ICS 03.060
CCS A 11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0318—2024

证券期货业信息技术架构管理指南

Guidelines for information technology architecture management of securities and futures industry

2024-11-20 发布　　2024-11-20 实施

中国证券监督管理委员会　　发 布

目　　次

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。

本文件由全国金融标准化技术委员会证券分技术委员会（SAC/TC 180/SC4）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：上交所技术有限责任公司、华锐分布式（北京）技术有限公司、上海艾芒信息科技有限公司、中证信息技术服务有限责任公司、富国基金管理有限公司、广发证券股份有限公司、国信证券股份有限公司、海通证券股份有限公司、恒生电子股份有限公司、汇添富基金股份有限公司、上海金融期货信息技术有限公司、上海期货交易所。

本文件主要起草人：林征、刘凯、孙增、范宋锃、曹雷、张帆、郭东波、龚大平、姜源、况家兴、李强、毛银杰、苏兆聪、蔚赵春、朱于、路一。

引　言

近些年，证券期货业机构正广泛开展信息技术架构转型，业务架构、应用架构、数据架构、技术架构等架构理念已成为行业基本共识。随着架构转型的不断演进，架构管理已成为行业机构共同关注的领域。在满足业务快速发展和创新需求下，如何使信息技术架构得以有序演进，成为需要业界解决的难点。

为适应证券期货各类业务需要，融合新技术发展与创新，解决证券期货业机构在信息技术架构管理过程中的难题，降低信息技术架构管理的安全风险与成本，规范行业架构管理流程，本文件提出了证券期货业的信息技术架构管理指南，旨在提升行业整体信息技术架构管理标准化水平。

证券期货业信息技术架构管理指南

1 范围

本文件规定了证券期货业信息技术架构管理的制定原则、组成结构、管理机制、更新机制。

本文件适用于证券期货业机构在信息技术架构管理过程中的整体规划、设计操作、制度建设和更新升级。

2 规范性引用文件

本文件无规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

架构 architecture

对系统软硬件整体结构与组件的描述。

3.2

信息技术架构 information technology architecture

对信息技术服务和信息技术组件结构以及之间交互关系的描述。

3.3

组件 component

在系统中，实现其部分功能的可识别区分的部分。

3.4

数据分片 data sharding

将数据库表中的数据，按照一定的分片规则分散存储到多个数据存储节点，以均衡节点间数据容量和访问负载。

3.5

虚拟机 virtual machine

通过各种虚拟化技术，为用户提供的与原有物理服务器相同的操作系统和应用程序运行环境的统称。

3.6

重大变更 major changes

可能会影响信息技术架构安全稳定运行或引发网络安全事件的变更。

3.7

基线 baseline

经过一次正式评审并通过的规则或产品，并以此作为后续开发的基础。

3.8

有效性 effectiveness

对某一系统或产品，具有提供安全程度的性质。

3.9

一致性 consistency

在某一系统或构件中，整体与部分或部分与部分间统一的、标准化的和无矛盾的程度。

3.10

网络安全事件 cyber security incident

由于人为原因、软硬件缺陷或故障、自然灾害等，对证券期货业网络和信息系统或者数据造成影响，发生网络和信息系统服务能力异常或者数据损毁、泄露，对国家金融安全、社会秩序、投资者合法权益造成损害的事件。

3.11

访问控制 access control

一种保证信息技术架构资源只能由被授权主体按授权方式进行访问的方式。

3.12

授权 authorization

赋予某一主体可实施某些动作权力的过程。

3.13

口令 password

用于身份鉴别时所输入秘密的字、短语、数或字符序列。

3.14

应急预案 contingency plan

对突发事件所采取的备份、应急响应和灾后恢复的计划。

3.15

重要信息系统 important information system

支持证券期货业机构关键业务功能，如出现异常将对证券期货市场和投资者产生重大影响的信息系统。

3.16

评估 assessment

系统化地检验一个实体满足与适用标准的符合程度。

3.17

验证 verification

将某一活动或处理过程的输出与其相对应的安全需求或规范相比较，并证实该输出满足需求或规范的过程。

3.18

第三方 third party

就所涉及的问题而言，公认与相关各方均独立的个人或团体。

4 制定原则

4.1 整体性原则

信息技术架构由业务、应用、数据、技术等各个模块组成，其管理应覆盖需求、设计、开发、维护、更新等环节，并符合整体管控要求。

4.2 稳定性原则

信息技术架构能够持续稳定运行，并具备与业务需要、技术应用相匹配的容量、性能。

4.3 可扩展性原则

信息技术架构能够持续满足业务需求并能融合新的技术，以支持不断发展的业务需要和技术应用。

5 组成结构

5.1 业务架构

业务架构通过整体业务拆分、系统模型设计，将现实业务需求转化成具体业务模型的描述。业务架构是连接具体业务与信息技术其他架构的核心支撑点，是保障企业战略、治理、组织和关键业务流程得以顺利实施的关键。

业务架构包括但不限于以下内容：

——业务目标：清晰了解需求方问题，厘清业务架构的范围和边界，将企业战略转化成具体业务运营模式；

——组织结构：将具体业务模型与组织单元相匹配，明确管理职责、工作流程和协调机制，合理分配业务权限，便于运营监测和业绩评估；

——业务流程：明确业务流程中的需求和交付物，建立标准化流程体系；

——业务服务：企业及其各业务单元与需求方进行有效沟通，向需求方提供满足业务需要的内外部服务。

5.2 应用架构

应用架构是根据业务场景需要，设计应用层次结构，制定应用规范、定义接口和数据交互协议等内容。应用架构是建立企业业务架构和数据架构的桥梁，主要提供支撑架构实践所需的功能和应用服务。

应用架构包括但不限于以下内容：

——具有明确的范围和边界，清晰的关联关系，可行的路线图规划；

——系统技术可以支撑系统的有效运行；
——系统功能设计合理，系统与子系统、系统与外部系统之间相互协调，功能模块齐全，满足各方面业务需求；
——应用架构各组件具有可扩展性，能适应新技术的要求。

5.3 数据架构

5.3.1 概述

数据架构是对数据类型、数据结构及其交互关系的统一定义，通过构建数据统一处理平台，统一数据定义规范，标准化数据表达，形成有效且易维护的数据资产。数据架构用于实现数据标准化，减少数据冗余，提升数据质量以及系统性能，实现数据在系统间的高效共享和全生命周期管理，发挥数据资产的价值。

5.3.2 计算层

计算层负责计算来自各个计算节点的运算请求，并将计算结果返回给相应的计算节点，实现算术运算和逻辑运算。以架构中数据准确性为前提，保障数据在复杂业务场景中的计算效率。

计算层包括但不限于以下内容：
——具有可以被不同应用程序调用的算法模块；
——满足数据架构所需的计算能力要求；
——支持在可信的环境运行。

5.3.3 存储层

数据存储是数据保护的重要方式，存储层负责执行计算层数据操作请求，并实现数据在硬件层面的长期保存，确保数据不丢失。存储层对系统数据实施安全保护措施，保障数据完整性、保密性、可用性。

存储层包括但不限于以下内容：
——支持高效、安全、稳定地提供数据写入、查询、读取、更新及删除服务；
——具有统一数据定义范式，标准化数据表达规范；
——支持将同一份数据的不同物理副本切分到不同的物理节点上；
——具有充足的储存空间，满足大容量数据存储的要求；
——具备对数据的安全保护功能，并定期对数据进行备份，防止系统数据的非法生成、变更、泄漏、丢失、破坏、销毁等；
——支持在数据存储节点出现故障后进行快速自检与恢复。

5.3.4 管理层

数据管理是保障数据安全，有效整合数据资源的方式。管理模块涉及数据的采集、清洗、存储、建模分析、数据应用、销毁等全生命周期，负责协调各类数据单元和保障数据有效性使用，主要包括主数据管理、元数据管理、数据模型管理、数据标准管理、数据质量管理、数据安全管理、数据共享管理等。

管理层包括但不限于以下内容：
——提供数据库参数配置和运行监控接口；
——提供负载均衡和资源隔离功能，确保各类数据单元提供稳定服务；
——具备角色权限管理、安全防护机制、节点间数据迁移能力和审计能力；
——提供数据架构集群节点的参数配置、运行状态监控、性能数据采集等集群状态监控与配置功能。

5.4 技术架构

5.4.1 概述

技术架构主要是支持业务、数据和应用架构所需的逻辑软件和硬件能力的描述，主要包括服务平台、逻辑架构及物理架构等。

5.4.2 服务平台

通过服务平台整合，优化技术架构各个模块，向需求方提供各项服务。服务平台可以分为系统管理、用户管理、账户管理、接口层、统计分析等功能模块。

5.4.3 逻辑架构

逻辑架构主要是识别功能模块，规划功能模块接口，明确功能模块之间的关联关系和关联机制。逻辑架构是依据逻辑关系将架构进行分层，将具体功能嵌入到每一层中，清晰地管理代码的组织结构。

5.4.4 物理架构

物理架构是将软件组件与硬件组件进行有机结合，并使用网络组件在系统软件应用和物理资源之间建立连接。物理资源主要包括信息技术（IT）基础设施，软硬件组件等。其中，IT 基础设施包括技术标准、基础组织、基础数据、基础软件、技术设备、通信网络、机柜、供配电类设备、空气调节类设备、监控类设备、消防类设备、安防类设备、虚拟机、安全系统、机房物理环境等；硬件组件主要有台式计算机、服务器、路由器、交换机等；软件组件主要有中间件、数据库、操作系统等。

技术架构包括但不限于以下内容：

——清晰明确的范围、边界和接口定义，统一的技术开发规范，确保整体架构的兼容性与安全性；

——支持前后台分离，各模块间的独立性，功能相互协调，信息加密传输，实施灵活高效的部署架构；

——基于具体的技术框架、关键技术系统间通讯方式、关键实现技术和现有服务组件完成架构设计，实现安全架构在物理安全、网络安全、主机安全、应用安全等方面的要求，满足业务需求；

——通过高可用、关键技术节点冗余等技术手段，保障业务连续性。

6 管理机制

6.1 组织保障机制

6.1.1 机构设置

机构设置是架构管理工作开展的基础，主要包括组织架构、岗位设置、团队建设、岗位职责等内容。其目标是对架构管理岗位进行职责规划与安排，指导各个岗位职能的执行，以确保有效落实企业战略目标。

证券期货业机构可设立信息技术架构管理工作组（以下简称“架构工作组”），可视情况作为信息技术治理委员会下属部门，或由治理委员会承担其职责统筹协调。架构工作组负责对信息技术架构开展权限管理、质量审查、安全监测、有效性评估，并完成分级响应工作。

架构工作组要覆盖信息技术、业务、合规、风险管理等部门，也可聘请外部专业人员担任架构工作组委员或顾问。

架构工作组职责包括但不限于以下内容：

——制定架构管理规划，包括但不限于架构设计规划、安全规划、数据规划等内容；

——制定架构投入预算及分配方案；

——制定架构建设及重大变更方案；

——处理其他对架构管理产生重大影响的事项。

6.1.2 岗位设置

岗位设置目标是对架构管理岗位职责进行划分，更有效地执行各项具体要求，保障企业战略目标的落实。证券期货业机构可设立系统架构师、质量检查员、安全监测员岗位，并定义各工作岗位职责。证券期货业机构可根据各个部门和岗位的要求明确其管理职责、工作程序和操作流程，对架构建设、质量审查、运行监测、数据安全和应急响应等重要环节负责。

系统架构师岗位与质量检查员岗位、安全监测员岗位可由不同人员担任。

6.1.3 职责划分

系统架构师根据具体业务理解，依据具体业务场景，结合可行的信息技术手段，制定信息技术架构解决方案，并推动解决方案的落地实施。

系统架构师岗位主要职责：

——负责架构需求评估确认、技术路线选择、技术框架搭建、系统功能设计等工作；

——参与评审项目计划、需求分析、系统建模、软件设计等内容，包括立项评审、技术架构评审、上线评审和后评估等流程，并对架构持续优化；

——对功能需求和非功能需求进行技术选型，识别技术架构风险，评估技术实际工作量；

——对可复用的模块、接口、类库等组件进行识别、分析、设计、维护和更新；

——持续跟踪项目实施进度，推进信息技术架构解决方案落地，检查架构建设和管理执行情况。

质量检查员依据现行法律法规和公司规章制度，对信息技术架构进行内部质量审查，保障架构质量安全。

质量检查员岗位主要职责：

——负责建立和完善质量审查体系，检查架构安全防护措施执行情况；

——负责检查信息技术架构中安全质量，及时提出存在的问题，并要求相关部门及人员及时处理；

——信息技术系统架构上线或变更升级后，重新进行安全质量检查；

——检查完毕应出具内部质量审查报告，并由架构工作组提交信息技术治理委员会审议。

安全监测员依据现行法律法规和公司规章制度，对信息技术架构进行异常监测，保障架构持续安全稳定运行。

安全监测员岗位主要职责：

——负责建立和完善监测指标体系，并依据指标执行监测架构运行情况；

——负责用户权限管理，建立权限管理规则和检验创建账户方式，验证用户身份信息，防止非法用户访问；

——负责对架构各种硬软件资源的合理分配和科学使用，避免造成系统资源的浪费；

——负责实时架构监控，发现异常现象及时要求相关部门或人员采取有效措施，及时完成修复工作。

6.2 权限管理机制

证券期货业机构应建立健全权限管理机制，具备可靠的访问控制、操作管理和权限管理制度，防止权限滥用，确保交互过程中的合法性和安全性。

信息技术架构权限管理机制包括但不限于以下内容：

——信息技术架构应具备授权管理功能，对于所有需要授权使用信息技术架构的访问者，采用静态口令、数字证书、动态口令等至少一种方式进行身份验证，发放口令、证书等识别信息时，采取严格的管理机制，防止被中间截取；

——依据安全策略控制，防止访问者对信息技术架构的授权访问被恶意提升或转授，防止访问者使用未经授权的功能，防止访问者访问未经授权的数据等非法访问活动；
——访问控制的覆盖范围包括与信息技术架构访问相关的主体、客体及它们之间的操作；
——遵循最少功能和最小权限原则，分配信息技术架构管理、操作和访问权限，并履行审批流程。

6.3 质量审查机制

证券期货业机构应建立健全信息技术架构质量审查机制，开展内部质量审查，确保架构的安全性和稳定性。

信息技术架构质量审查机制包括但不限于以下内容：
——质量审查应遵循完整、稳定、可扩展的原则，审查包括架构的流程设计、功能设置、参数配置和技术实现等内容，符合现行行业法律法规及国家主管部门有关规定；
——具备完善的信息安全防护措施，符合要求的信息系统备份能力，确保相关系统能够安全、平稳运行；
——架构上线或变更升级前，应对架构的执行程序、源代码进行严格审查、测试，确保运行质量安全；
——至少每年开展一次信息技术架构相关产品及服务审查，出现明显质量问题的，应当立即核实有关情况，采取必要的处理措施，明确修复完成时限，及时完成修复工作；
——对信息技术架构知识产权、版权、专利、商标、声明等进行事前合规审查，可根据需要引入第三方审查服务，通过审查架构的自主性和可用性，避免法律纠纷；
——使用信息技术手段开展相关质量审查活动，应出具相应的审查报告以及年度评估报告，并由架构工作组提交信息技术治理委员会审议。

6.4 安全监测机制

证券期货业机构应建立健全安全监测机制，对机构的重要信息技术架构模块进行监控和分析，可以基于内部审计系统、日志分析系统、内部控制系统等开展安全监测工作。

信息技术架构安全监测机制包括但不限于以下内容：
——制定监测指标体系，监测指标集可以分为三类：访问类、操作类和控制类；
——梳理重要信息系统权限资源和数据资源，重点监测基础设施安全、性能和容量安全、系统可用性安全、数据安全等；
——建立日常运行监测与预警机制，重点监测架构的异常情况，超过警报阈值时应及时预警，并及时向架构工作组报告架构管理安全监测预警信息。

6.5 有效性评估机制

6.5.1 总体要求

为保障信息技术架构的安全稳定，应由架构工作组对架构进行有效性评估，并报信息技术治理委员会或指定专门委员会审议，需要时可聘请外部专家参与评审。

证券期货业机构可建立健全有效性评估机制，定期开展信息技术架构管理及执行情况的有效性评估，具体包括架构性能评估、IT能力评估、架构目标状态评估、架构变革前期条件要素评估等。

6.5.2 架构性能评估

包括但不限于以下内容：
——架构性能的可拓展程度；

——当前各项能力绩效水平；
——未来期望各项能力绩效水平；
——未来如何实现各项能力期望状态；
——成功部署目标架构对业务组织可能产生的影响。

6.5.3 IT 能力评估

包括但不限于以下内容：
——变更流程基线和目标状态水平；
——运营流程基线和目标状态水平；
——基线能力效率水平；
——成功部署目标架构对 IT 组织可能产生的影响。

6.5.4 架构目标状态评估

包括但不限于以下内容：
——架构治理流程、组织结构、人员角色和岗位职责情况；
——架构性能水平；
——架构与业务需求的匹配度；
——可重用性潜力水平。

6.5.5 架构变革前期条件要素评估

包括但不限于以下内容：
——当前状态和预期目标差距；
——每个条件因子影响水平；
——条件因子相关性。

6.6 分级响应机制

6.6.1 总体要求

证券期货业机构应充分分析信息技术架构建设及管理过程中可能出现的各类突发事件，并对其制定相应分级响应预案，通过评审及培训，提高风险防范意识和突发事件处置能力，从而使事件造成的影响和损失降到最低。

6.6.2 响应级别分类

响应级别分类见《证券期货业网络安全事件报告与调查处理办法》。

6.6.3 分级响应基本要求

包括但不限于以下内容：
——按照国家和行业主管部门要求制定统一的分级响应预案框架，包括启动预案的条件、组织构成、资源保障、事后总结和改进等内容；
——根据架构管理重要程度制定不同安全等级的响应预案；
——定期组织架构管理相关人员分级响应培训，使其掌握岗位职责要求和处置流程；
——对突发事件开展业务影响分析，确定并实施重要业务恢复目标和恢复策略。

7 更新机制

7.1 评估分析

证券期货业机构应定期或在有重大变化时对信息技术架构进行评估，建立变更管理流程并持续监控，以确保架构能对业务需求快速响应，使架构对业务的价值最大化。

评估分析包括但不限于以下内容：

——当前信息技术架构是否满足业务需求；

——架构更新方案是否可行；

——架构更新前资源配置充足水平；

——架构更新时对具体业务影响程度；

——架构更新后质量审查和安全监测执行情况。

7.2 应急预案

为科学应对信息技术架构管理过程中突发网络安全事件，证券期货业机构可建立健全信息技术架构管理应急响应制度，有效预防、及时控制和最大限度地消除突发事件的危害和影响，可制定架构安全事故应急预案。

应急预案包括但不限于以下内容：

——制定应对网络安全事件的应急预案，包括应急目标、数据备份、处理流程、恢复措施、应急披露等内容；

——制定应急处置联络手册，明确详细的联络方式，并及时更新，在发生变化时及时通知相关部门；

——事先储备应急所需的备品备件等物资并定期盘点，对于有时效性的应急物资应做到及时检查更新；

——在年度应急演练中，可将由信息技术架构有可能引起的网络安全事件作为重要场景之一；

——根据架构变更、业务发展等情况，持续更新应急预案。

7.3 变更申请

根据系统架构师变更评估分析的结果，架构工作组可视情况作出变更申请决定。风险管理部门应判断变更方案是否能够将信息技术架构变更的预估风险控制在可接受的范围内。合规部门应审查变更流程的合规性，确保技术团队依据相关法律法规合理执行变更流程。

对于可能涉及重要信息系统的重大变更，架构工作组应提交信息技术治理委员会审批。

变更申请包括但不限于以下内容：

——变更原因：为满足新业务需求或由于技术迭代进行更新等；

——变更内容：对主要变更内容的具体说明，如：数据接口、参数配置、功能模块等；

——变更实施流程：变更的具体步骤，可覆盖变更的全生命周期；

——数据备份：在变更实施前，备份相关业务数据及其他重要数据，以防止重要数据丢失；

——变更回退机制：在架构变更过程中，如果出现故障影响到其他业务功能的正常运行，能够将其回退到上一版本；

——变更影响评估：主要评估变更前与变更后的性能差异，对业务发展的影响，相关部门及人员岗位职责和操作流程的变化程度等。

7.4 升级更新

证券期货业机构要支持信息技术架构的安全升级更新，及时提升架构的先进性。

升级更新包括但不限于以下内容：

——校验架构的完整性和稳定性，防止被篡改或替换；

——架构升级更新时，应同步备份相关业务数据，确保更新升级前后数据的一致性；

——至少采取一种安全机制，保障升级更新的有效性；

——当因重大安全问题需要升级更新时，应积极引导用户同步升级更新，并保障升级更新前后版本的安全性。

参 考 文 献

[1] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求
[2] GB/T 35273—2017 信息安全技术 个人信息安全规范
[3] GB/T 25069—2022 信息安全技术 术语
[4] JR/T 0060—2010 证券期货业信息系统安全等级保护基本要求（试行）
[5] JR/T 0158—2018 证券期货业数据分类分级指引
[6] JR/T 0022—2020 证券交易数据交换协议
[7] JR/T 0204—2020 分布式数据库技术金融应用规范 安全技术要求
[8] JR/T 0205—2020 分布式数据库技术金融应用规范 灾难恢复要求
[9] JR/T 0166—2020 云计算技术金融应用规范 技术架构
[10] JR/T 0203—2020 分布式数据库技术金融应用规范 技术架构
[11] 证券期货经营机构信息技术治理工作指引（试行）（中国证券业协会、中国期货业协会，2008年9月3日）
[12] 证券期货业信息安全保障管理办法（中国证券监督管理委员会令 第82号）
[13] 证券基金经营机构信息技术管理办法（中国证券监督管理委员会令 第152号）
[14] 证券期货业网络安全事件报告与调查处理办法（中国证券监督管理委员会公告〔2021〕12号）