附件 1

风险数据管理实践

一、风险数据战略

证券公司围绕经营战略目标，结合公司金融科技战略或者数字化转型战略，统一制定和规划数据战略。同时，将风险数据战略作为数据战略的组成部分，结合外部监管要求和内部风险管理战略，明确其战略目标和实施路径，以支撑风险数据管理工作的开展。

证券公司可以将风险数据战略的实施情况纳入公司整体战略规划考核评价体系。依据自身战略规划考核评价的要求，按季度分解风险数据战略，明确各季度的工作内容、目标和战略督导目标，并通过 KPI/OKR 对实施过程进行持续监控。从资金投入、差距分析、趋势分析、资源分析、战略机会点、合规紧急性六个方面对风险数据战略的项目优先级进行综合打分，确保重点任务得到贯彻执行。通过项目双周报、战略规划月报、年度总结汇报等形式跟进风险数据战略的实施情况。依据项目优先级划分原则对具体的任务或项目进行打分，并参考项目效益指标，由风险管理部门、数据管理部门的负责人共同评价战略任务的进度和成效。

二、风险数据治理

（一）风险数据治理组织

数据治理委员会作为公司数据治理工作的最高决策层，负责公司级数据治理规划等重大事项的审议。数据治理委员会下设公司数据治理工作组作为管理层，负责公司级数据治理工作的统一规划和监督实施。

公司数据治理工作组可以将风险数据治理的执行工作授权至跨部门协作小组，由数据管理部门、风险管理部门、财务管理部门、合规管理部门、主要业务单位（含子公司）相关人员组成，负责风险数据治理工作的组织、执行与汇报。其中，数据管理部门负责在公司级数据治理架构下规划及牵头推进风险数据治理工作，保证风险数据管理工作符合公司级数据治理要求；风险管理部门负责在公司级数据治理标准之下提出风险数据需求及风险数据质量要求；合规部门负责督导合法合规获得和使用风险数据；主要业务单位（含子公司）及财务部门负责按照风险数据需求提供源端系统数据，落实公司关于风险数据质量、风险数据标准等治理要求。

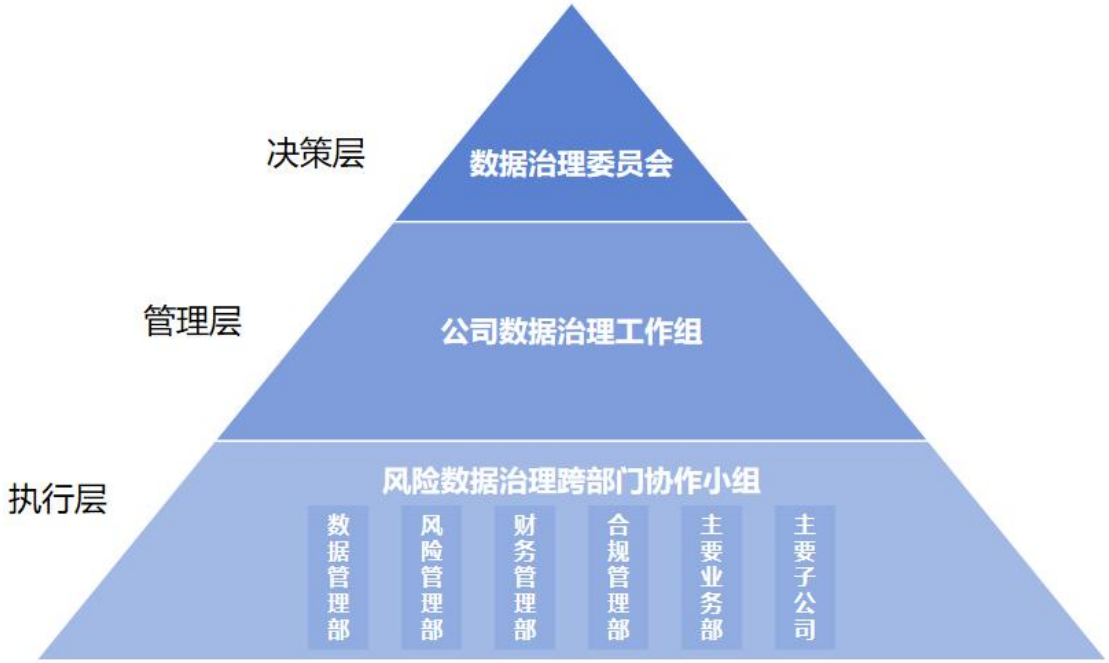


图 1 风险数据治理组织

对于业务复杂程度较高、体量较大的证券公司，由首席信息官指定固定部门或团队负责对接、服务风险数据需求；风险管理部门内部设置专岗或兼岗对接风险数据治理、风险数据质量控制工作，业务单位（含子公司）设置专岗或兼岗负责源端数据治理和质量控制工作。对于业务复杂程度较低、体量较小的证券公司，根据自身管控的重点难点领域，设置相匹配的团队或岗位负责开展风险数据治理和质量控制工作。

（二）风险数据制度建设

证券公司数据管理制度体系建设通常包括以下几个方面：“数据治理管理办法”作为数据工作的顶层制度，全面覆盖数据治理工作的各个方面；“数据安全管理办法”筑牢数据安全防线，保障数据全生命周期的安全性与保密性；“数

据标准管理办法”统一数据标准，确保数据的一致性与规范性；“数据质量管理办法”强化数据质量管理，提升数据的准确性与可用性。同时，证券公司根据实际业务需求与发展情况，可以制定“数据应用管理办法”，进一步拓展数据的应用价值。

在上述核心制度框架下，可以进一步细化制定对应的次级制度与实施细则，确保每一项管理工作都有章可循、有据可依。证券公司在“数据治理管理办法”等制度框架下，可以结合《证券公司全面风险管理规范》以及《证券公司并表管理指引（试行）》等外部监管要求，在重点领域制定对应的风险数据管理办法或细则，例如“风险数据标准管理手册”“风险数据质量考核实施细则”等，也可以在公司级数据管理制度中体现。

特别地，证券公司可以在新业务评估制度中体现对风险数据的管理要求。在新业务评估时同步开展风险数据管理相关工作，业务部门在建设系统、产生数据的过程中，考虑风险数据的要求，数据管理部门依托于业务部门的样例数据和数据结构前置开展风险数据的采集、转换、加工工作，在业务部门开展业务前，相关数据原则上已具备进入风险数据集市满足风险管理使用的条件；开展业务后，相关数据及时进入风险数据集市满足风险管理使用的条件。

（三）风险数据文化建设

证券公司基于自上而下的全员渗透策略开展风险数据文化建设，明确数据驱动目标并强化责任体系。通过系统性全员培训，加强理念宣传、提升员工的数据处理技能与风险意识；通过重视人才培养、打造数据平台和健全考核机制等针对性举措增强风险数据文化认同感与风险数据管理水平。

三、风险数据架构

证券公司结合监管要求、公司战略目标与业务发展规划，梳理并预测未来一段时间内风险管理工作对数据的需求，在公司风险数据治理整体规划及公司数据架构的基础上，形成风险数据架构规划。同时，建立风险数据架构的持续优化机制，定期对数据架构进行评估和审查，根据业务发展需求、技术发展趋势和监管要求的变化，及时调整和优化数据架构。

（一）风险数据分布

1.数据分层

风险数据集市建设优先考虑构建“依赖型数据集市”，选择成熟稳定的分布式大数据平台作为技术支撑，确保具备高并发处理能力、可扩展性和数据安全性。对于业务复杂程度较高、体量较大的证券公司，可以探索采用湖仓一体架构。针对应用系统数据存储选择，对于数据量较小的应用系统，

如一些专项风险分析工具，可以选择集中式存储，以降低成本和管理复杂度；对于数据量大的应用系统，如涉及大量客户交易数据的风险监控系统、涉及多年资讯数据的风险计量模型类系统，可以选择分布式集群模式。

证券公司可以通过搭建“贴源层-整合层-集市层-应用层”的分层架构，明确各层功能定位与数据处理逻辑。

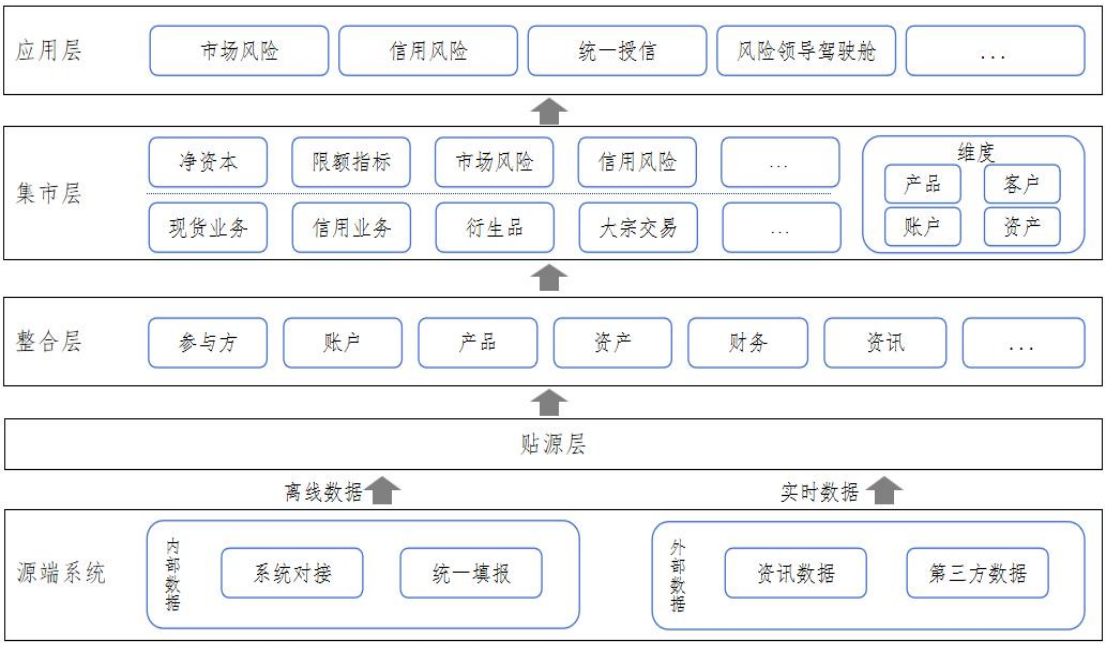


图 2 数据分层设计示例

（1）贴源层

从业务系统直接抽取原始数据，仅进行必要的格式转换和存储策略处理，如数据初步清洗、数据分区等，保持与源端系统的高度一致性。

（2）整合层

运用数据清洗、数据转换、数据匹配等技术，将来自不同格式、不同标准的数据转化为统一标准的数据。建立数据

关联模型，挖掘数据之间的内在联系，为后续的数据分析和应用提供更丰富的信息。例如，针对场外衍生品业务、信用业务以及第三方工商数据等多元数据来源中的参与方主体，实施统一识别机制，构建客户唯一标识 OneID。

（3）集市层

提供全面、准确、及时的风险数据支持，进一步细化为指标数据层和数据服务层。指标数据层在整合层的基础上，运用统计分析方法和算法，生成各种统计指标和度量值，如风险价值（VaR）、业务规模等。数据服务层直接面向业务系统提供场景化、可落地的数据和服务，一般是视图表形式。

（4）应用层

基于风险数据集市层，在各风险业务需求或专项应用系统中直接支持风险评估、管理和监控等，将数据转化为实际的业务决策支持。同时，建立数据反馈机制，将应用层的使用情况和需求反馈给集市层和整合层，促进数据架构的不断优化和完善。

2.数据流转

证券公司持续推动源端系统化接入，建立风险数据集市与内部业务系统、外部数据源之间的稳定数据接口，实现数据的自动集成和传输。对于应用系统生成且需共享复用的数据，明确数据共享的规则和流程。

交互式场景下，系统直接交互有耦合度高、安全管控难、维护扩展成本高等问题，可以采取以下方案解决。降低耦合度方面，引入消息中间件，如 Kafka，以发布-订阅模式实现异步通信，各系统独立运行；采用服务总线架构，通过企业服务总线进行消息路由等，新增或修改服务无需改其他系统代码。加强安全管控方面，建立统一身份认证中心，使用 RBAC 等模型授权；传输敏感数据用 SSL/TLS 加密，存储加密、共享时脱敏。降低维护扩展成本方面，将系统拆分为微服务并容器化，如用 Docker，各服务独立开发部署；引入自动化运维工具，像 Ansible 实现自动化部署、配置管理与监控，利用 Prometheus 等实时监控系统状态。

3.数据目录

证券公司结合风险场景，围绕数据资源目录、数据资产目录、数据服务目录三个方面在公司级数据治理框架下构建风险管理领域的专项数据目录。

（1）数据资源目录

根据风险业务的特点和需求，制定适合公司的数据资源分类标准。例如，按照风险类型（信用风险、市场风险、流动性风险等）、数据主题（客户信息、交易数据、财务数据等）、数据来源（内部系统、外部数据供应商等）进行分类。将盘点和分类后的数据资源信息录入到数据资源目录系统

中（或采用其他可行的目录管理方式），经审核和确认后，确保数据的准确性和完整性。将审核通过的数据资源目录在公司内部进行发布，供相关风险管控人员查询和使用。同时，可以建立目录更新机制，及时反映数据资源的变化情况。

（2）数据资产目录

数据资产目录建设的实践步骤如下:

一是对数据资源目录中的数据进行评估，筛选出具有较高价值的数据资源作为数据资产，评估过程可以采用定量分析和定性分析相结合的方法，例如通过数据分析模型计算数据的价值得分，结合专家评审意见进行综合判断;

二是设计数据资产目录模型，明确数据资产的属性信息，可以包括资产名称、资产描述、资产类型、数据来源、数据质量等级、使用权限等;

三是将加工整合后的数据资产信息录入到数据资产目录系统中，并建立数据资产的版本管理机制，记录数据资产的变更历史;

四是定期对数据资产进行复审和更新，确保目录的时效性和准确性。

（3）数据服务目录

数据服务目录建设的实践步骤如下:

一是了解风险管理人员在风险监测、风险评估、风险预

警等业务场景下的数据需求，包括所需的数据类型、数据格式、使用频率、访问方式等;

二是设计数据服务目录模型，明确数据服务的基本信息、服务描述、服务接口、使用说明、服务等级协议（SLA）等内容;

三是将测试通过的数据服务信息录入到数据服务目录系统中，并进行发布;

四是建立持续维护机制，建立数据服务运营管理体系，对数据服务的运行状态、使用情况、性能指标等进行实时监控和管理，及时处理服务故障和用户反馈，并不断优化服务质量和用户体验，根据业务发展和用户需求的变化，对数据服务目录进行动态更新和调整。

（二）风险数据建模

在数据模型方面，整合层可以参考 SDOM 模型的主题域逻辑采用三范式建设，集市层可以按照业务逻辑采用维度建模。模型管理可以基于“应管尽管”原则，由技术人员承担建模角色，建立公司级统一模型管理流程，涵盖模型新增、变更、审批和发布等流程和节点。

1.风险数据模型建设

按照“贴源层-整合层-集市层-应用层”四层分类，每层可以参考如下建模规范。

（1）贴源层

贴源层为每条记录标注数据来源信息，并添加数据采集时间字段，可以采用规范的表命名方式来清晰标识数据来源。比如按照“ODS_TXX_源端表名”的格式进行命名，其中“XX”代表数据来源端系统的专属编码。以“ODS_T93_TTRD_ACC_BALANCE_SECU_HIS”为例，其中“93”代表自营投资交易管理系统，“TTRD_ACC_BALANCE_SECU_HIS”则为源端系统表名，代表证券账户余额历史表。

（2）整合层

整合层的建设可以参考金融领域模型标准以及 SDOM 模型标准。

在**数据组织**方面，采用主题域分类方式对数据进行重新编排。依据金融业务的内在逻辑和关键要素，将数据划分为账户、参与方、资产、交易、产品、协议、事件、合约、资讯、财务等多个主题域。例如，在同一客户的建设过程中，风险管理部门提出同一客户的定义和判断逻辑，数据管理部门将各种来源的客户相关信息放在整合层的参与方主题域，并识别客户唯一标识 OneID。

在**数据建模**方面，采用三范式与维度模型相结合的建模方式，以消除数据冗余，确保数据的一致性和完整性。同时，尽量引用公司统一的参考数据，以保障数据在整个金融体系

中的准确性和一致性。

（3）集市层

集市层是数据价值深度挖掘与高效呈现的关键层级。

一是在数据组织方面，该体系遵循分层架构原则，集市层需要避免跨层访问贴源层数据。

由于维度数据承担着连接业务场景、统一口径、支撑多领域分析决策的核心枢纽作用，可以在集市层构建统一的风险维度数据体系，涵盖客户、账户、产品、资产类型、同一业务等核心业务维度。例如，在同一业务场景中搭建的内部证券账户标签表模型，为账户定义统一的标签属性体系，涵盖账户的业务属性标签，确保不同业务系统对账户定义口径一致，快速支撑账户分层管理、风险账户识别等场景，避免因标签混乱、维度孤立导致统计偏差或业务决策失误。



图 3 账户标签模型示例

指标数据层承担着生成各类统计指标与度量值的职责，

是业务数据分析的核心支撑。该层按照“业务+开展单位”的方式进行模型组织，根据业务设计概念模型和逻辑模型。针对应用系统回采的经过整合计算的数据放入单独的风险域。

数据服务层聚焦于提供场景化的数据服务，依据不同的业务场景进行组织，这种组织方式能够确保数据服务与实际业务需求紧密贴合。

二是在数据建模方面，业务术语、数据元、参考数据的引用与整合层保持一致，并严格遵循既定标准，根据风险场景的实际需要，制定风险专项业务域的参考数据。

（4）应用层

应用层聚焦于风险领域的核心业务需求。在命名规范方面，针对证券公司自研的应用系统，按照公司制定的数据标准进行建模，并引用统一的参考数据;针对外采系统，对于重要的风险管理应用数据，可以要求开发商使用与证券公司一致的命名规范和参考数据规范。

2.风险数据模型管理

（1）需求提出阶段

由风险管理部门提出需求，主要包括以下两方面：一是阐述需求的背景，例如新建模型是因为开展新业务，还是现有业务的风险状况发生了变化；二是明确需求的具体内容，

包括所需风险数据的类型（如客户信用数据、市场交易数据等）、数据的粒度（是按日、周还是月统计）、数据的时效性要求（实时数据还是定期更新的数据）以及数据的应用场景（用于风险预警、风险评估还是风险决策等）。

（2）模型设计阶段

模型设计阶段的实践步骤如下:

一是模型设计人员根据需求，评估当前模型是否能满足业务需求，如不满足，可以进行模型调整或新增模型，评估涉及哪些层级的调整。对于属于同一业务的业务类型，原则上在原数据模型基础上进行调整;

二是开展具体模型设计，数据管理部门基于业务需求和数据现状，设计概念模型，确定核心实体及其关系;

三是将概念模型转化为逻辑模型，定义实体属性、数据类型、主键外键等，利用专业工具绘制逻辑模型图，针对模型调整内容开展影响分析，对于有影响的下游使用方，进行技术评审的时候考虑邀请其参与评审，评估对数据准确性、处理效率等方面的影响;

四是将分析结果与调整方案提交原模型使用方确认，确保满足业务需求，并组织模型评审，贴源层和整合层只需技术评审，集市层和应用层需技术和业务一起评审，评审通过后实施开发。

（3）模型开发及发布阶段

数据管理部门负责风险数据模型代码交付、测试用例设计及测试执行，可以包括模型代码开发、代码规范性扫描、测试用例设计、数据准确性测试、性能测试等内容，验证运行效率、算法准确性等技术指标；业务部门负责从实际应用出发，验证其与业务需求的契合度及问题解决能力。

（4）模型运营阶段

在模型上线运行过程中，如业务需求重大调整或数据源更新（如新增维度、提升质量），则触发模型变更流程。数据管理部门先评估变更必要性与影响，开展变更设计并制定回滚方案。实施时，先在测试环境模拟多种场景验证，通过后再部署到生产环境，密切监控运行状态。变更完成后，持续跟踪表现，收集业务反馈解决问题。

（5）模型退役阶段

因业务发展或技术迭代使部分模型不再适用时，数据管理部门负责评估使用情况，制定退役计划，包括通知部门、停止调用、清理数据代码等，确保不影响业务，同时做好记录归档。

（三）风险数据集成与共享

本部分着重描述数据集成的实践内容，数据共享已在数据模型管理、数据目录设计部分体现。

1.集成需求管理

风险管理部门明确获取的源端数据来源、数据内容、数据范围以及数据就绪的时间要求后，提出数据需求。数据管理部门与各数据提供方的业务、技术管理人员明确数据集成的数据源类型、数据格式、集成方式、集成频率、业务约束条件以及数据集成时机。源端数据产生方负责提供被集成数据的业务元数据和技术元数据，包括但不限于业务域、业务对象、业务属性、业务规则、表名、字段名、字段类型，以及业务对象、业务属性与表、字段的对应关系。

2.集成平台接入

源端数据产生方完善信息化建设工作，实现风险数据的线上化管理，具备与数据集成和调度执行平台的统一对接能力；对于暂时不具备相应技术条件的源端单位、子公司等，可以由证券公司数据管理部门支持其信息系统建设工作。针对由业务人员录入、上传或手动调整的数据，证券公司可以建立统一的业务数据报送系统。该系统支持对文件数据的自动解析入库，以及对人工数据的统一填报、存储、质量校验，并提供统一的数据集成入口。证券公司数据管理部门可以建设统一的数据集成和调度执行平台，由数据管理部门统一负责数据集成作业的对接和执行。

3.数据集成调度

数据集成和调度执行平台支持定时的集成作业调度，以及基于源端系统数据就绪状态标志位的集成作业调度。平台支持自定义调度日历管理，包括沪深交易日历、港股交易日历、夜盘交易日历、法定工作日历等，并支持其他特殊的自定义调度日历。监管对风险管理数据有一定的时效性要求，数据集成以标志位集成调度方式为主，对于无法提供集成标志位的源端单位，与数据管理部门商定符合风险管理要求的定时集成时间，并配置数据完整性的质量校验。

4.源端变更通知机制

数据管理部门作为数据集成方，负责与风险管理部门、源端系统管理单位明确源端系统数据库变更以及数据集成异常时的职责划分和处置方案，包括数据变动及异常发生时的报告机制、处置的时效性要求以及上下游协同处置流程等，针对重要的风险数据使用场景，可以建立分级应急处置机制。

源端系统数据、表结构、访问权限发生变化时，源端系统管理单位及时通知数据管理部门进行相应调整；当源端系统管理单位自行发现数据异常，或主动对数据进行调整时，在数据变动前及时通知数据管理部门和风险管理部门；当在集成过程中发现异常时，数据保障部门参照预先定义的事件级别，执行相应的处置和报告流程，在规定的时间内与上游

源端系统对接人联系；对于数据恢复时间较长、影响较大的，将数据异常情况通知数据管理部门和风险管理部门，并在公司数据治理委员会的评估和指导下，开展后续处置工作。

（1）源端变更通知管理范围

源端变更通知管理范围涵盖风险数据领域相关的全量源端系统变更场景，包括数据结构变更、数据内容变更、数据接口变更、业务逻辑变更。其中：数据结构变更范围包含表级变更（数据底层表名称修改、表下线、表拆分或合并）、字段级变更（数据底层表字段名称修改、字段新增、字段下线、字段类型调整）；数据内容变更范围包含码值变更（字段码值修改、新增、下线）、字段值格式变更（如日期从YYYY-MM-DD 变更为 YYYYMMDD）、数据范围变更（如客户分类从两类变更为三类）；数据接口变更包含数据库级变更（数据库迁移后 IP 地址、端口变化）、文件格式变更（如 csv 变更为 json）、API 参数变更等；业务逻辑变更范围包含数据时效变更（如从月更新变为日更新）、业务规则变更（如成本包含税费变为不包含税费）等。

（2）源端变更通知机制的协作分工角色及职责

数据产生方对接人：数据专员为本单位对接人，评估本单位涉及系统对应的源端变更对下游的影响；

源端变更通知负责人：填写源端变更明细表，根据模板

执行业务变更通知;

风险数据领域业务对接人：负责分析源端变更对于风控系统报表层影响，并发起相应报表需求（如有）;

风险数据域产品对接人：负责分析源端变更对风险数据集市影响，并推动技术对接人进行相应适配调整;

风险数据域技术负责人：负责协助分析源端技术变更影响，并执行相应适配调整。

（3）执行源端变更的具体流程

在正式变更前，数据源端系统管理部门负责填写源端变更明细表并以公司级正式方式通知风险管理部门和数据管理部门，评估对现有系统的变更影响，制定相关产品及技术方案；变更时可以通过线上化流程记录变更日志以备审计。

（四）元数据管理

风险数据管理场景下的元数据管理涵盖风险监测、监管报送、风控报表等核心业务场景。针对子公司部分，由于存在法人隔离、数据安全等多方面严格要求，数据采集一般通过中间库实施，并建立有效机制保障获取元数据的准确性，对于子公司以文件方式提供的数据场景，同步完善元数据内容，包括但不限于数据范围、字段说明、更新频率等。

风险数据管理体系中的元数据管理包括业务元数据、技术元数据及管理元数据，其中业务元数据信息至少包括业务

术语、定义和解释、业务规则、数据质量规则、数据安全级别及信息标签等。技术元数据信息至少包括模型表结构、数据格式、存储信息、更新频率、ETL 规则及映射关系、数据血缘等。管理元数据信息至少包括数据所有者、责任部门、责任人、版本控制、数据生命周期等。

四、风险数据标准

本部分以同一客户数据为主要数据场景介绍数据标准每个部分的构成。

（一）词根

基于公司词根库，获取“同一”（SAME），“客户”（CUST），“编码”（CODE），组成“同一客户编码（SAME_CUST_CODE）”作为唯一标准字段编码。

（二）业务术语

术语名称：同一客户

业务定义：指由证券公司根据《证券公司全面风险管理规范》《证券业务示范实践第 4 号——证券公司同一业务同一客户风险管理》及相关内规，通过股权控制、实际控制人或其他重大关联关系识别出的，应被视为一个风险整体进行管理的客户群组，包括个人、机构、产品三种类型。

（三）数据元

“同一客户编码”数据元属性及值如下表所示：

表 1 “同一客户编码”数据元示例

数据元名称	同一客户编码		
数据元编码	BD001024		
业务含义	为每个被识别出的“同一客户”群组分配的唯一、稳定的标识符。该编码贯穿该群组在所有业务系统中的生命周期，用于风险敞口聚合、关联交易监控等核心风控场景。		
制定依据	【自律规则】《证券公司全面风险管理规范》 【示范实践】《证券业务示范实践第 4 号——证券公司同一业务同一客户风险管理》		
参考数据	无		
主题目录	主体/参与方	**通用数据元**	代码
业务条线	风控合规	**数据分级**	公司机密
数据精度	STRING	**数据类型**	代码

（四）参考数据

参考数据名称：群组类型

代码值与含义：01-实体群组（基于实际股权控股关系）；02-虚拟群组（基于产品管理等间接控制关系）

应用：此参考数据用于分类管理不同类型的同一客户群组。同时，可以建立与不同条线已有群组类型的映射规则，确保在全局视角下分类标准的一致性与灵活性。

（五）主数据

主数据涉及到管理过程，以同一客户主数据为例，具体实践步骤如下。

1.主数据对象的识别与盘点

遵循“由点到面”识别核心对象：“点”聚焦单一客户，构建含基础信息、业务角色的业务实体，锁定信用风险直接目标；“面”在单一客户基础上，穿透股权等构建客户群组关系网络，实现风险链路传导。数据现状盘点采取“业务风险驱动”策略，梳理清洗各业务数据现状，优先纳入业务尽调数据中的客户对象。盘点阶段，组建由风险管理部牵头、业务部门协同、数据管理部门执行的专项小组。业务端负责梳理涉及的风险场景与角色需求：风险管理部明确风险业务范围及角色，信用业务部界定融资方等数据范围与频率；数据管理部门负责评估数据完整性等，如统计机构客户“统一社会信用代码”缺失率。最终整合结果，明确主数据对象清单等，为后续建设提供基线。

2.主数据标准制定

主数据标准制定兼顾公司规范与业务特性，同一客户主数据标准可以通过“技术标准+业务管理标准”双维度体系构建：技术标准是刚性约束，确保数据“同物同名、同码同义”；业务管理标准保障技术标准落地。

技术标准设计采用“自上而下对齐+自下而上适配”思

路：既遵循公司主数据管理规范，确保同一客户主数据与现有体系兼容，又结合业务场景补充专项标准。首先定义主数据对象标准，包括业务含义、管理范围与核心属性，如“信用风险业务关联方”定义交易对手、融资方、发行人、担保人等角色，核心属性规范客户编码、客户名称、证件类型、证件号、客户类型等字段的定义；其次制定单一客户编码规则，如“4 位大写拼音缩写+8 位数字序号”；接着建立字段标准，统一定义客户代码等属性；再明确关联标准，如实际群组关联满足实控人相同、股权控股、业务绑定三类条件之一；最后制定映射标准，统一数据字典，消除系统间数据格式差异，如交易所代码统一映射。

证券公司可以配套建立业务管理制度保障上述标准落地，例如数据管理部门牵头风险管理部门和数据产生单位在公司框架下制定“同一客户主数据管理细则”，明确“谁产生、谁维护”的责任分工，规范“新增-变更-注销”全生命周期管理流程，并纳入考核形成刚性约束。经数据治理工作组审批后发布生效。

3.主数据建设与质量管控

主数据建设与质量管控是主数据管理的核心内容，数据汇聚时根据数据源优先级分层接入，非实时信息如子公司 T+1 报送数据等用 ETL 工具每日批量抽取,高时效性信息通过

日间轮询或者实时采集接入。数据处理采用“清洗-转换-整合”流程，清洗阶段自动处理数据重复等问题，复杂矛盾数据通过流程化的形式由人工处理；转换阶段按标准完成字段映射与编码统一；整合阶段按层级合并数据。主数据质量预警时按照主数据管理流程进行问题流转处理，纳入风险数据质量整体工作范畴。

4.主数据推广运营

证券公司可以通过培训、分阶段系统对接与试点验证的方式达成主数据推广使用的目的。培训依角色进行差异化设计，业务人员经“实操+答疑”掌握基础操作，技术人员通过获取接口文档与测试环境支持完成集成。系统对接按照“核心系统优先+逐步扩展”原则，先对接授信系统解决数据问题，再对接业务系统生成报表，最后覆盖子公司系统实现复用。

（六）指标数据

指标元数据是指标管理的基础和核心。指标元数据围绕指标全生命周期管理需求设计，包含业务类、技术类、管理类三大核心属性组。通过明确业务、技术、管理维护职责，确保指标的标准化、可追溯性，实现业务与技术协同。

表 2 指标管理元数据核心属性

属性类别	核心属性（部分必填）

属性类别	核心属性（部分必填）
业务类	名称（唯一标识）、别名（简写）、指标含义（衡量内容）、业务口径（计算定义）、口径类型（统计/考核等）、时间粒度（日/月等）
技术类	技术口径（计算公式）、数据精度（Decimal(26,8)）、标准数据源（系统/表/字段）、计算方式（离线/实时）
管理类	编码、指标状态（待审核/上线）、主题目录（编目检索）、归口管理部室/人（责任归属）、数据质量规则、版本号（审核自动生成）

以下以国际子公司股票持仓成本指标为例，列出各项属性的参考样例。

表 3 国际子公司“股票持仓成本”指标属性示例

基本信息	**指标名称**	当日国际自营账户股票持仓成本（证券代码级）		
	指标编码	FX0302024		
	主题目录	所有指标/风险条线/股票/持仓		
业务属性	**业务含义**	当日国际自营账户股票持仓成本	**统计维度**	内部证券账号 ,多空头标志，资产类型，组织业务单元 ,证券代码 ,交易所 ,资产状态，币种

	业务口径	FICC_POSITION 的持仓成本（CCCB）	**口径类型**	统计口径
	业务限定	限制证券类别(ZQLB)为股票，限制取交易日期(TRAN_DATE)为上个沪深交易日到当日	**时间跨度**	20240930 至今
	制定依据	业务规则	**时间粒度**	每日（交易日）
技术属性	**技术口径（数仓）**	SELECT SUM(HOLD_COST) FROM MDWUSER.T_MDW_T05_IH_SELF_HOLD WHERE PROD_TYPE_NAME = '股票' GROUP BY HOLD_DATE ,PROD_CODE ,PROD_NAME ,COMP_CODE ,OU_CODE ,EXCH_CODE	**指标来源**	风险一体化平台
	数据格式	DECIMAL(26,8)	**数据精度**	小数保留 8 位
	指标脚本路径	MDWUSER.P_PDM_T03_COMP_STK_STOR_HOLD_D	**查询条件**	RISK_BUSI_CODE ='ZT_010101'

				AND OU_CODE ='ORG-21473' AND ASSET_TYPE_CODE ='SPT_S'
	更新频率	日	**度量单位**	元
管理属性	**归口管理部室**	风险管理部	**指标使用部室**	风险管理部
	数据分类	结算管理	**数据分级**	公司受限

五、风险数据安全

证券公司应当在风险数据集成到风险数据应用过程中进行全流程的数据安全管理。在风险系统设计、应用开发、系统运维和日常运营等环节中落实用户身份认证、角色权限管理、授权访问机制、权限审批流程、审计日志记录等工作。另外，证券公司需要着重管理因为外包或第三方服务而可能引发的数据安全风险，加强外来人员数据访问的安全管理，并在外包或第三方服务合同中明确相应的责任条款。以下按照制定管理策略、数据采集、数据传输、存储与加工、数据使用、数据提供与共享的流程介绍风险数据安全管理各环节。

（一）风险数据安全管理策略

证券公司应当制定统一的数据分类分级标准，对各类风险数据进行分类分级，比如根据国家标准 GB/T 42775-2023《证券期货业数据安全风险防控数据分类分级指引》，数据可以分为公开、公司内部、公司受限、公司机密四个安全级别，作为后续制定数据安全管理策略与进行数据全生命周期管理的基础。公司机密级别数据类型主要是个人生物识别信息（如面部识别信息、指纹识别信息）、口令密码（如账户登录密码、支付密码）等。风险数据通常不涉及公司机密级别数据，风险数据的分类分级示例如下。

表 4 风险数据分类分级示例

数据分类	数据类型说明	数据分级
风控指标	业务规模、业务集中度、业务整体维持担保比等	公司受限
客户财产信息	持仓证券、持仓数量、持仓规模	公司受限
客户信用信息	负债余额、信用状态	公司受限
客户基本信息	名称、手机号等	公司受限
客户证件信息	身份证号、统一信用代码	公司受限
公司业务信息	业务编码、开展单位编码、资产分类等	公司内部
证券信息	证券代码、证券名称	公开

（二）风险数据采集

1.管理实践

证券公司应当在数据收集方面确保合法合规。在收集证

券公司及子公司含个人客户信息的风险数据前，先确认收集过程合法正当。不得窃取、超范围收集、未经合法授权收集或者以其他非法方式获取数据。例如证券公司通过 APP 开户采集个人客户基本信息后，若需要将此信息用于证券交易以外的用途，应当通过隐私政策等方式向用户告知个人信息收集使用的目的、方式、范围，并征得用户同意，获得合法授权。

对于证券公司采集的子公司数据，由子公司承诺其数据采集流程合法，包括通过提供尽职调查报告、签订数据安全协议或合同等方式予以佐证。证券公司在此过程中通过制定数据安全标准合同、尽职调查报告模板等，协助子公司确认数据采集已合法取得授权。例如，子公司采集个人客户基本信息时，可以根据实际管理需要选择数据采集的合规路径，比如与客户签订涉及个人资料隐私政策条款的协议，向个人客户明确告知数据将从子公司传输至证券公司的用途，并承诺后续使用处理不超出协议告知范围；或者使用隐私计算技术（如可信数据空间技术方案），无需采集子公司个人客户基本信息数据，仅采集证券公司及子公司针对个人客户的统一编码信息，用于满足证券公司同一客户管理等风险管理需求。

若子公司为跨境子公司，针对从跨境子公司采集的入境

数据，证券公司需要根据跨境子公司所在地的法律法规及监管要求，确认入境数据的使用与转移符合当地法律法规；针对证券公司传输至跨境子公司的出境数据，证券公司需要根据《数据出境安全评估办法》《数据出境安全评估申报指南》《促进和规范数据跨境流动规定》等政策要求进行评估和申报。

2.管理案例

以下以证券公司与香港子公司传输同一客户系统中的个人客户剩余授信余额数据为例，介绍数据安全管理实践。

证券公司首先评估数据出入境的真实发生规模、类型、范围以及传输方式，根据入境和出境的不同采取不同的管理策略:

（1）由香港子公司传输入境的数据，子公司应当确保传输行为符合香港的数据跨境制度《个人资料（私隐）条例》《跨境资料转移个人保护指南》《跨境资料转移指引:建议合约条文模板》等。如涉及粤港澳大湾区范围内数据的互相传输，可以参照《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》。证券公司作为数据接收方需要确保接收后的数据使用及处理不超过子公司已有的声明范围，并按照双方约定的数据跨境标准合同或其他协议中的数据安全要求，实施接收数据的数据安全保护措施。

（2）由证券公司传输至香港子公司的数据，根据数据实际出入境发生的数量和具体传输类型的不同，适用的出境安全评估路径也有所不同，包括数据出境安全评估、数据出境标准合同备案、个人信息跨境处理活动安全认证等。

（三）风险数据传输、存储与加工

在数据传输和存储方面，公司受限级、公司机密级的数据存储需要满足公司统一的数据安全要求，并做好数据隔离工作。风控指标、客户财产信息、客户信用信息、客户基本信息、客户证件信息的数据传输需要遵循加密传输要求。

在数据加工处理方面，从源端系统采集到终端用户使用，不同岗位角色在数据加工处理过程中被赋予不同权限功能。如开发人员将数据传输到开发测试环境时，对客户姓名、身份证、手机号等数据进行脱敏，采取屏蔽遮盖转换等匿名化处理。证券公司需要进行第三方合作管理与外包人员管理，确保外包人员访问公司受限级及以上数据前已获得公司审批，并签订相应的保密协议。

（四）风险数据使用

在应用方面，证券公司根据风险数据分类分级结果，形成数据分类分级与系统数据访问权责矩阵，并对不同数据分级实施差异化的安全管理措施。以下按前表中的数据分类分级结果示例，对差异化数据安全管理措施进行举例。

表 5 差异化数据安全管理措施示例

数据分类	数据分级	访问岗位	访问权限	安全管理措施
风控指标、客户财产信息、客户信用信息、客户基本信息、客户证件信息	公司受限	风险管理岗、数据具体来源业务单位对接风险管理部的业务管理岗等	查询数据、数据导出等	数据访问授权需精确到字段级，数据访问、系统操作等进行日志记录，日志记录需留存半年以上 ;导出设置下载水印；系统对用户的异常行为进行监控；针对其他无法访问本数据级别的用户，系统对界面该数据字段采取屏蔽或遮盖等处理。
公司业务信息	公司内部	可访问系统的所有人	查询数据、数据导出等	数据访问、系统操作等进行日志记录；导出设置用户水印；系统对用户的异常行为进行监控。
证券信息	公开	可访问系统的所有人	查询数据、数据导出等	-

（五）风险数据提供与共享

风险数据在涉及监管报送或提供给公司外部使用者时，需要确保已经过公司授权审批，获得相关风险数据归口管理部门的同意。在对外提供时，确保客户财产信息、客户信用

信息、客户基本信息、客户证件信息、风控指标、公司业务信息等“公司受限”与“公司内部”级别数据的传输经过加密，对传输通道两端主体身份进行鉴别和认证，可以通过数字水印等方式加强溯源能力。

六、风险数据质量

（一）事前控制

事前控制阶段的工作主要是建立管控体系。其中，闭环风险数据质量问题处理流程是该体系中的重要工具。同时，事前控制阶段还可以建立与风险管理需要和业务复杂程度相匹配的风险数据质量规则库。

1. 建立问题处理流程

闭环的处理流程是后续实施事中监控和事后考核评价的重要基础。以下为闭环风险数据质量问题处理流程示例。

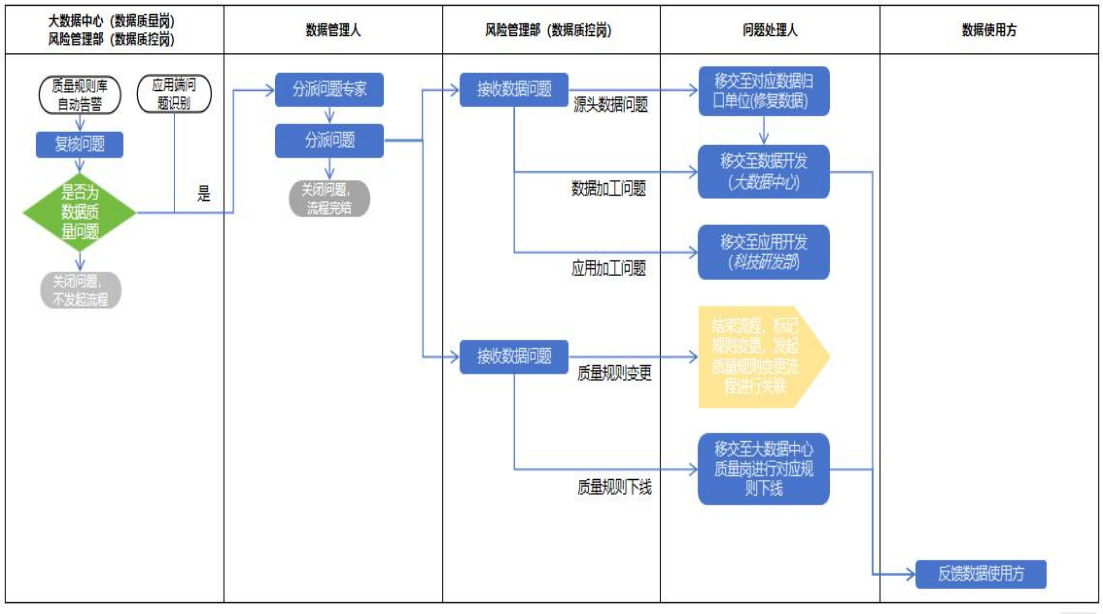


图 4 风险数据质量问题处理流程示例

2.建立风险数据质量规则库

（1）规则设定和收集

规则设定和收集一般包括以下四个步骤:

一是提出质量规则。风险管理人员根据既定的模板填写业务口径的质量校验规则；技术人员收到校验规则后，与风险管理人员共同梳理规则涉及的实体表及具体字段，明确数据校验的技术实现方式。

二是质量规则测试。规则明确后，技术人员使用历史数据作为样本数据进行测试，排查逻辑冲突等情况，并针对规则校验出的异常数据，制定相应的数据清洗策略，确保规则在实际场景中能有效执行。比如，对于重复的客户记录，排查源端数据、集成过程配置等问题，通过指定主键字段进行去重处理；对于格式错误的日期字段，采用标准化格式转换进行清洗；对于缺失的关键信息，根据业务场景设定默认值或标记待补充状态。

三是补全质量规则基本要素。根据数据的重要性、历史数据测试情况拟定规则执行的触发机制，包括定时校验或批处理伴随校验，发生问题后是否必须立即处理，明确异常数据的呈现内容、告警对象等，并根据当前情况在业务规则基础上补充技术规则字段。

四是质量规则入库和启用。完成技术补充与逻辑验证

后，技术人员按技术规则要求将规则结构化录入规则库，并维护相关元数据，启动质量规则的监控。

风险数据质量校验规则可以按以下维度分类:

一是按照逻辑类型，分为单列规则、跨行规则、跨列规则、跨表规则;

二是按照制定方，分为技术规则、业务规则（包括监管规则）;

三是按照反映的数据质量类型，分为准确性规则、规范性规则、完备性规则、唯一性规则、一致性规则、及时性规则;

四是按照执行强制性，分为拦截类规则、预警类规则;

五是按照数据层级，分为源端规则、数据集市层规则、应用层规则。

表 6 风险数据质量校验规则类型

分类规则	校验规则名称	规则功能
按规则逻辑分类	单列规则	对于某列进行单独校验，如缺失值、明显区别其他分区的数据错误等。
	跨行规则	针对数据条目间错误校验，如重复数据等。
	跨列规则	减少跨列间变量重复等结构问题。
	跨表规则	校验数据表间关联勾稽关系是否合理。

分类规则	校验规则名称	规则功能
按规则制定方分类	技术规则	用于减少技术类问题的校验规则。
	业务规则	因业务特有逻辑而对数据进行校验的规则，以及为满足监管要求而对数据进行校验的规则。
按数据质量类型分类	准确性规则	对于数据取值范围、数据间校验关系、概念等进行校验的规则。
	规范性规则	遵循统一的标准、规则和格式的规则。
	完备性规则	要求覆盖数据库中所有必要信息的校验规则。
	唯一性规则	要求数据（包括字段、记录、数据集等）在系统内或跨系统、跨数据存储中没有重复记录的规则。
	一致性规则	要求同一数据在不同系统、存储位置、应用程序中应保持相同的结果的规则。
	及时性规则	对于数据变化敏锐感知、及时更新的规则。
按规则执行的强制性分类	拦截类规则	系统强制执行，不受业务逻辑变化影响。
	预警类规则	仅对异常进行预警，不干预数据处理流程。
按规则适用的数据层级分类	源端规则	控制源端数据质量，保证源端数据传递到数据集市进行加工时的数据质量，由源端数据产生方负责数据质量。
	数据集市层规则	控制数据集市加工后的数据质量，保证数据从集市传递到应用系统时的数据质量，由数据集市加工方负责数据质量。

分类规则	校验规则名称	规则功能
	应用层规则	控制应用层加工后的数据质量，保证数据从应用层传递到应用场景实际使用时的数据质量，由应用层加工方负责数据质量。

为便于事后考核与评价，可以重点考虑“按数据质量类型分类”方面的管理，以便量化评估当前风险数据质量是否符合公司所需高质量风险数据的要求。例如，在**唯一性方面**，针对核心业务实体设定唯一标识约束，技术实现上可以通过数据库唯一索引或哈希校验机制，实时捕获重复数据并标记异常；在数据量趋势方面，结合业务周期特性，设定合理的波动阈值（如每日交易记录数量保持在历史同期均值的±20%范围内），若出现突增或突降则触发预警机制；在**准确性方面**，对基础字段进行数据类型、格式及取值范围校验（如身份证号匹配18位正则表达式、交易金额不得为负数、质押标的证券代码符合交易所编码规范等），并重点验证字段间的勾稽关系，通过公式校验确保业务逻辑一致性；在**完备性方面**，检查关键字段的非空性（如客户表中的证件类型、交易表中的交易方向、结算方式等不得为空）。

以下以股票质押业务指标为例，建立跨层级可追溯的数据质量规则链。以股票质押业务“客户履约保障比例”指标为例，在实际使用场景中，需要保证该指标值处于业务实际

触及的范围内，例如字段不得为空，且最小值为 0。根据规则分类，上述规则属于单列规则及完备性和准确性规则；考虑到字段取值若超出规则范围，指标结果将无业务意义，可以设置为拦截类规则；字段取值与业务规则相关，一般由指标使用方提出，多为业务类规则。具体规则情况如下表。

表 7 “股票质押业务客户履约保障比例指标”应用层校验规则示例

规则编码	场景分类	数据主体	具体规则	逻辑类型	规则制定方	数据质量类型	强制性分类	阈值	版本
YY1KHFZ1	应用层	履约保障比例	履约保障比例大于 0	单列	业务	准确性	拦截	<=0	V1.0
YY1KHZC1	应用层	履约保障比例	非空	单列	业务	完备性	拦截	-	V1.0

应用层指标均由数据集市层数据加工而来，数据集市层对涉及的输入数据等由源端加工形成的数据进行数据质量检验。例如，对于“股票质押业务客户履约保障比例指标”，数据集市会记录客户负债、客户资产等结果数据，以及用于计算的过程数据或基础数据，如质押标的证券市值、待购回期间产生的权益、其他担保物价值等。上述字段均设定检验规则，除单列规则外，也可以将字段间勾稽关系作为单独校验规则，如设定“质押标的证券市值、待购回期间产生的权益、其他担保物价值之和应等于客户资产”等规则。完成数

据集市层数据质量规则设置，继续根据集市层数据追溯至源端设定类似或独特的数据质量校验规则。部分规则列举如下表。如后一层级直接使用前一层级数据，证券公司可以视数据重要程度、传输方式、数据可控程度决定是否需要在两个层级分别设置，或者仅前一层级设置校验规则。

表 8 “股票质押业务客户履约保障比例指标”集市层与源端校验规则示例

规则编码	场景分类	数据主体	具体规则	逻辑类型	规则制定方	数据质量类型	强制性分类	阈值	版本
JS1KHFZ1	集市层	客户负债	客户负债应大于 0	单列	业务	准确性	拦截	<=0	V1.0
JS1KHZC1	集市层	客户资产	客户资产应不小于 0	单列	业务	准确性	拦截	<0	V1.0
JS1ZYBDSZ1	集市层	质押标的证券市值	质押标的证券市值应不小于 0	单列	业务	准确性	拦截	<0	V1.0
JS1KHZC2	集市层	客户资产	客户资产应等于质押标的证券市值、待购回期间产生的权益、其他担保物价值之和	跨列	业务	准确性	拦截	-	V1.0

规则编码	场景分类	数据主体	具体规则	逻辑类型	规则制定方	数据质量类型	强制性分类	阈值	版本
JS1SJRQ1	集市层	数据日期	最新数据日期应为上一个交易日	单列	业务	及时性	预警	-	V1.0
	…								
YD1KHZC1	源端	证券市值	证券市值应等于证券价格、持有数量之积	跨列	业务	准确性	预警	-	V1.0
YD2KHZC2	源端	证券数量	证券持有数量应大于 0	单列	业务	准确性	拦截	<=0	V1.0
	…								

上述例子仅为展示数据质量规则设定逻辑，证券公司可以结合自身数据情况，针对必要的重要数据和关键环节设置校验逻辑。

（2）规则持续更新

质量规则更新通常发生在业务需求变更、数据源调整、质量问题复盘、监管合规要求或数据标准升级等场景下。例如，期货子公司的“资金核算变动历史表”如果触发了“数据数量完备性”，则按照闭环流程执行更新。在数据集市内

首先评估“资金核算变动历史表”下游引用情况，经分析，该数据在数据集市内只有风险并表场景使用，变更与影响范围可控，规则可变更。其次，针对数据量重新设计规则逻辑，增加过滤条件“金融工具资产类型为 0”，数据波动阈值及告警级别保持不变，并在测试环境中充分验证数据量波动、唯一性等场景。最后，通过业务方与数据所有者评审后上线至生产环境，持续监控规则命中率与问题发现效果，并据此迭代优化，从而保证数据质量始终稳定可控。

（二）事中监控

事中监控的核心工作是风险数据质量监测与问题处理。证券公司通过已建立的闭环风险数据质量问题处理流程进行问题跟踪处理，做好问题的根因分析和记录。

1.风险数据质量监测和预警

证券公司风险数据质量校验规则的监测结果可以分为“预警”和“拦截”两类。对于“预警”类校验规则，如果数据没有通过校验规则，数据进入下一个环节，但是事后需要数据使用方关注和分析预警信息；对于“拦截”类校验规则，如果数据质量水平低于可接受的水平（阈值），则技术人员进行干预，相关数据禁止流入下一个使用环节。对于重要的应用类风险数据，业务人员向技术人员提出明确的处理时间，例如不得超过 1 个工作日。证券公司需要将重要的应

用类风险数据的质量水平纳入日常数据质量监测，针对数据质量问题，启动问题处理流程，制定数据质量提升计划。

2.根因解决和记录数据问题

（1）确定问题跟踪责任人

风险数据责任人机制包括数据产生方、数据加工方、数据使用方。在发现数据问题时，问题发现方或数据治理（数据质量）的专岗（兼岗）作为监督数据更正的责任人。如果可以根据规则类型（源端规则/数据集市层规则/应用层规则）确定数据责任人，则将被规则约束的数据处理人（风险数据产生方/风险数据加工方）作为实施数据更正的责任人。

（2）问题诊断

发现问题的途径一般包括数据监控系统触发报警、数据使用人员在使用过程中发现数据矛盾、监管报送过程中发现数据不符合规范要求等，前述情形发生后即触发数据处理流程。通过数据产生方提供原始数据的生成日志、数据加工方追溯 ETL 过程代码与配置、数据管理部门检查系统接口传输记录的方式，定位问题的起源以及引发问题的隐形根因。通常可以将引发数据质量问题的原因分为五大类，并由专人记录问题台账以及问题产生的根本原因，便于事后进行回检。五大类原因总结如下:

一是源端数据录入问题，包括人工填报不规范、人工填

报错误、人工线下填报延误、人工源端系统维护问题等;

二是源端数据处理问题，包括源端系统人工执行问题、源端数据加工问题、源端数据传输等;

三是源端数据变更问题，包括业务调整历史数据问题、源端数据口径变更等;

四是数据集市加工问题，包括集市数据口径变更、集市加工问题、集市传输问题;

五是应用层数据加工问题，包括应用层数据口径变更、应用层人工执行问题、应用层系统维护问题等。

（3）制定修正方案

根据诊断结果，问题跟踪责任人牵头制定相应的修正方案，修正方案可以与源数据产生方、数据加工方和数据使用方（包括可能受数据直接或间接影响的所有数据使用方）共同协商，共同确定解决问题的最优解，评估内容包括实施成本和优势、实施计划和方案。

对于第一类源端数据录入问题，可以通过建立手工数据管理机制、建立录入端数据标准、明确权责关系、加强前端校验等方式进行源端数据录入质量管控；对于第二类源端数据处理问题，可以通过制定源端数据质量规则、建立源端数据质控管理机制、加强代码规范性管理等方式进行管控；对于第三类源端数据变更问题，可以通过建立数据修改规范、

业务调整变更流程、数据结构变更流程、数据口径变更流程等变更控制机制，及时通知下游数据使用者，实现对数据影响的分析和流程化控制，来确保对存储数据的所有更改都在实施之前得到定义、讨论和测试；对于第四类数据集市加工问题以及第五类应用层数据加工问题，均可以通过建立数据口径变更管理机制、完善数据质量规则库、优化系统自动验证功能等方式加强管控。

（4）方案实施

证券公司可以通过明确分工、过程监控与沟通、严格执行计划的方式修正数据问题。

一是明确分工，数据产生方根据修正方案的要求，确保原始数据生成过程的准确性和规范性；数据加工方作为方案实施的牵头者，负责按照既定的实施计划，对 ETL 过程进行调整和优化；数据使用方配合数据加工方和数据产生方，提供方案实施过程中所需的反馈信息，如数据使用过程中的具体需求和问题，确保方案实施不会对正常的数据使用造成影响。

二是过程监控与沟通，技术人员对方案实施过程进行全面监控，特别是系统接口传输记录等方面，确保数据在各个环节正常流转。数据产生方、加工方和使用方可以定期召开沟通会议，汇报方案实施进展，及时解决实施过程中出现的

问题，确保各方工作有效协同。

（5）效果验证

为了保证验证效果，可以设定验证指标和标准，并将其与质量度量指标关联。例如，准确性方面可以设定数据错误率低于一定比例，完整性方面可以检查数据缺失值的比例等。如果数据未达到质量要求，分析原因后提出进一步的改进措施，重新进入问题诊断和修正方案制定等环节，继续进行闭环管理；如果数据达到质量要求，则关闭问题处理流程，并对整个处理过程进行总结。例如，总结过往经验发现，很多数据问题都来自于复杂的数据处理过程，因此需要针对数据处理的全过程进行重点管控。

（6）问题归类和记录

根据问题解决效果对数据问题的根本原因进行归类，评估修正方案的有效性，作为下次同类问题制定修正方案时的经验参考，示例如下。

表 9 风险数据质量问题根因分析记录示例

问题描述	问题根因	细分问题根因	数据质量类型	数据质量类型细分	问题归口业务	问题归口单位	问题所属资产类型
同一业务系统宽表里债券业	源端数据处理	源端数据加工	完整性	数据缺失	债券投资业务	子公司 1	债券

务规模指标异常波动 ,缺少固定收益部数据		问题					
影响数据表范围	**影响同一业务系统的风控指标**	**临时解决方案**	**长期解决方案**	**问题处理岗位**	**问题跟进验证岗位**	**问题发现时间**	**问题解决时间**
表名 1、表名 2	1、债券投资业务规模合计 2、债券资产规模合计	重推、重采数据	增加源端及 ODS 层数据表质控，当数据缺失，自动二次推送集成	大数据开发岗	风险管理部、债券投资业务管理岗	2025/5/7	2025/5/8

（7）应急处理方案

发现风险数据质量问题时，原则上先发起问题处理流程，再处理和更正数据问题。如果应用层数据时效性要求较高，证券公司可以先行处理问题数据，并重点开展问题的根因分析和归类工作，后续补充问题处理流程或者发起简易的问题记录流程，确保问题记录无遗漏。

制定临时性的应急处理方案可以遵循下表中的原则。

表 10 临时性应急处理方案原则

方案类型	具体内容
临时数据替代方案	在数据质量未达标但需要紧急使用时，可启用预设的临时替代数据（如基准值、默认值或历史合规数据）。明确替代数据的使用场景、有效期及适用范围。
数据隔离缓冲区	对未通过拦截类规则的数据，临时隔离至专用缓冲区，标记为“待处理状态”，避免流入下游环节，同时触发告警机制。
标记与追溯机制	对问题数据添加“质量标识符”，记录问题类型、触发规则、处理状态等元数据，便于后续追溯与分析。

后续补录可以遵循下表中的原则，并使用标准化的补录模板，原则上，若补录未在一定时间内（例如 48 小时内）完成，系统自动通知至相应管理机构，仅当问题已被完全修复且风险可控时，经管理机构审批后可以豁免补录。

表 11 风险数据补录原则

补录要求	操作规范
时效性	紧急处理完成后，必须在 24 小时内启动完整的问题处理流程（参照闭环流程），补全记录并归档。
责任人	由数据责任人（产生方、加工方、使用方）共同确认补录内容的完整性。

补录要求	操作规范
完整性	补录内容包含：临时处理方案实施细节、问题根因分析、临时处理与最终修复的差异分析、风险评估及改进计划。

表 12 标准化补录模板示例

字段	内容要求
问题 ID	自动生成唯一编码，格式：QID-YYYYMMDD-流水号。
缓冲处理详情	记录临时方案类型、实施时间、涉及数据范围及负责人。
风险评估表	填写缓冲期间的潜在影响（如数据偏差率、监管处罚风险）。
根因分析报告	必须包含技术日志、规则执行记录、上下游系统接口日志。

（三）事后考核评价

事后考核评价过程的核心工作是风险数据质量回溯及提升报告、风险数据质量考核评价。

1.风险数据质量回溯及持续提升

风险数据质量回溯及提升报告的内容包括重要风险数据的质量趋势、重点领域数据质量情况、问题剖析、问题影响范围、异常问题提升措施及计划、前期问题提升措施执行情况等。

（1）风险数据质量回溯

证券公司可以基于业务复杂程度以及体量情况，选取定性、定量或两者相结合的方法，按照风险数据质量整体水平、数据分层、业务领域、业务开展单位等不同维度，对数据质量现状和问题进行比较分析。例如，针对定量分析，证券公司通过设计质量监测指标、预警阈值进行量化管控，提前与相关业务单位对设计、使用的质量监测指标进行商议及确认。以下为风险数据质量监测指标示例。

表 13 风险数据质量监测指标示例

指标名称	计算方式
风险数据健康度良好天数	监测周期内未发生风险数据问题的时间。例如，本月风险数据健康度良好天数为 25 天，即本月 25 天未发生风险数据质量问题。
风险数据质量问题数量	监测周期内，监测对象（如源端单位、业务领域等）发生风险数据质量问题的总次数。例如，本月部门 A 风险数据质量问题数量为 7 起，即基于问题根因分析，本月风险数据质量问题来源于部门 A 推送的数据质量问题，共发生 7 起。
风险数据质量问题表数量	监测周期内，监测对象（如贴源层）发生风险数据质量问题涉及的表数量。例如，本月贴源层风险数据质量问题表数量为 6 张，即本月贴源层共有 6 张风险数据表发生质量

指标名称	计算方式
	问题。
风险数据总体质量水平	完整性*权重 1+准确性*权重 2+及时性*权重 3+一致性*权重 4+唯一性*权重 5+规范性*权重 6。
完整性	[1-∑关键字段空值数/(记录数×关键字段总数)]×100%
及时性	[1-(影响表数量×问题天数)/(表总数×周期天数)]×100%
…	

以下为采取定量分析方式对源端单位风险数据质量进行报告的示例。

表 14 源端单位风险数据质量问题情况统计

源端单位	表总数（张）	本月问题数量（起）	问题情况排名[1]
部门 1	51	3	2
部门 2	36	1	3
部门 3	28	0	-
子公司 1	34	0	-
子公司 2	25	2	1

上表集中展示了各源端单位风险数据表总数、本月风险数据质量问题数量、问题情况排名。本月问题情况排名第 1

[1] 排名根据风险数据体量归一化后进行分布，排名计算公式为“问题数量/表总数”；排名数字越小，表示该源端单位风险数据质量问题越突出。

位的源端单位为子公司 2，问题均为数据就绪延迟，涉及表 18 张；经过子公司 2 排查，相关问题主要为业务人员数据填报延迟以及源端系统脚本执行异常；针对上述问题，后续公司需要加强各源端单位数据填报与加工管控，减少因人工上传遗漏或延迟以及系统数据处理异常导致的类似问题。

（2）风险数据质量提升

对于风险数据存在显著变化、超过风险管理容忍度、短期内解决难度较大、高发类、高危类等异常问题，数据管理部门组织相关部门进行根因分析和讨论，明确问题解决及提升措施，包括明确质量维度、业务领域、实施方案、组织、人员、计划等因素。通过风险数据质量回溯及提升报告等形式，定期向数据治理委员会、数据源端单位、数据使用方等汇报问题提升措施执行情况，确保数据质量问题有效获得解决。

2.风险数据质量考核

证券公司可以基于公司业务复杂程度以及体量情况，选取定性、定量或两者相结合的方法进行风险数据质量考核。例如，针对定量考核，建立风险数据质量考核指标体系，同时包括负向考核指标和正向考核指标两类。负向考核，即对于所生产（或加工）风险数据存在质量问题，拒绝或拖延配合风险数据标准落地、异常数据排查及整改等风险数据治理

工作的，予以考核减分。可以视情况设置正向考核，即按照监管部门要求和证券公司风险管理需要，能够积极履行风险数据报送义务，对风险数据治理工作产生正面积极影响或作出一定贡献的，予以考核加分。

风险数据质量考核以风险数据管理工作现状为前提，形成常态化机制，根据不同阶段的工作重点，选取重点领域的关键环节，设置考核指标和分值，并结合各单位实际情况进行差异化设置。随着数据工作的逐步推进，对考核指标和分值可以做出相应的调整。