Q/GUOSEN

国 信 证 券 股 份 有 限 公 司 企 业 标 准

Q/GUOSEN-ENG-ARI 02-2024

柜面业务智慧运营建设标准

2024-10-30 发布 2024-11-01 实施

国信证券股份有限公司 发布

前　　言

本标准依据《JR/T 0173—2020 银行业集中营运规范》中规定进行编制，并参考 GB/T22239-2019《信息安全技术网络安全等级保护基本要求》、JR/T 0171—2020《个人金融信息保护技术规范》相关要求。

本标准于 2024 年 10 月初次起草发布，11 月首次实施，在编制过程中得到各位同仁的大力支持，在此表示感谢！由于编制时间紧促，难免有遗漏之处，恳请广大参阅者多提高贵意见，以供参考校正。

本标准由国信证券股份有限公司提出。

本标准起草单位：国信证券股份有限公司。

本标准主要起草人：吴士荣、李锋、陈士忠、韩勉霞、张奥博。

本标准于 2024 年 11 月首次发布。

1 范围

本标准规定了柜面业务智慧运营建设的标准规范，包括柜面业务运营标准、柜面业务系统管理标准、柜面业务数据管理标准、柜面业务服务创新要求标准等内容。

本标准适用于国信证券柜面业务智慧运营建设的标准规范。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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。

（1）GB/T22239-2019《信息安全技术网络安全等级保护基本要求》

（2）JR/T 0171—2020《个人金融信息保护技术规范》

3 术语和缩略语

国信证券柜面业务智慧运营建设名词条解释。

表 1 术语说明

术语、缩略	解释
柜面业务	证券公司在营业网点为客户提供账户开立、证券买卖、资金存取、信息查询、投资咨询等业务服务。
智慧运营	运用人工智能、大数据、RPA 等先进技术来提高证券柜面业务运营的效率、安全性和便利性的一种运营模式。

4 柜面业务运营标准

4.1 柜面业务分类标准

表 2 柜面业务分类标准内容

业务分类	业务定义	标准要求描述
管理模式	指柜面业务采用的运营模式。	柜面业务的运营模式包括总部集中审核和区域中心集中审核模式。各渠道终端受理的业务通过集中作业中心统一分发给总部和区域中心进行业务办理。
组织架构	指负责柜面业务的所有相关部门。	柜面业务的组织架构包括集中运营总部、系统运行总部、金融科技总部、技术管理部。集中运营总部负责统筹柜面业务的所有事项；系统运行总部保障柜面业务所涉及系统的正常运行；金融科技总部提供柜面业务数字化、智能化的能力支持；技术管理部负责柜面业务系统建设的研发管理规范。
人员岗位	指从事柜面业务的人员分	柜面业务的人员岗位有业务受理岗、业务

	配。	审核岗、业务质检岗等。

4.2 柜面业务流程标准

表 3　柜面业务流程标准内容

业务大类	业务小类	业务定义	标准要求描述
服务准入	客户识别	指客户办理柜面业务对客户身份进行识别。	支持系统内和系统外客户身份识别，同时支持读卡识别和手动录入识别两种识别方式。
	客户准入	指客户办理柜面业务对客户准入条件进行检查。	根据系统后台配置规范性检查项，对客户办理业务进行一系列的准入项检查。
	资质检查	指客户办理柜面权限业务对客户资质进行检查。	根据系统后台配置规范性检查项，对客户办理业务所要求的资质项进行检查。
业务受理	客户业务讲解	指客户临柜办理业务双录时进行业务讲解。	根据系统后台配置的双录话术，针对客户办理业务进行相应业务的讲解。
	业务风险说明	指客户临柜办理业务双录时进行风险告知。	根据系统后台配置的双录话术，针对客户办理业务进行相应风险内容的解读。
	客户信息录入	指客户临柜办理业务时，检查信息录入是否完整。	根据后台规则配置必填项、选填项、以及逻辑关系，检查客户信息录入是否完整，勾稽关系是否正确。
	客户资料收集	指客户临柜办理业务时上传影像类资料。	根据系统后台配置影像节点和影像模版，要求客户上传相关影像类资料。
	客户服务签署	指客户临柜办理业务时签署电子协议。	根据系统后台配置协议节点和协议模版信息，要求客户签署相关协议。
业务审核	审核内容	指柜面业务受理提交后，审核人员审核提交内容。	审核人员对业务受理端提交的客户信息、影像资料、业务检查等信息进行人工审核，确保信息准确性和完整性。
	审核处理	指柜面业务受理提交后，审核人员进行审核并出具审核意见。	经审核，若提交信息和材料不符合业务要求，需驳回受理岗重新处理；经审核通过后方可执行后续流程。
业务抽检	业务抽检	指集中运营总部针对办理完结的业务进行质量检	根据后台配置抽检规则进行抽

		查。	检。

4.3 柜面业务智慧运营场景标准

表 4　柜面业务智慧运营场景标准内容

业务大类	业务小类	业务定义	标准要求描述
业务智能化	智能服务模式	指通过运用一系列先进的技术手段，对柜面业务进行智能化改造和升级。	a）同时支持多种业务场景的在线办理和远程办理； b）实现业务流程的自动化处理，减少人工干预和错误率。
	功能	指智能化业务在业务处理、风险防范等方面的功能。	a）在业务处理方面支持多渠道业务的在线办理和远程办理，满足不同客户的需求； b）具备自动任务机制和后台批量任务跑批能力，提供实时的风险监控和应急预案，确保各业务运营的安全性和稳定性。
	安全	指在数据安全、身份认证等方面具备的安全特性。	a）具备完善的数据备份和恢复机制，防止数据丢失或损坏； b）采用身份核验、人脸识别、OCR 识别、语音识别等智能技术确保客户身份的真实性和合法性。
	应用	指智能化服务在系统兼容性、易用性和维护性等方面应满足的要求。	a）支持 windows 系统下多种类型的 PC 设备； b）系统具备简洁明了的操作界面，并为用户提供详细的用户使用手册； c）系统支持不停服升级，支持 7x24 小时一线服务，在线解决客户在业务办理过程中的问题。

5　柜面业务系统管理标准

5.1 客户信息管理标准

表 5　客户信息管理标准内容

业务分类	业务定义	标准要求描述
收集个人信息合	指柜面业务受理客户资料时应具有	a)不以欺诈、诱骗、误导的方式收集个人信息；

法性	合法性。	b) 不隐瞒产品或服务所具有的收集个人信息的功能； c) 不从非法渠道获取个人信息。
个人信息的展示限制	指客户信息对外展示时采取的一系列限制措施。	涉及通过界面展示个人信息的（如显示屏幕、纸面），个人信息控制者宜对需展示的个人信息采取去标识化处理等措施，降低个人信息在展示环节的泄露风险。例如，在个人信息展示时，防止内部非授权人员及个人信息主体之外的其他人员未经授权获取个人信息。
安全策略管理要求	指在确保客户信息在收集、存储、使用、传输直至销毁的各个阶段都得到充分保护。	安全基本原则：金融业机构应遵循“权责一致、目的明确、选择同意、最少够用、公开透明、确保安全、主体参与”的原则，设计并实施覆盖个人金融信息全生命周期的安全保护策略。 数据安全策略：应依据国家与行业主管和监管部门要求，结合机构自身风险管控策略和偏好、安全建设预算等因素，制定本机构数据安全总体安全策略、方针、目标、原则。 数据分级规程：应制定本机构数据分级规程，识别并维护本机构数据资产清单，并标注相应的数据级别。 数据安全管理制度：应制定数据安全管理制度及实施细则并定期评价更新，确保基于数据分级的数据安全制度体系覆盖机构数据全生命周期。 数据脱敏技术规范：明确不同安全级别数据脱敏规则、脱敏方法和脱敏数据的使用限制，配置脱敏数据识别和脱敏效果验证服务组件或技术手段。 密码使用和密钥管理：建立合理、统一的密码使用和密钥管理技术规范和制度。 第三方机构管理：建立第三方机构管理制度，并至少满足相关要求，包括对第三方机构的监督和安全检查评估。 日志记录与审计：应对数据生命周期全过程进行日志记录并开展以数据为中心的安全审计，对日志进行统一管理和处理，建立并执行审计策略。 检查评估：金融业机构定期或不定期开展数据安全相关检查和评估，包括合规审查、安全巡检、安全评估等方面。

5.2 系统运行标准

表 6　系统运行标准内容

业务分类	业务定义	标准要求描述
PAD 终端和 H5 终端应用安全要求	指 Web 应用程序在安全运行中的相关标准。	涉及 C2、C3 类别信息的 Web 应用的安全技术要求如下： a)应具备对网站页面篡改、网站页面源代码暴露、穷举登录尝试、重放攻击、SQL 注入、跨站脚本攻击、钓鱼、木马以及任意文件上传、下载等已知漏洞的防范能力； b)处理个人金融信息相关的 Web 应用系统与组件上线前应进行安全评估； c)应具备对处理个人金融信息的系统组件进行实时监测的能力，有效识别和阻止来自内外部的非法访问。
安全管理制度体系	指外包服务机构与外部合作机构在安全管理制度方面的管理规范。	建立外包服务机构与外部合作机构管理制度，包括但不限于： a)对个人金融信息生命周期过程中相关的外包服务机构与外部合作机构进行审查与评估，评估其个人金融信息的保护能力是否达到国家、行业主管部门与金融业机构的要求；应通过协议或合同的方式，约束外包服务机构与外部合作机构不应留存 C2、C3 类别信息；对于 C2 类别信息中的支付账号等信息，若因清分清算、差错处理等业务需要确需留存，金融业机构应明确其保密义务与保密责任，并应根据安全要求落实安全控制措施，并将有关资料留档备查；对可能访问个人金融信息的外包服务机构、外部合作机构及其人员，金融业机构应要求外包服务机构与外部合作机构向有关人员传达个人金融信息保护安全要求，与其签署保密协议，并对协议履行情况进行监督； b)不将存储个人金融信息的数据库交由外部合作机构运维； c)定期对外包服务机构与外部合作机构的个人金融信息保护措施落实情况进行确认，确认的方式包括但不限于外部信息安全评估、现场检查等； d)国家法律法规与行业主管部门另有规定的，按照相关要求执行。
		a)多活技术架构：采用两地三中心部署，支持多活架构，重要数据和业务逻辑应实现容灾备份，确保在灾难发生时能够迅速恢复业务； b)数据库管理工具：应支持 Chat2DB、Datagrip、

数据库部署管理	指数据库部署管理的相关策略，旨在确保数据库的高效运行、数据安全和系统稳定性。	Navicat Premium 和 DBeaver 等数据库管理工具； c)数据库部署方式：应通过数据库分片、主从复制或数据库集群等方式实现分布式部署，以提高读取性能、负载均衡和故障恢复； d)数据库存储：采用 S3 存储，以提供卓越的可扩展性、高数据可用性、严密安全性及高效性能的对象存储服务。
柜面终端管理	指确保网站在上线后能够持续稳定地提供服务，同时不断优化以满足用户需求和业务目标。	a)监控和日志分析：应使用如 Nagios、Zabbix、New Relic 等工具监控网站性能和服务器状态； b)性能调优：根据监控数据，对服务器、数据库和应用程序进行性能调优； c)故障响应和恢复：建立快速响应机制，对系统故障进行处理； d)安全维护：定期更新软件和插件，修补安全漏洞，使用 WAF 等工具来防止网络攻击； e)数据备份与保护：定期备份数据，测试备份恢复流程，确保在需要时能够迅速恢复数据。
客户信息管理与监测	指系统运行时对客户信息进行管理与监测，确保客户信息安全和隐私得到妥善保护。	a)客户信息的监测与审计：应建立客户档案，并编制客户一览表供查阅； b)数据安全性：保护客户数据不被泄露或篡改，采用数据加密技术，如 SSL/TLS 加密，以及数据库加密，确保数据在传输和存储过程中的安全； c)客户信息识别与交易记录保存：应采取必要的措施，采集、记录、存储、报送与客户身份识别有关的信息。

5.3 系统性能与质量标准

表 7　系统性能与质量标准内容

指标大类	指标分类	指标定义	标准要求描述
性能指标	模块可延伸性	指系统在面对不断变化的负载需求时的适应能力。	可通过增加节点的资源提升性能，模块功能支持应用服务器集群、缓存集群、数据库集群等拆分和合并。
	服务可伸缩性	指系统能够适应不断变化的负载和用户需求的能力。	通过负载均衡、分布式计算和弹性伸缩等技术实现服务可伸缩性。
			a)高可用性：配置数据库的高可用性策略，确保数据库在故障发生时，能够快速恢复并继续提供服；

	数据库稳定性	指数据库在各种条件下保持高可靠性、高可用性和高性能的能力。	b)采用高可用架构：通过主从复制、集群和负载均衡等技术，确保系统在单点故障或网络中断的情况下仍能正常运行； c)数据库复制和分片：数据库复制和分片可以提高数据库的可伸缩性和可用性，从而增强数据库的稳定性。
访问性能指标	访问速度	指用户访问系统时所感受到的响应速度。	页面加载时延控制在 500ms 以内。
	吞吐量	指系统在单位时间内能够成功处理的数据量或请求数。	支持不少于 1000 笔/秒的并发处理。
	系统容量	指在最大负载状态下或某项指标达到所能接受的最大阈值时，系统对请求的最大处理能力。	支持不少于 100000 笔/日的处理能力，并支持弹性扩缩容。
质量指标	可测试性	指涉及到软件在测试过程中的难易程度，以及发现和修复缺陷的效率。	可测试性高的原则：具备高内聚、低耦合、接口定义明确、行为意图清晰的设计。
	数据备份	指将文件系统或数据库系统中的数据复制到其他存储介质的过程。	系统采用数据库同步机制，并建立了双库备份系统。
	容灾能力	指在发生自然灾害、硬件故障、人为操作错误等灾难事件时，信息系统能够快速恢复业务运行的能力。	应建设至少 3 个机房，其中包含 1 个生产机房，2 个灾备机房，提高容灾能力。

5.4 系统使用技术标准

表 8　系统使用技术标准内容

业务大类	业务分类	业务定义	标准要求描述
系统运行环境	开发技术	指共同支持着系统的正常运行和持续迭代的开发技术。	应考虑编程语言、框架、容器化/编排、前端技术、后端技术等。
	框架选型	指框架选型需要考虑多个因素以确保框架的适用性和系统性能的最优化。	框架应成熟稳定、高效开发、良好性能、易于维护、跨平台能力、兼容性、安全性等。
	服务器选型	指服务器选型应考虑多个因素以确保服务器性能与可扩展性、可靠性和可用性等。	应满足信创要求，采用鲲鹏 920 服务器。

	中间件选型	指中间件选型时考虑多个因素以确保中间件的适用性和系统的稳定性。	应满足信创要求，采用东方通等中间件。
开发管理	设计文档管理	指确保团队协作顺畅、项目进度可控、文档版本一致的文档管理工具。	应统一文档需求编号，实现版本管理，文档支持多人共享和协作等。
	日志管理	指日志数据的收集、存储、分析和可视化的管理过程。	应合理配置日志级别、实现日志轮转和存储、设置日志访问权限、保障日志的安全性、日志集中管理和监控分析。
	部署管理	指将开发完成的软件应用安全、高效地部署到生产环境中的管理过程。	应支持两地三中心部署，支持日志、业务数据可监控，并提供标准格式，支持对接 S3 存储，支持 simba 流水线持续发布。

5.5 网络安全标准

表 9　网络安全标准内容

业务分类	业务定义	标准要求描述
互联网管理	指有效管理互联网环境中的安全风险，确保客户信息的安全和隐私得到保护的标准。	a)网络安全工具：应使用网络安全工具进行网络封包分析、漏洞攻击、网络扫描、无线网络密钥破解、入侵防御系统和系统漏洞扫描； b)安全策略：制定全面的网络安全策略，包括访问控制、数据保护、网络安全、事件响应和合规性等方面； c)监控和审计：施持续的监控和审计，使用工具如 Splunk 进行日志收集和分析，及时发现和响应安全事件。
代码管理	指代码存储、版本控制、质量保证、集成与部署的标准流程及最佳实践。	a) 应采用 Git 等版本控制系统对代码进行版本管理; b) 版本控制系统应记录代码的修改历史、作者、时间等，便于追踪和回溯； c) 采用合理的分支管理策略，分支的创建、合并和删除遵循一定的规范和流程。
口令管理	指创建、存储、使用和更新口令的一系列策略和实践。	a)SSO 单点登录和 MFA 多因素身份验证相结合：通过 SSO 机制进行统一认证后，尽可能使用多因素身份验证，包括密码加短信口令双重验证、扫码登录、手机验证码等多种方式，以增强系统安全性； b)定期更换密码：用户应定期或不定期地修改密

		码，以防止长期使用同一密码带来的安全风险； c)限制登录次数：过限制某些网络服务的登录次数，防止远程猜测、字典法、穷举法等攻击。
操作系统管理	指确保系统稳定性、安全性和性能的最佳实践。	a)安全性机制：应提供多种安全机制，如用户身份验证、进程隔离、文件权限控制等，以保护计算机系统不受未经授权的访问、篡改和删除； b)安全增强技术：包括安全漏洞打补丁、停止服务和卸载软件、升级或更换程序、修改配置或权限等。
应急管理	指在网络安全事件发生后，通过快速响应和处理来减小事态蔓延并降低损失的一系列行动。	应建立安全运维机制，定期进行漏洞扫描、渗透测试、安全加固等。

5.6 客户端标准

表 10　客户端标准内容

业务分类	业务定义	标准要求描述
基础设备	指客户临柜办理时应具备的基础设备。	应包括 PC 电脑、打印机等。
业务办理相关设备	指客户临柜办理业务时应具备的相关设备。	应包括摄像头、高拍仪等。

5.7 监控与审计标准

表 11　监控与审计标准内容

业务分类	业务定义	标准要求描述
用户量监控	指柜面业务用户数据的采集、分析、可视化等相关标准。	应包括用户访问量监测分析。
流量监控	指柜面业务受理、办理实时流量分析、带宽使用分析等相关标准。	应包括流量态势感知、网络性能监控、流量回溯分析等。
日志留存	指将柜面业务受理、办理的日志数据进行保存。	应采用日志管理工具来集中管理、监控和分析日志

6　柜面业务数据管理要求标准

表 12　数据管理要求标准内容

业务分类	业务定义	标准要求描述

数据分类	指数据应按照“先行业领域、再业务属性”的思路进行分类。	a）数据首先应按照市场信息、客户信息、交易信息、风险管理信息进行分类和管理； b）分类应准确反应数据的实际内容和用途，避免分类错误或遗漏； c）同一行业领域或业务属性的数据应采用相同的分类标准和规则，以确保数据的一致性和可比性； d）对敏感数据（如客户信息、交易信息等）应采取加密、脱敏等安全措施，确保数据的安全性和隐私性； e）分类应符合相关法律法规和监管要求，如《证券法》、《个人信息保护法》等；
数据存储	指数据的存储位置、访问频率、保留时间、容量和性能要求的相关标准。	a)分层存储：根据访问频率和重要性放置在不同级别存储设备上； b)数据访问频率与性能要求：根据数据的访问频率和性能要求，定义不同的存储策略。
数据合法性	指柜面业务数据遵循相关法律法规标准。	严格遵循国家相关法律法规，包括但不限于《证券法》、《证券公司监督管理条例》、《个人信息保护法》等，对数据的收集、使用、存储、传输和披露等方面确保自身业务数据符合相关规定。
数据来源	指柜面业务数据来源的方式。	应包括公开收集的数据和自行生产的数据。
数据传输安全性	指采取必要措施，确保数据在传输阶段处于有效保护和合法利用的状态。	应采用加密技术对数据进行加密，保护传输的数据安全。
数据保密	指保护数据保密性的相关标准。	a）对敏感数据进行明确标识，如客户身份信息、交易密码等，以便进行更严格的保密管理； b）实施严格的访问控制策略，确保只有授权人员才能访问相关数据； c）采用多因素认证、权限管理等手段，提高访问控制的安全性。

7 柜面业务服务创新要求标准

柜面业务创新服务是指利用数字化、智能化技术等创新方式实现业务办理和服务。

表 13　服务创新要求标准内容

业务分类	业务定义	标准要求描述
人脸识别	基于人的脸部特征信息进行身份认证的生物识别技术。	具备高识别准确率，在柜面业务办理过程中准确识别并验证客户身份，完成“人证合一”的身份验证。
OCR 识别	对客户证件信息进行提取，完成身份识别。	要求准确识别并提取客户身份证件的文字信息，包括姓名、身份证、照片等关键内容，OCR 系统应具备一定的容错能力，确保在复杂情况下的准确识别。
智能语音识别	利用人工智能技术实现语音话术识别。	a）语音识别系统必须能够准确地将客户的语音输入转化为文字，确保信息的准确无误； b）对于证券业务中的专业术语和复杂表达，系统应具备相应的识别能力，避免误识或遗漏。
身份信息核验	通过对比公安部数据库，对客户提供的身份信息进行真实性、合法性验证的过程。	a）根据客户提供的身份信息与公安部数据库对比，实时查询并确保客户提供的姓名、身份证号等关键信息的真实性和合法性； b）在进行身份信息核验前，必须获得客户的明确授权，确保客户知晓并同意其身份信息被用于核验目的。
电子签名和数字证书	在客户业务办理的电子协议签署环节，联合第三方 CA 数字认证机构，为客户协议加盖数字证书签名，提升客户体验，保障双方权益。	a）电子签名应确保是签名人真实意愿的表达，并且电子签名的制作数据由签名人本人控制； b）电子签名应采用先进的技术手段，如哈希算法和公钥私钥加密等，确保签名数据的完整性和不可篡改性； c）数字证书应由权威的、公正的、可信任的机构发放，以确保其权威性和可信度。
大数据核查	利用大数据技术对客户的账户信息进行全面核查分析。	a）利用大数据技术，多维度对客户的账户信息进行核查分析、关联性分析等； b）收集的数据应准确无误，通过先进的技术手段对数据进行清洗和校验，确保数据的准确性； c）应反洗钱监管要求，对客户的账户信息进行核查验证，对账户信息和行为特征进行风险评级和风险监测。