

ICS 03.060

CCS A 11

Q/BSX

绍兴银行股份有限公司企业标准

Q/BSX 0001-2026

金融信创产品兼容及安全性标准

Financial Information Technology Application Innovation Product

Compatibility and Security Standard

2026-09-22 发布

2026-09-22 实施

绍兴银行股份有限公司发布

目 次

前 言 2

引 言 3

1 范围 4

2 规范性引用文件 4

3 术语和定义 4

4 总体原则与要求 5

5 信创产品技术架构标准 6

6 兼容性技术要求 7

7 安全性技术要求 8

8 适配验证与测试规范 9

9 成熟度评估体系 10

10 实施与监督 10

附录 A（规范性）信创产品分类与代码 11

附录 B（规范性）适配验证测试用例库 12

附录 C（规范性）安全性评估检查表 14

前 言

本文件依据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》起草。

本文件是绍兴银行股份有限公司金融信创标准体系的核心标准，旨在落实金融业信息化核心技术安全可控战略要求，推进信息技术应用创新（信创）在金融领域的标准化、规范化应用。

本文件由绍兴银行股份有限公司金融科技部提出并归口。

——本次为第一次发布。

引 言

编制目的

为贯彻落实《国家标准化发展纲要》关于推进金融业信息化核心技术安全可控标准建设的部署要求，系统推进金融信息技术创新业务约束、技术接口、适配验证、研发测试、成熟度评估等标准体系建设，特制定本标准。

本标准旨在： a) 规范银行信创产品的技术架构，支持构建分布式和集中式并存的双核架构格局； b) 统一信创产品的兼容性要求，确保与现有金融基础设施的互联互通； c) 强化信创产品的安全性防护，健全金融网络安全与数据安全标准体系； d) 建立科学的适配验证与成熟度评估机制，为信创建设提供操作指导。

标准定位

本标准属于绍兴银行企业标准，适用于本行及所属各级机构在信创产品规划、选型、开发、测试、部署、运维全生命周期的标准化管理。

金融信创产品兼容及安全性标准

1 范围

本文件规定了绍兴银行信息技术应用创新（信创）产品的技术架构、兼容性、安全性、适配验证、成熟度评估等技术要求和管理规范。

本文件适用于： a) 绍兴银行核心业务系统、一般业务系统、办公管理系统的信创化建设与改造； b) 金融机具（含智能终端、自助设备、支付终端等）的信创选型与部署； c) 基础软硬件（含服务器、操作系统、数据库、中间件、办公软硬件等）的采购与使用； d) 信创产品的研发测试、适配验证、成熟度评估和持续改进。

本文件不适用于： a) 非金融业务系统的信息技术应用； b) 境外金融机构的信息技术系统。

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 25000.51—2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE）第 51 部分：就绪可用软件产品（RUSP）的质量要求和测试细则

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

JR/T 0071—2020 金融行业网络安全等级保护实施指引

JR/T 0154—2017 人民币现金机具鉴别能力技术规范

JR/T 0199—2020 金融科技创新安全通用规范

JR/T 0214—2021 金融数据安全 数据安全分级指南

JR/T 0223—2021 金融信息系统适配验证技术规范

JR/T 0231—2021 银行业第三方软件开发工具包（SDK）安全接入指南

JR/T 0258—2022 金融数据安全 数据生命周期安全规范

3 术语和定义

下列术语和定义适用于本文件。

3.1 信息技术应用创新 information technology application innovation; ITAI

基于国产芯片、操作系统、数据库、中间件等基础软硬件，开展信息系统规划、建设、应用和运维，实现金融业信息化核心技术安全可控的创新实践活动。

注：简称“信创”。

3.2 信创产品 ITAI product

符合信息技术应用创新要求，采用国产化核心技术，满足金融行业业务需求和安全标准的信息技术产品。

注：包括硬件产品（如服务器、金融机具）、软件产品（如操作系统、数据库、业务软件）以及软硬件一体化产品。

3.3 适配验证 adaptation verification

通过技术测试和业务验证，确认信创产品与银行现有业务系统、技术平台、数据环境的兼容性、功能性和性能符合性的过程。

3.4 双核架构 dual-mode architecture

信息系统同时支持传统集中式架构和信创分布式架构的技术格局，两种架构并存互补、协同运行、渐进迁移的系统架构模式。

3.5 安全可控 security controllable

信创产品在技术、供应、运维等方面具备自主管理能力，安全风险可识别、可防范、可控制，不受单一外部主体制约的状态。

4 总体原则与要求

4.1 基本原则

4.1.1 安全可控原则

信创产品应满足安全可控要求，核心技术自主可控，供应链安全可靠，符合国家金融安全战略。

4.1.2 兼容并存原则

信创系统应与传统系统兼容并存，支持双核架构格局，确保业务连续性，实现平稳过渡。

4.1.3 标准引领原则

以标准化引领金融业数字生态建设，推动金融科技标准实施，确保信创建设质量。

4.1.4 持续改进原则

建立信创产品成熟度评估机制，持续优化技术架构，提升产品性能和安全水平。

4.2 总体要求

信创建设应满足以下要求：

- a) 业务连续性：信创改造不得影响核心业务正常运行，应具备完善的回退机制和应急预案；
- b) 数据完整性：数据迁移过程应确保数据完整、准确、一致，满足金融数据要素标准要求；
- c) 安全合规性：符合网络安全等级保护、密码应用、数据安全等监管要求；
- d) 性能可靠性：信创系统处理能力、响应时间、并发性能应不低于被替代系统；
- e) 运维可管理性：具备完善的监控、运维、故障处理能力，满足智能运维标准要求。

5 信创产品技术架构标准

5.1 架构技术要求

5.1.1 架构定位

构建分布式与集中式并存的双核架构格局： a) 集中式核心：保留传统核心业务系统的稳定性和事务处理能力； b) 分布式信创核心：新建系统优先采用分布式信创架构，具备弹性扩展能力。

5.1.2 架构协同

双核架构应满足以下协同要求： a) 数据层统一：采用统一的数据标准和数据交换格式； b) 服务层互通：通过标准化接口实现服务调用和业务协同； c) 渠道层整合：对外提供统一的客户服务渠道，屏蔽后端架构差异。

5.2 核心技术组件标准

5.2.1 服务器端技术

信创服务器应满足： a) 采用国产 CPU 架构（如 ARM、C86 等），支持多路互联； b) 支持国产操作系统（如麒麟、统信 UOS 等）； c) 具备高可用集群能力，支持负载均衡和故障自动切换； d) 性能指标应满足银行业务峰值处理需求。

5.2.2 终端技术

信创终端应满足： a) 支持国产操作系统和浏览器； b) 具备国密算法支持能力； c) 与办公系统、业务系统、外设（打印机、读卡器等）兼容适配； d) 支持统一身份认证和终端安全管理。

5.3 业务系统标准

5.3.1 系统分类

核心业务系统信创改造应分阶段实施： a) 账务核心：最后实施信创改造，确保账务准确性和稳定性； b) 产品服务层：优先实施信创改造，支持产品快速创新； c) 渠道接入层：同步实施信创改造，支持多渠道统一接入。

一般业务系统、办公管理系统应结合信息化建设规划，统筹推进信创适配改造工作。

5.3.2 技术要求

核心业务系统应满足： a) 支持高可用部署，满足灾备体系标准； b) 交易处理具备原子性、一致性、隔离性、持久性； c) 支持弹性伸缩，应对业务高峰； d) 具备完善的日志审计和可追溯能力。

一般业务系统、办公管理系统，参考上述要求执行，根据系统重要等级、业务风险等级合理确定技术指标。

6 兼容性技术要求

6.1 业务约束标准

6.1.1 业务流程兼容性

信创产品应： a) 支持现有全部业务流程，不得改变业务规则和业务逻辑； b) 支持与现有外围系统的业务交互，保持接口契约一致； c) 支持业务参数的灵活配置，适应不同场景需求。

6.1.2 数据格式兼容性

信创产品应： a) 支持标准数据格式（JSON、XML 等）的解析和生成； b) 支持金融行业通用报文库标准，确保报文格式兼容； c) 支持数据编码标准（UTF-8、GB18030 等）。

6.2 技术接口标准

6.2.1 接口规范

信创系统接口应符合： a) 采用 RESTful API 或 gRPC 等标准协议； b) 接口定义遵循 OpenAPI 规范； c) 支持 JSON Schema 数据校验； d) 接口版本管理遵循向后兼容原则。

6.2.2 数据交换标准

信创系统数据交换应满足： a) 支持实时同步和批量交换两种模式； b) 支持数据压缩和加密传输； c) 支持断点续传和失败重试机制； d) 数据交换延迟应满足业务时效性要求。

6.3 软硬件适配标准

6.3.1 基础软硬件适配

信创产品应明确适配的： a) CPU 架构（如鲲鹏、飞腾、海光等）； b) 操作系统版本（如麒麟 V10、统信 UOS V20 等）； c) 数据库版本（如达梦、OceanBase 等）； d) 中间件版本（如东方通、宝兰德等）。

6.3.2 金融机具适配

金融机具信创产品应满足： a) 符合金融机具标准； b) 支持国产操作系统和驱动； c) 与银行核心业务系统、支付系统无缝对接； d) 具备固件升级和安全防护能力。

7 安全性技术要求

7.1 网络安全标准

7.1.1 等级保护要求

信创系统应满足： a) 符合网络安全等级保护要求； b) 通过相应等级的测评并获得备案证明； c) 关键信息基础设施应满足增强保护要求。

7.1.2 安全区域划分

信创系统网络应： a) 按业务功能和安全等级划分安全域； b) 实施严格的访问控制和边界防护； c) 部署入侵检测、流量监控等安全设施。

7.2 数据安全标准

7.2.1 数据分级分类

信创系统数据应进行分级分类： a) 识别核心数据、重要数据和个人信息； b) 实施差异化的安全保护策略； c) 重要数据应实施加密存储和传输。

7.2.2 数据生命周期安全

信创系统数据全生命周期应满足要求： a) 数据采集：明确采集目的，获得用户授权； b) 数据传输：采用 TLS 1.2 以上协议或国密 SSL 协议； c) 数据存储：敏感数据加密存储，密钥分离管理； d) 数据使用：实施脱敏处理，控制使用范围； e) 数据销毁：彻底删除，不可恢复。

7.3 密码应用标准

7.3.1 密码算法要求

信创产品应支持： a) SM2、SM3、SM4 等国密算法； b) RSA、AES 等国际算法（用于兼容过渡期）； c) 优先采用国密算法，逐步替代国际算法。

7.3.2 密码应用要求

信创系统密码应用应符合： a) 采用经认证的商用密码产品； b) 实施密钥全生命周期管理； c) 定期进行密码应用安全性评估。

7.4 安全运营标准

7.4.1 安全运营中心建设

建设信创安全运营中心： a) 统一采集信创系统安全日志； b) 实施 7×24 小时安全监控； c) 具备威胁情报分析和应急处置能力。

7.4.2 漏洞管理

信创产品应建立漏洞管理机制： a) 定期开展漏洞扫描和渗透测试； b) 及时修复高危漏洞； c) 建立供应链安全审查机制。

8 适配验证与测试规范

8.1 适配验证流程

8.1.1 验证阶段

信创产品适配验证分为三个阶段： a) 实验室验证：在测试环境完成功能、性能、兼容性测试； b) 准生产验证：在准生产环境完成压力测试和业务仿真； c) 生产验证：在生产环境灰度发布，逐步扩大范围。

8.1.2 验证内容

适配验证应包括： a) 功能一致性验证：信创功能与原系统功能一致； b) 性能基准验证：满足业务性能基准要求； c) 兼容性验证：与周边系统、软硬件环境兼容； d) 安全性验证：通过安全测试和漏洞扫描。

8.2 研发测试标准

8.2.1 测试类型

信创产品研发测试应包括： a) 单元测试：代码级功能验证； b) 集成测试：模块间接口和交互验证； c) 系统测试：端到端业务流程验证； d) 验收测试：用户场景和合规性验证。

8.2.2 测试工具

信创测试应采用标准化工具： a) 自动化测试平台，支持测试用例管理和执行； b) 性能测试工具，支持高并发模拟； c) 安全测试工具，支持漏洞扫描和渗透测试； d) 兼容性测试工具，支持多环境适配验证。

8.3 测试用例管理

测试用例应按照附录 B 进行标准化管理： a) 建立信创测试用例库，覆盖核心业务场景； b) 测试用例与需求、缺陷关联管理； c) 定期更新测试用例，适应业务变化。

9 成熟度评估体系

9.1 评估模型

9.1.1 成熟度等级

信创产品成熟度分为五个等级： a) 初始级（L1）：产品基本可用，存在明显缺陷； b) 已管理级（L2）：产品功能完整，性能基本满足要求； c) 已定义级（L3）：产品标准化程度高，文档齐全； d) 量化管理级（L4）：产品具备量化管理能力，质量可控； e) 优化级（L5）：产品持续优化，达到行业领先水平。

9.1.2 评估维度

成熟度评估应覆盖以下维度： a) 技术能力：架构先进性、性能指标、扩展性； b) 产品质量：功能完整性、可靠性、安全性； c) 工程能力：开发规范、测试覆盖、文档质量； d) 服务能力：技术支持、运维保障、持续改进。

9.2 评估方法管理

9.2.1 评估流程

成熟度评估应遵循以下流程： a) 自评：供应商依据标准进行自评，提交评估报告； b) 第三方评估：委托具备资质的机构进行独立评估； c) 现场评估：评估团队现场核查和测试； d) 评估确认：银行方确认评估结果，决定是否准入。

9.2.2 评估报告管理

评估报告应包括： a) 评估依据和方法； b) 评估发现和建议； c) 成熟度等级评定； d) 改进措施和跟踪计划。

9.3 持续改进机制

信创产品应建立持续改进机制： a) 定期复评，监控成熟度变化； b) 根据评估结果制定改进计划； c) 重大版本升级需重新评估。

10 实施与监督

10.1 实施要求

10.1.1 实施计划

制定信创标准实施计划： a) 明确实施范围、时间表和责任人； b) 分阶段、分批次推进信创改造； c) 建立实施保障机制，确保资源投入。

10.1.2 培训与宣贯

应开展信创标准培训： a) 技术人员掌握标准技术内容； b) 管理人员理解标准管理要求； c) 供应商明确标准准入条件。

10.2 监督检查

10.2.1 内部审计

定期开展信创标准执行审计： a) 检查标准执行情况； b) 识别标准实施偏差； c) 督促整改落实到位。

10.2.2 合规评估

定期进行合规评估： a) 评估信创产品符合性； b) 评估标准体系有效性； c) 提出标准改进建议。

10.3 标准更新

本标准应根据以下情况及时更新： a) 国家金融信创政策调整； b) 监管要求发生变化； c) 技术发展趋势要求； d) 实施中发现重大问题。

附录 A（规范性）信创产品分类与代码

A.1 分类原则

信创产品按照技术层次和应用领域分类，采用层次编码法。

A.2 分类代码表

表格

大类代码	大类名称	中类代码	中类名称	小类代码	小类名称
10	基础硬件	11	计算设备	111	信创服务器
				112	信创终端
				113	金融机具
		12	存储设备	121	信创磁盘阵列
				122	信创备份设备

大类代码	大类名称	中类代码	中类名称	小类代码	小类名称
20	基础软件	21	操作系统	211	服务器操作系统
				212	桌面操作系统
		22	数据库	221	关系型数据库
				222	分布式数据库
		23	中间件	231	应用服务器
				232	消息中间件
30	应用软件	31	核心业务系统	311	核心账务系统
				312	支付清算系统
		32	渠道系统	321	手机银行
				322	网上银行
		33	管理系统	331	风险管理
				332	合规管理
40	安全产品	41	密码产品	411	加密机
				412	签名验签服务器
		42	安全防护	421	信创防火墙
				422	信创入侵检测

附录 B（规范性）适配验证测试用例库

B.1 功能性测试用例

B.1.1 业务功能测试（示例）

表格

用例编号	用例名称	测试目的	测试步骤	检查结果
F-001	账户开立	验证信创核心开户功能	1. 录入客户信息 2. 提交开户申请 3. 系统处理 4. 查询账户状态	☐ 通过 ☐ 不通过
F-002	转账汇款	验证信创支付功能	1. 发起转账交易 2. 系统处理 3. 接收方确认	☐ 通过 ☐ 不通过
F-003	账户查询	验证信创环境下账户信息查询功能	1. 输入账号/客户号发起账户查询 2. 查看返回账户信息	☐ 通过 ☐ 不通过

B. 2 性能测试用例

B. 2. 1 并发性能测试（示例）

表格

用例编号	用例名称	测试场景	检查结果
P-001	登录并发	用户集中登录	☐ 通过 ☐ 不通过
P-002	交易并发	高峰期交易处理	☐ 通过 ☐ 不通过
P-003	账户查询并发	多用户同时发起账户余额查询	☐ 通过 ☐ 不通过

B. 3 兼容性测试用例

B. 3. 1 软硬件兼容性测试（示例）

表格

用例编号	测试项	测试环境	测试步骤	检查结果
C-001	国产 CPU 适配	鲲鹏+麒麟 V10	1. 部署系统	☐ 通过 ☐ 不通过

用例编号	测试项	测试环境	测试步骤	检查结果
			2. 执行业务操作	
C-002	国产数据库适配	达梦 V8	1. 数据库迁移 2. 数据读写测试	☐ 通过 ☐ 不通过
C-003	国产中间件适配	东方通 V7	1. 中间件迁移 2. 中间件性能测试	☐ 通过 ☐ 不通过

附录 C（规范性） 安全性评估检查表

C.1 网络安全检查表（示例）

表格

检查项	检查内容	检查方法	合规标准	检查结果
区域划分	是否按安全等级划分安全域	查看网络拓扑图	GB/T 22239	☐ 符合 ☐ 不符合
访问控制	是否实施严格的访问控制策略	检查防火墙规则	JR/T 0071	☐ 符合 ☐ 不符合
入侵检测	是否部署入侵检测系统	检查安全设备	GB/T 22239	☐ 符合 ☐ 不符合

C.2 数据安全检查表（示例）

表格

检查项	检查内容	检查方法	合规标准	检查结果
数据分级	是否完成数据分级分类	查看数据资产清单	JR/T 0214	☐ 符合 ☐ 不符合
加密存储	敏感数据是否加密存储	检查数据库配置	JR/T 0258	☐ 符合 ☐ 不符合

检查项	检查内容	检查方法	合规标准	检查结果
脱敏处理	非生产环境数据是否脱敏	检查测试数据	JR/T 0258	☐ 符合 ☐ 不符合

C.3 密码应用检查表（示例）

表格

检查项	检查内容	检查方法	合规标准	检查结果
算法合规	是否使用国密算法	检查加密配置	GB/T 39786	☐ 符合 ☐ 不符合
密钥管理	密钥是否安全托管	检查密钥管理系统	GB/T 39786	☐ 符合 ☐ 不符合
密评报告	是否通过密码应用安全性评估	查看评估报告	GB/T 39786	☐ 符合 ☐ 不符合