企业数据资产审计的逻辑框架与实现机制

王敬勇　王盛丹　薛丽达

一、引言

2020年，中共中央、国务院发布的《关于构建更加完善的要素市场化配置体制机制的意见》，明确将数据作为与劳动力、资本等并列的生产要素，并提出要加快培育数据要素市场。数据资产作为一种新兴的资产形式，逐渐成为加速数字经济发展和推进数字中国建设的关键战略资源。为了更好地发挥数据资产的作用，党中央先后制定了《关于构建数据基础制度更好发挥数据要素作用的意见》《数字中国建设整体布局规划》等一系列重要决策部署，为数据资产管理研究工作的开展指明了方向、提供了遵循。但数据资产仍面临内部控制构建缺陷（余应敏等，2019）、隐私保护不可控（吴超，2018；Petrie，2016）、应用赋能增值不充分（徐涛等，2022）、流通缺少统一规范（刘悦欣和夏杰长，2022）等问题，这些问题的存在不仅影响企业的战略决策准确性和市场分析精准度，还可能引发法律诉讼等一系列严重后果。

目前，学术界关于数据资产的研究主要围绕数据资产确权、数据资产科目设置、数据资产管理等方面展开。在数据资产确权方面，有学者认为应该构建一套数据新型财产权制度（龙卫球，2017；程啸，2018），但有其他学者指出法律不应对企业的数据采取绝对性与排他性的财产权保护，而应针对不同类型的数据设计不同的保护制度（丁晓东，2020），或建立数据使用权（付新华，2022），以促进企业数据的使用、访问和共享。对于数据资产科目设置问题，目前学术界主要有三种观点：观点一认为应该将数据资产作为无形资产科目下的二级科目列示，属于无形资产观（游静等，2018；符文娟等，2022）；观点二认为应当将数据资产化进入存货科目，按照存货确认规则进行会计确认，属于存货资产观（秦荣生，2020）；观点三则认为将数据资产作为一级科目进行列示较为合理，属于数据资产一级科目观（李雅雄等，2017；张俊瑞等，2020；罗玫等，2023）。针对数据资产的管理，学者们从不同的方面提出了理论与模型，有学者以信息生态为基本理念，构建出适用于企业数据资产管理的信息生态模型（崔金栋等，2017；李菲菲等，2019）。李题印等（2022）通过对数据资产管理体系要素进行剖析，提出了企业数据资产管理体系逻辑框架，从而为实现数据资产保值与增值提供了依据。此外，还有学者将区块链技术与数据资产相结合进行研究。赵明等（2021）提出了基于区块链技术的数据资产管理新模式，对区块链体系中的各个层次进行结合应用；蔡昌等（2021）构建了基于区块链技术的数据资产确权与税收治理模式，进一步完善了数据资产的分配方式。

尽管学术界已经就数据资产的确权、科目设置及管理等方面开展了广泛研究，但这些研究主要集中在理论探讨和宏观政策制定层面，对于如何有效审计数据资产，确保其价值最大化的讨论仍相对有限。本文对企业数据资产审计的逻辑框架进行了系统性研究，明确了数据资产的审计本质、目标、方法等，探讨了企业数据资产审计的实现路径，旨在丰富企业数据资产审计的相关理论，帮助企业有效防范和降低与数据资产相关的风险，确保数据资产的有效利用和价值增长，以促进数字经济的健康发展。

二、企业数据资产审计的主要进展

企业数据资产审计领域的进展不仅体现在对数据安全性、个人信息合规与保护的规范和监督上，更在于算法决策过程中的透明度和公平性，以及对算法处理过程中可能引起的系统性风险的管理。

（一）企业数据资产审计的发展

《网络安全法》《数据安全法》和《个人信息保护法》的推行，要求企业不仅要关注数据资源和网络信息系统的安全性，还应构建一套全面的数据管理体系，包括数据的储存、共享、监控及安全风险评估，以此降低数据安全风险产生的可能性（许彩慧等，2024），在此背景下衍生出了安全审计和个人信息合规审计。白利芳等（2023）在云储存服务背景下，分析了云数据在其生命周期各阶段所面临的安全风险及相应的安全审计需求，其中保证云端存储数据的完整性是首要问题，其次便是确保在数据遭到破坏时可以恢复。王敬勇等（2024）从社交网络的角度探讨了云安全风险审计，并将利益相关主体分为云应用开发商、云服务提供商和云租户，提出了具有针对性的审计治理建议。刘国城（2020）强调了过程建模在互联网安全审计中的重要性，将其视为一个整合技术、工具和流程的动态抽象过程，并提出了大数据时代互联网安全审计过程建模的理念与智能化服务策略。敬力嘉（2022）在个人信息保护合规计划中提出区分原则，认为应以企业类型和规模来区分对个人信息保护合规的需求，在开展审计工作时需要遵循区分原则，

以实现相关审计要求的个别化。

（二）企业数据资产审计的突破

《网络安全法》《数据安全法》和《个人信息保护法》三大法规主要关注原始数据，即直接采集的结构化、半结构化或非结构化数据（肖冬梅，2024）。李雅雄等（2017）指出，数据资产是企业经过加工后能够实现特定商业目的并带来经济利益的可计量资源。这意味着原始数据本身并不构成企业的资产，只有经过算法加工后的数据才有真正的价值。然而，企业为了实现特定的利益诉求及利润最大化目标，在研发算法时往往会植入自身价值导向和利益意图（郑智航，2021），这时审计就需要确保数据和算法的使用不会导致不公平或歧视性结果，引发道德争议和伦理风险。欧盟于2016年出台的《通用数据保护条例》规定，在特定情况下需要进行数据保护影响评估（DPIA），强调对算法决策过程的透明度和可解释性的要求，以及企业在处理个人数据时必须遵守的合法性、公平性和透明度原则（Kaminski等，2019）。此外，欧盟在2020年公布的《数字服务法》中规定大型在线平台有义务采取一定的措施，确保所使用的算法系统设计不会在平台用户之间造成歧视，并要求其承担算法透明性、可控性和可问责性的风险管理义务，这都对算法审计产生了需求。算法审计通过向算法模型输入不同的测试数据，模拟演绎不同的运行场景，根据运行结果反推算法的内部决策逻辑，并推测算法的潜在外部影响，以揭示可能的歧视偏见、信息失真、隐私侵犯等伦理问题（徐明华和魏子瑶，2023）。

综上所述，国内与数据资产相关的三部法规以及欧盟的《通用数据保护条例》和《数字服务法》都对数据处理和算法透明度进行了规范，这表明法律和监管框架正在逐渐强化对企业数据资产的审计和问责要求，标志着企业数据资产审计领域向更加综合、深入和前瞻性的治理模式迈进。

三、企业数据资产审计的逻辑框架

（一）企业数据资产审计本质

企业数据资产审计的本质是审计师通过实施审计程序对企业数据资产进行系统的审查和评估，以此确保这些资产的真实性、准确性、效益性等，并将审计结果传递给利益相关者。这一过程不仅涉及传统的审计技能，如财务分析和内部控制评估，还包括对数据分析技术、信息技术和数据安全保护技术的深入运用。企业数据资产审计有以下几个特征：第一，企业数据资产审计的主体应当独立于数据资产的创建者、使用者和管理者，同时需要具备相关的专业知识和技能。第二，企业数据资产审计的对象具有可复制、可共享、无限增长和可供给的特性（秦荣生，2020），与传统意义上的物理资产有着显著区别，这就需要审计人员采取针对性的措施来获取充分、适当的审计证据。第三，审计应覆盖数据资产形成的整个生命周期，包括数据收集、数据存储、数据分析以及数据应用（Rassier等，2019），这意味着企业数据资产审计不仅应关注数据的最终结果，如数据分析的准确性和使用的效率性，还需对数据处理的过程进行评估，识别企业是否遵守了合规性原则。

（二）企业数据资产审计目标

审计目标定义了审计活动的方向和终点，明确了企业希望通过审计活动实现的具体成果，是建立企业数据资产审计逻辑框架的重要基础。本文参照郑石桥等（2019）的研究，将审计目标分为终极目标和直接目标，终极目标决定了直接目标的方向，而直接目标是终极目标实现的基础。企业数据资产审计的终极目标是给管理层和利益相关者提供关于数据资产状态和效能的可靠信息，降低代理关系中各方之间的信息不对称水平，帮助企业做出更明智的决策，并提升数据资产的管理效率和价值创造能力。

企业数据资产审计的直接目标是评估数据管理策略、流程和责任体系，确保数据在使用过程中的安全合规，避免泄露和滥用，并识别内部控制流程中的风险，从而提出改进措施以减少错误和效率损失。具体分为四个方面：一是审查数据资产是否有未授权访问、泄露、损坏或丢失的风险，其管理模式是否符合安全性目标；二是检查数据资产的管理和使用是否遵守了相关法律法规和内部政策，其行为是否符合合规性目标；三是审查被审计单位披露的数据资产有无虚假记录或遗漏，其信息是否符合真实性目标；四是评价数据资产管理制度是否完善，这包括数据的收集、处理、储存等流程中，其制度是否符合健全性目标。

（三）企业数据资产审计原则

1. 独立性原则。企业数据资产审计的主体应当独立于数据资产的创建者、使用者和管理者，同时合理设置组织架构和管理关系，积极营造审计环境，确保审计活动正常进行，不受任何干涉。

2. 持续性原则。大数据时代下，机器人流程自动化、机器学习、数据可视化等新技术融入审计流程，使得审计人员可以持续性地观测和监督数据资产相关内容，实现对项目从立项到执行再到最后完成的持续跟踪与分析（马蔡琛等，2020），及时发现数据资产处理与使用过程中存在的风险点，打造“事前防范—事中监控—事后问责”的全周期企业数据资产审计。

3. 全面性原则。审计范围应覆盖数据资产形成的整个生命周期，包括数据收集、数据存储、数据分析以及数据应用，审计对象应包含数据、信息系统、设备设施、操作人员等多种维度，审计内容应涵盖协议、隐私政策、访问记录、系统日志等，确保审计监督无死角。

4. 重要性原则。在审计过程中应该重点关注对企业生产运营有显著影响的数据资产，例如敏感个人信息、产品研发数据等，确保审计资源能得到有效分配，精准识别出被审计单位的重大风险，使企业数据资产审计的价值得到最大化体现。

（四）企业数据资产审计要素

企业数据资产审计要素包括审计主体、客体、内容、依据、方法和结果。

1. 企业数据资产审计主体。鉴于本文的研究对象是企业数据资产，适宜采用“内部审计+社会审计”的双重审计模式，审计主体分为两类：企业内部审计机构和外部第三方独立审计机构。一方面，凭借综合性、实时性和深入性等优势，内部审计机构可以对数据资产内部控制和风险治理进行审计监督，以及时揭示和防范数字风险，保障业务的合规开展；另一方面，第三方独立审计机构作为市场治理体系中的重要一环，能够凭借独立性强、技术工具先进和审视角度多元化的特点，弥补内部审计盲区，提升审计防御体系的整体效能。

2. 企业数据资产审计客体。企业数据资产审计客体不仅包括数据本身及其管理过程，也涉及企业内部不同层级的组织单元和个人。在委托代理关系中，代理人可以是负责数据管理和保护的组织单元（如IT部门、数据管理部门等），也可能是领导这些组织单元的自然人（如部门经理、CIO、数据保护官等）（苏炜等，2021）。审计的目的是评估这些代理人在处理企业数据资产时的行为和决策是否合规、有效、安全，是否符合企业的数据治理政策和目标。

3. 企业数据资产审计内容。根据经典审计理论，审计内容可以划分为审计对象、审计主题、审计业务类型、审计标的和审计载体五个层级（金银凤等，2019）。数据资产的审计内容也由上述五个层级组成，但是具体内涵有较大特色。

审计目标确定了审计工作的方向和最终目的，而审计内容是实现审计目标的具体路径和手段。前文的分析已经将企业数据资产审计的具体目标分为安全性、合规性、真实性和健全性，与此相对应的审计主题可以分解为安全、行为、信息和制度四个维度，这反映了审计的重点和方向。为了对各类代理问题和次优问题进行系统、全面的审查，审计人员应当按照不同的审计主题开展不同类别的审计活动，包括数据资产安全审计、数据资产合规审计、数据资产报表审计和数据资产制度审计这四种业务类型。这些业务类型将作用于具体的审计对象，从而保障数据资产审计目标的顺利实现。表1详细展现了审计目标、审计主题、审计业务类型和审计对象之间的对应关系。在企业数据资产审计实施过程中，审计主题还需要细分到审计标的，并确定各类审计标的的载体，审计载体作为审计证据的来源，包括纸质、电子、实物、音频等存在形式，由于数据资产的独特属性，无纸化的电子数据载体占绝大多数。电子数据载体有无形性、可复制性、不稳定性、易篡改性等特点，这要求审计人员不仅要验证数据本身的可靠性，也需要验证技术的可靠性（谢志华和程恺之，2023）。

4. 企业数据资产审计依据。目前已有《个人信息保护合规审计管理办法（征求意见稿）》《数据合规审计指南》等指导性文件，但缺少针对数据资产的审计准则。根据现有的数据保护和治理法规体系，本文将从法律层面、标准层面、行业规范以及企业内部规章这四个方面对企业数据资产审计依据进行全面分析。

（1）法律层面依据。《个人信息保护法》第五十四条规定，个人信息处理者应定期对其处理个人信息遵守法律、行政法规的情况进行合规审计；第六十四条要求，若监察中发现个人信息处理活动的风险或安全事件，相关部门可约谈处理者或要求其接受合规审计，并进行整改。《网络安全法》第十条明确要求企业采取必要措施维护网络数据的完整性、保密性和可用性。《数据安全法》第二十七条则要求企业在开展数据处理活动时，应建立健全全流程数据安全管理制度，采取必要措施保障数据安全。这些法律要求企业重视数据安全保护和合规性审查，为企业数据资产审计提供了明确依据。

（2）标准层面依据。《信息安全技术 大数据服务安全能力要求》（GB/T 35274-2023）提到，应建立数据资产操作审计机制，实现数据资产管理操作行为的可审计和可追溯；《信息安全技术 个人信息安全规范》（GB/T 35273-2020）对个人信息安全审计作出要求，将个人信息保护

表1 企业数据资产审计的目标、主题、业务类型与对象

审计目标	审计主题	审计业务类型	审计对象
安全性	安全	数据资产安全审计	数据访问控制
			数据泄露防护
			数据环境安全
合规性	行为	数据资产合规审计	数据管理和来源合规
			数据使用和共享合规
真实性	信息	数据资产报表审计	数据资产的实际存在性和完整性
			数据资产的入账和账实相符情况
			数据资产控制权的合法性
			数据资产成本计量的准确性
			数据资产的列报和披露是否符合会计准则
健全性	制度	数据资产制度审计	数据标准和治理策略
			数据治理结构和组织
			数据治理流程和实践

政策、相关规程和安全措施列为审计对象；《信息安全技术 网络安全等级保护基本要求》(GB/T 22239-2019)规定，应在网络边界、重要网络节点等进行安全审计，并提出在对较高等级保护对象的安全建设和安全整改中需使用一些关键技术，其中就包括了审计追查技术。

(3)行业规范依据。针对特定行业的数据资产审计，需要结合行业相关规范和标准，以下是各行业的具体要求：对于工业、电信行业，《工业和信息化领域数据安全管理办法(试行)》第二十七条规定数据处理者应记录日志，定期进行安全审计并形成报告，涉及核心、重要数据时需至少每半年进行一次安全审计；对于金融行业，《个人金融信息保护技术规范》要求对共享、转让中的个人金融信息进行监控和全过程审计，并对信息安全管理开展内部审计，根据审计结果完善制度和流程；对于互联网行业，《互联网平台落实主体责任指南(征求意见稿)》第八条要求超大型平台经营者应定期委托第三方独立机构对指南规定的主体责任遵守情况进行审计，出具的审计报告中应该包含实现合规的操作建议。

(4)企业内部规章依据。数据作为一种新的资产类别，企业应制定规范流程，涵盖数据采集、存储、调用分析和退役全过程，以确保数据资产质量并为审计提供具体的标准依据(徐涛等，2022)。《个人信息保护法》要求企业完善内部审计风险防范制度，对信息处理全过程开展合规审计评估，并建立合规风险库(闫夏秋，2023)。华为在《华为云安全白皮书》中提到其建立了专门的安全审计团队，重点审查华为云在法律和流程遵从、业务目标达成、决策信息的可靠性、安全运维和安全运营上是否存在风险。审计团队每年至少开展一次为期两个月的审计，审计结果要向董事会和公司高层管理者汇报，保证发现的问题得到解决并最终形成闭环(余应敏等，2019)。

5. 企业数据资产审计方法。为了使审计目标能顺利实现，审计人员应综合使用多种审计方法。一是访谈法，审计人员可以与相关人员进行面对面、书面、邮件或视频等形式的交流和沟通，了解企业数据资产处理活动的基本情况。二是观察法，对企业数据资产存储的机房环境、相关数据库设备运行情况和数据资产管理活动的内部控制执行情况进行实地察看。三是检查法，对数据资产安全管理制度、隐私政策、合同条款、运行文档等资料进行审阅和核对。四是控制测试，审计人员评价作用于企业数据资产上的内部控制是否能够在各个不同时点按照既定设计得以一贯执行，以确认控制措施是否能达到既定的目的。五是实质性程序，在控制测试基础上，对发现的与数据资产处理有关的问题实施实质性分析程序和细节测试。

由于数据资产具备一些独特的性质，会使审计人员在实施审计时面临诸多困难，例如数据资产的所有权归属难界定、数据资产难辨认以及数据强时效性所导致的数据资产价值难估量(马圆明和吴东方，2023)。为了适应这一变化，审计可以融入大数据技术，利用其先进的数据处理技术来应对挑战。大数据挖掘能够为审计提供海量数据及数据分析，自动确认审计重点和审计难点，自动计算重要性水平并生成审计实施方案，从而显著提高审计效率，控制审计成本并减少主观判断，降低审计风险(李闻一等，2020)。

6. 企业数据资产审计结果。审计团队可以基于数据资产的敏感性、业务重要性和合规性要求等因素，制定具体的数据资产分类标准，如表2所示，使其快速定位关键数据资产，确保审计资源的合理分配，同时提升审计证据的准确性和有用性。在出具审计报告前，审计人员应与被审计单位的管理层进行充分沟通，讨论在审计过程中发现的问题和关键事项，并基于审计工作底稿和收集到的证据，撰写审计报告初稿。参照财务报告审计的意见类型，企业数据资产审计报告的意见类型包括无保留意见、保留意见、否定意见和无法表达意见，选择

表2 数据资产分类

数据资产分类	描 述	业务重要性	敏感性级别	合规性要求
财务数据	与企业的财务管理、报告和分析相关的数据，包括财务报表、税务申报资料、审计资料、财务预测模型等	高	中到高	需符合企业会计准则、税务法规
研发数据	与产品研发、技术创新、试验试制等活动相关的数据，包括性能测试结果、耐用性测试数据、软件测试报告、开发环境配置等	高	高	需符合知识产权保护规定、行业标准
员工数据	包含员工个人信息的数据，如HR记录、工资信息、绩效评估数据等	中	中	需符合劳动法和隐私保护法规
运营数据	支持日常业务运营的数据，如市场活动效果、销售渠道表现、库存数据等	中	低到中	需符合行业标准和企业自身制定的准则
公共数据	被企业对外公开发布，供公众访问和使用，且不含敏感信息的数据，包括行业趋势、市场分析数据等	低	低	一般无特殊合规要求
商业关系数据	(a)客户数据：包含个人或企业客户的基本信息、购买历史、服务偏好、交易记录等 (b)供应商数据：涵盖供应商的联系信息、合同条款、供货记录、质量评估、付款历史等 (c)用户数据：关于用户的使用行为、偏好设置、反馈意见、互动记录等	高	高	需符合数据安全法、个人信息保护法

的意见类型应基于审计目标和发现，以此来准确反映被审计单位的数据资产管理和利用状况。在经过复核和必要的修改后，提交最终审计报告给被审计单位的管理层、审计委员会或其他相关的监管机构。

四、企业数据资产审计的实现机制

（一）企业数据资产审计的运行机制

企业数据资产审计的运行机制本质上是对其内容的深入理解，也是各审计关系人相互作用的过程。本文基于“内部审计+社会审计”这一联合审计模式，将企业数据资产审计的运行机制分为动态监管、合作协同、价值提升三个方面进行探讨（如图1所示）。

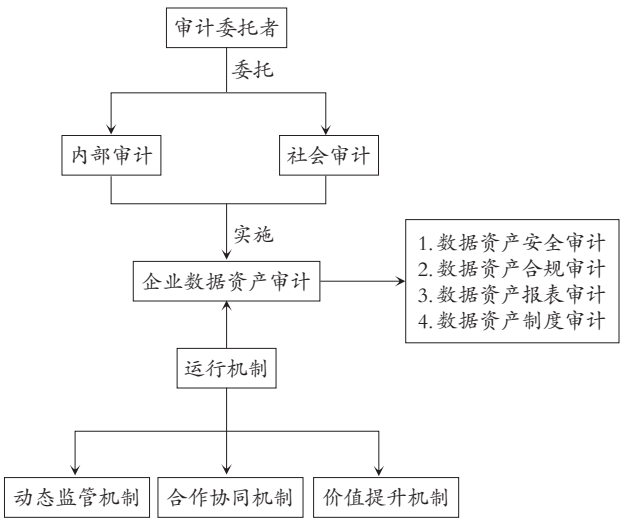

图1 企业数据资产审计运行机制

1. 动态监管机制。企业数据资产审计的动态监管机制通过实时监控、分析和评估数据资产管理活动，对其生命周期内各环节的风险进行全面审查，从而确保数据资产的安全性、隐私保护性和透明性。机制的实施基于三个核心环节：数据校验、资产上线和运用反馈，形成闭环管理，使数据资产从采集到销毁都受到有效监管。首先，数据校验阶段聚焦于数据资产的初期处理，审计人员使用自动化或半自动化的数据质量评估工具，对数据的准确性、合法性和完整性等进行审查。这包括评估数据资产是否存在充分合理的合法性基础，在采集过程中是否存在误导、欺诈等情况，以及审阅隐私政策、告知同意书等的条款是否清晰，内容是否准确完整。其次，资产上线阶段涉及数据资产的分类、入表和交易等操作。基于对企业数据资产的综合评估，审计部门通过建立合理的分类评价表，使数据资产能依据重要性水平被有效识别和监控。同时，通过鉴证企业数据资产在财务报表中确认的信息是否准确、完整，是否采用合适的计量方法进行定价，以保障其价值无误，进而提升市场内数据资产的交易透明度，消除需求者的购买顾虑，保障了数据资产的有序流通。最后，运用反馈阶段侧重于企业对数据资产的实际应用情况。审计部门通过分析数据使用的成本和效益，可以发现低效、重复和浪费的数据资源配置问题，进而提出改进建议。企业根据审计发现的问题，制定整改计划和措施，实施必要的技术和管理干预，以确保数据资产管理的持续改进和优化。

2. 合作协同机制。企业数据资产审计的合作协同机制需要多主体参与，包括内部审计机构、第三方独立审计机构与企业内有关部门。首先，内部审计与社会审计的联动是基于对审计资源、专业技能和独立性的互补需求所造就的。内部审计机构深谙企业数据资产的管理流程、内部控制的治理体系以及组织架构，能够进行全面的风险评估和持续性的监控。然而，其受限于资源配置和审计深度，需要引入独立第三方审计机构进行交叉协同审计，以增强审计的独立性和客观性。基于审计保险需求，第三方独立审计机构会向企业指派技术型审计师，以提供匹配的技术审计鉴证服务，提高企业数字化业务信息质量（耀友福，2024）。这促使两大审计主体在技术层面上实现协同与整合，通过共享审计工具、数据分析技术等资源，确保审计活动能够紧跟企业业务的数字化进程以及相关技术的最新发展趋势。其次，审计机构与企业内有关部门之间的协同作业有助于企业数据资产审计和管理活动更好地服务于企业的业务需求，制定更为全面和有效的风险管理策略。这要求企业建立一个跨部门的数据治理委员会，负责制定和监督数据管理政策、协助审计工作展开等。委员会成员应来自不同的部门，如运营部、研发部、财务部、法务部，并清晰界定各部门在数据资产治理方面的职责。

3. 价值提升机制。企业数据资产审计的价值提升机制通过数据安全、数据合规、数据质量和数据治理四个角度综合发挥作用，确保数据资产的安全性、合规性和真实性，实现价值最大化。在数据安全角度，审计人员通过实施数据资产安全审计，重点审查企业的数据访问控制、数据泄露防护以及数据环境安全，包括数据加密、访问权限管理和网络及物理环境安全措施，以发现企业潜在的安全漏洞和风险点，防止外部攻击和内部滥用的风险。在数据合规角度，聚焦于数据管理和来源合规、数据使用和共享合规两方面，实施数据资产合规审计，确保企业的数据管理活动遵守法律法规以及行业标准，从而降低法律风险和合规成本，在保护个人隐私和企业声誉的同时，提升数据资产的可用性。在数据质量方面，审计人员通过执行数据资产报表审计，确保数据资产在报表中的公允性，评估相关财务信息的准确性和完整性。在审计过程中，应评估企业是否采用恰当的方法确认数据资产，分类、评估及列示是否适当，并重点关

注数据资产的减值准备处理。在数据治理角度，审计人员实施数据资产制度审计对企业数据治理架构、政策、流程等体系的构建进行审查，判断是否存在“数据孤岛”现象。在揭示出治理漏洞后，企业应根据审计建议建立更规范、高效的数据治理框架，促进数据共享和协作。

综上所述，企业数据资产审计的价值提升机制通过识别和解决数据安全、合规、质量和治理方面存在的问题，不仅提升了企业数据管理的效率和效果，也为企业提供了一个可靠的数据基础，支撑业务创新和决策优化。基于此，企业能够更好地利用其数据资产，实现业务目标，增强市场竞争力，最终实现价值最大化。

（二）企业数据资产审计的评价机制

审计主体应以具体的审计事实为基础，充分利用企业数据资产审计结果，通过落实审计整改、审计结果分析和运用等工作开展企业数据资产审计评价工作。审计整改是实现审计闭环管理、充分发挥审计效能的重要节点，而审计结果的分析和运用可以充分发挥数据资产的价值，帮助利益相关者在数据资产管理、风险控制等方面做出更加科学和合理的决策。

1. 审计整改。审计整改的目的不仅是纠正已经发生的机会主义行为，更重要的是提供数据资产管理制度和安全合规治理的审计建议，若整改得不到落实或执行不当，审计的治理和监督效用将大打折扣。因此，在进行审计整改工作时，需遵循以下几个步骤：一是建立跨部门协作机制。由于数据资产具有特殊属性，会使审计问题呈现多样化、复杂化等特性，单凭个别部门的力量无法有效推进整改。这时就应建立一个跨部门的协作机制，通过“上下联动”和“平行统筹”的方式，将知识技能、技术手段、管理系统等进行有效组合，确保各相关部门能够高效沟通和协作，对于审计整改任务的分配和责任归属有清晰的界定。二是制定细化的审计整改效果评价标准，根据审计发现问题的性质，制定具体、可量化的效果评价标准，这些标准应该涵盖问题整改的全面性、效果的持久性以及改进措施的创新性等方面，为衡量审计整改效果奠定基础。三是建立整改跟踪检查机制，为了避免在审计整改过程中出现重视程度不够、整改主体责任落实不到位等状况，审计部门不仅要在整改完成后进行一次性的效果评估，还需要建立持续的整改跟踪检查机制。这包括对未达标问题的持续跟踪和对已整改措施的定期回访，确保审计整改能实实在在地解决问题，而非形式主义。

2. 审计结果分析与运用。审计结果分析和运用是审计工作中的重要一环，对企业数据资产审计结果的分析有助于加深审计结果运用深度，而审计结果运用水平和质量是审计监督效能发挥的关键。为了让审计结果对于使用者来说更易于理解和接受，审计机构应采用多种方式展现审计结果，例如通过数据可视化技术，将复杂的数据转换为图表、图像等，这种多元化呈现形式可以帮助管理层更直观地理解和分析审计结果。

审计结果的分析不能仅停留在发现实际问题上，更重要的是能够得到充分有效的运用。审计部门应与监管机构建立审计成果共享平台，促进信息共享和各监管部门的协作，共同应对企业数据资产管理中的挑战。通过将审计发现的问题和建议反馈给被审计单位和相关监管部门，可以推动数据资产管理制度的完善和实践改进。此外，将审计结果公开在社交媒体、网站和其他数字平台上，有助于提高审计工作的透明度，鼓励企业、公众和政府部门的互动，从而形成良好的审计氛围。

（三）企业数据资产审计的保障机制

1. 加强党的领导。审计实践已经充分证明，坚持党的领导对于保障审计活动沿着正确的政治方向前进至关重要，这是推动审计工作高效、高质量开展的前提条件。习近平总书记在二十届中央审计委员会上提出，要坚持围绕党和国家中心工作开展审计，坚持围绕总体国家安全观开展审计，坚持围绕以人民为中心的发展思想开展审计，坚持围绕促进党的自我革命开展审计。这为企业数据资产审计工作指明了方向，加深了对审计工作规律的认识，促使其有效发挥审计监督效能。

2. 推进企业数据资产审计制度建设。首先，应该建立和完善针对企业数据资产审计的法律法规框架，这包括数据管理、保护、安全以及审计活动本身，通过出台专项法律法规，不仅能为企业数据资产审计提供明确的法律依据，还能确保审计活动的合法性和正当性。其次，根据数据资产的特性及企业的业务需求，制定合理的审计评价标准是保证审计质量的关键，这些标准应涵盖数据完整性、安全性、可用性、合规性等多个方面。同时，考虑到不同行业、不同类型的数据资产可能有不同的管理和审计需求，审计评价标准应具有一定的灵活性和适应性，以满足不同情境的需求。在制定审计准则时，还可以在不同行业和领域实施试点项目，通过实地案例研究来收集经验，从而对企业数据资产审计标准进行测试和改进，为政策制定提供实践依据。

3. 推进企业数据资产审计复合型人才的培养。高校、企业和审计机构应建立跨学科的联合学习平台，培养学生在数据分析、编程、网络安全和数据隐私法规方面的理解与应用能力。实践是培养复合型人才的关键，通过模拟企业数据资产审计项目、参与企业数据治理活动和案例研究，学生能够在实际操作中理解理论知识的应用，提升解决复杂问题的能力。对于在职的审计和数据管理专业人员，审计机构和企业应提供定期的职业培训和继续教育机会，包括参加行业会议、专业研讨会和在线课程等。此外，跨部门交流和轮岗计划也是培养复

隐私计算赋能大数据审计分析机制研究

王晓勤

随着云计算、人工智能、物联网等信息技术的飞速发展，大数据已经成为各行各业的重要生产要素。在审计领域，大数据的应用为审计工作带来了巨大变革。理论框架方面，学者们提出了多种大数据审计模型和方法，如基于云的大数据审计平台、基于机器学习的审计数据分析模型等。技术实现方面，随着大数据技术的不断发展，数据采集、存储和处理的速度和质量得到了显著提升，为大数据审计提供了有力的技术支撑。应用实践方面，大数据审计已经在社保、金融、农业、税务、海关等领域得到了广泛应用，并取得了显著成效。

尽管大数据审计在理论和实践方面都取得了显著进展，但仍存在一些问题和挑战。一方面，由于各种因素导致被审计单位提供的数据不完整，甚至数据被恶意篡改等，审计数据的完整性、准确性难以保证。另一方面，用于审计的数据中通常会包含大量隐私数据和保密数据，数据在流转过程中容易被非法获取，审计数据存在隐私泄露的风险。因此，如何确保数据在审计过程中的完整性和隐私性是开展大数据审计的关键。

隐私计算作为一种新兴的技术，为大数据审计提供了新的解决方案。通过密码算法、安全协议、联邦学习等技术，可以实现数据在审计全流程中的隐私保护和安全共享，包括原始数据安全和隐私保护、计算过程中的数据安全和隐私保护以及计算结果的安全和隐私保护。

审计大数据的数据脱敏与完整性校验

由于审计大数据通常包含大量的敏感信息，如个人隐私数据、企业业务数据以及安全级别很高的核心数据等，如果不经过脱敏处理，一旦泄露，将给个人和企业带来严重损失。此外，随着大数据技术的不断发展，审计大数据的应用场景也越来越广泛。在数据采集、传输、交换和共享的过程中，如果缺少有效的数据脱敏措施，可能会导致数据泄露和滥用的问题。数据脱敏技术可以实现对敏感数据的变形，使其在不违反系统规则的条件下，对真实数据进行改造并提供测试使用，从而保护敏感隐私数据的可靠性。数据脱敏是一个复杂且重要的过程，其主要目的是在保护敏感信息的同时，确保数据的安全性和可用性。因此，数据脱敏将成为未来审计大数据处理中不可或缺的一环。

如下页图1所示，为了在不影响审计质量的前提下确保数据隐私，可首先对原始数据进行数据脱敏。在大数据审计中，数据脱敏主要包括四个步骤。首先，识别

合型人才的有效手段，通过在不同部门工作，员工可以更深层次地理解数据资产在企业运营中的作用和复杂性，提升综合分析能力。

4. 创新审计技术与方法的运用。通过自动化工具和智能分析平台，审计人员能够高效处理海量数据，识别风险点并提出改进建议。区块链技术具有去中心化、防篡改和可追溯等特点，有助于判定数据资产所有权并解决争议；机器人流程自动化（RPA）技术则能模拟人类与计算机的交互，适用于数据处理量大、人员需求高的重复性工作。结合人工智能（AI）和机器学习（ML）算法，RPA还能分析非结构化数据，识别复杂模式和趋势，使审计人员专注于更高价值的分析和决策任务。将区块链与RPA相结合，企业数据资产审计可以实现自动化和智能化转型，这不仅能提升审计的精确性，还能增强数据资产的安全性和效益性，为数字经济时代的企业提供高效科学的审计服务。

五、总结

本文通过深入探讨企业数据资产审计的逻辑框架与实现机制，提供了一套系统性的理论框架与审计实践方法，以应对数字时代的风险挑战。企业数据资产审计工作必须结合国内外新形势，进行多维度的扩展性研究，这需要审计理论的不断丰富和完善，也需要审计实践的不断探索与创新，以及审计人员能力、技术水平的不断提升。只有这样，才能在信息时代的大背景下，有效应对数字风险，保障数字经济健康发展，为构建更加公平、透明、高效的数字治理体系做出更大的贡献。

基金项目：国家社会科学基金项目（项目编号：19AGL033）；江苏省研究生科研与实践创新计划项目（项目编号：SJCX24_1198）；江苏高校优势学科建设工程项目（PAPD）。

作者单位：南京审计大学社会审计学院

原载《财会月刊》（武汉），2024.16.90~96