

附件 5

ICS 35.240.40

CCS A 11

JR

中华人民共和国金融行业标准

JR/T 0272—2023

金融业办公信息系统基本要求

Basic requirements for office information systems used in financial
industry

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 总体设计原则	1
5 功能类要求	2
6 非功能类要求	6
参考文献	11

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。

本文件起草单位：中国人民银行科技司、中国工商银行股份有限公司、中国金融电子化集团有限公司、中国农业银行股份有限公司、中国银行股份有限公司、中国建设银行股份有限公司、招商银行股份有限公司、中国民生银行股份有限公司、中国光大银行股份有限公司、平安银行股份有限公司、浙商银行股份有限公司、上海浦东发展银行股份有限公司、永中软件股份有限公司、福昕鲲鹏（北京）信息科技有限公司、北京慧点科技有限公司、上海泛微网络科技股份有限公司、北京致远互联软件股份有限公司、北京金山办公软件股份有限公司、中软信息系统工程有限公司、深圳市蓝凌软件股份有限公司、北京数科网维技术有限责任公司。

本文件主要起草人：李伟、陈立吾、周祥昆、车珍、詹志建、刘帅、张燕、徐志扬、敦宏程、刘承岩、关志伟、郭运雷、李璨与、陈雪峰、张佑飞、孙兴建、陈磊、何明燕、程昊宇、姜云兵、韩竺吾、李未姝、姜蕴、周建元、张洲、吕峥、孔亮、徐永久、姚震、严明、潘文凯、杨新伟、程屹、刘杨、梁勇、白雪冬、张治、余继杨、张树玲、曹琳、于娜、王富嵩、石晶。

金融业办公信息系统基本要求

1 范围

本文件规定了金融行业办公信息系统基本要求，主要包含总体设计原则、功能类要求和非功能类要求。

本文件适用于指导金融机构办公信息系统的规划、建设、运行和管理。

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/T 22239—2019 信息安全技术 网络安全等级保护基本要求
- GB/T 33481—2016 党政机关电子印章应用规范
- GB/T 37095—2018 信息安全技术 办公信息系统安全基本技术要求
- JR/T 0071—2020 金融行业网络安全等级保护实施指引
- JR/T 0255—2022 金融行业信息系统商用密码应用 基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

办公信息系统 office information system

面向金融机构员工提供办公服务的信息系统。

注：办公信息系统以金融机构日常办公需求为基础，以信息技术（IT）为支撑，为金融机构员工提供办公服务，辅助员工完成日常办公。

3.2

多活 multi-active

信息系统利用2个及以上多地理节点部署的信息系统协同工作，实现业务并行多点接入、业务并行多点处理、数据并行多点存储的能力。

注：当部分地理节点的信息系统发生灾难或故障时，只有部分业务受到影响，并且部署于其他地理节点的信息系统可以及时完成业务接管。

[来源：JR/T 0207—2021，3.8，有修改]

4 总体设计原则

办公信息系统设计过程应遵循如下总体设计原则。

- a) 规范性原则：办公信息系统应优先注重规范性，办公信息系统所采用的软硬件产品在功能、性能、可靠性、安全性等方面均应符合国家要求。
- b) 适用性原则：办公信息系统建设采用的技术应在适用的生命周期内满足金融机构的数字化办公需求，选用的硬件设备及操作系统、数据库产品、应用软件应符合金融业信息技术创新应用现状，并兼顾发展趋势。
- c) 整体性原则：办公信息系统的整体设计应有效地实现后台一体化管理，前台应满足用户个性化需求，所有组件间的同类办公信息均能共享和互通，系统集成程度高。
- d) 可靠性原则：办公信息系统应平稳运行，如在使用过程中出现人为因素或者外部事件所引起的系统端崩溃，应快速恢复。
- e) 开放性原则：办公信息系统在提供日常办公服务的同时，应支持同其他专业系统的协同交互，例如支持与财务报销、人力资源等系统的协同。
- f) 易用性原则：办公信息系统的设计，应重视用户界面的友好性，满足简洁大方、功能齐备、美观实用等需求。
- g) 安全性原则：办公信息系统应采用成熟的技术平台，支持身份认证技术及安全加密技术，支持多因素认证登录。数据传输过程中和数据库中应采用国家密码管理部门认可的密码算法和密码技术，保证数据的安全性。系统应建立规范灵活的权限管理体系，实现对系统资源和数据不同粒度的有效管控。

5 功能类要求

5.1 概述

根据金融业办公业务特点，日常办公业务分为基础服务、行政办公、沟通协作和综合事务4个类别。

5.2 基础服务类要求

5.2.1 门户服务

金融业办公信息系统应提供统一的门户服务，为用户提供各类信息资源和与用户相关的信息服务。门户服务应满足以下要求。

- a) 提供主要办公业务的统一入口。
- b) 符合GB/T 37095—2018的要求。
- c) 提供支持用户开展日常办公的主要业务功能，可实现对基础服务、行政办公、沟通协作和综合事务的处理。
- d) 注重整体设计，保持设计风格的一致性。
- e) 注重用户的体验感，满足不同用户的使用习惯。
- f) 支持单点登录功能，用户通过统一入口，无需密码即可访问其权限内的其他内网系统，实现“一次登录、全网共享”。

5.2.2 流程管理

办公信息系统的核心为流程管理，基本要求如下。

- a) 应支持常用办公业务办理，实现一网通办。
- b) 应建立针对主要流程审批的待办中心，实现统一待办。
- c) 应具备审批文档自动存档功能，支持查询和审计。

- d) 宜支持移动端审批功能，并保持移动端和个人电脑端（PC端）数据同步。
- e) 宜提供统一的分类流程调转界面。
- f) 宜支持同其他各类系统审批的对接，实现全流程审批统一管理。
- g) 宜支持审批表单及审批流程自定义，满足个性化需求。
- h) 宜具备权限代理功能，由代理人代替委托人出具审批意见并提交流程。
- i) 宜支持流程跟踪、分析及统计功能，易于跟踪流程执行情况，辅助流程持续改进，提升流程审批效率。

5.2.3 移动端操作

金融机构宜根据自身需求，建立符合国家安全要求的移动端办公系统。移动端办公系统宜具备以下功能。

- a) 支持主流操作系统。
- b) 移动端功能布局宜根据机构实际统筹规划。
- c) 移动端数据宜和桌面端数据同步。
- d) 移动端支持流程审批、通讯录、日程管理等功能。
- e) 移动端支持各类系统接入，建立开放的移动端办公生态。
- f) 移动端支持通过远程安全访问途径访问办公数据。

5.3 行政办公类要求

5.3.1 督办管理

督办管理的基本要求如下。

- a) 应结合金融机构具体需求，提供基本督办工作流程。
- b) 应实现督办事项相关要素的查询、统计、导出等功能。
- c) 宜实现和日程管理功能的对接。
- d) 宜实现督办工作全流程用户权限控制。
- e) 宜实现督办日志的自动存档。

5.3.2 公文管理

办公信息系统应提供完备的公文管理功能，系统流转公文应符合国家公文管理规定。公文管理功能应包括公文的起草、公文的审批和签发、公文的接收和转达、公文的权限管理和安全控制等，具体要求如下。

- a) 公文的起草功能：
 - 应支持机构内公文的起草。
 - 应支持外部来文的登记。
 - 应支持公文的在线编辑。
 - 应支持修订记录的保存和修订记录的删除。
 - 如金融机构涉及涉密领域，应支持公文的密级划分。
 - 应支持添加发文附件。
- b) 公文的审批和签发功能：
 - 应支持公文审批流程的灵活配置，宜包含会签、核稿、排版、校对等环节。
 - 应支持公文角色的灵活配置，宜包含综合岗、发文人、核稿人、秘书等角色。
 - 应支持填写审批留言和意见。

- 宜支持公文的撤回。
- 宜支持流转记录的查看。
- 宜支持已发公文修改后重发。
- c) 公文的接收和转达功能：
 - 应支持公文的阅知。
 - 应支持公文的会同办理。
 - 应支持公文的搜索。
 - 应支持公文的浏览。
 - 应支持公文的归档。
 - 宜支持将公文的收文转为发文。
- d) 公文的权限管理和安全控制：
 - 应支持按不同密级、不同角色授予不同权限。
 - 应支持权限申请和审批。
 - 应支持临时转授权。
 - 应支持对公文正文、附件等实体的加密保护。

5.3.3 印章管理

办公信息系统应提供印章管理功能，基本要求如下。

- a) 应为金融机构提供签章基础服务，提供印章申请、审批、使用、存档服务。
- b) 电子印章应符合GB/T 33481—2016的相关要求。
- c) 应提供符合国家密码管理部门要求的盖章、验章和信息解析服务。
- d) 带有电子印章的文件，其印章应支持在未联网、未连接智能密码钥匙状态下可见、可验。

5.3.4 档案管理

办公信息系统宜提供档案管理功能，基本要求如下。

- a) 符合国家档案管理要求和金融机构具体需求。
- b) 具备档案接收功能。
- c) 具备档案查询、借阅功能。
- d) 支持档案管理功能模块与其他业务系统衔接。

5.4 沟通协作类要求

5.4.1 通讯录

办公信息系统宜提供通讯录功能，基本要求如下。

- a) 支持通讯录的查询功能。
- b) 支持通讯录查询权限控制。
- c) 支持和邮件、人力、即时通讯等系统的信息同步。
- d) 支持用户自定义个人通讯录，提供排序、用户标签等功能。
- e) 宜具备限制用户批量复制通讯录信息的功能，防止通讯录被恶意复制转发。

5.4.2 邮件

办公信息系统宜提供邮件管理功能，具体宜包括邮件撰写、邮件显示、邮件处理和邮件报告4项基本功能，基本要求如下。

- a) 邮件撰写：系统宜给用户提供了编辑邮件的功能。

- b) 邮件显示：系统宜支持在计算机上显示邮件信息（包括来信包含的声音和图像）。
- c) 邮件处理：系统宜提供发送邮件、接收邮件等基本的对邮件进行处理的功能，具体包括以下内容。
- 系统宜具备邮件收取、邮件发送、邮件撤回、附件发送、邮件搜索、自定义邮件模板、邮件分类、邮件权限设置、邮件账号设置、邮箱后台管理等基础功能。
 - 收信人宜能按不同方式对来信进行处理，例如阅读后删除、存盘和转发，对于不愿意接收的信件可直接在邮箱中删除。
 - 宜具备与邮件系统相配套的可追溯、可审计的归档功能。
 - 宜支持邮件的数据安全、安全存储、反垃圾、防病毒、安全传输等。
 - 宜支持多客户端同步，支持与即时通讯系统之间的交互。
- d) 邮件报告：系统宜提供邮件服务器向发件人报告邮件传送情况的功能，例如发送成功、发送失败等。

5.4.3 即时通讯

办公信息系统宜在满足GB/T 22239—2019中关于数据安全、安全存储、安全传输等要求的基础上提供即时通讯功能，基本要求如下。

- a) 提供基本的文字交流、图片交流、语音交流、视频交流、文件交流功能。
- b) 支持单聊、群聊等会话模式。
- c) 支持多端消息同步，确保多端消息一致。
- d) 支持在线感知功能，支持查看在线状态。
- e) 支持系统可扩展，支持与邮件、会议等系统之间的交互。
- f) 支持数据共享，支持电子白板、屏幕截图、文档共享等数据共享手段，支持高效协同。
- g) 支持信息已读状态和未读状态的查询。

5.5 综合事务类要求

5.5.1 会议管理

办公信息系统宜提供会议管理功能，具备会议的会前、会中、会后的在线管理能力，具体要求如下。

- a) 会前管理宜具备：
 - 会务支持，包括发布会议通知、会议安排、预定会议室等功能。
 - 征集会议议题、议案、汇总、退回、回复意见、待办、催办推送等功能。
 - 会议材料起草、审批、会签、传阅、回复、归档等功能。
 - 会议材料上传、下载、分发到云文档或存储对象等功能。
 - 重要参会人对会议材料提醒、圈阅、批注、修订、预沟通等功能。
- b) 会中管理宜具备：
 - 远程会议室：音频传输、视频传输、共享屏幕等功能。
 - 现场会议室：电子桌签、电子会议材料系统等功能。
- c) 会后管理应具备：
 - 会议材料分类、归档功能。
 - 查询调阅历届会议资料（权限控制）功能。
 - 与会人员对会议议题逐项表决功能。

5.5.2 日程管理

日程管理宜满足以下要求。

- a) 支持日程的新增、修改、查询和删除。
- b) 支持日程编排冲突自动提醒。
- c) 支持日程的提醒。
- d) 对接机构内会议系统、邮件系统等主要办公系统，实现与重要事务的关联。

5.5.3 信息发布

信息发布宜满足以下要求。

- a) 根据金融机构的具体需求，明确信息发布的流程、内容和用户范围。
- b) 提供机构重要事务信息发布区，包含通知公告和重要新闻的发布、管理、查询和撤回的功能。
- c) 提供团队风采展示区、员工风采展示区。

6 非功能类要求

6.1 通用要求

办公信息系统应按照GB/T 37095—2018的要求进行设计和建设。系统应采用具有自主知识产权、适配金融业信息技术创新应用环境的软硬件产品，且避免与特定软硬件产品的依赖关系。

系统的部署环境（包括但不限于服务器硬件、操作系统、应用服务器中间件、数据库管理系统）、软件产品本身（包括但不限于自身使用的技术架构、第三方组件）、用户使用环境（包括但不限于终端硬件、操作系统、浏览器）应符合GB/T 37095—2018的要求，且应符合金融业信息技术创新应用的相关要求。

6.1.1 应用架构

办公信息系统在应用架构设计方面应考虑分层建设，从提升复用、降低耦合的角度出发，宜将系统划分为3层，包括业务产品层、业务基础层、技术基础层，具体内容如下。

- a) 业务产品层：主要负责与用户直接交互的各类办公业务场景，包含与具体业务密切相关的业务组件，例如电子公文、行政用印、会议管理等。
- b) 业务基础层：主要负责为用户直接交互的各类办公业务场景提供基础支撑，包含可支撑具体业务开展的通用性业务组件，例如人员管理、权限管理等。
- c) 技术基础层：主要负责不直接与用户交互的各类办公业务场景，支撑上层业务产品层与业务基础层组件运行并与办公业务无关的公共性、通用性技术组件。

6.1.2 性能容量

6.1.3 性能容量设计原则

在系统的设计阶段，应对系统的性能容量进行设计和评估，原则如下。

- a) 最优化原则：选择性能较优的技术方案，减少后续因性能容量问题导致的改造和维护，保证上线后系统的安全性、稳定性和高效性。
- b) 适度超前性原则：在评估中央处理器（CPU）和存储容量时，除了应分析系统本身变化引起的CPU和存储容量变化外，还应预估投产后的一段时间内业务量的增长对CPU和存储容量的影响。
- c) 一体化原则：对于批量作业性能的评估，应考虑批量作业执行窗口时间对联机性能的影响。
- d) 持续评估原则：定期或按实际运行表现对办公信息系统的性能容量进行评估。

6.1.4 性能容量设计要求

性能容量设计的过程应满足以下要求。

a) 性能设计要求应包括：

- 独立业务并发要求：核心业务中的某一业务在一定用户数并发访问时，响应时间在用户可接受范围内，且应用服务器的CPU、内存、输入/输出（I/O）均在正常值范围内。
- 组合业务并发要求：1个或多个模块的多个业务在一定用户数并发访问时，响应时间在用户可接受范围内，且应用服务器的CPU、内存、I/O均在正常值范围内。

b) 容量设计要求应包括：

- 用户容量：考虑在特定的环境下，系统能支持的在线用户数满足金融机构要求。
- 并发容量：考虑在特定的环境下，系统能支持并发用户数满足金融机构要求。
- 数据容量：考虑在特定的环境下，系统能支持关键业务数据量满足金融机构要求，包括流程模板数、流程实例数。

6.1.5 性能容量设计指标

性能容量设计指标宜参考下表。

表 性能容量设计指标

指标项	简要说明
响应时间	从客户端发起业务请求到收到服务端响应的整个过程所经历的时间，可分为客户端响应时间和服务端响应时间。
并发用户数	在同一时间段内系统所支持的访问用户数量。
吞吐量	反映单位时间内系统处理的用户请求的数量。
指令成功率	办公信息系统成功执行完指令的数量占发出总指令数的百分比。
服务器资源占用	反映在负载下系统的资源利用率。

6.1.6 可靠性

6.1.7 可靠性设计原则

根据系统访问量、恢复时间目标（RTO）及恢复点目标（RPO）要求，应设计不同的部署模式，不宜存在单点情况。对于单点部署的系统应具备健康监控、异常告警、数据备份等功能。高可用方案根据办公系统重要性等要求，可采取冷备、热备、多活等多种模式，例如金融机构内对于邮件和即时通讯软件的依赖较高，则宜将其部署为双活甚至多活的模式。

6.1.8 可靠性设计要求

办公信息系统的服务器因为各种原因失效时，其他正常工作部分应接管失效部分的任务，确保任务正常运行，系统应具有维持其功能的能力，可以快速切换保证业务的正常运行。可靠性设计的具体要求如下。

- a) 部署方式：办公信息系统应支持横向的应用服务器的扩展，形式包括集群部署、分布式部署等相关部署方式。
- b) 重试机制：办公信息系统应具备超时机和重试机制。超时机和重试机制可进行单独的设置，避免因超时或重试导致请求响应速度慢，以及请求堆积引发的系统无法正常处理等问题。
- c) 熔断机制：办公信息系统应具备熔断机制，当所依赖的服务恶化或者调用失败次数达到某个阈值时，系统应迅速熔断并立即切断当前服务或切换其他备用服务。

- d) 缓存机制：办公信息系统应具备缓存机制，对热点数据进行缓存，避免因大量请求查询数据库导致数据库服务堵塞、宕机。

6.1.9 日志规范

办公信息系统日志管理功能包含日志查询、导出等功能。日志规范具体要求如下。

- a) 内容规范：办公信息系统日志宜分为用户登录日志、用户操作日志、管理员登录日志、管理员操作日志、系统运行日志、系统错误日志等。具体日志可包括但不限于操作时间、网络地址、操作类型、操作主体、操作客体和操作结果，流程相关功能还可增加流程处理环节、处理时效等信息。
- b) 设计规范：日志可包含但不限于统一日志格式、日志输出分级、业务逻辑与日志解耦、业务数据与日志分离、关键事件定义、业务指标（请求量、成功率、延时等）、管理方案（存放时长、压缩备份等）。

6.2 安全要求

6.2.1 总体要求

安全管理整体应满足JR/T 0071—2020、JR/T 0255—2022的要求。

6.2.2 安全访问

办公信息系统安全访问应包括但不限于身份认证、访问控制、增强防护、权限分立。安全访问具体要求如下。

- a) 身份认证：用户身份认证应通过统一的身份认证管理系统，运维账号和密钥应进行统一管理。
- b) 访问控制：应建立安全的访问控制，防止匿名用户未授权访问。应禁止目录列表浏览，防止站点信息泄露和文件被未授权下载。受保护资源访问应对用户权限进行校验，防止水平越权和垂直越权操作。
- c) 增强防护：应充分考虑互联网访问安全管控设计及终端安全访问控制设计。
- d) 权限分立：应具备管理员权限分立功能，包含系统管理员、安全管理员、审计管理员的三员权限划分。

6.2.3 安全加密

办公信息系统安全加密应符合国家密码管理部门的相关要求，包括但不限于口令加密、传输加密、数据加密、文档加密。安全加密具体要求如下。

- a) 口令加密：用户口令应加密存储。系统能提供账户口令的更换周期控制，口令强弱度的校验等措施。
- b) 传输加密：对数据传输的过程进行加密处理，加密算法和签名算法应符合国家密码管理部门的要求。
- c) 数据加密：敏感数据、核心数据等应支持加密存储。
- d) 文档加密：用户文档应支持指定文件类型的文档加解密、权限管理。
- e) 展示水印：办公信息系统各类终端在展示各类信息时应有可唯一识别用户与终端的水印。

6.2.4 安全审计

安全审计应覆盖所有用户行为和安全事件。应采用日志审计方式记录每个用户行为并确保日志不被修改或未预期的删除。使用第三方组件和中间件时应定期进行安全检测，确保安全漏洞及时修复。

6.2.5 安全编码

系统开发过程应考虑以下安全编码要求。

- a) 校验信息：用户输入的信息需要被校验，校验内容应包括特殊字符、恶意代码等。防止SQL注入攻击、跨站脚本攻击（XSS）注入、脚本注入、缓冲区溢出等。
- b) 错误处理：应用系统应有统一的错误处理能力，在编码时应有效屏蔽系统技术错误信息，避免错误详情直接反馈到客户端。

6.3 运维要求

6.3.1 可用性

办公信息系统应减少停止操作、启动操作对服务的影响，系统停止操作时间、启动操作时间应控制在业务可允许的时间范围之内。

6.3.2 可维护性

系统建设应充分考虑对后续维护管理工作的支持，通过维护管理工作的开展能够保证应用系统满足持续健康提供服务的总体要求，例如建立全面的系统管理功能、友好的系统维护界面及充分详尽的日志信息等。

6.3.3 可扩展性

系统应具备灵活可扩展的架构设计，以应对需求变化对系统产生的变更影响，例如系统扩容时，不需要对系统架构进行变更，只做硬件扩容即可满足系统容量要求。

6.3.4 故障隔离设计

系统应设计有效的故障隔离机制，减少系统之间及本系统内部模块、服务之间的耦合性。当某服务出现故障时，应具备有效措施将故障对象隔离或者关闭，以保证系统其他功能不受影响。

6.3.5 管理台设计

系统的管理台功能应部署在单独的设备或者服务上。管理台功能应设置明确的权限级别，区分用户和技术人员的权限，对权限设置操作需要有详尽的操作记录。管理台账号应启用口令复杂度检查功能，初次登录后需要强制修改默认口令。管理台账号登录宜根据业务系统的等保等级，决定是否采用多因子登录，例如短信验证码、人脸识别、指纹识别等。

6.3.6 容错机制设计

应用系统应具备在紧急情况下针对应用程序的强制停止措施，并降低因强制停止应用产生的数据丢失的可能。

6.3.7 应急演练要求

每年宜组织主用系统与备份系统之间的应急切换演练。

6.4 监控要求

6.4.1 基础设施监控

应制定办公信息系统监控规范，明确监控范围和基础设施监控指标集，实现监控对象指标配置、告警规则实施和数据采集的自动化。数据采集应全面覆盖基础设施各项监控指标。宜实现监控智能化，通过告警聚合分析，实现精准故障定位。通过对监控数据的趋势及故障影响分析，实现故障预警和自愈。

6.4.2 系统可用性监控

应根据金融机构自身系统可用性要求进行监控、分析和度量，及时发现影响系统可用性的问题和隐患，能够通过短信、邮件等方式对管理员发出告警，方便进行及时处置，并落实自动化恢复手段，缩短故障恢复时间。

应定期组织对监控失效、应急处置不当、软硬件基础设施故障、高可用失效等影响系统可用性服务交付的问题进行分析并优化。

6.4.3 应用性能监控

应对系统交易量、成功率、每秒交易率、响应时间等指标进行监控，满足办公信息系统的日常运行和高峰需要，实现资源弹性供给、自动扩充或收缩容量，兼顾资源利用效率的情况下，有效控制风险与成本。

参 考 文 献

- [1] JR/T 0207—2021 金融信息系统多活技术规范 术语
-