数据合规审计的实践向度与风险因应
——一个概念建构的分析框架及其考证

徐京平,朱沛雯

(西北政法大学 管理学院,陕西 西安 710122)

[摘　要]数据合规审计作为新时代数字经济高质量发展的重要支撑,其核心在于通过对数据合规开展审计,推动数据全生命周期循环治理体系的建设。以“源头采集 - 存储传输 - 处理使用 - 销毁归档”的数据全生命周期为主线,构建数据合规审计的理论分析框架。在系统阐释其概念建构与实践向度的基础上,提出数据合规审计风险因应的四条路径:以数据地图追溯破解数据源头与采集的合规风险,将被动审计升级为主动与持续的闭环监督;以分级授权制度筑牢数据存储与传输的合规防线,实现风险的持续管控;以日志存证系统规范数据处理与使用的合规路径,将静态合规检查转化为动态技术性监督;以自动化管理平台加固数据归档与销毁的合规屏障,实现对数据全生命周期末端的实质性验证。

[关键词]数据合规审计;数据全生命周期;数据要素;数据治理;合规治理;数据安全;数字经济

[中图分类号]F239.44　　[文献标志码]A　　[文章编号]1004 - 4833(2026)04 - 0030 - 12

一、引言

数字经济时代,数据作为关键生产要素的战略地位在国家顶层设计中被不断巩固与加强。2014 年大数据首次写入国务院《政府工作报告》,标志着我国开始进入数字经济时代。2020 年 5 月,《关于构建更加完善的要素市场化配置体制机制的意见》将数据列为与土地、劳动力、资本、技术并列的第五大生产要素。伴随数据的价值被广泛认可,其规范化管理与资产化进程加速推进。2025 年 1 月,国家发展和改革委员会、国家数据局公布《公共数据资源登记管理暂行办法》《公共数据资源授权运营实施规范(试行)》和《关于建立公共数据资源授权运营价格形成机制的通知》,初步构建完成公共数据资源开发利用“1 + 3”政策体系。2025 年 2 月发布的《个人信息保护合规审计管理办法》(国家互联网信息办公室令第 18 号)(后文简称《办法》),作为规范审计活动的专门办法,其出台凸显了国家在数据价值释放与公民权益保护之间寻求价值均衡的监管决心,也标志着对数据处理活动合规性的审查与监督进入制度化、强制化的新阶段。

递进的政策演进勾勒出一条清晰的脉络:数据要素的市场化配置与价值释放是国家战略方向,而其规范化与合规化管理是实现这一目标的保障与前提。从确立数据的生产要素地位到《办法》的出台,表明我国政策重心已从宏观倡导转向微观规制,从价值确认转向风险防控。在此背景下,数据合规审计逐渐跃升为一项关系数据要素市场健康、有序和可持续发展的重要保障。通过独立、客观且专业的审查和评价,数据合规审计可以有效识别数据处理流程中存在的合规偏差与潜在风险,既为监管提供决策支持,亦为数据主体权益保护构筑坚实的防线。然而,数据合规审计在理论认知、实践模式和风险因应三个层面仍存在较为明显的空白和挑战:一是概念内涵有待清晰界定;二是具体内容与方法等实践向度亟须体系化探索;三是在审计过程中,面对数据合规风险的动态性和复杂性,如何精准识别、科学研判并采取高效的应对策略是实务中亟待突破的关键挑战。基于此,本文围绕数据合规审计的概念建构、实践向度与风险因应展开探讨,力求厘清其学理根基,系统构建多维实践框架,并针对关键风险因子探索切实可行的应对策略,以期为我国数据要素市场的合规、高效与安全运行提供理论支撑与实务参照,亦为构建中国审计学自主知识体系提供有益支撑。

[收稿日期]2025 - 11 - 12

[基金项目]国家社会科学基金项目(25XGL003);审计署重点科研项目(24SJ03003);西北政法大学省部级科研机构科研项目(SJJG202409)

[作者简介]徐京平(1984—),男,山东烟台人,西北政法大学管理学院教授,博士生导师,博士,从事审计法规与国家审计理论研究,E-mail:13759996123@139.com;朱沛雯(1999—),女,宁夏银川人,西北政法大学管理学院硕士研究生,从事国家审计与数据治理研究。

二、文献回顾与理论溯源

(一)技术倒逼下传统合规审计的范式跃迁

1. 承继基础:传统合规审计的本质核心

传统合规审计的根本在于依据合规标准,独立监督、鉴证及评估组织行为的合法性与合规性[1]。该本质在其发展进程中始终保持稳定,构成数据合规审计的重要根基。从功能定位来看,传统合规审计以合规标准为重要依据,侧重于合规性内部审计,并随时代发展持续向现代化形态演进[2]。传统合规审计的功能包含合规监督、合规鉴证与合规评估等,并形成了"审查-鉴证-改进"的闭环。从实施逻辑来看,传统合规审计始终坚持重要性原则,在审计计划、实施和评价的过程中,都借由明确的行为偏差容忍度与优化审计资源配置来保障审计效率与风险防控之间的动态平衡。同时,传统合规审计高度重视企业合规管理体系的完整性和有效性,其审计结果直接影响审计收费与审计质量,成为完善企业治理[3]、提升企业价值的重要支撑[4]。从应用场景来看,传统合规审计最初围绕金融会计展开[5],随后逐步延伸至经营性审计与综合合规审计,强调内部审计机构设置与职能落实,注重与企业内部控制之间的协作[6]。在传统合规审计的发展进程中,会计师事务所等专业服务机构的参与进一步强化了其专业性和独立性,为数据合规审计的主体资格认定和专业标准确立提供了重要的参照[7]。由此可见,数据合规审计作为传统合规审计在客体端的自然延伸与范式承继,本质特征依然是对组织数据行为的"合规性"进行独立、系统化的监督和鉴证。

2. 发展动因:数据合规审计的时代特性

数据合规审计的时代特性源于数字经济时代政策、要素与治理的多重协同驱动[8],其发展不仅承继了传统合规审计的制度基础,更积极回应了时代赋予的新使命。在政策法律层面,随着社会经济的发展,传统合规审计逐渐演进为现代形态,并不断向数据领域延伸,其中个人信息保护合规审计成为重要载体[9]。《办法》为数据合规审计填补法律空白的同时,推动数据安全治理由制度化迈向法治化[10]。尽管规则体系间存在交织的争议[11],但是传统合规审计已经由"合规导向审计"转变为"审计驱动合规",并与多重治理场域深度嵌套。在要素价值层面,数据作为新型生产要素[12],远非局限于系统或者应用程序输出的文件、数据库、文档或网页等内容[13],其多元资产属性界定[14]、数据环境的精细化分类和处理行为的广义拓展也倒逼审计必须覆盖数据全生命周期[15]。而数据合规全流程管控的要求和数字安全之间的双重内涵很大程度上映射出其合规与安全并重的目标[16]。在治理需求层面,政府审计从单一财务合规向财务与经营双重合规拓展[17],与此对应的是数据领域从个人信息保护延伸至企业整体的合规治理。因此,在多重因素的共同推动下,数据合规审计或将成为数字经济时代不可或缺的治理工具。

(二)多维视角下数据合规审计的理论考据

从法学视角来看,数据合规审计的正当性根基可追溯至法学规制理论所赋予的秩序框架和法理支撑。早期研究主要集中于诠释和遵从成文法规,旨在为数据处理划定出清晰的"可为"与"不可为"边界[18]。"元规制"理论认为国家不会直接进行事无巨细的干预,而是借由构建制度框架与设定目标来引导和监管企业的自我规制[19]。在数据合规领域,呈现出"企业-政府"二元共治的模式,数据合规审计正是检验企业自我规制是否有效的关键问责机制。此外,规制理论视角下的精巧规制理论认为数字金融平台算法合谋从规制主体、手段和效果三个方面造成反垄断规制困境,即法律责任主体难以确定、协同行为认定困难、反垄断执法效果较差[20]。在数据合规领域,可通过数据合规审计活动来确定数据处理的责任主体,利用技术工具监测违规行为,将审计结果转化为可持续改进的规制策略,进而提升规制效能。

从数据科学视角来看,数据科学可以看作是大数据时代的一门新科学,其是以揭示数据时代特别是大数据时代新的挑战、机会、思维和模式为研究目的,由大数据时代新出现的理论、方法、模型、技术、平台、工具、应用与最佳实践组成的一整套知识体系[21]。数据科学主要以统计学、机器学习和数据可视化为理论基础。统计学的抽样理论指导审计人员从海量数据中科学选取样本,从而高效推断出总体合规情况,实现审计资源的合理分配[22]。机器学习领域的异常检测理论通过建立正常行为基线,自动识别出偏离模式的异常数据访问或者操作行为,从而发现潜在的内部威胁或者未知的风险模式[23]。数据可视化中的视觉编码理论研究如何将数据属性准确映射为视觉元素,用直观的元素来呈现复杂的审计结果,辅助快速定位风险[24]。此外,数据全生命周期理

论为数据合规审计提供了贯穿数据“从产生到销毁”的全流程审计框架和控制节点,是对数据合规进行系统性审计的流程基础[25]。

从管理学与审计学视角来看,基于管理学视角,内部控制理论强调通过控制环境、风险评估、控制活动、信息沟通与监督五要素,构建贯穿数据全生命周期的结构化保障体系[26],这为数据合规审计奠定了系统性的程序基础。风险管理理论确立了数据合规审计活动的基本逻辑,即审计资源和重点的配置必须基于对数据处理各个环节中潜在风险的持续识别、评估与排序,以此来确保监督行为与组织面临的最高级别合规风险相匹配[27]。基于审计学视角,数据合规审计的起源可追溯至审计缘起的重要理论之一,即受托责任理论。该理论认为,由于资源所有权和经营权的分离,产生了委托人对独立第三方鉴证的需求[28]。在数字经济中,数据主体和数据处理者之间形成了一种新型的“数据受托关系”。为了独立验证数据处理者是否履行了安全与合规等受托责任,数据合规审计应运而生,其在“委托 - 代理 - 鉴证”这一根本逻辑上与受托责任理论一脉相承[29]。目前该领域的前沿理论是大数据审计理论,强调运用数据挖掘、关联分析与可视化等大数据技术,对海量、多源及异构的数据进行全量或大规模样本分析,从而突破传统抽样审计的局限,实现更全面、及时与精准的审计监督[30]。

除上述理论外,经济学与社会学也为数据合规审计提供了理论依据。从经济学视角来看,基于经济理性人假设,数据合规审计通过系统性增加违规行为被发现的概率与代价,从而改变企业在数据合规问题上的成本收益计算,促使其主动选择合规[31]。从社会学视角来看,数据合规审计是一种嵌入特定社会结构与制度环境中的社会行为与治理模式。新制度主义理论认为组织采纳此实践旨在获取合法性,以应对法规强制、行业规范及头部企业示范等制度压力[32]。社会技术系统理论进一步揭示了审计对象作为技术与社会耦合的复杂整体[33],推动数据合规审计焦点从静态合规检查转向动态风险评估。因此,数据合规审计作为一项由法学、数据科学、管理学与审计学等多学科理论共同奠基与形塑的复合治理实践,其不仅是法律遵从的技术性验证工具,更是数字时代一种将外部规制要求内化为组织治理结构、并促进多元主体协同的重要制度化治理工具,其发展与应用标志着治理模式从单向强制向技术赋能与动态反馈的系统性演进。

(三)文献述评

综上所述,数据合规审计作为数字经济治理的关键制度安排,正从理论探索走向实践应用。已有研究在传统合规审计的范式跃迁、多学科理论溯源等方面奠定了研究基础,但数据合规审计作为一个交叉融合的新兴领域,其理论体系、实践路径与风险因应还有待进一步挖掘。从现有文献来看,以下几点有待进一步研究:第一,理论整合尚需深化。法学、数据科学、管理学与审计学等多学科理论虽已有引入,但是大多呈平行论述状态,缺乏能够统摄各个视角的系统性整合框架。本文将着力构建以数据全生命周期为主线、融通多学科理论的数据合规审计概念体系与三级分析框架。第二,实践向度尚待体系化。现有研究大多停留在原则性倡导阶段,对于数据合规审计“审什么、怎么审、依据什么审”等实操层面的系统探索明显不足。本文将围绕“源头采集 - 存储传输 - 处理使用 - 销毁归档”四个环节,系统构建可落地、可扩展的实践框架,实现从应然到实然的转变。第三,风险因应路径尚需精准化。就权属纠纷、算法歧视、形式化销毁等复杂的风险而言,现有研究缺乏有针对性、可操作性的风险应对策略,技术工具与审计程序的结合亦不充分。本文将针对各环节关键风险,提出数据地图、分级授权、日志存证与自动化管理平台四项技术因应路径,形成“风险识别 - 措施匹配 - 效果验证”的闭环体系,为数据合规审计从被动合规走向主动治理提供实践参照。

三、数据合规审计的概念建构

前文所述既说明了数据合规审计的复杂性与独特性,也表明任何单一的传统理论框架,无论是法律解释、数据科学,还是经典审计模型,均无法充分覆盖数据合规审计的完整内涵与实践要求。因此,为了系统整合上述多维属性并有效指导实践,对数据合规审计进行独立且系统的概念建构已成为理论发展的必然要求。基于此,本文对数据合规审计的概念建构框架如图 1 所示。

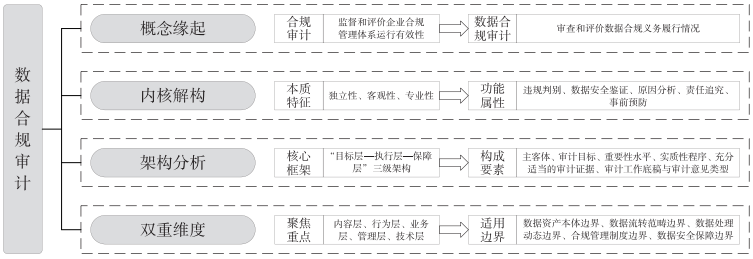

图 1　数据合规审计的概念建构

(一)概念缘起:传统合规审计在数据时代的细分延展

传统合规审计是对企业合规管理体系运行有效性实施监督和评价的重要技术抓手与保障手段,主要目的是确认组织行为的合法性与合规性。根据受托责任理论,审计是以系统方法,从行为、信息和制度三个维度独立鉴证经管责任履行情况并将结果传达给利益相关者的制度安排[34]。传统合规审计是企业治理与风险控制的重要机制,其形态主要紧扣财务报告可靠性、经营行为合法性、内部控制有效性等维度,其基本概念可以追溯至受托责任观与风险管理理论。然而,这种传统审计范式在面对汹涌而至的数字化浪潮时,就逐渐显现出内在局限性,审计对象的物理边界也日益模糊。与此同时,数据资产凭借其无形性、流动性、易复制性以及规模爆炸性等特征,逐渐颠覆传统审计赖以生存的凭证基础与资产控制逻辑。传统合规审计在应对数据这一新型生产要素的全生命周期管理风险时,其固有的审计框架、技术工具与知识储备等均面临严峻挑战,亟待范式转型。

数据合规审计的产生源于数字经济发展导致数据价值与风险同步提升的时代必然性,跨学科理论的协同支撑明确了其核心定位。数据合规审计既继承了传统合规审计的责任鉴证本质,又根据数据要素的特性,把法学的合规基准、数据科学的技术构建、管理学与审计学的范式革新相融合,成为数字时代独有的专项审计形态。一方面,大数据、人工智能和云计算等技术的深度应用,在重塑业务模式的同时,催生海量、高速与多元的敏感数据,这些数据在收集、存储、处理以及跨境等环节潜藏着隐私侵犯、数据泄露及算法歧视等新型风险[35]。另一方面,以 GDPR 为代表的全球数据保护立法浪潮明显提升了合规要求,且设定了高昂的违规成本,企业为规避法律风险、维护市场信任和履行社会责任,对数据活动进行独立、系统验证的需求空前强烈。因此,本文结合《数据合规审计指南》相关释义①,对数据合规审计的概念界定如下:数据合规审计是指由具备独立性与客观性的专业机构,依据相关法律法规、政策标准及行业规范,通过系统技术方法,对被审计单位的数据和数据资产、数据环境、数据处理行为、数据合规管理与数据安全的全链路进行审查、监督与评价的活动。

(二)内核解构:数据合规审计的本质特征与功能属性

数据合规审计的本质特征是兼具独立性、客观性与专业性的数据治理。其中,独立性要求审计主体和被审计对象之间不存在利益关联,以保证审计过程和结果不受干扰,这是受托责任理论对于鉴证中立性的重要诉求,也是法学“元规制”理论中第三方监督机制的基本要求;客观性要求审计人员根据确凿证据和既定标准作出判断,避免主观臆断,这契合法学“以事实为依据、以法律为准绳”的基本原则,确保了审计结论的公正性;专业性则强调审计人员须具备数据管理、法律法规与信息技术等多领域知识,为评估数据在处理过程中是否处于合法、合规与可控状态提供度量标准和验证依据,运用专业知识对数据的完整性、准确性、安全性进行系统评估,以精准识别数据合规风险。

数据合规审计的功能属性分为以下五个方面:一是违规判别功能,违规判别是数据合规审计的基本功能,即系统审查数据处理活动是否严格遵循国家法律法规、强制性标准及行业规范,精准识别违法或违规的操作,为合规状态提供客观的判定依据;二是安全鉴证功能,数据安全鉴证既关注技术层面的安全控制,又重视技术与社会耦合的动态风险,通过持续监控和深度分析,揭示各环节潜在的安全漏洞与异常行为,构建全链条安全屏障;三是溯源分析功能,当不合规事件发生时,经由溯源调查并展开结构化复盘,锁定根本原因,从而促使治理体系得以不断优化;四是责任追究功能,数据合规审计依靠审计轨迹和证据固化,创建起权责分明、响应迅速的问责机制,对主观恶意或重大过失予以惩戒,从而形成行为约束和威慑;五是事前预防功能,数据合规审计通过对风险管理框架、内控流程与合规培训等制度的前瞻性测试评估,主动识别系统性风险与隐患,提升组织对风险的预见和主动防控能力,实现从被动合规向主动治理的转型。

(三)架构分析:数据合规审计的核心框架与构成要素

数据合规审计的核心框架以风险导向、全生命周期覆盖与多维度协同为设计逻辑,构建“目标层 - 执行层 - 保障层”三级框架,实现对法学、数据科学、管理学与审计学理论的体系化转化,同时结合数据合规审计的构成要素,形成闭环式审计管理体系。数据合规审计的目标层聚焦合规基准,数据处理活动严格遵循国家法律法规、行业标准及企业内部制度三重依据,明确审计需达成的合规目标,同时结合业务场景设定风险优先级,确保审计资

①详见中国电子信息行业联合会发布的《数据合规审计指南》(http://www.citif.org.cn/CFEII/miit/#/news/newsDetail/5fb01fde85c14adaa3459648ddab765b)。

源向高风险领域倾斜。执行层贯穿数据全生命周期关键节点,按照“采集 - 存储 - 使用 - 销毁”四阶段拆解审计任务,采集阶段核查合法性授权,存储阶段验证安全防护措施,使用阶段监督合规目的限制,销毁阶段确认数据彻底清除。保障层则依托技术工具与组织机制双重支撑,通过搭建审计管理平台实现流程数据化,建立跨部门协作机制,并制定审计质量复核标准,确保框架落地的有效性与一致性。

数据合规审计的构成要素包括主体、客体、审计目标、重要性水平、实质性程序、充分适当的审计证据、审计工作底稿与审计意见类型,各要素相互关联,共同支撑审计工作的专业性与独立性。依据受托责任理论,数据合规审计的主体是执行审计行为的责任方,主要是专业机构。《办法》对专业机构进行了界定,即具备开展个人信息保护合规审计的能力,有与服务相适应的审计人员、场所、设施和资金等的组织实体。数据合规审计的客体是开展审计工作的具体对象,涵盖数据和数据资产、数据环境、数据处理行为、数据合规管理与数据安全五类。数据合规审计的目标是就数据处理活动是否在所有重大方面遵循法律法规、行业标准及内部制度获取合理保证,并依据风险高低来分配审计资源。重要性水平指根据数据违规行为的性质与潜在影响,确定可容忍的偏差限度,用以区分重大不合规和一般性瑕疵。实质性程序则通过细节测试、分析性程序、穿行测试等具体方法来检查数据合规状况。充分适当的审计证据要求审计人员采用文档审查、日志审计、自动化检测工具等方式,获取足够且相关、可靠的证据来支撑审计结论。审计工作底稿记录审计程序、证据来源、测试结果及职业判断,是质量复核与责任追溯的依据。审计意见类型根据审计发现的不合规事项的性质和影响范围,出具无保留意见、保留意见、否定意见或者无法表示意见,为报告使用者提供明确的决策依据。

(四)双重维度:数据合规审计的聚焦重点与适用边界

基于审计重点的分析视角,数据合规审计的实践首先从系统性识别和验证审计重点开始,其覆盖范围须具备多维性与层次性:一是在内容层面,数据合规审计要仔细审查数据对象的具体内容是否严格遵循被审计单位的信息发布规则;二是在行为层面,数据合规审计可以通过对操作日志的追溯,识别渎职、越权或舞弊行为,确保责任可追溯;三是在业务层面,数据合规审计要求重点核查权限授予、审核放行、痕迹保留等环节的合规记录,实现合规要素的全链条耦合;四是在管理层面,数据合规审计侧重对治理架构进行评估,即数据合规制度的完备性、管理机制的有效性、培训体系的覆盖度及合规文化的渗透程度;五是在技术层面,数据合规审计需验证技术工具对数据可用性、完整性及安全控制的保障能力,确保电子环境中的技术应用符合监管要求。以上所聚焦的五大重点共同构成数据合规审计的纵向穿透力,形成从数据内容到管理生态的立体化监督。

基于审计边界的分析视角,数据合规审计的边界厘定需明确审计权责的作用域与效力范围,避免审计泛化或关键领域遗漏。其一,数据资产本体边界,即通过分析数据目录、字典及资产登记表,对特定数据集合的定义、属性、来源、质量、敏感性与生命周期等核心特征进行确权式审计。其二,数据流转范畴边界,涵盖数据在开放系统、封闭环境及跨组织传递中的安全状态审查,尤其关注环境切换时的合规性断点。其三,数据处理动态边界,数据合规审计须覆盖从数据分级分类、流通交易到治理决策的全周期操作链,重点验证授权管理、关键人员行为与流程规范的匹配度。其四,合规管理制度边界,要求审计主体对其合规框架开展符合性诊断与有效性评价。其五,数据安全保障边界,须对数据本体、处理环境及行为所依赖的系统平台实施安全性验证,确保平台的完整性、真实性与抗风险能力。边界的厘定本质上是建立数据合规审计的“应然”范畴,既须避免侵入业务自主空间,又须确保风险高发领域无监管盲区,最终形成逻辑自洽的数据合规审计谱系。

四、数据合规审计的实践向度

基于上文对数据合规审计的内核解构、架构分析及双重维度的系统性理论建构,可以看出,数据合规审计并非抽象的理论模型,而是在“目标层 - 执行层 - 保障层”的框架下,具象化为可操作和可验证的治理活动。数据合规审计的实践向度围绕数据全生命周期展开。数据全生命周期是指数据从产生或采集开始,经过存储、处理、分析及应用直至最终归档或销毁的完整过程。需要特别指出的是,不同审计主体在实践向度中存在显著差异:国家审计聚焦法定监管职责和公共数据安全,强调对重要数据和核心数据的强制性审查;内部审计侧重流程自控与整改闭环,服务企业数据合规管理体系的改进;社会审计依据委托约定提供专业机构鉴证,重点关注数据处理的合法性与公允性。本文立足社会审计视角,以独立专业机构鉴证为核心场景,展开数据合规审计的实践向度分析。数据合规审计基于数据全生命周期的实践向度如图 2 所示。

(一)数据源头与采集合规审计

数据源头与采集作为数据处理全生命周期的初始阶段,其合规审计是“核心框架”中执行层审计任务的起点。在此过程中,关键风险点主要集中在三个方面:一是权属风险,包括第三方提供的数据是否有合法处分权证明、上游数据主体是否明确授权或数据是否存在多重授权冲突;二是来源风险,包括公开渠道获取数据时存在爬虫违规抓取受限信息、未留存溯源时间戳与渠道链接,内部数据生成存在越权采集或冗余记录等违反业务流程规范的行为;三是采集风险,包括超目的采集、强制授权、敏感个人信息未单独获取同意及风险告知、同意撤回渠道隐蔽或流程烦琐等引致的风险。

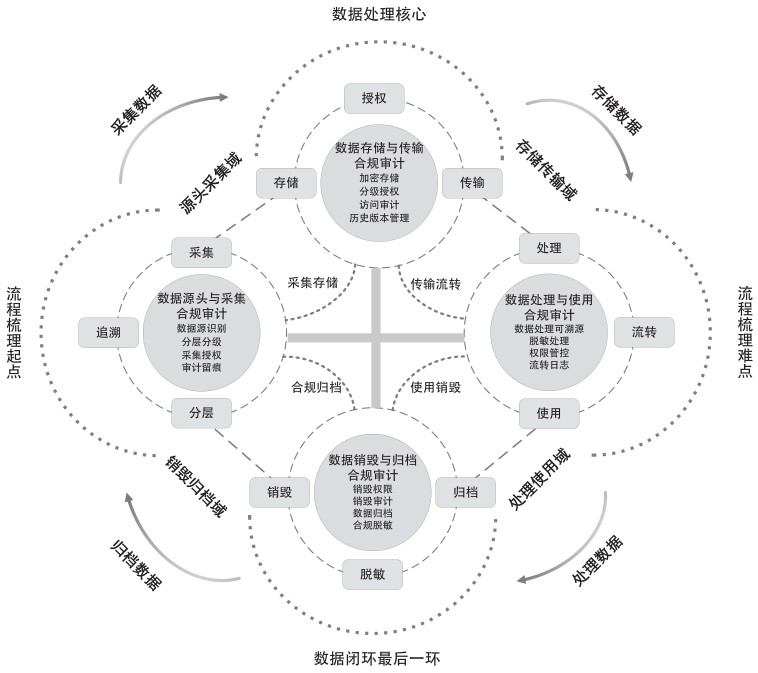

图2　数据合规审计的实践向度

在数据源头合规审计环节,需围绕数据权属明确性、来源合规性这两个方面来开展内部与外部分层审计。第一,对内部生成的数据应着重审查数据产生场景的合规性,审计人员可通过追踪数据从生成到入库的穿行测试,验证控制措施的实际运行情况。第二,对外部获取的数据要细化来源类型,建立差异化核查标准。若数据来源于合作第三方,则需要对第三方的数据权属证明文件做进一步的审核,确认其合法处分权;若数据来源于公开渠道,则需要对获取方式的合法性进行核实,并留存获取时间与渠道链接等溯源信息;对于跨境获取的数据还需结合《中华人民共和国数据安全法》中关于数据跨境流动的要求,对是否履行了必要的安全评估或者备案程序进行核查,确保符合我国的监管规定。在数据合规审计过程中,审计人员要保持职业审慎,重点针对第三方数据协议中禁止二次转让、保密义务和责任追偿等条款的明确性以及用户同意界面的独立性、告知内容的通俗性、撤回操作的便捷性、敏感个人信息单独同意记录的完整性和风险告知的针对性进行审查。

在数据采集合规审计环节,数据采集过程和用户同意机制的合规性审计是两个重要的程序。前者的关键在于把合法、正当、必要原则转化为可落地的审计执行方案,保证采集行为全程可控与可追溯,审计人员需用“目的-范围”匹配分析法核查采集前是否书面明确目的,避免过度采集,同时比对数据范围与目的的关联性,通过场景化抽查,验证数据项的匹配程度,排查默认勾选、一揽子授权等强制采集行为。后者的核心是验证用户同意的明示性和可撤回性,审计实践中要重点审查同意获取的形式和内容,在形式上要确认是否采用单独、明确的同意界面,而不是嵌套在服务条款中,避免默示同意或者捆绑同意,在内容上要核查是否清晰地告知用户采集的数据类型、用途、保存期限和第三方共享情况。实践中,审计人员需综合运用不同的审计程序,通过模拟操作、访谈业务人员与检查同意日志等方式,结合穿行测试以及实质性分析程序,兼顾书面制度与实践落地,确保合规性。

(二)数据存储与传输合规审计

数据存储与传输环节的审计是“安全鉴证”功能在数据操作层面的具体体现。在此过程中,关键风险点集中在两个层面:其一,存储层面,包括敏感数据未单独存储且未采用 AES-256 等合规加密算法、分类分级制度未落地、权限分配违反最小必要原则、备份数据未加密且无异地备份机制、销毁流程形式化、云存储服务商无 IDC 资质或 ISO27001 认证等风险;其二,传输层面,包括敏感数据明文传输、内部传输未脱敏处理、第三方传输超协议范围使用、跨境传输未通过安全评估或未完成标准合同备案等风险。

在数据存储合规审计环节,审计人员首先通过检查企业数据分类分级制度文件,结合观察技术工具对存储环境进行抽样扫描的操作过程,并执行穿行测试,追踪数据从创建到存储的全流程控制,以了解内部控制设计。存储环境中,需核查敏感数据加密算法的合规性及密钥管理流程与数据分类标识的准确性,还需审查云存储中

的服务商资质文件、服务协议中关于数据安全的责任划分条款、双人复核与应急响应机制。权限管控中，需测试权限申请与审批这一关键控制活动，通过检查权限变更日志与抽样验证权限分配的合理性，同时运用数据分析技术识别“僵尸权限”及异常权限组合。备份销毁中，需观察备份与销毁的实际操作，检查备份数据的一致性及销毁过程影像，并对第三方机构资质执行函证或检查其认证证书，以获取外部审计证据。

在数据传输合规审计环节，需基于场景化风险映射思路，针对内部传输、第三方传输与跨境传输三类场景构建差异化审计框架。在内部传输端，数据合规审计聚焦技术防护有效性，通过抽样检测传输链路，核查是否全程启用加密协议，杜绝明文传输敏感数据。在第三方传输端，数据合规审计要强化协议约束和过程管控，审查数据共享协议的合规性，通过访谈业务负责人，交叉验证是否存在超协议传输。在跨境传输端，数据合规审计则实施全流程刚性监督，依据《数据出境安全评估办法》，核查重要数据与大量个人信息是否通过国家网信部门安全评估，标准合同是否完成省级备案且条款符合法定模板，同时通过穿行测试，验证传输链路是否通过合规通道，数据是否经脱敏或者匿名化处理，并检查日志留存机制，确保全流程可追溯。

（三）数据处理与使用合规审计

数据处理与使用环节是实现数据价值的核心阶段，也是合规风险的高发区域。在此过程中，关键风险点也应精准识别，具体包括：第一，在处理环节，包括超授权处理、算法训练数据中混入未授权敏感信息、算法决策存在歧视或不公平性以及处理流程缺乏留痕等风险；第二，在使用环节，包括数据共享/转让未向用户告知且未获取单独同意、接收方无数据安全保障能力、公开披露数据去标识化失效与跨境使用未履行法定程序等风险。

在数据处理合规审计环节，审计人员需通过执行穿行测试，验证从授权起点到处理末端的完整性，并识别关键控制点。具体而言，一是文档溯源，要调取并审查企业的核心授权文件，通过检查和分析程序重点，确认企业对于处理主体、处理范围与处理期限三者之间的对应关系是否进行了明确规定，防止因模糊表述而导致授权边界不清。二是行为验证，可采用场景抽样与日志分析相结合的方法，一方面选取高频出现的数据处理场景，通过人员访谈与操作记录比对来验证实际操作与授权内容是否一致，另一方面可借助日志分析工具提取近期敏感数据的处理记录，执行细节测试，识别没有获得授权的账号操作。三是技术核验，在自动化处理场景下，还可以对算法训练数据的授权来源进行核查，确保其均来自合法授权数据，且没有混入未授权的敏感信息，同时对算法决策逻辑进行审查，实施重新执行程序或者利用专业工具进行模拟测试，从而验证系统防止数据滥用的机制是否有效，保障全流程处理行为符合授权边界。

在数据使用合规审计环节，需构建“场景分类－义务核查－风险验证”的实践框架，保证企业履行告知或者获取额外同意义务，保障数据流转安全。在数据共享与转让场景中，重点聚焦三个方面：一是协议合规性审查，主要通过检查程序确认企业与接收方协议是否明确了数据范围、用途、保密义务、违约责任及禁止二次转让等条款，必要时可向接收方发函询证以确认关键条款；二是告知与同意义务验证，主要确认企业是否在共享或者转让前向用户告知接收方身份和数据用途，并获得单独同意；三是接收方资质核验，主要查验其数据安全保障能力证明，必要时访谈其安全负责人、执行控制测试或者重新执行部分安全流程来验证保障措施与约定的一致性。在数据公开披露场景中，数据合规审计的重点是通过“重标识”模拟攻击测试去标识化效果，调阅风险评估报告核对评估方法的完整性。一方面，可使用技术手段模拟“重标识”攻击，检验数据是否不能识别特定个人且不可复原；另一方面，可调阅企业风险评估报告，用分析程序核查是否包含个人信息识别、泄漏风险和去标识化有效性评估等内容，结合专业判断保证评估的科学性与完整性。

（四）数据销毁与归档合规审计

数据销毁与归档标志着数据全生命周期的终结。此环节的数据合规审计旨在落实“责任追溯”逻辑，并通过闭环验证确保数据销毁与归档行为符合规定，其审计发现直接服务于“风险导向整改”，是构成完整数据合规审计闭环管理的最终步骤。在此过程中，关键风险点需从以下两个方面重点把控：第一，销毁环节，包括电子数据未按“3 次随机覆写”或加密密钥销毁标准执行、物理介质未粉碎/焚烧、仅格式化或删除文件、销毁流程无“申请－审批－执行－影像记录”闭环及第三方销毁机构无国家认可资质等风险；第二，归档环节，包括归档范围不当、敏感数据未加密归档、保存期限超法定要求、访问权限失控及云归档服务商安全责任划分不明确等风险。

在数据销毁合规审计环节，围绕“制度完整性－执行有效性－效果可验证性”三个层级展开。在制度完整性层面，首先调阅企业数据销毁管理制度，重点核查其是否覆盖不同数据载体的销毁标准，其次确认制度是否明

确销毁责任主体、审批流程及异常情况处理机制,以避免制度漏洞导致的操作无据可依。执行有效性与效果可验证性层面,可以采用“流程追溯 + 技术检测”方法,一方面,调取近期敏感数据销毁记录,执行穿行测试,追溯全流程,核查申请单内容是否完整、过程影像是否清晰记录介质标识与操作细节,并确认第三方机构是否具备国家认可资质,验证其是否一贯有效运行;另一方面,使用专业工具检测已销毁的电子存储介质是否达到不可恢复标准,随机抽查物理介质残骸,确保碎片尺寸无法通过技术手段拼接。

在数据归档合规审计环节,需以范围合理、期限合规与访问可控为抓手,结合法规要求和企业实际,构建多维度核查机制。在归档范围核查中,调取企业归档清单与分类分级文档,核查是否涵盖已过业务有效期但仍需留存的合规数据以及是否剔除无价值的冗余数据,并确认敏感数据是否单独标记且加密存储,避免与普通数据混存带来的风险。在保存期限与访问控制核查方面,则侧重法规适配性与权限安全性。针对保存期限,需按数据类型逐项对照法规要求,核查系统是否具备自动到期提醒与处置记录,防范超期留存的风险。访问控制核查则通过绘制权限图谱与调取访问日志,验证权限分配是否遵循“最小权限 + 按需授权”原则,检查是否存在一人多权或越权访问等情况。针对云归档场景,还应审查云服务商资质和服务协议中的安全责任划分,确保全流程合规安全。

(五)数据合规审计的前沿探索

在构建覆盖数据全生命周期的数据合规审计框架时,业界的前沿探索为我们提供了重要的实践参照[36]。其中,国家数据局发布的《基于数据可信流通设施环境番茄生长模型场景的数据流通案例》(以下简称《案例》),系统呈现了一个多主体、长链路场景下以数据流通安全审计为核心的合规治理实践。

第一,审计对象与数据流识别。《案例》涉及的审计对象包括四类主体,即数字农场、数字农业服务商、农作物研发机构以及数据交易所。数据流贯穿采集、加工、流转与应用全过程:数字农场通过物联网设备采集番茄生长数据,依据服务协议共享给数字农业服务商;服务商依协议将数据提供给研发机构;研发机构融合区域环境、气候等数据,加工形成番茄生长模型,再授权服务商对外经营;服务商最终将模型通过物联网设备反馈至农场用户,指导其作业;模型亦可在数据交易所上架流通。这一数据流完整覆盖从采集、存储、传输、处理、使用到销毁归档的全生命周期链条,为审计对象识别与风险点定位提供了清晰路径。

第二,控制点识别与数据全生命周期框架验证。在数据源头与采集阶段,服务商与农场签订服务协议,明确数据共享范围与用途,从源头上固化授权边界。在数据存储与传输阶段,基于区块链技术的数联网实现主体身份认证与全链路互联互通,“链式授权”机制将每一环节的协议生成不可篡改的凭证,记录授权范围与数据来源。在数据处理与使用阶段,可信执行环境保障模型加工安全,数据经加密传输至该环境,研发机构在其中生成模型,并输出经安全检测的模型,以防止通过模型欺诈带出原始数据,原始数据用后即毁。在数据销毁与归档阶段,原始数据在模型生成后直接销毁,本地交互日志与区块链凭证共同构成可追溯的归档记录。

基于此,数据全生命周期审计框架所预设的各阶段关键控制点均在《案例》中得到具体体现。同时,该案例展示了数据合规审计并非单一环节的孤立检验,而是依托区块链、可信执行环境等技术嵌入以及“链式授权”、合规知识库与大语言模型辅助等流程创新,实现从采集到归档的全链路覆盖与风险可控。

五、数据合规审计的风险因应

在数据全生命周期审计实践中,已识别出四大类关键风险场景,风险因应是指在识别和评估这些具体风险后,为降低风险发生的可能性或减轻其潜在影响而采取的一系列精准策略和实操行动,以实现“风险识别 - 措施匹配 - 效果验证”的逻辑闭环。数据合规审计各实践环节的风险因应如表 1 所示。

表 1　数据合规审计的风险因应

实践环节	风险点	风险因应
数据源头与采集环节	权属纠纷、强制授权、敏感信息采集不合规	以数据地图追溯破解数据源头采集的合规风险,将被动审计升级为主动与持续的闭环监督
数据存储与传输环节	加密缺失、权限冗余、明文传输、跨境不合规	以分级授权制度筑牢数据存储传输的合规防线,实现风险的持续管控
数据处理与使用环节	超授权处理、算法训练数据违规、算法歧视、去标识化失效风险	以日志存证系统规范数据处理使用的合规路径,将静态合规检查转化为动态技术性监督
数据销毁与归档环节	形式化销毁、流程无闭环、超期留存、权限失控	以自动化管理平台加固数据归档销毁的合规屏障,实现数据全生命周期末端的实质性验证

（一）以数据地图追溯破解数据源头采集合规风险

数据采集环节面临权属纠纷、强制授权与敏感信息采集不合规三大核心风险，且因数据流转链路复杂、传统审计缺乏全链路追溯能力，易陷入责任模糊、核查低效与证据不足的困境。数据地图凭借其全景可视化与全流程追溯能力，成为精准破解此类风险的技术支撑。

针对数据权属纠纷风险，数据合规审计的难点在于如何在数据要素经多手流转后，仍可清晰界定各方的责任。基于此，数据地图为审计提供“取证地图”。具体而言，数据地图构建的自动化数据全景图能够帮助审计人员穿透数据流转的多层嵌套关系，精准定位数据采集的物理终端与逻辑源头，从而明确数据权属的初始责任主体，避免源头责任认定的错位。在此基础上，数据地图搭载的流程可视化功能还能按照时间线与主体关联维度，完整回溯数据从原始采集、算法加工、多源融合到对外共享与产品化输出的每一步流转路径。同时，数据地图能够自动标记数据共享接口调用、数据加工规则变更与数据产品对外输出等权属或控制权发生转移的关键节点，为审计工作提供连续、完整且可追溯的技术证据链。

针对强制授权风险，数据合规审计的痛点是数据采集环节的授权失配，既存在未经用户同意的无授权采集，也存在超出用户明确授权范围的越权采集。数据地图通过将全链路数据流转轨迹与用户授权日志元数据的深度绑定，打破两者之间的信息壁垒，为审计工作构建动态核验场景。具体而言，审计人员可一键锁定特定数据集的精准采集时点、采集主体及采集渠道，同步调取该时点生效的用户授权协议版本、明确授权范围及授权有效期等重要信息，通过采集行为与授权内容逐维度的交叉比对，精准判定是否存在无授权采集、超范围采集与过期授权采集等违规情形。数据地图系统具有智能监测功能，对没有关联有效授权链路的采集行为自动发出异常警报，详细标明采集节点、数据类型和操作主体，给审计人员指明核查的方向，不需要对所有环节进行全面排查，就可以针对高风险环节进行定向的深度核查，从而降低审计成本。

针对敏感信息采集不合规风险，数据合规审计的主要障碍是敏感数据类型繁多、流转链路长且保护措施的执行情况难以全程追溯。具体而言，审计人员利用数据地图集成的数据分类分级与智能标记功能，可以率先精准识别敏感数据的源头，从而将个人生物识别信息、行踪轨迹与金融账户信息等敏感数据进行分类整理，明确审计核查的对象。在此基础上，审计人员可以借助可视化流转路径，从数据采集、入库、加工、分析与传输的全链路进行回溯，逐节点核查是否严格遵循预设保护策略。同时，数据地图系统可以实时检测出敏感数据的违规流转行为，并生成警报记录，保存完整的处置日志。这些记录将直接成为审计取证的依据，助力数据合规审计从违规结果倒查溯源，精准定位保护措施失效的关键节点与责任主体。

（二）以分级授权制度筑牢数据存储传输合规防线

数据的存储与传输是数据合规审计全生命周期中风险高发的重要环节。加密缺失和权限冗余等存储风险以及明文传输和跨境未合规等传输风险，都会引发数据泄露或者监管处罚等严重后果。分级授权制度作为重要的管控手段，可以通过精准界定访问操作权限、绑定合规逻辑等方式，破解传统审计静态核查和风险追溯不足的困境，构建覆盖存储与传输全链路的安全防护体系，为数据安全筑牢关键屏障。

在存储环节，针对加密缺失风险，数据合规审计主要关注补偿性措施是否有效，一方面核查权限配置与数据分级标准的匹配度，确保未加密敏感数据仅对特定的高级别角色开放，从访问源头降低泄露风险。另一方面深度分析权限审计日志，逐一核验未加密敏感数据的访问行为。针对权限冗余风险，数据合规审计以最小必要原则为抓手，一是核验权限是否依据岗位与角色进行细粒度划分，杜绝一人多权或者权责不符的现象；二是借助自动化工具的校验记录和权限变更日志，完整回溯权限新增、扩容和转移的全流程轨迹，定位长期没有使用或者超出职责范围的冗余授权，推动及时清理优化。

在传输环节，针对明文传输风险，数据合规审计的重点是分级授权和传输操作的关联监督，一是核查传输发起权限的管控精度，确认是否仅赋予特定必要角色，杜绝无权限发起传输的隐患；二是通过交叉比对传输日志与权限审计日志，锁定明文传输的操作主体、时间、数据类型及应用场景，对照既定数据分级管控策略，判断是否存在敏感数据违规明文传输的情形。针对跨境未合规风险，数据合规审计以授权体系的特殊管控效能为抓手，优先验证跨境传输是否设立独立于普通传输的授权流程，确保权限与经认证的合规角色和对应的法律依据严格绑定，杜绝无依据与越角色的跨境传输。

(三)以日志存证系统规范数据处理和使用合规路径

数据处理与使用是数据合规审计中数据价值转化的两大核心环节。超授权处理、算法训练数据违规、算法歧视及去标识化失效四大风险,易突破数据安全边界,侵犯数据主体合法权益,且因处理流程隐蔽性强而导致操作轨迹易灭失。自动化审计日志生成与集中管理系统(以下简称日志存证系统)可通过完整与不可篡改等关键操作,构建标准化且可追溯的数据源,成为数据合规审计破解此类风险、实现技术性监督的重要支撑,为数据处理合规筑牢基础。

在数据处理环节,针对超授权处理风险,一方面,系统应实时记录每一项数据操作的执行主体、时间戳、操作对象、具体内容及操作结果,形成标准化日志并汇聚归档;另一方面,审计人员可通过检索分析集中化日志,将操作记录与经批准的权限策略清单逐一对标,识别偏离授权范围的异常操作序列。针对算法训练数据违规风险,一方面,系统详细记录训练任务触发时间、数据源调用路径、数据预处理步骤、数据清洗规则及训练结果输出流向等关键信息;另一方面,审计人员可以依托日志数据,回溯训练数据集的完整谱系,核验数据源的合法性、是否获得对应授权及授权范围是否与训练用途一致。针对算法歧视风险,日志存证系统详细记载模型输入的数据特征、数据分类标准、参数配置版本、算法处理路径及批量输出结果,确保算法运行轨迹可回溯、可分析。审计人员可基于日志数据开展事后复核分析,对比不同群体和不同类别输入数据的分布特征,拆解算法对各类数据的处理路径与权重分配,分析不同群体数据的输出结果差异模式,精准识别是否存在基于性别、地域及身份等因素的不合理系统性偏见。

在数据使用环节,针对去标识化失效风险,数据合规审计的隐患在于去标识化后的数据仍存在被重新识别的风险,异常关联查询与多数据集拼接还原身份等行为的隐蔽性较强。因此,需依托日志存证系统,通过实时监控访问行为、分析日志模式,构建去标识化的动态评估体系。具体来看,日志存证系统可以完整记录对已去标识化数据集的所有查询、检索、聚合、导出及关联分析行为,包括访问频率、访问时段、查询条件与关联数据集等信息,形成全面的访问日志。审计人员也可以通过分析日志模式,排查异常风险点,精准识别潜在的重识别攻击路径,同时评估去标识化技术控制措施的实际防护效果,针对失效的环节推动技术优化和流程完善。

(四)以自动化管理平台加固数据归档销毁合规屏障

数据销毁环节的形式化操作及流程无闭环风险以及归档环节的超期留存及权限失控风险,易导致数据被非法恢复、滥用或者泄露。数据合规审计借助自动化数据管理平台,通过预设策略、自动执行与不可篡改留痕等方式构建受控环境,为末端环节的数据合规审计提供技术支撑,实现从制度约束到技术管控的转型。

在数据销毁环节,针对数据销毁形式化操作风险,一方面,以自动化数据管理平台为核心,自动记录每一次销毁任务的全量信息,形成不可篡改的标准化销毁日志;另一方面,审计人员可直接调取日志数据,穿透表面操作,核查销毁动作的真实性,确认数据是否被彻底清除。针对数据销毁流程无闭环风险,第一,自动化数据管理平台可自动串联销毁全流程,完整记录数据从归档状态变更为待销毁、系统自动执行销毁操作、操作人员确认完成及残留数据清理核查等关键节点,形成连贯可追溯的操作链路;第二,审计人员依托平台日志,系统核验各环节是否无缝衔接、是否存在流程缺失或断点;第三,锁定各环节操作主体与时间节点,明确责任归属,确保销毁流程从启动到收尾形成完整合规闭环。

在数据归档环节,针对数据归档超期留存风险,可借助自动化留痕技术,通过策略与日志联动,构建动态预警与核查体系。首先,自动化数据管理平台预设归档策略,尤其是敏感数据的优先归档与按期限自动销毁策略;其次,实时记录策略执行日志,包括数据归档时间、预设留存期限、到期提醒触发及自动清理执行结果等信息;最后,审计人员定期核查归档策略配置与实际执行日志的一致性,比对数据实际留存时长与预设期限,推动过期数据合规清理。针对数据归档权限失控风险,一是自动化数据管理平台在自动减少人工干预的同时,生成完整、稳定的权限操作日志;二是审计人员依托日志数据,全程监控权限动态变化,核验权限分配是否与岗位职责匹配、变更是否履行合规审批流程、是否存在超出职责范围的权限或长期闲置权限,推动冗余权限清理优化。

(五)技术工具的风险边界与因应补充

需要审慎指出的是,以上四项技术工具的有效运行高度依赖组织的数字基建水平、数据治理成熟度及资源配置能力。在实践中,技术工具的适用条件、固有局限和潜在失败场景须得到充分识别,审计人员也应建立替代程序与补充程序的应对预案,以避免技术依赖引发的审计盲区,在工具失效或条件不满足时,及时启动替代程序

与补充程序,培育以风险为导向、以证据链为核心的动态审计能力。

第一,在日志缺失、数据血缘断裂或跨系统数据字典不统一的场景下,数据地图将会丧失全链路追溯的能力,甚至呈现误导性路径。此时,审计人员应转向手工数据流程图绘制与关键节点访谈,通过对源系统、ETL 环节和数据湖入口的抽样核验,重建核心数据流转逻辑。

第二,在中小企业缺乏专职数据安全岗位或跨国集团内部授权体系冲突频繁的场景下,分级授权往往流于形式,权限冗余与越权操作难以根除。此时,审计人员可采用基于角色的访问控制基线比对与最小必要原则穿行测试,通过模拟越权访问、异常时间段操作分析等手段,主动发现授权漏洞。对于第三方不配合审计的情形,应启动合同条款强制审计或第三方安全认证核验,并辅以接口调用日志的独立分析,实现间接审计覆盖。

第三,当系统存在日志伪造、时间戳漂移或关键操作未记录时,存证数据将丧失法律证据效力。此时,审计人员应首先实施日志完整性校验与生成者 - 存储者分离审计,验证日志链条的防篡改性;针对算法黑箱或去标识化失效等高复杂风险,可引入影子模式灰度测试或基于合成数据的结果差异分析,以替代对原始日志的绝对依赖。

第四,在跨境场景中,若第三方云服务商或境外子公司拒绝开放管理接口,平台将无法实现销毁与归档流程的闭环管理。此时,审计人员应转为人工流程见证与截屏/日志导出独立复核,并依赖合同遵从性测试与监管问询记录完成替代取证;对于中小企业面临的成本约束,可推荐轻量级脚本审计工具或开源日志分析方案,并采用基于风险分期的滚动审计模式,优先覆盖高敏感数据资产,以可控成本实现关键环节的合规验证。

六、结语

在数字经济纵深推进的当下,数据作为与土地、劳动力、资本与技术并列的第五大生产要素,其安全合规流通已成为激活数字经济高质量发展的重要抓手,数据合规审计正从边缘议题逐渐跃升为贯通政策法律、行业治理与企业运营的公共议题。首先,本文以法学、数据科学、管理学与审计学等视角为锚,厘清数据合规审计多学科交叉的理论根基,并以概念建构为起点,将数据合规审计置于从传统合规审计到数据治理的演化脉络之中,揭示其在独立性、客观性和专业性上的本质特征。其次,本文围绕数据全生命周期,系统勾勒出一套可落地、可扩展、可迭代的实践框架,该框架不仅涵盖从数据源头采集、存储传输、处理使用到销毁归档各环节的数据合规审计要点与方法,更通过行业前沿案例,展现数据全生命周期审计理念在复杂场景中的实际应用与探索方向。最后,本文构建了与实践向度各环节的具体风险形成精准对接的风险因应体系,借助数据地图、分级授权制度、日志存证系统与自动化管理平台四大技术工具,生成了“风险识别 - 措施匹配 - 全流程管控”的逻辑闭环,既针对性破解了权属纠纷、加密缺失、算法歧视、形式化销毁等具体风险,又充分考虑了中小企业的合规门槛。

至此,数据合规审计不再是孤立的合规形式,而是成为连接国家、市场与社会信任的价值基础设施,其不仅以独立、客观与专业的审查为数据要素市场的健康运行提供安全阀,更以持续改进的治理闭环为数字经济的可持续增长注入动力源。面向未来,数据技术的加速演进与全球监管格局的持续重塑,将继续考验审计制度的弹性与前瞻性。然而,只要立法者、监管者、行业组织与企业能够在“共享风险、共担责任、共创价值”的共识下不断深化协作,数据合规审计便有望在变动中沉淀出更具韧性的制度内核,成为数字中国乃至全球数字治理体系中可信赖的公共产品。

参考文献:

[1]赵精武. 个人信息保护合规审计的基本框架与制度衔接[J]. 法律科学(西北政法大学学报),2025(3):83 - 97.

[2]孟志华,黄晓怡. 合规审计:研究综述与展望[J]. 财会月刊,2025(2):90 - 95.

[3]廖义刚,余梁. 审计师会关注企业合规管理水平吗? ——基于年报文本信息的经验证据[J]. 审计研究,2025(2):120 - 133.

[4]Han S,Mei J,Deng J. Does internal compliance auditing increase corporate value? The influence of accounting information quality and agency problems [J]. Finance Research Letters,2025,86:108897 - 108897.

[5]Nicknora T A. Anti-money laundering compliance and financial performance of selected commercial banks in south sudan:A survey of literature on compliance audits[J]. Open Journal of Business and Management,2024,12(5):3543 - 3556.

[6]闫夏秋. 企业合规视角下的内部审计:现实挑战与应对[J]. 财会月刊,2023(18):97 - 102.

[7]张军,张筱楠,陈仙云,等. 个人信息保护合规审计——会计师事务所的机遇和挑战[J]. 中国注册会计师,2025(6):79 - 82.

[8]罗岭,卫振炎. 数字经济发展、双元审计质量与企业创新持续性[J]. 南京审计大学学报,2024(1):21 - 31.

[9]赵翰隽,殷楠. 个人信息保护合规审计探究[J]. 财会月刊,2024(8):80-85.
[10]梅傲. 数据安全法治的法理检视及治理之道[J]. 法学杂志,2025(4):54-68.
[11]徐怀宁,田亚男. 户枢不蠹:数据要素市场化与审计质量[J]. 审计与经济研究,2025(3):29-38.
[12]徐京平,陈思奇. 国家审计、公共数据开放共享与治理效率提升[J]. 财会研究,2025(3):51-61.
[13]United States Government US Army. Army information technology implement ation in structions[M]. Charleston:Create Space Independent Publishing Platform,2013.
[14]中国信通院. 数据资产管理实践白皮书(3.0 版)[R/OL]. (2018-12-17)[2025-09-26]. http://www.caict.ac.cn/kxyj/qwfb/bps/201812/P020181214608773379834.pdf.
[15]梁勇,范全义,徐博文. 企业数据环境建设研究与实践[J]. 计算机集成制造系统,2004(S1):195-199.
[16]郑智航. 数字安全价值的生成逻辑及其法治保障[J]. 华东政法大学学报,2025(4):32-45.
[17]青岛市审计学会课题组,侯杰,商建波,等. 拓展深化国有企业审计研究[J]. 审计研究,2015(3):20-26.
[18]李玉华. 数据法学(第五卷)[C]. 北京:中国人民公安大学出版社,2024.
[19]段俊熙,徐亚文. 迈向二元共治的数据合规——基于规制理论的视角[J]. 西南交通大学学报(社会科学版),2024(6):74-90.
[20]程雪军. 生成式人工智能下数字金融平台算法合谋的精巧规制[J]. 经济体制改革,2025(6):114-121.
[21]朝乐门,邢春晓,张勇. 数据科学研究的现状与趋势[J]. 计算机科学,2018(1):1-13.
[22]谢笑盈,林凌斌,金康伟,等. 基于数据学习的动态抽样方式设计[J]. 统计与决策,2021(1):5-9.
[23]刘烃,信息物理融合系统异常行为检测理论与方法[D]. 西安:西安交通大学,2015.
[24]朱舜山,齐翔林,汪云九. 基于视觉编码的图象处理研究——Ⅰ. 原理、算法及实现[J]. 生物物理学报,1996(2):297-303.
[25]曹志鹏,陈佳宁. 数字普惠金融、生命周期与民营企业非效率投资[J]. 南京审计大学学报,2024(2):68-78.
[26]白华,胡礼燕. 超越 COSO:中国内部控制规范体系探索[J]. 会计与经济研究,2020(6):11-31.
[27]周利敏. 融合数字风险管理的现代应急管理创新实践与理论建构[J]. 南京社会科学,2024(12):73-83.
[28]冯均科,陈淑芳,张丽达. 基于受托责任构建政府审计理论框架的研究[J]. 审计与经济研究,2012(3):9-15.
[29]陈凡. 事业单位的受托责任与经济责任审计[J]. 审计理论与实践,2003(11):66-67.
[30]徐荣华,朱婧,戴欣瑜. 大数据审计:理论框架、研究进展与未来展望[J]. 外国经济与管理,2024(11):122-137.
[31]袁艺,茅宁. 从经济理性到有限理性:经济学研究理性假设的演变[J]. 经济学家,2007(2):21-26.
[32]张楚辉,李卓卓,裴雷. 多学科交叉与多场景嵌入:国内外数据伦理研究综述[J]. 信息资源管理学报,2025(2):91-107.
[33]张涛. 通过算法审计规制自动化决策以社会技术系统理论为视角[J]. 中外法学,2024(1):261-279.
[34]郑石桥. 国有资源委托代理关系、审计目标和审计期望差[J]. 会计之友,2015(15):129-136.
[35]贺勇,李佳蔚,刘筱祎. 数字平台算法审计:现实理据、客观挑战与关键进路[J]. 南京审计大学学报,2025(2):10-20.
[36]国家数据局. 数据流通安全治理典型案例之五|基于数据可信流通设施环境番茄生长模型场景的数据流通案例[EB/OL]. (2025-07-08)[2025-12-31]. https://www.nda.gov.cn/sjj/ywpd/zcgh/0708/20250708223508815159107_pc.html.

[责任编辑:刘　茜]

The Practical Dimension and Risk Response of Data Compliance Auditing: An Analytical Framework for Conceptual Construction and Its Verification

XU Jingping, ZHU Peiwen

(School of Management, Northwest University of Politic Science and Law, Xi'an 710122, China)

Abstract: As an important support for the high-quality development of the digital economy in the new era, data compliance auditing focuses on conducting audits on data compliance to establish a cyclic governance system for the entire data lifecycle. This article takes the data lifecycle of 'source collection—storage and transmission—processing and usage—destruction and archiving' as the main thread, constructing a theoretical analytical framework for data compliance auditing. Based on a systematic explanation of its conceptual construction and practical dimensions, this article proposes four approaches to address data compliance audit risks: tracing data sources and collection compliance risks through a data map to upgrade passive auditing to active and continuous closed-loop supervision; strengthening the compliance defense of data storage and transmission through a graded authorization system to achieve continuous risk management; standardizing the compliance path of data processing and usage through a log evidence system to transform static compliance checks into dynamic technical supervision; and reinforcing the compliance barrier of data archiving and destruction through an automated management platform to achieve substantive verification at the end of the data lifecycle.

Key Words: data compliance audit; data full lifecycle; data elements; data governance; compliance governance; data security; digital economy