证券期货业 IT 审计数据元
标准研究报告

【摘要】本课题在对证券期货业IT审计相关政策、标准、方法进行系统梳理基础上，通过“分层解耦、多维关联”的方法，设计构建了行业IT审计数据元模型，模型创新性地将“IT监管-IT技术-IT审计”三个维度的要求在数据层面进行了对齐、关联。课题组基于该模型整理形成了IT审计数据元规范草案，通过在课题组所在公司IT审计活动进行验证，课题研究能够有效解决IT审计覆盖不全面、系统兼容性差等核心问题，可为IT审计的标准化、自动化与智能化奠定坚实的数据基础。

关键词：IT审计；数据元；属性框架

目录

一、 引言.....3
（一） 研究背景.....3
（二） 遇到的问题、困难和挑战.....4
（三） 研究意义与价值.....6
（四） 研究目标.....7
二、 研究方法.....9
三、 研究结果.....12
（一） 行业概述.....12
（二） 行业 IT 审计体系分析.....13
1. 行业 IT 审计体系概述.....13
2. 行业现有 IT 审计标准.....14
（三） 证券期货业 IT 审计数据元规范研究.....17
1. 国际 IT 审计模型框架.....17
2. 证券期货业 IT 审计数据模型与属性框架设计.....18
3. IT 审计的数据元属性设计.....21
4. IT 审计的指标评估模型探索.....23
（四） 证券期货业 IT 审计数据元规范验证方案.....24
四、 研究结论与建议.....24
（一） 研究结论.....24
1. 规范与现有标准体系的兼容性分析.....24
2. 规范可行性验证情况.....25
3. 规范创新性分析.....25
（二） 建议与对策.....26
1. 对监管部门的建议.....27
2. 对行业机构的建议.....27
3. 对技术服务商的建议.....28

一、引言

（一）研究背景

进入 21 世纪以来，全球金融行业经历了一场波澜壮阔的数字化革命。作为现代金融体系的核心组成部分，中国证券期货业的信息化建设取得了举世瞩目的成就。从最初的交易无纸化、办公自动化，到如今的核心交易系统、风险控制系统、客户关系管理系统、大数据风控平台以及基于人工智能的投顾服务，信息技术已从业务支撑工具演变为驱动业务创新与发展的核心引擎。IT 系统的安全性、稳定性和有效性，直接关系到资本市场的公平、效率和稳定，关乎广大投资者的切身利益，乃至国家金融安全的大局。

在此背景下，中国证监会与行业自律组织对行业机构的 IT 治理与安全管理给予了前所未有的高度重视。近年来，一系列旨在强化 IT 风险管控的监管规定、指引和行业标准相继出台，其内容覆盖了信息系统等级保护、数据安全管理、网络安全、应急响应、云平台治理、应用系统生命周期管理等多个方面。据统计，各类成文的 IT 相关监管要求与行业标准已累计达到 4000 余项，构成了一个庞大而复杂的合规体系。

IT 审计作为公司治理和风险管理的第三道防线，是确保这些 IT 监管要求得以有效落地、IT 风险得以识别和控制的

关键机制。IT 审计通过对 IT 系统及其相关流程进行独立、客观的审查与评价，为公司管理层和监管机构展示真实、客观、全面的信息系统状况，是公司治理、合规管理的重要手段。然而，面对数量庞大、内容繁杂且不断更新的监管要求，传统上依赖审计人员逐条对照检查、主要凭借个人经验进行判断的审计模式，已显得力不从心。这种模式不仅审计成本高昂、周期漫长，更难以保证审计的全面性、一致性和及时性，无法适应金融科技快速迭代和风险形态动态变化的新环境。

因此，构建一套科学、统一、可扩展的 IT 审计标准体系，实现审计工作的规范化、系统化乃至自动化，已成为提升证券期货业整体 IT 治理水平的迫切需求。本课题“证券期货业 IT 审计数据元标准”正是在这一时代背景下应运而生，旨在通过标准化的语言和结构，为行业 IT 审计的现代化转型提供基础性支撑。

（二）遇到的问题、困难和挑战

当前，证券期货业在开展 IT 审计工作时，主要面临以下几个方面的深层次问题和挑战，其核心是数据层面的不一致与割裂：

审计数据定义不规范，缺乏统一“语法”：行业内对 IT 审计涉及的各类对象、过程和结果缺乏统一、精确的数据定义。

例如，对于“系统漏洞”的严重等级划分、对于“数据备份完整性”的验证标准等，都可能因机构或审计师的理解不同而得出迥异的结论。这种数据定义的不规范，导致审计结果难以在不同项目和不同机构间进行横向比对与聚合分析，严重制约了行业级风险视图的构建。

审计数据模型覆盖不全，难以应对新技术：现有的审计数据模型多围绕传统 IT 架构设计，对云计算、容器化、大数据平台、区块链平台、人工智能模型等新技术资产，以及敏捷与 DevOps 等新开发模式所产生的新型数据缺乏描述能力。这导致针对新技术的审计无据可依，相关风险数据无法被有效采集和评估，形成审计盲区。

审计数据与其它系统数据兼容性差，形成“数据孤岛”：IT 审计数据与 IT 技术标准（如系统日志格式、配置管理数据库 CMDB）、业务标准中的数据定义不一致，缺乏有效的映射关系。例如，审计系统难以直接从技术监控平台获取标准化的性能数据，或无法与业务连续性计划中的关键业务指标进行关联分析。这种兼容性的缺失，导致审计数据采集困难，审计自动化推进受阻。

审计证据数据难以机器处理，自动化程度低：大量审计证据以非结构化的文档形式存在，缺乏机器可读的统一格式。审计证据的收集、整理和分析大量依赖手工操作，审计结论的得出也高度依赖审计师的主观判断，缺乏基于统一数据标

准的自动化分析与判定能力，导致审计效率低下且质量不均。

（三）研究意义与价值

本课题专注于证券期货业 IT 审计数据元规范细则的研究，是推动行业 IT 审计工作向标准化、规范化、数字化转型的重要基础性工程，具有深远的理论价值和实践意义。

1、理论创新价值：构建了行业 IT 审计的数据基石

本研究首次建立了证券期货行业 IT 审计数据元规范体系，填补了行业在 IT 审计数据标准化领域的空白。通过构建“IT 审计监管-IT 系统建设运营-IT 审计”三维数据模型，创新性地实现了从监管要求到技术实现、再到审计执行的全链路数据贯通。所提出的四类 23 项数据元属性（基础属性、监管规则属性、IT 技术属性、IT 审计属性），为理解和使用复杂信息系统环境下的审计对象提供了全新的方法论工具，丰富了金融科技治理的理论体系。

2、实践应用价值：破解 IT 审计工作的核心痛点

本研究的核心价值在于系统性地解决了行业长期面临的 IT 审计难题。一是破解了“数据定义不统一”的困境，通过统一的数据元标准，使不同机构、不同审计项目的结果具备可比性，为行业风险视图构建奠定基础。二是解决了“审计覆盖不全面”的问题，通过标准化的资产域、行为域分类体系，确保了对传统架构和云计算、大数据等新技术领域的

全面覆盖。三是打通了“数据孤岛”的壁垒，通过标准化的数据格式和接口定义，实现了审计数据与技术数据、业务数据的有效对接，为审计自动化提供了可能。

3、行业推广价值：赋能行业数字化转型与风险防控

本标准的推广应用将产生显著的行业价值。对于行业机构，基于统一数据元的审计工作将极大提升审计效率和质量，降低合规成本，同时为机构 IT 治理的持续改进提供数据支撑。对于监管部门，标准化的审计数据为实施科技监管提供了基础，支持行业风险的趋势分析和精准监管。对于整个行业，统一的“数据语言”将促进技术服务商开发兼容的产品生态，推动行业 IT 审计技术水平的整体提升，进一步增强证券期货业关键信息基础设施的风险抵御能力，为资本市场的稳定运行提供坚实保障。

本研究不仅产出了一份技术标准，更是推动行业 IT 审计工作从“经验驱动”向“数据驱动”转变的关键举措，对提升行业 IT 治理整体水平具有里程碑意义。

（四）研究目标

为解决上述数据层面的核心挑战，本课题设定了清晰的研究目标，旨在通过建立统一的数据元标准，为行业 IT 审计提供基础性数据支撑：

1、构建统一的 IT 审计数据元体系：研究并建立一套行

业通用的 IT 审计数据元标准，对审计相关的所有数据实体进行规范化、结构化的定义，明确其属性、表示和允许值，解决数据定义不统一的根源性问题。

2、建立全面覆盖的 IT 审计数据模型：构建一个涵盖“IT 审计监管”、“IT 系统建设运营”（可细分为治理、资产、行为）和“IT 审计”三个维度的数据模型，系统性地补全对云计算、容器化、大数据平台、区块链平台、人工智能模型等新技术，以及敏捷与 DevOps 等新开发模式所产生的新型数据的描述能力，确保对传统及新兴 IT 活动与对象的全面覆盖。

3、定义标准化的数据元属性框架：明确每个数据元的基础属性、监管规则属性、IT 技术属性和 IT 审计属性，打通从监管要求到技术实现，再到审计执行的全链路数据关联。

4、提升数据的互操作性与机器可处理性：通过规范数据类型、值域和格式，标准化逻辑接口，增强 IT 审计数据元与现有 IT 技术标准、业务数据标准之间的兼容能力，打破“数据孤岛”，为审计数据的自动采集、交换与集成分析铺平道路。

5、形成可落地的标准草案：最终产出具备高度可操作性的《证券期货业 IT 审计数据元》草案，基于此探索建立一套合理的存储结构及动态更新的机制，并通过可行性验证，确保该标准能够切实指导行业机构的 IT 审计数据治理与实践。

二、研究方法

为确保课题研究的科学性、系统性和实用性，本课题综合采用了以下多种研究方法，其核心是围绕“数据”进行标准化设计:

（一）多维度数据模型构建法

为系统化解构复杂的 IT 审计对象，本课题采用多维度数据模型构建法作为研究的顶层设计框架。该方法论借鉴了企业架构（Enterprise Architecture）的思想，特别是 Zachman 框架中“从不同参与者视角描述同一复杂系统”的核心理念。我们通过引入“分层解耦”的原则，将宏观的治理要求、中观的资产实体与微观的运行行为进行分离，进而构建了 “IT 审计监管维度 - IT 系统建设运营维度 - IT 审计维度” 的三维融合数据模型。该模型旨在打破传统审计中各类要素混杂的困境，为后续的数据元标准化提供了一个结构清晰、关系明确的容器，确保了研究范围的完整性与逻辑的自洽性。

（二）标准化数据元建模法

为实现审计数据的精准、无歧义定义与机器可读，本课题采用了标准化数据元建模法。此方法是实现数据治理与互操作性的关键。我们对三维模型中识别出的所有数据对象进行本质属性的抽象与定义。通过规范其“中文名称”、“编号”、“数据类型”、“值域”等基本属性，并扩展其与监管、技术、审

计流程相关的上下文属性，最终形成了一套结构化的数据元属性描述规范，为将非结构化的审计要求转化为可被信息系统直接处理的结构化数据奠定了坚实基础。

（三）量化指标拆解与验证法

为克服 IT 审计中过度依赖定性描述与主观判断的弊端，本方法专注于如何将模糊的定性要求转化为清晰的定量指标。

1、三级转化模型

我们建立了“定性描述→量化阈值→验证路径”的转化链条。

（1）定性描述：首先，准确理解监管条文或制度中的原始要求，将原则性的监管要求或控制目标分解为可观测、可测量的关键问题。

（2）量化阈值：然后，通过专家研讨、历史数据分析、行业对标等方式，为每个问题设定具体的、可测量的数值型阈值或明确的二元状态（是/否）。例如，将“定期进行安全演练”转化为“每半年至少进行一次全链路应急演练，演练成功率达 95%以上”。

（3）验证路径：最后，明确如何获取证据来验证是否达到阈值。这包括证据来源（如系统日志、配置管理系统、访谈记录）、采集方法（自动拉取、手动提交）和验证程序（抽样比例、核查脚本）。

2、配套执行手册

为每个关键的审计项开发配套的执行手册，详细说明其指标定义、计算公式、数据来源、验证步骤和判断标准，确保不同审计人员在执行同一审计项时尺度统一。

（四）智能分析模型构建法

为了最大化利用标准化、结构化后的审计数据，本课题前瞻性地探索了数据分析技术在审计中的应用。

1、纵向趋势分析模型：基于时间序列数据，对同一机构的特定审计指标（如漏洞数量、故障率、合规得分）进行历史趋势分析，识别其IT治理水平的改善或恶化趋势，实现动态风险预警。

2、横向同业对标模型：在匿名化和聚合的前提下，将单一机构的审计结果与行业平均水平或标杆机构进行横向比较，帮助机构识别自身在行业中的位置和差距。

3、智能诊断与报告：探索利用数据可视化技术和交互式钻取功能，使审计人员能够从高层面的结论快速定位到具体的风险点或异常数据。同时，研究基于模板的动态报告生成技术，自动将审计发现、证据和分析结果汇总成标准化的审计报告初稿，大幅提升审计工作效率。

三、研究结果

（一）行业概述

中国证券期货业是一个高度信息化、技术密集型的行业。其业务具有高实时性、高并发性、高可靠性和高安全性的典型特征。从经纪业务到投资银行，从自营投资到资产管理，从场内交易到场外衍生品，几乎所有的业务环节都深度嵌入在 IT 系统之中。行业机构，包括证券公司、期货公司、基金管理公司以及各类交易所、结算机构等，其 IT 系统不仅承载着每日数以万亿计的交易和结算，更关乎市场信心和金融稳定。

近年来，行业在金融科技领域的投入持续加大，数字化转型步伐加快。移动互联网、云计算、大数据、人工智能等技术的应用，在提升服务效率、创新业务模式、优化客户体验的同时，也使得技术架构日益复杂，系统关联性不断增强，新型风险随之涌现。例如，微服务架构虽然提升了系统弹性，但也增加了攻击面；公有云的使用带来了弹性与成本优势，但也引入了第三方依赖风险; AI 模型的决策过程如果缺乏透明度和监督，可能引发合规与声誉风险。

在此背景下，监管机构持续强化穿透式监管和科技监管，对行业机构的 IT 治理、网络安全、数据保护提出了更高、更细的要求。IT 审计作为验证合规、揭示风险、促进改善的重

要手段，其角色正从传统的“合规检查员”向“风险前瞻者”和“价值守护者”转变。因此，构建一个适应未来发展的现代化IT审计体系，已成为行业高质量发展的内在需求和必然选择。

（二）行业IT审计体系分析

1. 行业IT审计体系概述

我国证券期货业的IT审计经过多年发展，已初步形成了一套以监管提出合规要求为输入，能够系统、全面覆盖IT活动各方面，通过定期或专项内外部审计形式，可突出重点IT活动或领域的IT审计体系。展开来看，行业IT审计体系有以下特征:

（1）以监管合规为导向，IT审计需求以监管对机构信息技术各类活动的监管要求为依据。（2）覆盖IT活动各方面，IT审计能够覆盖基础资源、基础软硬件、应用系统、数据等不同资源，同时能够兼顾系统需求、研发、测试、上线、运营等不同阶段。（3）审计方法全面，基于行业审计规范，结合访谈、检查、测试等多种审计方法。（4）突出行业特色审计领域，结合行业特色，重点突出IT治理审计、信息系统生命周期审计、数据安全审计等重点活动和领域。

然而，该体系在很大程度上仍依赖于文档审阅、访谈和抽样测试等传统方法，体系的标准化、自动化程度不高，且各部分之间的逻辑关联性未能通过数据模型得到有效体现。

2. 行业现有 IT 审计标准

（1）国内已有的 IT 审计规则、标准

国内监管体系：重点梳理了《网络安全法》《数据安全法》，以及由中国证监会、中国证券业协会、中国期货业协会等发布的《证券期货业网络和信息安全管理办法》、《证券基金经营机构信息技术管理办法》、《证券期货业网络安全等级保护基本要求》、JR/T 0146 系列（证券期货业信息系统审计指南）等核心监管文件及行业重要标准。

（2）国际已有的 IT 审计规则、标准

国际标准与法规：课题组对不仅对 COBIT (Control Objectives for Information and Related Technologies)、ITIL (Information Technology Infrastructure Library)、ISO27001(信息安全管理体系) 等主流的 IT 治理与管理框架进行了学习和梳理，还参考了诸如美国 SOX 法案（萨班斯-奥克斯利法案）中关于 IT 内部控制的要求、欧盟 GDPR（通用数据保护条例）中关于数据隐私的审计要点等，以吸收其在 IT 风险控制方面的先进经验。

（3）现有 IT 审计规范分析

课题组投入大量资源，对国内外与 IT 审计相关的政策

与标准进行了系统性的梳理和“原子化”解构。我们发现，当前规范体系复杂且庞大，存在多源性、碎片化、滞后性等特点。

多源性与碎片化：国内外规范出自不同监管机构、标准组织，其术语体系、结构框架和控制目标存在显著差异。

- 国内监管的纵向细分:国内监管体系呈现出多层次、多部门的特点。例如，《网络安全法》和《数据安全法》奠定了顶层法律基础；证监会发布的《证券基金经营机构信息技术管理办法》是行业运营的综合性规章；而《证券期货业网络安全等级保护基本要求》则提供了具体的技术和管理控制点。这些规范虽各有侧重,但控制点之间存在大量交叉与重叠。例如,“数据安全”的要求同时散见于《数据安全法》、《信息技术管理办法》和“等保 2.0”中，但三者的表述粒度、检查重点和证据要求并不完全一致，导致机构在拆解和落实时，极易产生歧义。
- 国际框架的横向差异：国际标准同样如此。COBIT 聚焦于高阶的 IT 治理目标，ISO27001 提供了一套完整的信息安全控制集，ITIL 则详述了服务管理流程。当审计人员试图综合运用这些框架时，会发现对一个控制点（如“变更管理”）的描述，COBIT 关注治理有效性，ISO27001 强调安全风险

评估，而 ITIL 规定具体操作流程。这种框架间的“语言不通”，使得构建统一的、自动化的审计数据采集模型变得异常困难。

规范内容的“滞后性”：成文的法规和标准更新周期长，难以跟上云计算、人工智能、敏捷开发等技术的迭代速度。现有的核心审计规范和指南成型时，云原生、微服务、AI 大模型等尚未成为主流。因此，规范中缺乏针对这些新对象的特异性控制要求。例如，对于容器安全的审计，传统规范中关于“服务器安全配置”的检查项无法直接适用，需要对“镜像漏洞扫描、运行时安全、编排工具配置”等新维度进行审计，但这在旧有体系中是空白。

原则性规定缺乏可操作性：许多规范条文使用“应加强”、“应确保”、“必要的”等原则性表述。例如，《数据安全法》要求“采取相应技术措施和其他必要措施，保障数据安全”。但何为“相应”和“必要”？在审计云上数据加密时，是应用层加密、数据库透明加密还是云服务商提供的服务端加密？不同的选择对应不同的风险和控制措施，原则性规定无法为审计提供清晰的、可验证的判断标准。

规范体系的“孤岛效应”：IT 审计规范、IT 技术标准与业务数据标准由不同的组织制定，目标各异，彼此间缺乏预设的“接口”，数据无法顺畅流转。一方面是与技术标准脱节。IT 审计规范要求检查“系统日志完整性”，但各类操作

系统、数据库、应用系统产生的日志格式千差万别。审计规范并不会规定日志应采用何种标准格式（如 CEF、CEE），导致审计工具难以自动解析和采集证据，大量依赖手工操作。另一方面是与业务标准关联薄弱。IT 审计的终极目标是支撑业务稳定运行。然而，IT 审计规范中很少要求将 IT 控制失效与具体的业务影响（如交易延迟、客户损失、财务影响）进行量化关联。例如，审计发现“数据库性能阈值告警响应缓慢”，这一技术发现很难直接映射到《证券法》中关于“保障交易系统安全、连续、稳定运行”的业务合规要求，使得 IT 审计的价值在管理层眼中被打折扣。

（三）证券期货业 IT 审计数据元规范研究

1. 国际 IT 审计模型框架

为提升行业 IT 审计体系的成熟度，本课题系统研究了国际主流的 IT 治理与管理框架，并从中汲取精华。

（1）COBIT：由 ISACA 发布，是国际范围广泛认可的 IT 治理框架之一。COBIT 提供了端到端的 IT 治理和管理目标体系，将 IT 流程与企业目标紧密相连。其最新版本 COBIT 2019 强调了对企业 I&T（信息与技术）的整体治理，并提供了完善的管理目标和绩效指标。本课题借鉴了 COBIT 的流程分类和关键目标指标（KGIs）、关键绩效指标（KPIs）的设计思路，用于构建治理域的管理目标和审计指标。

（2）ITIL：ITIL 是 IT 服务管理领域的事实标准。它详细描述了 IT 服务从设计、转换到运营、改进的全生命周期管理流程。本课题在“行为域”的设计中，大量参考了 ITIL 关于事件、变更、问题等管理流程的最佳实践，将其作为评估 IT 运维行为规范性的重要依据。

（3）ISO/IEC 27001 ：该标准为建立、实施、维护和持续改进信息安全管理体系（ISMS）提供了要求。其附录 A 中的 114 项控制措施，为网络安全和数据安全领域的审计提供了丰富的控制点来源。本课题将这些控制点进行了吸收和转化，映射到三维框架中的相应位置。

（4）NIST Cybersecurity Framework (CSF)：由美国国家标准与技术研究院发布，该框架通过识别（Identify）、保护（Protect）、检测（Detect）、响应（Respond）、恢复（Recover）五个核心功能，提供了一个动态的、基于风险的网络安全治理思路。本课题在行为域中关于安全事件的监测与响应部分，深受 NIST CSF 的启发。

通过融合这些国际先进框架的精华，并结合中国证券期货业的特定监管环境和业务特点，本课题构建的审计域框架既具备了国际视野，又确保了本土的适用性。

2. 证券期货业 IT 审计数据模型与属性框架设计

我们依据行业实践，成功构建了 IT 审计数据模型和一

套完整的数据元属性框架。

作为数据元定义的顶层框架，IT 审计数据模型由三个维度组成：

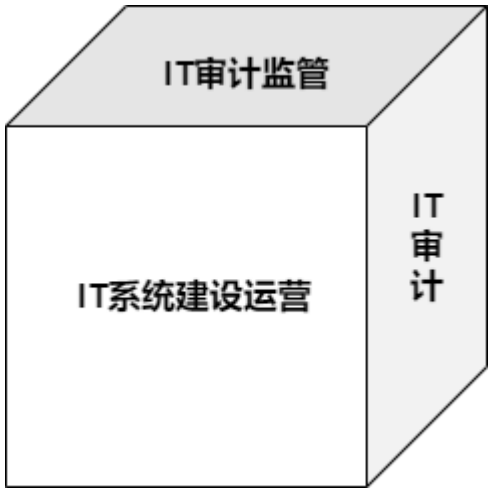

图 1IT 审计数据模型

（1）IT 审计监管维度

此维度定义了数据的合规来源。我们系统性地梳理了国家有权部门、行业监管部门发布的累计 4000 余项 IT 相关管理要求，将其作为数据元的合规依据。数据元中的“监管规则属性”直接与此维度关联。

（2）IT 系统建设运营维度

此维度定义了数据的实体来源和上下文。它涵盖了机构在 IT 技术标准与最佳实践指导下进行系统建设与运营所产生的全部数据。本课题将其进一步划分为：

- 治理域：关注 IT 管理的制度、组织和流程，对应数据元中的“数据遵循制度/规范”、“数据归属组织机构”等属性。
- 资产域：关注具体的 IT 资源，包括机房、设备、基础

软件、信息系统、数据、文档等，对应“数据所属资产类型”属性。

- 行为域：关注 IT 资产的活动，包括建设管理、安全管理、运维管理等，对应“数据所属活动”属性。

（3）IT 审计维度

此维度定义了数据在审计活动中的用途。它涵盖了审计计划、执行、报告等阶段所需的数据，直接对应数据元的“IT 审计属性”，如“审计目标”、“检查方法”、“审计结论”等。

这个三维模型确保了每一个数据元都能被清晰地定位和定义，明确了它从何而来（监管/技术）、属于何物（资产）、源于何事（行为）、用于何途（审计）。

数据模型的价值：该模型明确了 IT 审计数据的三大来源（监管、技术、审计）及其相互关系，为数据元的采集、整合与应用提供了逻辑清晰的顶层设计。它确保了数据定义的范围既无遗漏，也无冗余。

在数据模型确立后，我们采用标准化数据元建模法精确界定每个审计数据的各项特征，共计定义了 23 项属性，归属四大类，分别是基础属性、监管规则属性、IT 技术属性和 IT 审计属性，形成 IT 审计数据属性框架。

属性框架是数据模型的具体实现，它的构成具有以下**创新性**：

- 全链路打通：通过“监管规则属性”关联法规，通过“IT 技术属性”落地到具体资产和活动，通过“IT 审计属性”

指导审计执行，实现了 “监管-技术-审计” 的全链路数据贯通。

- 增强可操作性: “检查方法”（访谈、检查、测试）、“证据材料类型”（电子、书面、实物）等属性的明确，为审计人员提供了清晰的操作指南。
- 明确责任主体: “数据归属组织机构”、“数据归属人员”等属性，将数据管理责任落实到具体的组织和个人，强化了主体责任。

3. IT 审计的数据元属性设计

我们严格遵循 GB/T 1.1 及金融行业数据元标准（JR/T 0304 系列）的规范设计四大类 23 项数据元属性。

（1）基础属性：描述证券期货业 IT 审计数据的基本特性。基础属性包括中文名称、编号、适用机构、数据类型、安全级别、实际取值。

（2）监管规则属性：在证券期货业 IT 审计业务中，监管规则属性用于界定、分类和关联审计数据所涉及的外部监管要求与合规标准，确保审计活动与法律法规、行业规范及政策性文件保持一致。监管规则属性包括关联外规名称、关联外规条款和合规取值要求。

（3）IT 技术属性：IT 技术属性是指证券期货行业信息技术系统在支撑业务运行过程中所具备的各类特征和特性

的集合。这些属性按照管理视角和功能维度可划分为数据遵循制度/规范、数据归属组织机构、数据归属人员、数据所属资产类型、数据所属系统、数据所属活动。

（4）IT 审计属性：描述数据与证券期货业 IT 审计业务相关联的特性。IT 审计业务属性包括数据所属审计主题、审计主题标识、审计方法、检查频次、审计规程、审计目标、证据材料类型。

对每个属性，我们都采用名称、说明、数据类型、值域、约束、备注等描述符进行严格定义。特别是“值域”，我们采用了包括字符类型（a,n,c,an,anc）、格式（M!an, anc..M）、代码表（如审计结论、资产分类）等多种方式予以精确约束，确保了数据值的规范性和一致性。

同时，为实现数据的有效管理和应用，本课题为关键属性建立了统一的分类与编码体系。

资产域分类体系：建立了“一级分类（如机房、设备、信息系统）”和“二级分类（如计算设备、网络设备、核心交易系统）”的两级资产分类树，为 IT 资产数据的归集提供了标准目录。

行为域分类体系：同样采用两级分类（如一级“建设管理”，二级“规划设计、采购管理”等），对 IT 活动进行标准化描述。

审计主题编码：对“物理环境”、“网络安全”等审计主题，既定义了中文名称，也规定了英文标识符，便于信息系统实

现。

数据元唯一编号：设计了“适用机构代码-序号”的编号规则，确保每一个数据元在全行业范围内具有唯一性标识。

4. IT 审计的指标评估模型探索

拥有指标后，需要模型来对指标数据进行综合评估。我们探索了两种主要的评估模型：

（1）加权评分卡模型

适用于对多个指标进行综合性评价。例如，对“网络安全”这一审计领域，可以包含“漏洞管理”、“入侵防护”、“安全日志”等多个指标。通过专家打分法或层次分析法为每个指标赋予权重，最后计算加权得分，得到该领域的总体审计评分。该模型直观易懂，便于横向和纵向比较。

（2）基于规则引擎的自动判定模型

对于有明确阈值的指标，可以构建规则引擎。系统自动采集证据数据，与预设的审计标准（阈值）进行比对，直接输出“通过”、“警告”或“不通过”的判定结果。例如，规则可定义为：“IF 漏洞修复率 ＜95% THEN 判定为不通过”。这种模型极大地提高了简单审计项的自动化判定效率。

在实际应用中，通常将两种模型结合使用，以实现对不同粒度审计目标的高效、科学评估。

（四）证券期货业 IT 审计数据元规范验证方案

理论研究和标准设计最终需要接受实践的检验。在课题研究周期内，我们选取一家证券公司作为试点单位，开展《证券期货业 IT 审计数据元标准》（草案）的可行性验证。

验证工作分为两个阶段：

（1）映射验证：请试点机构利用本标准草案，对其现有的 IT 审计规程和检查清单进行映射和改造。验证标准条款的覆盖是否全面，定义是否清晰，能否有效指导审计实践。

（2）技术验证：在试点机构的信息系统和审计工具中，尝试按照本标准草案定义的元数据格式，对部分审计项进行自动化的数据采集和初步分析，验证标准的可机器处理性和技术可行性。

四、研究结论与建议

（一）研究结论

1. 规范与现有标准体系的兼容性分析

目前金融领域数据标准相关研究进展迅速，不仅有 JR/T 0319-2024《证券期货业数据标准属性框架》等已发布实施标准，还有《数字金融 金融科技风险管理数据元》等即将完成研究的标准。课题组在编制本规范时，充分考虑与相关标准关系，在模型、属性设计中，充分借鉴相关规范内容，并在

内容梳理、规范编写等过程中充分考虑与相关规范的兼容性、一致性。

2. 规范可行性验证情况

通过在项目组所在单位内部的可行性验证，最终验证结果表明:

- 覆盖性：本标准草案能够覆盖试点机构 90%以上的现有 IT 审计需求，并对新技术领域提供了有效的审计指引。
- 可操作性: 审计人员普遍反映，结构化的元数据标准使审计目标更明确，证据要求更具体，减少了争议和模糊地带。
- 技术可行性：基于标准格式进行数据对接在技术上是可行的，但需要对现有系统和格式进行一定的适配改造。

在验证过程中，项目组所在单位相关部门、参与验证人员也提出了一些建议，如需要提供更多的示例、加强对复杂指标计算方法的指导等，这些都已作为标准后续完善的输入。

3. 规范创新性分析

经过深入研究与实践验证，本课题得出以下核心结论:

（1）构建了行业统一的 IT 审计数据元框架

本研究成功创建了以三维数据模型和四类属性为核心的 IT 审计数据元标准框架。该框架逻辑严谨，覆盖全面，系统地解决了 IT 审计数据定义混乱、关联性弱的核心问题，为行业提供了一套统一的“数据语言”。

（2）奠定了 IT 审计数字化的数据基石

所定义的 IT 审计数据元标准，为实现审计证据的结构化、审计流程的标准化和审计分析的自动化提供了关键前提。这是推动行业 IT 审计从“经验驱动”迈向“数据驱动”的根本保障。

（3）显著提升了审计工作的规范性与效率

通过明确每个数据元的业务属性和技术属性，本标准极大减少了审计过程中的主观理解和歧义。同时，标准化的数据格式为审计工具自动采集和处理证据奠定了基础，将显著提升审计效率。

（4）研究成果具备高度的实践价值与推广前景

可行性验证表明，本标准草案设计合理，具备很强的可操作性。它的推广应用，将有效打通机构内部及行业间的数据孤岛，为构建行业级 IT 风险洞察能力提供数据支撑，有力助推整个证券期货业 IT 治理水平的提升。

（二）建议与对策

为确保本研究成果能够顺利转化为行业生产力，特提出

以下建议:

1. 对监管部门的建议

帮助进行标准完善，尽快发布《证券期货业 IT 审计数据元规范》行业标准。项目组通过本研究，已经验证通过对 IT 审计数据元进行规范化，能够有效提升 IT 审计、IT 技术的协同，对机构 IT 合规有较强的推动作用，但本课题仍局限在少数机构，相关成果能否在行业中广泛推广有待进一步验证。建议监管部门组织开展标准的完善，由行业标准化机构、各类行业机构代表共同优化规范内容，待规范内容成熟后尽快审议发布，并在全行业推广实施。

探索在行业监管数据报送、行业审计平台等行业公共平台中应用本规范。行业公共平台是推广行业标准的窗口，本规范建立的数据元模型能够关联 IT 审计数据涉及监管要求、IT 系统建设运营情况、IT 审计检查等不同领域的内容，相关内容与行业公共平台有高度关联，若将本规范在行业监管数据报送等行业公共平台中应用，不仅可以提升相关数据的规范化程度，还能带动行业机构各相关领域数据的规范化。建议在行业公共平台中选取试点业务，对本规范

2. 对行业机构的建议

开展内部数据元对标：各机构应组织科技、审计、合规

部门，系统学习并应用本标准，以此为基础梳理和改造现有的审计规程、检查清单和证据材料模板，实现内部审计数据的标准化。

推动系统改造与数据治理：在规划和升级审计管理系统、IT 运维监控系统、配置管理数据库时，应要求其数据模型与本标准的数据元属性框架对齐。以此为契机，推动机构内部的 IT 数据治理。

培养数据素养：加强对 IT 审计人员的培训，使其掌握本标准的内涵与应用方法，培养既懂审计、懂技术又懂数据的复合型人才。

3. 对技术服务商的建议

研发兼容标准的产品：鼓励审计软件、运维监控系统等技术服务商，主动使其产品支持本标准定义的数据元模型。开发支持标准数据格式的导入、导出、分析和可视化功能。

提供标准落地解决方案：针对机构在标准落地过程中遇到的数据采集、系统对接等挑战，开发相应的工具和实施方法论，提供端到端的解决方案，降低行业实施成本。

共建产业生态：积极参与行业生态建设，与机构共同探索基于统一数据元标准的审计分析模型和创新应用，共同推动 IT 审计技术的发展和进步。

角色	姓名	单位	职务
课题负责人:	罗清平	中国银河证券	副总经理（主持工作）
课题成员：	李沁蕾	中国银河证券	内控管理岗
	孟宪哲	中国银河证券	内控管理岗
	姚任远	中国银河证券	内控管理岗
	戴雯	中国银河证券	内控管理岗
	张海龙	金证科技	执行董事
	陈曦	金证科技	高级产品经理
	张天元	金证科技	高级产品经理
	相烨	金证科技	高级开发经理
	邹培岩	金证科技	产品经理