处理流程，明确紧急情况发生时的紧急处理流程和业务恢复机制等。这些内容应事前设计，进行定期的测试和演练，并不断修订完善，以确保流程的有效性；

e) 要针对不同等级的灾难事件过后的环境恢复工作制定处理流程，并通过技术和业务评审；

f) 有关灾难备份的技术方案、应急处理流程、恢复工作流程等文档应由指定小组定期根据技术环境和业务环境的变化组织修订，并定期演练；所有文档应分地点妥善保管。

6 管理规范

6.1 目标

银行集中式数据中心应建立银行集中式数据中心生产运行系统的管理规范和流程，以确保银行集中式数据中心生产系统安全平稳运行，应达到以下目标：

a) 整个生产运行流程应得到控制；

b) 对流程的每一个环节，应有形成文档的管理规范；

c) 管理规范应规定实施这些规范岗位或人员的职责，被委派履行职责的人员应具备一定的资格，并为其配备必要的资源；

d) 流程和规范应随着业务发展和时间的推移加以修改，但修改工作应是谨慎的，并且应得到批准。所有文档应经过审核和／或评审。

6.2 操作管理

操作管理是指一系列用于规范计算机系统运行过程中所有人工干预过程的方法、原则和具体要求。操作管理应以满足客户需求为原则，同时贯穿银行集中式数据中心的经营管理策略。操作管理的两类基本文档是运行操作手册和各类系统操作手册,应符合以下规范和要求：

a) 操作管理的流程应形成文档并保持；

b) 操作管理的调度应形成长期（如 1 年）和短期的调度方案，调度方案应随着运行系统需求、客户需求、制度、政策、法律法规等变化而修改；

c) 调度方案应形成运行操作日志文件，运行操作日志应包括手工提交的每一个作业的提交条件、提交时机、提交方式、作业命令、复核方式等要素，编写运行操作日志时应注意特殊日期、变更等因素；

d) 运行操作日志应得到审核和批准；

e) 运行操作日志应随需求变化而修改，修改应得到批准，并确保修改后的文档能够得到实施；

f) 生产运行的实施应确保准确性；

g) 各类系统的操作手册应确保其有效性，操作手册应包含常规操作手册及应急操作手册；

h) 银行集中式数据中心应向客户提供系统运行报告，通报客户有权了解的运行信息。

6.3 监控管理

生产运行系统应得到有效的监控。为实施监控策略银行集中式数据中心应配备必要的监控手段及人力资源，应符合以下规范和要求：

a) 银行集中式数据中心应明确需要监控的内容、手段、时间，应明确监控信息向各个岗位及管理者转递的方式及时机，并将监控信息形成文档加以保管；

b) 监控信息应及时得到的分析，分析结果用于及时发现运行系统的缺陷并加以改进，用于改进生产运行系统的性能；

c) 应制定监控信息存储及保存策略。

6.4 维护管理

维护是指为保证生产运行系统持续、稳定、高效、安全运行而采取的活动，应符合以下规范和要求：

a) 生产运行系统应得到有效地维护。维护活动应制度化、程序化（具体技术规范，见第5章）；

b) 维护工作应分为日常维护、性能管理及问题管理；

c) 日常维护应制定详细的维护日志，明确各个系统或设备的维护内容、时间、方式、方法，设备、系统、数据库及其管理系统的维护应结合运行及监控信息；

d) 性能管理是指通过信息系统运行过程中对各项性能数据进行采集、分析和评价，掌握和预测性能状况及变化趋势，发现各类资源的性能问题，并采取有效措施加以调整和优化；

e) 银行集中式数据中心应明确性能管理中各部门的职责，明确各项活动的流程及使用的技术手段和方法；

f) 问题管理（见6.5）；

g) 维护信息应形成文档并保存。

6.5 问题管理

问题管理是指对生产系统运行中出现的问题采用的解决策略和方案的程序（procedure）。银行集中式数据中心对问题管理的程序应流程化、制度化和文档化。管理流程中应明确问题的受理、解决、反馈、分析、纠正、预防、建档入库等环节的内容、方式及授权策略，应符合以下规范和要求：

a) 银行集中式数据中心应建立受理客户提供的生产系统运行故障的机制，该机制应包括从受理客户要求到解决客户需求并反馈的各个环节，应明确对客户不同需求的解决时限、解决方式、解决责任单位和／或责任人。针对生产系统发生的问题应明确在问题解决的不同阶段相关岗位的职责和授权；

b) 当解决问题引发变更时，应按照变更管理（见6.6）的程序进行实施；

c) 银行集中式数据中心应建立得到客户的认可的向客户通报生产运行系统发生的故障及其解决情况的机制，应明确问题通报的方式及时机；

d) 在问题管理中，应明确各个环节的接口方式，明确各个环节的审核机制；

e) 银行集中式数据中心应对问题进行合理的分类并建立问题管理库，以便问题的追踪解决和进一步分析，并作为以后解决同样问题的模板。有条件的银行集中式数据中心应建立自动的问题管理流程。

6.6 变更管理

变更是指对生产系统、生产环境的改动，应符合以下规范和要求：

a) 对生产系统的变更应得到充分的控制。变更方案一般应经过测试(见6.7)，对于无法测试或不具备测试条件的变更，应得到充分论证和审批；

b) 变更管理应流程化、文档化和制度化。变更流程中应明确变更发起方、实施方的职责，应明确变更方案的测试、审批流程及实施策略。对有可能影响客户利益的变更应事先通知客户并得到客户的确

认。变更方案中应包括应急及回退方案；

c) 银行集中式数据中心应有条件地接受客户提出的变更申请，应明确受理变更申请的条件、方式，明确对申请的审批、实施及其反馈的时限和流程；

d) 银行集中式数据中心应建立变更审批机制并明确授权；

e) 有条件的银行集中式数据中心应建立自动的变更管理流程；

f) 变更实施后应及时更新资源配置库（见6.9）。

6.7 测试管理

银行集中式数据中心应根据生产系统的配置情况建立相应的测试环境及测试管理流程，以满足变更测试、性能分析、问题分析及其它研究的需求，满足银行集中式数据中心下辖机构的测试需求，应符合以下规范和要求：

a) 测试环境的系统配置应与生产环境相一致，应建立起与生产环境配置相关联的测试环境配置管理流程及文档管理流程，以确保测试环境与生产环境的一致性。银行集中式数据中心应制定测试环境使用的调度方案及原则并通知到相关部门；

b) 银行集中式数据中心应有形成文档的管理流程。根据银行集中式数据中心的实际情况，制定中长期测试计划。测试之前应制定测试方案，并将测试方案通知到相关部门。测试内容、要素、流程、资源需求等应在测试方案中体现，测试部门之间的分工及协作方式也应在测试方案中明确；

c) 测试结束后，要及时组织测试验收并形成测试报告及变更实施意见。

6.8 应急管理

银行集中式数据中心应建立对影响生产系统正常运行的突发事件的应急策略和措施并形成文档，应明确以下要求：

a) 应明确启动应急管理的条件；

b) 明确启动应急体系后的工作流程及各个岗位的职责；

c) 明确应急措施实施后的善后流程。

6.9 资源配置管理

银行集中式数据中心应建立资源配置（包括计算机相关资源）管理程序并形成文档，应符合以下规范和要求：

a) 资源配置管理应有相应的数据库支持并与变更管理相协调；

b) 应制定必要的管理措施及人员设置以保证该数据库内容的有效性、一致性；

c) 资源配置管理数据库是变更管理及性能分析的基础。

6.10 数据管理

银行集中式数据中心应建立各类数据管理规范并形成文档，应符合以下规范和要求：

a) 生产系统的数据应得到备份，应有完整的备份及恢复策略和手段；

b) 银行集中式数据中心应为生产数据的管理制定规范，明确各类数据的管理方式及期限；

c) 应有完整的数据保存、清理和转存规则并形成文件；

d) 数据的保存应确保其安全性；

e) 应有明确的各类存储介质的保存方式；

f) 对各类数据应明确其相应的保密级别和使用的审批机制。

6.11 档案管理

银行集中式数据中心生产运行中形成的有关档案应得到妥善保存，应符合以下规范和要求：

a) 应明确各类档案的收集、保存方式及期限，应明确档案使用的授权原则和审批手续；

b) 档案的清理和移交应有明确的审批和授权流程；

c) 档案的有效性应被标识，至少应分为有效资料档案（档案的内容于目前生产运行系统一致）、无效参考档案（档案的内容记录了生产运行系统过去的一种状态或其它信息，与目前生产管理系统不一致）。

6.12 服务质量管理

银行集中式数据中心应明确为客户提供的服务内容、方式及承诺，应设立服务质量管理岗位，应符合以下规范和要求：

a) 服务质量部门通过对服务活动有计划的评审、审计、跟踪、报告，使各部门和管理层了解掌握银行集中式数据中心提出给客户的各类服务活动存在的问题，为各部门、管理层提高各类服务质量采取行动提供依据；

b) 服务质量管理部门的活动涉及银行集中式数据中心所有部门，具有以下职责：负责确定服务质量管理的工作计划和工作范围，参加与服务有关的计划的评审，检查该计划是否符合计划制订的流程，并对评审过程中出现的问题进行跟踪；审计和跟踪其他部门的工作过程和服务活动结果；负责收集、整理客户的意见并进行相应的落实。

6.13 安全管理

6.13.1 通则

银行集中式数据中心信息安全是在统一的安全管理策略指导下，通过有效的技术控制，保持银行集中式数据中心信息系统安全稳定运行状态，保障银行各类信息业务正常开展的动态管理过程。银行集中式数据中心应制订相应的安全策略、安全制度和管理办法，采取安全管理措施，并采用一定的安全技术来实现安全管理，所采用的安全产品及技术应符合主管部门的规定。

银行集中式数据中心信息安全是信息系统保密性、完整性和可用性的安全特征的组合，是信息系统或产品的安全策略、安全功能、安全管理、安全维护、安全检查、安全恢复、安全审计等概念的总称。包括：

a) 银行集中式数据中心信息系统的安全威胁：银行集中式数据中心计算机信息系统安全威胁的主要来源有：银行集中式数据中心内部计算机生产系统发生的问题或事故；社会公共基础设施发生问题或事故；银行集中式数据中心赖以合作的商业伙伴、承包商和服务提供商发生问题或故障；非授权访问；假冒身份；数据完整性被破坏；病毒侵害；通信线路被窃听等；

b) 银行集中式数据中心信息安全管理涉及范围：银行集中式数据中心信息安全管理包括对组织、人员、实体、环境、数据、网络系统、应用系统、操作维护、机密资源、紧急响应等环节的安全控制、流程管理和检查审计；

c) 银行集中式数据中心信息安全组织管理：银行可成立安全决策部门（如：计算机信息安全决策委员会），作为全行信息安全的负责人核心。银行集中式数据中心应成立由主要领导人负责、各部门主要负责人参加的安全生产管理部门（如：安全生产管理委员会），是银行集中式数据中心信息安全高层管理机构。银行集中式数据中心内应设置专职岗位履行安全管理职能；

d) 银行集中式数据中心人员安全管理：银行集中式数据中心应适时对从事信息系统工作的人员进行适当的安全知识及相应技能的培训，特别是对于从事敏感工作的员工，在其上岗前进行必要的资格认证和建立岗位责任相关安全合约；对涉及银行集中式数据中心计算机信息系统的实施、及使用其信息和设施的第三方人员，应在签有保密协议的条件下工作；

e) 银行集中式数据中心机密资源安全管理：银行集中式数据中心安全管理部门负责机密资源的管理，所有机密资源应登记造册，严格保管，不得以任何形式非法复制、修改和外泄资源内容。机密资源的使用应指定专人。严格执行双人操作，认真做好使用记录，不使用时应存放在脱机介质上。机密资源的备份介质应定期检查和转存，以确保其可用性和完整性。存储机密资源设备发生故障需由外单位人员进行现场维护与维修时，应有相关人员全程监督。需要废弃、销毁含机密资源的介质时，应严格审批手续，做好登记，由双人负责实施，保证彻底销毁；

f) 银行集中式数据中心安全生产运行流程管理：银行集中式数据中心安全管理部门应在生产活动之前严格审查实施方案的安全性，审查生产活动实施计划中流程是否符合整体安全策略，是否制订相应应急措施等内容；生产过程中应检查相关部门安全管理规定的执行情况；生产活动结束后，应对照实施

计划评价实施效果，评估其对整体生产安全体系的影响，进行相应的追溯、评估和审计工作。定期向领导提供必要的各项生产项目的安全报告；

g) 安全审计管理：银行集中式数据中心应按照安全策略、标准、规范、对计算机信息系统安全体系进行全面的审查和核实；对安全事故进行审查和监控。检查策略的有效性及其对业务效率的影响，确保在最初风险评估的基础有变化时，根据明确规定的审查程序对安全体系进行审查和维护。采取适当的控制措施保障操作系统和审计工具的安全，保障审计工具的完整性，防止滥用。可聘请行内审计职能单位或部门、独立管理人员或专门提供此类服务的第三方组织独立对银行集中式数据中心安全体系实施的各项活动进行审查。应建立审计计划，说明对安全体系的那些方面进行评估和如何评估，采用计算机信息系统的安全审计所适宜的审计工具。审计要求应与适当的管理相一致，以最大限度地降低业务流程中断的风险。审计人员应是银行集中式数据中心生产运行安全检查审计部门专职人员，应具备相应的安全审计技能和相关安全知识。在审计过程中，应采取适当的控制措施保障系统和审计工具的安全。建立审计日志管理的制度，确定审计日志的保存期限、清除方式、保存方式等，防止重要日志记录的丢失、毁坏和篡改。

6.13.2 实体与环境安全指导原则

实体与环境安全的目标是保证设备、信息载体、安全区、园区环境和工作场所等物理安全和访问安全。实体与环境的安全管理至少满足以下原则：

a) 数据中心应设置较高的信息系统安全等级，根据信息处理设备重要（或敏感）程度，置放于不同安全等级的区域内。不同安全区域之间使用相应的安全防护设备和准入控制手段以及有明确标志的安全隔离带进行保护。应使这些设备免受未经授权的访问、损害或干扰。安全区应有适当的出入控制措施予以保护，未经批准或授权，任何人员不得出入。对于进入安全区内的人员，要有必要的监视措施。在选择和设计安全区域时，应将以下各种问题带来的损害考虑在内：火灾、水灾、爆炸、社会动荡以及其他形式的自然或人为的灾害。也应将有关健康和安全方面的规定和标准考虑在内；

b) 数据中心应防止信息或信息处理设施受损或被盗，防止资产流失、受损或毁坏以及业务活动中断，保证设备免受安全方面的威胁和环境的危害。对信息系统的相关计算机和数据通信设备及其连接关系，要编制与实际相符的物理连接图和逻辑结构图，并归档保存。生产运行系统和网络的关键设备应有备份策略；

c) 规定专人负责保存备份磁带和文档资料。对信息载体、设备的销毁和再使用，要有安全人员监督，进行安全处理，并进行记录；

d) 数据中心应针对上述指导原则制定相应的规章制度和技术规范，并定期修订和组织评审。

附录A
（资料性附录）
职能及相应机构设置举例

A.1 日常运行机构

A.1.1 日常操作

如：运行部。

A.1.2 系统监控

如：系统部。

A.1.3 应急处理

如：生产调度办公室。

A.2 技术支持机构

A.2.1 应用维护

如：应用维护部。

A.2.2 系统维护

如：系统部。

A.2.3 网络维护

如：网络部。

A.2.4 设备维护

如：设备部。

A.2.5 技能培训

如：生产调度办公室。

A.3 管理机构

A.3.1 业务管理

如：业务管理部。

A.3.2 数据及档案管理

如：办公室、运行部、设备部。

A.3.3 资源管理

如：办公室、系统部、生产调度办公室。

A.3.4 安全管理

如：安全部。

A.3.5 变更管理

如：生产调度办公室。

A.3.6 环境管理

如：系统部、办公室。

A.3.7 服务质量管理

如：生产调度办公室。

A.3.8 问题管理

如：生产调度办公室。

A.3.9 行政管理（人力、财物、后勤、文秘、保卫）

如：办公室。

A.4 组织结构（示例）

本示例主要在于描述一个能够实现银行集中式数据中心基本职能的组织架构，并考虑各部门之间的不可交叉性。