智能审计中数据安全治理模型构建研究

卢佩琳[1],化贵啟[2a],朱　翼[2b]

(1. 中国社会科学院大学 商学院,北京 102488;2. 南京审计大学 a. 统计与数据科学学院,b. 计算机学院,江苏 南京 211815)

[摘　要]随着智能审计在审计实践中的深入应用,数据安全问题日益凸显。当下数据安全治理聚焦于数据本体保护,缺乏对整个数据流程、全要素的动态评估和持续优化机制,难以满足智能审计场景下的安全需求。基于此,借助数据安全成熟度模型,构建涵盖数据安全过程、安全能力和能力成熟度等级三个维度的面向智能审计的数据安全治理模型。该模型围绕审计数据的采集、预处理、分析、线索核实以及报告生成五个阶段,将组织、制度、技术、人员等安全能力要素进行融合,并设定五级成熟度等级,旨在指导数据安全治理路径。虽然该模型拥有良好的结构通用性,但在行业定制、跨组织协同、跨境数据审计等复杂场景仍存在适配性方面的挑战,需要进一步拓展适配机制和评估方法。

[关键词]风险评估;审计风险;动态评估;数据安全成熟度模型;数据安全;智能审计

[中图分类号]F239　　[文献标志码]A　　[文章编号]2096-3114(2026)01-0056-13

一、引言

在数字经济蓬勃发展的背景下,数据已成为驱动国家治理、企业运营与审计监督的重要战略资源,数据安全治理也随之成为数字治理体系中的核心议题之一。国务院《“十四五”数字经济发展规划》在“着力强化数字经济安全体系”中明确将“提升数据安全保障水平”作为重要组成部分。在审计领域,《中华人民共和国审计法》第十六条亦明确了审计机关和审计人员的保密义务。由于审计业务日益数字化、自动化,如何确保审计过程中数据的机密性、完整性与可控性,成为提升审计质量与可信度需要解决的问题。

人工智能、大数据分析等新一代信息技术迅猛发展,审计工作也正在加速从传统的信息化、自动化阶段,向以大语言模型(下称,大模型)驱动、流程智能以及以数据挖掘为核心的智能审计新阶段迈进[1]。智能审计运用算法模型与审计流程系统进行深度融合,实现审计任务的自主分析和智能生成,在提高审计效率、扩大覆盖范围、增强风险识别等多个方面展现出显著优势。然而,以大模型为核心的智能审计系统在提高审计效率的同时,也面临数据安全的新挑战,其中包括越狱、数据中毒、模型幻觉以及模型记忆等问题,这些问题导致传统依靠访问权限控制和静态数据脱敏的保护方式难以应对大模型在推理过程中出现的信息泄露与输出偏差等风险[2]。因此,构建面向智能审计场景的全过程、动态化、安全可控的数据安全治理模型,已成为当前审计领域亟待解决的核心问题。

当前,智能审计实践中的数据安全治理存在多方面短板。一方面,数据保护措施主要集中在静态层面,如数据脱敏、访问控制、日志审计等,缺少对数据在采集、处理、分析、存储和销毁整个过程的系统性风险识别与动态响应[3];另一方面,审计组织在组织建设、制度流程、技术支撑、人员能力等方面所拥有

[收稿日期]2025-06-16

[基金项目]国家自然科学基金青年项目(62006121);教育部人文社会科学研究规划基金项目(23YJA870009)

[作者简介]卢佩琳(1985—),女,河南郑州人,中国社会科学院大学商学院博士生,主要研究方向为企业审计治理;化贵啟(1998—),男,江苏宿迁人,南京审计大学统计与数据科学学院博士生,主要研究方向为审计大数据统计,通信作者,邮箱:DA2508009@stu.nau.edu.cn;朱翼(1987—),男,江苏南京人,南京审计大学计算机学院副教授,硕士生导师,博士,主要研究方向为智能审计。

的安全保障能力尚未形成闭环,治理水平分布不均衡,难以支撑智能审计多场景与多系统的复杂安全需求[4]。

为了更好地进行数据安全治理,理论界与实务界已经提出多种数据安全治理模型和框架。早期的数据治理安全模型,比如以数据为中心的安全模型(Data-centric security model),主张凭借数据资产分类分级、访问控制和权限管理等相关手段,保障数据在存储及调用过程中的机密性、完整性和可控性[5]。然而,早期的这些模型多基于静态风险视角,治理边界被局限在数据存储层或者平台端口层,没有考虑数据在业务流程中生成、流动、共享和使用的全过程风险。随着系统复杂度上升,Gartner公司提出以数据为中心的审计与保护(Data-Centric Audit and Protection)框架,强调结构化与非结构化数据统一治理,并加入数据使用行为监控和风险状态感知机制[6]。虽然在风险动态感知方面进行拓展,但核心还是面向IT系统层级,精确对齐审计实践场景存在难度。面向云医疗服务机构的数据保护影响评估(DataProtection Impact Assessment (DPIA) for Cloud-Based Health Organizations)框架,则是强调数据处理活动之前的隐私风险预测和控制义务,着重突出数据处理最小化、用途绑定、合规审计记录等规范性机制[7]。即便在数据生命周期治理和跨境数据传输规范方面已经较为成熟,但在智能审计这个高强度协同、多节点任务驱动的场景下,适用性也是相对有限的。近年来,成熟度评估机制在数据安全治理中的应用逐渐受到重视。以阿里巴巴提出的数据安全成熟度模型(Data Security Maturity Model)为例,其构建了覆盖制度、技术与人员的分级能力评价体系[8]。该模型为数据治理能力的成长路径提供了理论支持,但多服务于互联网平台企业,缺乏面向审计任务链条的流程嵌入与阶段适配机制,特别是在智能审计所依赖的自动化分析、语义建模、模型迭代等环节中缺乏精细化的能力约束与过程评价。为凸显现有代表性的数据安全治理模型和框架的差异,表1给出上述模型与框架的对比。

表1 现有数据安全治理模型与框架梳理

数据安全治理模型	流程覆盖	风险类型	动态性与适配性
以数据为中心的安全模型[5]	侧重数据存储与调用	注重机密性、完整性、可控性	以静态规则为主并缺少业务适配
以数据为中心的审计与保护框架[6]	侧重数据治理	注重IT平台风险	具备风险动态感知能力但业务适配不足
面向云医疗服务机构的数据保护影响评估框架[7]	侧重数据处理活动,流程覆盖合规性环节	注重隐私保护、用途绑定、合规风险	合规循环完善但技术演化和业务适配不足
数据安全成熟度模型[8]	侧重制度、技术与人员	注重通用数据安全风险	分级评估清晰缺少动态演化与业务适配

大多数数据安全治理模型仍以一般性数据管理场景为主,缺乏对审计业务流程的深度嵌入与适配,难以直接支撑智能审计的数据安全治理。为弥补上述不足,本文以智能审计中的数据安全风险为出发点,结合审计流程复杂性、技术依赖强度等特点,借鉴数据安全成熟度模型的分层治理与持续改进理念,从数据安全过程、安全能力与能力成熟度等级三个核心维度出发,构建了面向智能审计的数据安全治理模型。该模型不仅覆盖审计全流程的数据安全要素,也系统嵌入了安全能力与成熟度等级评价机制,旨在推动数据安全治理从静态防护向动态管理、从碎片控制向系统治理的转型,为我国智能审计的数据安全治理体系建设提供理论支撑与路径参考。

二、理论基础

(一)智能审计相关概念的演进与技术逻辑梳理

在审计信息化持续推进的背景下,审计技术体系经历了“数字审计—大数据审计—智能审计—智慧审计”的演进过程,展现了从工具支持向系统智能跃升的趋势[9]。数字审计把ERP系统、数据库以及计算机辅助审计技术当作基础工具,进行审计数据的电子化采集和处理。大数据审计凭借分布式计算和数据挖掘技术,实现从样本抽查向全量分析的转变,显著拓宽了审计的覆盖范围并提升了审计的精

度。基于此,智能审计依靠自然语言处理、机器学习等人工智能技术,推动审计由规则驱动向模型驱动转型,并且广泛运用在风险识别、线索提取及报告生成等关键环节中,有效提升了审计工作的智能化水平。智慧审计运用大语言模型、区块链和物联网这类先进技术,推动审计系统拥有自学习、跨域感知和生态协同的能力,向更高级的战略审计形态进行演化。

智能审计作为承上启下的关键阶段,它不仅继承了大数据审计的分析能力,同时还引入了认知推理和自动化模型,以此推动审计职能从传统的监督向战略治理转型。学术界与实务界对于"智能审计"还没有形成统一的定义。罗斌元强调,它是以大语言模型这类前沿技术来重塑审计模式与能力[10]。许奎则是从目标和效能两个方面,把智能审计视为一个借助标准化、自动化和深度分析来显著提升审计监督效能的现代化体系[11]。虽然智能审计尚未在各类审计实践中全面普及,但是它在国家审计和企业内部审计中已经出现实践探索。例如,"金审三期"工程采用自然语言处理和数据标签挖掘技术,提高了审计平台的语义识别与风险预警能力。

(二)智能审计中数据安全风险与治理挑战

在智能审计实践过程中,数据已然成为审计活动的核心资源。它的安全性直接对审计的合规性、公信力与有效性造成影响。围绕数据开展的智能审计流程主要涵盖数据采集、数据预处理、数据分析、线索核实和报告生成五个阶段。该流程虽然显著提高了审计的效率和智能化水平,但也在各环节中引入了多样化的数据安全风险。尤其是在大模型被广泛应用的背景下,风险呈现新的特性。一方面,传统的数据安全风险依然存在,并且在智能审计场景中变得愈发复杂,主要体现在未授权访问风险、隐私泄露风险、证据链断裂与不可追溯风险等问题上。另一方面,大模型等人工智能技术的引入带来新型的数据安全风险,主要包括越狱、数据中毒、模型记忆和模型幻觉。

在现有研究与实践中,针对传统数据安全风险的治理,已经拥有较为成熟的应对机制,而针对新型的数据安全风险,学界与业界也已提出一系列具有针对性的治理策略。首先,对于越狱风险,可以借助MTSA(Multi-turn Safety Alignment for LLMs through Multi-round Red-teaming)框架,通过多轮对抗迭代优化的方式,提高多轮对话中的安全性[12]。对于越狱常见手段之一的提示注入攻击,可以运用PromptArmor方法,在大模型执行指令之前,对输入的内容进行注入提示的检测和清除[13]。其次,对于数据中毒风险,可以及时开展数据过滤,把训练语料中的异常样本剔除[14]。再次,对于模型记忆风险,可以运用差分隐私机制(在训练过程中向大模型参数或输出结果添加噪声,降低大模型对个体数据的可识别性),也可以采用联邦学习架构(数据在本地实现训练过程),或者结合同态加密与安全多方计算,实现大模型训练和推理对于密文数据的直接处理,从而阻断敏感信息在传输和计算过程的路径暴露[15]。最后,针对模型幻觉风险,借助检索增强生成技术约束大模型的回答基于外部真实语料,以提升生成内容的事实一致性[16],也可以选用模型蒸馏技术,把大型模型压缩成行为更为稳定、推理路径更为可控的小型模型[17]。

除数据安全风险本身外,许多审计组织还面临治理成熟度不足与安全能力不足等系统性治理挑战。一方面,虽然风险防控已经得到重视,但许多审计组织仍缺乏健全的安全能力体系[18]:治理架构不清晰,职责边界模糊以及部门协同不足;数据管理仍以被动防护为主;关键工具未有效集成;审计人员安全意识薄弱。另一方面,智能审计领域的数据安全治理水平仍处于从初始探索向规范化过渡阶段,尚未形成跨流程、跨角色、跨系统的统一治理标准[19]。大多数审计组织的数据安全治理水平体现为:有制度但执行不稳定;流程初步明确但缺乏量化评估;技术工具进行了部署,但缺乏综合联动。数据安全策略缺乏持续评估与反馈机制,导致安全措施无法随业务场景或技术变化及时更新。

三、面向智能审计的数据安全治理模型构建

本文构建的面向智能审计的数据安全治理模型参考了信息系统安全治理理论、数据安全成熟

度模型以及数据生命周期管理框架，由数据安全过程维度、能力成熟度等级维度以及安全能力维度三部分构成，该模型的具体结构如图 1 所示。

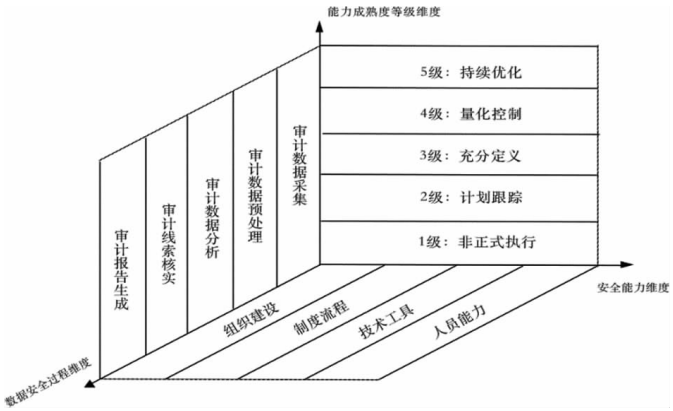

图 1　面向智能审计的数据安全治理模型

（一）数据安全过程维度

在数据安全过程维度中，智能审计的数据生命周期被划分成审计数据采集、数据预处理、数据分析、审计线索核实以及审计报告生成五个关键的阶段。而各个阶段在信息处理的内容方面存在显著的差异，所以其面临的安全风险也不相同。基于此，需从每一个阶段的功能特性出发，系统分析和处理其面临的主要数据安全问题及相应的控制策略。

1. 审计数据采集

这个阶段的核心任务是高效地获取海量、多源审计数据，数据根据来源分为内部数据（如财务系统、合同文本、内部控制文档等）和外部数据（如法律法规、企业年报、公开信息平台等）。在开展内部数据采集工作中，经常会借助自动化工具对本地系统进行批量调用，如借助 API 接口（不同软件应用程序之间进行通信和交互的一种途径）、数据库脚本等方式提取结构化与半结构化数据。这个过程面临诸多安全隐患，比如传输链路未进行加密、身份认证机制比较薄弱、跨系统通信协议不一致等，可能会导致敏感数据在传输过程中遭到篡改、窃取或者未授权访问。为了降低上述风险，应在采集流程中构建完善的访问控制机制，并利用加密协议来保障数据链路安全，同时，运用 API 令牌认证机制与接口调用限频策略，以防范恶意访问。

在外部数据采集任务中，当前越来越多的审计系统引入大模型驱动的数据抓取机制，如通过自然语言指令生成数据调用路径，或由嵌入式智能体自动搜索与提取目标信息，这带来了新的安全挑战：其一，若语义提示未经过严格过滤，则可能引发越狱风险尤其是提示注入攻击，绕过权限边界访问受限数据；其二，若大模型自动构造的数据抓取路径引用了未经验证的开放资源，则可能引发数据中毒风险，将低质量或虚假信息引入审计链条。为防范上述问题，应引入如 PromptArmor 之类的提示注入防护机制，在大模型执行前对输入指令进行解析、识别与剔除潜在恶意提示，确保数据调用行为不超越权限设定。同时，可结合启发式数据过滤策略，通过规则引擎剔除不符合可信度标准的数据源，从源头降低外部数据污染带来的风险。

2. 审计数据预处理

这个阶段主要任务包括数据清洗、格式统一、标准映射和敏感字段的脱敏处理。该阶段处理的数据体量极其庞大，类型十分复杂，并且还会涉及用户身份、财务数据等高敏感字段，所以很容易出现权限越界、敏感信息暴露、接口被非法调用等安全风险。为了有效防范上述风险，应当部署智能预处理引擎，配合数据分级分类策略，针对高敏感等级数据设置独立的处理流程和访问权限控制流程；同时还要构建完整的可追溯日志机制，记录每一步处理行为，从而确保数据处理过程能够清晰可见、实时查询、有效控制，提高整体数据治理的透明度和安全性。

此外，若是在这个阶段中引入大模型执行数据标签的自动生成和语义补全等任务，也可能引发新的数据安全方面风险。尤其在缺乏训练数据监管机制的情况下，大模型存在记忆训练语料中个体样本信息的风险。为应对模型记忆风险，运用差分隐私机制，在大模型训练的过程中向参数或输出中注入噪声，显著降低大模型对个体数据的可识别性，平衡数据可用性与隐私保护之间的关系。

3. 审计数据分析

这个阶段的主要任务是利用机器学习、知识图谱、异常检测等方法对数据展开深入挖掘,以找出潜在的舞弊行为、政策风险和管理漏洞。该阶段的安全挑战十分明显:一方面,数据访问频繁,用户协作密集,如果缺少细粒度权限控制和行为日志审计机制,就很容易引发敏感数据泄露、模型滥用、审计结果篡改等问题,要构建权限管理机制,结合动态访问控制和行为审计技术,实现用户访问路径的全过程记录和实时异常识别。另一方面,分析过程对大模型的依赖日益增强,带来了新型风险。首先,越狱风险日趋严峻,即用户通过精心构造的提示引导大模型输出原始数据或绕过权限限制。对此,可引入 MTSA 机制对用户输入进行上下文语义识别与行为模式分析,及时发现并拦截越权请求。其次,存在模型幻觉风险,即大模型基于训练偏差或语义误判生成与事实不符的分析结论。为降低该类风险,应采用检索增强生成技术,将结构化数据库、权威审计准则或真实业务文档作为外部知识源嵌入大模型上下文,使大模型输出具备可验证性与现实依据,从而提升其推理准确性与审计可解释性。

4. 审计线索核实

这个阶段主要任务是针对系统初步识别的异常数据开展事实核查、背景还原和逻辑关联工作,以此形成有法律效力和业务说服力的审计线索。该阶段面临的典型风险包含线索数据缺失、记录造假、跨系统数据引用不一致等问题,直接影响审计结论的准确性和可信度。对此,可以借助区块链、标签追踪等技术构建数据链路追溯体系,实现数据从采集到引用的全过程可视、可查、可验。同时,引入多维一致性比对机制和可信验证算法,提高线索数据的真实性、完整性、可验证性,为后续审计判断提供坚实的数据基础。

在审计线索核实中,大模型经常被运用到语义比对、文档摘要撰写、线索重构等任务中。然而,大模型可能会产生伪匹配、线索虚构、证据链断裂等模型幻觉风险。为了应对这一问题,可以选用检索增强生成技术,把权威数据源和结构化文档当作外部知识注入模型上下文,提高其推理准确性。同时,为了处理业务变更和知识更新不及时的问题,可以借助模型蒸馏技术,把最新的专业规则和领域知识迁移至轻量化模型中,提升线索核实过程中的稳健性与可信度。

5. 审计报告生成

这个阶段的主要任务是对审计发现、问题分类、改进建议、数据证据等内容进行结构化整合与表达。该阶段的核心风险主要包括篡改报告、数据泄露和非授权访问,尤其在报告传输和归档的过程中,如果缺乏强控制手段,就很容易被恶意用户窃取或者篡改审计结果。因此,应当强化报告生成系统的访问隔离和审批权限的控制,运用电子签章、内容加密、水印识别等多重防护手段,确保审计报告在内容、格式以及流转路径方面的统一性和保密性。同时,还需建立完整的报告版本管理机制与归档安全策略,实现报告在生命周期内的风险闭环。

大模型被运用撰写报告初稿和生成审计结论,在提高效率的同时还带来了新的数据安全风险:一是模型幻觉风险。大模型在没有充分地理解上下文或者是缺乏事实依据的情况下,会输出和实际不契合的审计结论或者分析意见。因此,可以借助检索增强生成技术,把权威审计规则、历史案例和结构化数据库当作外部知识注入大模型,提高生成内容的准确性与可信度。二是模型记忆风险。如果大模型在训练阶段接触过敏感数据,就有可能在生成报告的过程中无意识地嵌入训练语料片段,导致隐性信息泄露。为了降低这类风险,可以选用联邦学习方法,使大模型训练在本地完成,确保敏感数据不会被上传或者暴露于中心服务器,实现数据在源头的私密保护。

(二)能力成熟度等级维度

能力成熟度等级维度旨在刻画审计组织在数据安全治理工作中的发展阶段与能力水平,从而为其制定治理路径与战略优化方向提供系统参考。该维度主要借鉴能力成熟度模型和数据治理成熟度框

架,运用层级演进的思想,把数据安全治理能力成熟度划分成非正式执行、计划跟踪、充分定义、量化控制以及持续优化五个等级,每一个等级都代表了审计组织在制度、技术、应对能力等方面的不同成熟阶段。

1. 非正式执行(L1)

该等级的主要特征是制度缺失、技术空白和应对滞后。在制度方面,审计组织尚未建立起系统性的数据安全治理制度体系,对数据安全问题缺乏清晰明确的认知,相关工作依赖个别人员的经验。在技术方面,技术手段处于缺失的状态,通常不具备基本的安全防护机制。在应对方面,当面对数据安全事件,往往处于被动状态,难以及时识别风险并作出有效响应。为了提高该阶段的可识别性与可评估性,可以选用以下评判指标:是不是存在正式的数据安全管理制度;是不是设置专人来开展数据安全事务的管理工作;审计流程中是不是进行了任何安全控制点的配置工作;是不是启用如访问控制、传输加密、操作日志记录等这些基本的安全功能;是不是拥有数据安全事件的应急响应预案。如果上述大多数问题为“否”,那就可以判定该组织仍然处于非正式执行阶段。

2. 计划跟踪(L2)

该等级的主要特征是制度初建、技术介入、应对逐步规范。在制度方面,审计组织已经初步认识到数据安全的重要性,并且开始尝试构建数据安全治理制度体系。组织制定出基础的数据安全策略,并且设置简单的管理流程和监控措施。在技术方面,逐步把基本安全控制工具运用起来,对关键节点实施保护。审计人员接受初级安全教育,安全职责开始得到明确。在应对过程中,对于数据异常或者潜在风险,组织已经拥有最基本的应对能力。为了提高该阶段的可识别性与可评估性,可以运用以下评判指标:是否制定并且正式发布数据安全相关的制度文件;是否设置审计流程当中的关键安全控制点,比如权限审批以及数据脱敏节点等;是否启用基础的数据加密以及权限管理工具;是否开展数据安全基础培训并且记录其覆盖率;是否建立最基本的数据安全应急响应流程;是否有进行定期的数据安全检查或者制度回顾评估。如果组织满足上述的大多数指标,并且制度执行具有连续性,同时技术工具覆盖核心流程,就可以归入该等级。

3. 充分定义(L3)

该等级的主要特征是制度完善、技术集成、应对主动。在制度方面,审计组织已经形成较为系统的数据安全治理制度体系。组织拥有安全管理架构,设立专门的数据安全治理部门。在技术方面,运用多种安全控制措施,实现对关键系统和数据的有效保护。审计人员整体有着较强的安全意识和操作能力。在应对方面,组织可以主动识别审计过程中的安全隐患,及时响应并修复,安全事件处理拥有规范流程。为了提高该阶段的可识别性与可评估性,可以选用以下评判指标:是否已经建立起能够覆盖整个审计流程的安全制度,并且实现内部发布以及开展内部培训;是否设立了专职的数据安全岗位或者治理小组,对职责进行了明确分工;是否能够以实现制度标准化及模块化设计为目标,去支持跨业务场景复用;是否进行部署,包括运用访问控制、数据脱敏、行为监控、威胁检测等多重技术手段;是否开展全员中高级安全培训工作,并且设有定期考核机制;是否进行建立涵盖预警、响应、修复与复盘的安全事件处理机制。如果上述指标多数已达标,并且制度、技术、人员这三者之间能够形成闭环联动,那么组织就可以被判定为处于该等级。

4. 量化控制(L4)

该等级的主要特征是制度高效执行、技术深度融合、应对精准高效。在制度方面,审计组织已建立高效运行的数据安全治理制度体系,不仅全面覆盖审计流程,而且执行过程实现了自动化与数据化管控。制度实施产生的效果能够进行量化,组织已经开始依据关键绩效指标对安全管理水平进行监控。在技术方面,广泛开展智能审计平台、数据加密管理系统、身份认证体系、行为分析系统等部署工作,形成了一个多维度、自动化的安全防护网。在应对方面,平台可以对审计过程中的安全数据进行实时采集

与分析,实现快速预警与联动处置。安全应对能力比较突出,能够动态调整策略、量化评估风险,提升资源配置的科学性和效率。为了提高该阶段的可识别性与可评估性,建议运用以下评判指标:是否开展了数据安全治理绩效考核机制的建立工作,使其明确制度执行的量化目标;是否实现安全制度在审计全流程当中的规范覆盖与系统联动;是否进行具有自动监控与响应功能的安全管理平台的部署工作;是否能够依靠数据指标(比如事件响应时效、异常拦截率等) 去动态评估安全治理效果;是否形成数据驱动的策略优化机制。如果上述多数指标已达标,并且安全制度、技术系统与治理行为之间拥有高度协同,组织就可以被认定为处于该等级。

5. 持续优化(L5)

该等级都主要特征是制度自我演化、技术自主创新、应对前瞻主动。在制度方面,审计组织已经达到数据安全治理制度体系的最优程度,治理理念从控制与防护转变为引领与创新。组织能够按照外部监管政策、行业标准和内外部实践情况,动态调整并持续优化现有的制度体系,实现制度的自我演化。在技术方面,除广泛运用前沿安全技术,审计组织还拥有自主研发、集成优化和平台整合的能力,构建与业务深度融合的智能安全架构。在应对方面,应对机制高度敏捷,具有前瞻性威胁识别、趋势预判和策略仿真的功能,可以主动发现未知风险,构建闭环治理与自适应修复机制。为了提高该阶段的可识别性与可评估性,建议运用以下评判指标:是否开展覆盖外部环境感知以及内部反馈闭环的制度更新机制的建立工作;是否拥有定期审议和自我优化的数据安全标准流程这样的特性;是否拥有自主开发或者深度定制的数据安全管理平台,并且能够和主业务系统高度集成;是否形成以仿真、预测、策略测试当作核心的安全策略演练机制;是否建立跨审计类型、跨组织或者行业的数据安全协同机制以及标准接口;是否已经将数据安全治理能力纳入组织战略体系当中,把它作为可持续演进的重要构成部分。如果上述大部分指标都已经达标,而且组织具备制度、技术、应对这三位一体的演化能力,就可以被判定为处在该等级。

(三) 安全能力维度

安全能力维度是审计组织在制度、技术、人员、文化等方面开展系统性数据安全保障的能力,旨在系统评估审计组织在数据安全治理中的实际表现能力。结合审计业务所具有的实际特性,该维度包含组织建设、制度流程、技术工具和人员能力四个方面。

1. 组织建设

组织建设是数据安全治理的基础支撑,涵盖组织架构设置、治理制度体系构建、职责分工等内容。在实施智能审计过程中,审计组织需设立专门的数据安全治理机构或明确职能归属,明确界定各级部门及岗位承担的数据安全保障工作中的责任边界。为提高组织安全意识,应在机构内部进行数据安全文化培育,通过宣传教育、制度引导等方式强化审计人员对数据安全的认知和行为自律,共同构建安全可信的数据安全治理环境。

2. 制度流程

制度流程体现了审计组织在数据安全治理中的规范性与程序化程度,是保障数据安全治理工作有效落实的重要机制。在智能审计实践中,审计组织需制定完善的数据安全治理政策,建立覆盖数据采集、处理、分析、存储、共享等环节的标准化流程,并设定配套的安全控制措施和应急响应机制。面对快速变化的风险环境,需要定期开展数据安全风险评估工作,按评估结果动态调整安全策略,提高制度的适应性以及前瞻性。同时,需把审计实践当中所形成的安全经验以及应对措施制度化、流程化,推动数据安全治理模式由经验驱动向制度化、规范化转型,增强数据安全防护的一致性与持续性。

3. 技术工具

技术工具是提升数据安全治理效能的关键手段。审计组织应积极引入先进的数据分析、加

密防护、访问控制、异常检测、大模型风险防范等技术，构建覆盖全流程的数据安全治理技术体系。同时，应加强对自主可控安全技术的探索和运用，提升安全防御的本地化程度与可控性。技术工具不仅是保障数据安全的底层支撑，而且直接关联到审计效率、数据处理精度及风险识别能力。

4. 人员能力

人员能力是数据安全治理模型中最具活力且不可替代的要素，是实现数据安全治理模型有效运行的核心保障。在智能审计背景下，审计人员不但要运用基本的信息安全知识，还应理解大数据、大模型等技术在审计过程中的实际应用场景及其潜在安全隐患。为此，审计组织应建立定期的培训机制，提高审计人员的数据安全意识与专业技能。同时，应注重高端安全治理人才的引进和培养，形成内部培训与外部引才相结合的复合型人才梯队，为数据安全治理能力的持续提升提供坚实的人力支撑。

（四）模型的动态适配与演化机制

在该模型中，数据安全过程维度是风险暴露的起点，安全能力维度是即时响应的资源库，而能力成熟度等级维度则是后续优化与演化的评估机制。三者通过“触发—介入—反馈—再配置”的动态联动，构成数据安全治理闭环：数据安全过程维度产生事件，经事件总线标准化进入策略引擎；策略引擎根据规则与上下文从安全能力维度选取能力要素，由控制点编排器驱动自动或半自动处置，并在必要处引入人工复核；处置轨迹与结果以指标与证据的形式回写指标和证据仓，以供成能力成熟度等级维度周期化计算并反向驱动数据安全过程维度与安全能力维度的重配置与升级。

数据安全过程维度以智能审计数据生命周期为基础，是风险识别与防控的“时间轴”。当某个阶段出现问题时，安全能力维度首先被激活，实施即时防控。安全能力维度作为风险控制的“资源池”，旨在各阶段嵌入恰当的治理措施，提升过程各节点的风险应对能力。两者之间是通过能力嵌入过程机制实现联动。其一，组织建设着重强调治理结构和职责配置在五个数据安全阶段的前置约束和事后问责：在数据采集阶段，由数据接入审批小组负责来源、接口以及敏感标签的准入把关工作；在数据预处理阶段，由数据治理专员对脱敏与标准化过程负责，并受审计办内控监督；在数据分析阶段，设立跨部门安全工作组（如审计、IT、安全），开展权限分层和异常处置升级工作；在线索核实阶段，启用独立证据核实小组，以保障追溯性和一致性；在报告生成阶段，由独立审批委员会行使最终发布权。组织建设能力的触发规则，是策略引擎根据事件严重级别（如跨域访问、高敏标签、跨系统共享等情况）自动派工到相应组织角色，组织节点的介入会被强制留痕，并将其纳入绩效考核。其二，制度流程作为刚性约束会贯穿全过程：在数据采集阶段，运用白名单、接口权限、用途绑定和最小权限令牌等制度进行边界设定；在数据预处理阶段，以统一清洗规则、脱敏口径、用途限制及留痕规范实现过程一致性；在数据分析阶段，借助工具调用权限矩阵、行为审计制度与异常处置来限定分析模型的使用范围；在线索核实阶段，凭借版本控制、归档规范和证据审计规则保证其可追溯性；在报告生成阶段，依靠审批、加密、签名和信息披露制度确保权责落到个人。制度流程能力由策略引擎以“规则—策略—动作”三层映射落实到控制点，违例触发自动隔离与人工复核。其三，技术工具提供具体的自动化与半自动化执行力：在数据采集阶段由 API 网关、传输加密、令牌轮换与异常检测引擎实现实时拦截；在数据预处理阶段由自动清洗引擎与高风险样本隔离器执行先处置后审查；在数据分析阶段以检索增强生成校核、越狱检测、越权访问隔离、分析模型输出置信度阈值与工具调用沙箱构建核心防线；在线索核实阶段以区块链式时间戳与哈希链、差异比对与回滚器实现证据一致性；在报告生成阶段以数据泄露防护、防篡改签名、加密发布与水印追踪形成外发保护。其四，人员能力承担高不确定场景当中的判断和复核工作：在数据采集和预处理阶段，针对异常来源、漏脱敏样本开展抽检工作；在数据分析阶段，针对低置信度和可

疑输出进行校核并二次检索;在线索核实阶段,通过人工确认跨库比对与异常一致性;在报告生成阶段,对敏感信息、签名和加密流程进行终审。

在此基础上,能力成熟度等级维度构成了该模型的“演进轴”,旨在刻画审计组织在数据安全治理当中的阶段特性和成长路径。五个能力成熟度等级通过和数据安全过程维度与安全能力维度的量化指标相结合得以具体化,形成可评估、可追踪的判定标准。数据安全过程维度的相关指标如表2所示,安全能力维度的指标如表3所示。表2与表3所列的指标只是基础性的参考,并非将所有情形都包括在内,不同的审计组织应该结合自身业务特点和风险环境对指标进行适当调整。本文为避免设定绝对数值可能带来的不确定性以及局限性,统一运用区间化方法来界定能力成熟度等级阈值,从而在不同等级之间形成由低至高的渐进式划分。各组织也可以依据具体情况进一步细化或调整阈值区间,提升模型的适用性及灵活性。能力成熟度等级的提高遵循连续两期(4~8周作为一个周期)核心指标达标的综合判断,若任意关键指标在连续的周期内低于阈值,即触发整改及回退机制,并要求在规定的期限内提交优化和再评估计划,以保证治理能力的持续改进与动态演进。

综上,能力成熟度维度并非仅作为一种静态分级标签存在,而是充当数据安全过程维度和安全能力维度的动态调节器与演化驱动器。具体而言,能力成熟度等级的提升会使数据安全过程维度在控制模式上实现逐级跃迁:从早期的关键节点有限覆盖,逐步扩展成为全过程覆盖,并在此基础上实现自动化联动及自适应演化。与此同时,安全能力维度的演进表现为从组织与制度的框架化逐步过渡到技术配置的自动化和人员介入的智能化,实现深度耦合与整体优化。它的运行逻辑是:当数据安全过程阶段暴露风险时,策略引擎依据制度规范与上下文环境自动选择适配的技术动作,并在必要时触发组织或人员的介入;治理动作的执行结果以指标和证据的形式进行沉淀,然后进入能力成熟度等级评估器当中进行双维度指标的量化定级;评估结果反向作用于数据安全过程控制点的颗粒度设置、安全能力触发模式的优化及资源配置强度的调整。

表2　数据安全过程维度指标与区间阈值

阶段	指标名称	指标说明	计算公式
数据采集	异常调用识别率	成功识别出的异常接口调用占比	识别出的异常接口调用数÷总异常接口调用数×100%
	越狱拦截率	拦截的越狱请求占比	拦截的越狱请求数÷总提示注入请求数×100%
	加密传输覆盖率	采用加密协议传输的流量占比	加密流量数÷总流量数×100%
数据预处理	脱敏覆盖率	已完成脱敏的敏感字段占比	已完成脱敏字段数÷应脱敏字段总数×100%
	脱敏正确率	脱敏处理未出错的字段占比	正确脱敏字段数÷已脱敏字段总数×100%
	高敏数据隔离率	采用隔离流程处理的高度敏感数据占比	隔离处理的高敏数据数÷高敏数据总数×100%
数据分析	行为日志审计覆盖率	纳入日志审计的操作占比	纳入日志审计的操作数÷总操作数×100%
	越狱拦截率	被成功拦截的越狱尝试占比	拦截的越狱尝试数÷总越狱尝试数×100%
	RAG校核通过率	检索增强生成校核一致结果占比	校验一致结果数÷总校核结果数×100%
	隐私计算应用率	使用隐私计算的分析任务占比	采用隐私计算任务数÷总分析任务数×100%
线索核实	证据追溯完整度	具备完整追溯链的线索占比	完整追溯线索数÷总需追溯线索数×100%
	跨库一致性比对率	在不同库中识别一致的比对结果占比	一致结果数÷总比对结果数×100%
	匹配率	正确匹配线索占比	正确匹配线索数÷总匹配线索数×100%
报告生成	签名覆盖率	采用签名的报告占比	已签名的报告份数÷应签名报告总数×100%
	加密覆盖率	加密传输和存储处理的报告占比	加密传输和存储的报告份数÷总报告份数×100%
	违规外发率	违规外发文档占比	违规外发文档数÷外发文档总数×100%

注:表格中每一个指标都分为五个能力成熟度等级区间 L1,[0,20%];L2,(20%,40%];L3,(40%,60%];L4,(60%,80%];L5,(80%,100%]。下表同。

表3　安全能力维度与区间阈值

安全能力维度	指标名称	指标说明	计算公式
组织建设	数据安全治理机构覆盖率	是否设立专门的数据安全治理机构	设立数据安全治理机构数÷应设立机构数×100%
	岗位职责清晰度指数	岗位是否具备明确安全职责	有职责说明的岗位数÷涉及岗位总数×100%
	数据安全文化普及率	安全宣传与培训覆盖情况	参与安全文化活动人数÷全体人员数×100%
制度流程	制度覆盖率	制度建设是否覆盖审计全流程	已制定制度数÷应制定制度总数×100%
	制度更新及时率	制度是否按要求周期更新	按周期更新的制度数÷应更新制度总数×100%
	应急响应完善度	应急响应流程是否覆盖所有已识别的安全事件类别	有响应流程的事件类别数÷已识别事件类别总数×100%
技术工具	关键安全工具部署率	是否部署关键安全工具（API网关、加密、防篡改、数据泄密防护等）	已部署工具数÷应部署工具数×100%
	异常检测准确率	异常检测是否准确	检测出的真实异常数÷异常报警总数×100%
	大模型风险防护率	是否启用大模型风险防护（越狱防护、幻觉检测等）	启用防护的大模型风险数÷已识别的大模型风险数×100%
人员能力	培训覆盖率	员工是否参与安全培训	接受培训人员数÷全体人员数×100%
	培训考核合格率	培训是否达到考核标准	合格人数÷参加考核人数×100%
	关键岗位安全胜任率	关键岗位人员是否具备安全胜任能力	胜任人员数÷关键岗位人员数×100%

（五）案例示范

本研究选取国内某能源企业作为案例进行示范分析。该企业是国内领先的能源生产商之一，业务范围涵盖能源勘探开发、化工生产、成品销售等多个板块，下设多家区域子公司，供应链管理系统结构复杂。该企业基于现有大模型微调出与自身业务相适应的审计大模型，并部署了自主可控的智能审计平台。该平台具备审计知识智能问答、审计问题定性自动推荐、审计底稿解析与台账自动生成、审计报告初稿自动生成等功能，实现了从数据采集、预处理、分析、线索核实到报告生成的全审计流程覆盖。

本研究的各类数据主要来源于该企业的内部资料，包括内部审计报告、数据安全治理相关文档和具体的审计数据（如敏感财务字段的接口调用日志、数据脱敏处理记录等相关内容）。为确保数据具备准确性及代表性，本研究通过对企业审计部门相关人员进行访谈，深入了解智能审计平台应用中的数据安全治理实践情况，系统收集各维度所需的相关资料。其中，访谈对象涵盖审计部门主要负责人和IT技术人员，访谈内容聚焦于数据安全治理措施的具体实施情况、平台运行成效和当前面临的安全挑战等内容。

本研究根据企业实际状况开展了能力成熟度等级评估指标的制定工作，制定的指标如表4与表5所示。基于上一评估周期的相关结果，该企业整体处于充分定义等级（L3）。此次审计任务是围绕风险识别、能力匹配、指标量化、成熟度判定、反馈优化的逻辑链条展开的。

在数据采集阶段，审计系统检测到来自非白名单域的接口调用比例为5%，其中2%涉及敏感财务字段。此时，组织建设通过数据接入审批小组进行合规性把关，制度流程依据接口白名单与用途绑定机制限制访问，技术工具利用API网关与加密传输进行实时拦截，审计人员则对提示注入攻击等越狱手段进行抽查复核。最终得到的结果如下：异常调用识别率为95%，加密传输覆盖率为88%，整体满足L3等级要求，但加密传输覆盖率尚未达到L4等级要求。

在数据预处理阶段，自动脱敏引擎出现10%的未脱敏情况。组织建设由数据治理专员负责规则修订，制度流程通过统一清洗规则与隐私保护政策留痕，技术工具利用自动脱敏引擎与高风险样本隔离器处置数据，人员对关键字段进行二次审查。结果显示，脱敏覆盖率为90%，脱敏正确率为85%，整体达到了L4等级要求。

在数据分析阶段，凭证与账务的比对过程中，大模型输出中有13%的结果存在误差，检索增强生成事实一致性告警与提示注入攻击特征被命中。此时，跨部门安全工作组进行协同处置，权

限矩阵与行为审计制度限制高风险调用,检索增强生成模块和越狱检测器拦截风险请求,人员对低置信度结果进行人工校核。最终,RAG 校核通过率为 87%,越狱拦截率为 93%,整体达到 L4 等级要求。

表 4　数据安全过程维度指标与区间阈值

阶段	指标名称	能力成熟度等级区间
数据采集	异常调用识别率	L1(0%≤值<40%)、L2(40%≤值<70%)、L3(70%≤值<90%)、L4(90%≤值<98%)、L5(98%≤值≤100%)
	加密传输覆盖率	L1(0%≤值<40%)、L2(40%≤值<70%)、L3(70%≤值<90%)、L4(90%≤值<95%)、L5(95%≤值≤100%)
数据预处理	脱敏覆盖率	L1(0%≤值<30%)、L2(30%≤值<70%)、L3(70%≤值<80%)、L4(80%≤值<95%)、L5(95%≤值≤100%)
	脱敏正确率	L1(0%≤值<50%)、L2(50%≤值<70%)、L3(70%≤值<85%)、L4(85%≤值<95%)、L5(95%≤值≤100%)
数据分析	RAG 校核通过率	L1(0%≤值<40%)、L2(40%≤值<70%)、L3(70%≤值<85%)、L4(85%≤值<95%)、L5(95%≤值≤100%)
	越狱拦截率	L1(0%≤值<40%)、L2(40%≤值<70%)、L3(70%≤值<85%)、L4(85%≤值<95%)、L5(95%≤值≤100%)
线索核实	证据追溯完整度	L1(0%≤值<40%)、L2(40%≤值<70%)、L3(70%≤值<80%)、L4(80%≤值<95%)、L5(95%≤值≤100%)
报告生成	签名覆盖率	L1(0%≤值<40%)、L2(40%≤值<70%)、L3(70%≤值<80%)、L4(80%≤值<95%)、L5(95%≤值≤100%)
	加密覆盖率	L1(0%≤值<40%)、L2(40%≤值<70%)、L3(70%≤值<80%)、L4(80%≤值<95%)、L5(95%≤值≤100%)

表 5　安全能力维度与区间阈值

安全能力维度	指标名称	能力成熟度等级区间
组织建设	数据安全治理机构覆盖率	L1(值=0%)、L2(值=0%)、L3(值=100%)、L4(值=100%)、L5(值=100%)
制度流程	制度覆盖率	L1(0%≤值<40%)、L2(40%≤值<70%)、L3(70%≤值<80%)、L4(80%≤值<95%)、L5(95%≤值≤100%)
技术工具	关键安全工具部署率	L1(0%≤值<30%)、L2(30%≤值<70%)、L3(70%≤值<80%)、L4(80%≤值<95%)、L5(95%≤值≤100%)
人员能力	培训覆盖率	L1(0%≤值<20%)、L2(20%≤值<50%)、L3(50%≤值<80%)、L4(80%≤值<95%)、L5(95%≤值≤100%)

在审计线索核实阶段,审计系统监测到合同与凭证的版本留痕存在缺失,跨库一致性校验存在异常。此时,证据核实小组负责跨系统比对工作,制度流程要求对比对全程强制留痕。技术工具借助区块链式时间戳及哈希链,还有差异比对与回滚器来支撑可追溯性,证据核实小组要负责复核,由人工确认关键差异。结果显示,证据追溯完整度为 75%,达到 L3 等级水平。

在审计报告生成阶段,对报告初稿进行外发检测时,告警被触发(命中了敏感片段),存在外发对象授权不充分的情形。报告审批委员会是最终监督工作的行使机构,签名、加密和审批制度会强制执行,数据泄露防护工具及数字签名技术被运用进行技术保障,人员会对报告敏感信息与签名措施加以复核。最终结果显示,签名覆盖率为 87%,加密率覆盖率为 92%,整体达到 L4 等级水平。

基于对五个阶段的综合评估,本文发现数据安全过程维度中的大多数指标达到 L4 等级阈值,仍有部分指标停留在 L3 等级。此外,企业已经设立了专门的数据安全治理部门,以确保数据安全治理机构覆盖率达到 100%;同时,审计全流程的制度规范也已建立,制度覆盖率为 100%。然而,关键安全工具部署率为 80%,人员培训覆盖率为 60%。综合评定,该企业能力成熟度等级为 L3 等级,尚未晋升至 L4 等级。根据评估结果,生成的能力成熟度等级反馈清单如下:数据安全过程维度需加强数据采集阶段对

加密传输理念的普及工作;在审计线索核实阶段,建议增强证据追溯技术的创新。针对安全能力维度,企业应加强数据安全治理培训工作,着重提高培训的覆盖率和质量。依据晋级规则,若后续周期所有指标均达标,则可晋升至量化控制等级;反之,若任一关键指标连续两期低于阈值,则触发回退和限期整改。

四、结论

随着审计智能化进程的不断推进,审计数据在多源异构和模型驱动等技术特征下,面临日益严峻的数据安全挑战。本文从当前智能审计实践出发,揭示了在数据采集、处理、分析、核实及报告生成等关键流程中存在的数据安全风险,并指出目前数据安全治理仍以静态控制为主,缺乏全过程、动态化、能力导向的治理机制,难以满足智能审计对安全性、合规性和可信度的多重要求。针对上述问题,本文以数据安全成熟度模型为基础,面向智能审计,构建了包含数据安全过程、安全能力与能力成熟度等级三个核心维度的数据安全治理模型。该模型从审计数据生命周期全流程出发,覆盖数据采集、预处理、分析、线索核实到报告生成各个环节,同时嵌入组织、制度、技术与人员等关键安全能力要素,辅以成熟度等级作为动态评估机制,具有较强的适应性与系统性。

该模型强化了审计组织根据自身职责定位与发展阶段制定数据安全治理策略的可行性,具备较高的实践指导价值,但仍存在一定的局限性。首先,尽管该模型具备较强的通用性与结构完整性,但在适配不同审计类型(如国家审计、内部审计与社会审计)时,仍需结合各自特有的数据风险特征与治理需求,补充相应的能力要素与控制机制。比如,国家审计强调高敏感数据的保密性及跨部门协同,内部审计注重于效率与流程敏捷性,社会审计侧重于证据的公开可验证性和独立性。其次,模型尚未进行大规模实证验证,尤其在不同行政等级、组织规模以及信息系统架构下的实际可操作性。最后,模型在进行跨部门协同审计以及跨境数据审计中存在适用性边界。例如,不同组织之间安全能力水平与制度协调程度差异较大,可能削弱治理等级评估与动态反馈机制的执行效果;在跨境审计场景中,数据传输合规性、加密算法标准、法律管辖权差异等问题,同样对模型的“制度-技术-流程”一体化方面提出更高要求,需要后续借助法规融合与国际数据安全协议支撑模型的完善工作。

参考文献:

[1]刘国城,孙秋萍,陈婕妤. 国家审计智能化的研究态势、实践路径与保障措施[J]. 财会通讯,2024(1):14-21.

[2]崔永梅,杨婷羽,应文池,等. 人工智能审计的理论内涵、问责边界与框架构建——基于负责任创新视角[J]. 审计与经济研究,2025(4):11-22.

[3]徐京平,陈思奇. 科学规范审计的解构、归因与效应——基于 DeepSeek 应用[J]. 南京审计大学学报,2025(5):13-23.

[4]钱钢,叶祥,龙利民. 智能审计场景、核心技术与实现路径研究[J]. 会计之友,2024(20):14-21.

[5]Hennessy S D, Lauer G D, Zunic N, et al. Data-centric security: Integrating data privacy and data security[J]. IBM Journal of Research and Development, 2009(2): 1-12.

[6]Mattsson U, CTO P. Data centric security key to cloud and digital business[EB/OL]. [2025-12-30]. https://nyoug.org/wp-content/uploads/2015/09/Mattson_Security_Key.pdf.

[7]Georgiou D, Lambrinoudakis C. Data protection impact assessment (DPIA) for cloud-based health organizations[J]. Future Internet, 2021(3): 66.

[8]石永. 数据安全审计方法与内容的探索[J]. 中国内部审计,2021(2):40-42.

[9]黄佳佳,周立云,徐超. 基于大模型的审计知识智能问答系统构建研究[J]. 会计之友,2025(9):24-30.

[10]罗斌元,曾捷. AI 大模型智能审计模式研究[J]. 中国注册会计师,2025(9):79-83.

[11]许奎. 以智能审计体系推动审计监督范式转型[J]. 人民论坛,2025(20):103-105.

[12]Guo W, Li J, Wang W, et al. MTSA: Multi-turn safety alignment for llms through multi-round red-teaming[J]. arXiv preprint arXiv:2505.17147, 2025.

[13]Shi T, Zhu K, Wang Z, et al. PromptArmor: Simple yet effective prompt injection defenses[J]. arXiv preprint arXiv:2507.15219, 2025.

[14]Wang K, Zhang G, Zhou Z, et al. A comprehensive survey in llm (-agent) full stack safety: Data, training and deployment[J]. arXiv preprint arXiv:2504.15585, 2025.

[15]Feretzakis G, Papaspyridis K, Gkoulalas-Divanis A, et al. Privacy-preserving techniques in generative ai and large language models: A narrative review[J]. Information, 2024(11): 697.

[16]Fan W, Ding Y, Ning L, et al. A survey on rag meeting LLMs: Towards retrieval - augmented large language models[C]//Proceedings of the 30th ACM SIGKDD conference on knowledge discovery and data mining, 2024: 6491 - 6501.

[17]Fang L, Yu X, Cai J, et al. Knowledge distillation and dataset distillation of large language models: Emerging trends, challenges, and future directions[J]. arXiv preprint arXiv:2504.14772, 2025.

[18]林慧涓,陈宋生. 构建多维度 AI 审计框架思考[J]. 会计之友,2023(23):32 - 37.

[19]Fahlevi M, Moeljadi M, Aisjah S, et al. Corporate governance in the digital age: A Comprehensive review of blockchain, AI, and big data impacts, opportunities, and challenges[C]//E3S Web of Conferences. EDP Sciences, 2023: 02056.

[责任编辑:黄　燕]

A Study on the Construction of a Data Security Governance Model in Intelligent Auditing

LU Peilin[1], HUA Guiqi[2a], ZHU Yi[2b]

(1. School of Business, University of Chinese Academy of Social Sciences, Beijing 102488, China;
2a. School of Statistics and Data Science. 2b. School of Computer Science, Nanjing Audit University, Nanjing 211815, China)

Abstract: As intelligent audit becomes increasingly integrated into audit practices, data security concerns have gradually come to the forefront. Current data security governance focuses primarily on protecting data entities, lacking dynamic assessment and continuous optimization mechanisms for the entire data lifecycle and all its elements. This approach struggles to meet security requirements in intelligent audit scenarios. Therefore, leveraging a data security maturity model, we propose a data security governance model tailored for intelligent audit. This framework encompasses three dimensions: data security processes, security capabilities, and maturity levels. This model integrates security capability elements including organizational, institutional, technological, and personnel aspects across five stages of audit data: collection, preprocessing, analysis, lead verification, and report generation. It establishes a five-level maturity to guide governance pathways. While the model demonstrates strong structural versatility, challenges in adaptability persist for complex scenarios such as industry-specific customization, cross-organizational collaboration, and cross-border data auditing. Further development of adaptation mechanisms and evaluation methodologies is required.

Key Words: risk assessment; audit risk; dynamic assessment; data security maturity model; data security; intelligent audit