大数据时代企业会计信息风险与防范策略研究

刘振坤
新疆豫能投资集团有限公司，新疆 乌鲁木齐 830022

DOI:10.61369/SE.2026040040

摘　　要： 大数据技术的广泛应用正在深刻改变企业会计信息系统的运行环境与风险结构，不仅为企业会计信息处理带来了效率与精准度的提升，也催生了新型风险。本文以大数据时代为背景，系统分析企业会计信息面临的新型风险及其生成机理，提出技术防护、制度约束、人员提升与监管协同四位一体的防范策略框架，本研究旨在为企业构建适应大数据环境的会计信息风险治理体系提供了理论依据与实践路径。

关 键 词： 大数据时代；会计信息风险；数据安全；内部控制；风险管理

Research on Accounting Information Risks and Prevention Strategies in the Age of Big Data

Liu Zhenkun
Xinjiang Yueneng Investment Group Co., Ltd., Urumqi, Xinjiang 830022

Abstract: The widespread application of big data technology is profoundly transforming the operational environment and risk landscape of enterprise accounting information systems. While enhancing the efficiency and accuracy of accounting information processing, it has also given rise to new types of risks. Against the backdrop of the big data era, this paper systematically analyzes the emerging risks faced by corporate accounting information and their underlying mechanisms, proposing an integrated prevention strategy framework comprising technological safeguards, institutional constraints, personnel capacity building, and regulatory coordination. This study aims to provide both theoretical foundations and practical pathways for enterprises to establish accounting information risk governance systems adapted to the big data environment.

Keywords: big data era; accounting information risk; data security; internal control; risk management

引言

大数据、云计算与人工智能技术的快速渗透，正在深刻重塑企业会计信息系统的运行模式。财务共享中心、智能报销系统与业财一体化平台的普及，使会计信息处理从事后记录转向实时生成，从封闭系统转向开放网络。技术赋能的同时，数据泄露、信息失真、系统依赖与合规困境等新型风险同步涌现，传统以岗位牵制与凭证审核为核心的风险防控体系面临失效风险。如何识别大数据环境下会计信息风险的新特征，揭示其深层成因并构建系统性的防范策略，成为企业财务管理亟待解决的重要命题。

一、大数据时代企业会计信息风险的主要类型

（一）数据安全风险

数据安全风险是指会计信息面临被窃取、篡改、破坏或非法访问的威胁，是当前最受关注的风险类型。具体表现为：一是外部攻击风险，黑客利用勒索病毒、DDoS 攻击、SQL 注入等手段入侵会计信息系统，窃取或加密财务数据；二是内部泄露风险，员工账号被盗用、权限被滥用、离职账号未及时注销等问题，使内部人成为数据泄露的重要源头，部分企业存在多人共用账号、权限设置过宽等管理漏洞，进一步放大了风险；三是供应链风险，云服务商、软件开发商等第三方的系统漏洞可能成为攻击跳板，服务商自身的经营问题也可能导致企业历史财务数据丢失。

（二）信息失真风险

信息失真风险是指会计信息未能真实、完整地反映经济业务实质。大数据环境下，信息失真的成因更加复杂：一是数据源头的不可靠性，从外部获取的数据可能存在错误或被篡改，企业往往缺乏验证能力；二是异构数据转换中的信息损耗，非结构化数据在转换为结构化字段时依赖人工设定的规则，可能造成关键特征丢失；三是系统间数据口径不一致，不同业务系统对同一经济事项采用不同的编码规则或计量单位，导致业财数据自动对账失

作者简介：刘振坤（1986.03- ），男，汉族，河南原阳人，硕士研究生在读，高级会计师，研究方向：会计信息质量与企业高质量发展、集团企业融资管理。

败；四是自动化规则设置的偏差，系统自动执行的分摊逻辑、计提方法若存在配置错误，将造成系统性的信息偏差，且这类错误具有高隐蔽性[1]。

（三）系统依赖风险

系统依赖风险是指企业对会计信息系统的深度依赖所导致的运营连续性与数据完整性风险。从运营连续性看，系统宕机、网络中断、软件故障等问题都可能导致财务职能中断，全面上云的企业一旦遭遇区域性故障或网络问题，财务人员可能完全无法访问系统。而且，从数据完整性看，系统故障可能导致在途交易丢失、重复处理或部分处理，在缺乏完善日志记录机制的情况下，修复成本极高。此外，系统处理逻辑的代码实现与业务规则之间可能存在偏差，而普通财务人员难以发现这类问题。

（四）合规与法律风险

在合规与法律风险方面，企业处理会计信息时一旦踩到法律红线，就可能面临罚款甚至被起诉。具体来看，主要面临以下问题：在数据保护法规上，会计信息中大量包含核心经营数据，其处理活动受《网络安全法》《数据安全法》等法律的严格规制；跨境业务企业还需同时满足 GDPR、云法案等境外法规要求，不同法域之间的规则冲突使企业面临合规困境。在电子会计凭证上，电子发票、电子回单等无纸化凭证的真实性与完整性验证技术要求较高，现有技术标准和法律规范仍在完善中。在数据资产入表上，数据资源的确认条件、计量方法等缺乏统一标准，增加了财务报告的可比性风险。

（五）技术型舞弊风险

技术型舞弊风险也是大数据时代企业会计信息常见的一种风险，与传统手工篡改账目不同，技术型舞弊更具隐蔽性：舞弊者可利用系统权限修改数据库记录、植入恶意代码自动调整账目、或截获篡改数据传输中的交易信息[2]。由此可见，技术型舞弊风险对企业的技术防护与审计能力提出更高要求，传统的职务分离与授权审批措施难以有效应对，反舞弊机制需升级为岗位制衡、技术审计与行为分析相结合的多层防御体系。

二、企业会计风险的成因分析与生成机理

（一）技术逻辑与会计逻辑存在结构性张力

大数据技术的内生逻辑是效率优先、实时响应、自动化处理；而会计专业的核心逻辑则是谨慎性、可验证性、可追溯性。这两种逻辑之间存在根本性张力。以实时化处理为例：技术角度看，交易一旦发生即可自动采集、自动入账，效率最高；但从会计角度看，对存疑交易应暂缓确认、对缺乏原始凭证的交易应不予入账——这些“慢下来”的要求与技术的“快”形成冲突。当系统被设置为自动放行时，会计的专业判断便被自动化逻辑所替代，风险随之产生，以系统的“黑箱”特性为例：技术上将复杂逻辑封装在系统内部有助于降低使用门槛，但从审计角度看，这种封装使处理过程难以被外部验证，可追溯性受到损害。

（二）数据供应链中的质量控制困难

将会计信息处理视为从数据采集、清洗、转换到记账核算、报表生成的供应链，有助于理解质量风险的累积放大机制。但每个环节都可能引入偏差：源数据准确性依赖外部数据源的质量水平；数据转换依赖映射关系的正确性；分摊逻辑依赖参数设置的合理性。上游环节的微小偏差，经多环节处理后可能在下游放大为显著的信息失真。然而，传统会计控制按岗位而非环节设计，导致数据供应链的某些环节处于控制盲区——缺少明确岗位对数据清洗质量负责，也缺少流程对转换规则进行审核。这种控制覆盖的不完整，是信息失真风险的重要成因。

（三）业财融合的深度与边界问题

业财融合的核心目标是打破业务系统与财务系统之间的壁垒，实现数据自动流转。然而，融合的深度如何把握、边界如何划定，需要审慎权衡。过度融合可能带来两方面问题：一是风险传导的“跨系统跳跃”，业务系统的安全漏洞或数据错误可能直接波及相关联的财务系统；二是控制节点的“系统化替代”，传统控制体系中业务与财务之间的“界面”本身就是一道重要的独立校验环节，当这一界面被系统接口替代时，校验功能也随之消失。反之，融合不足则难以发挥大数据效率优势。因此，业财融合需要在“效率提升”与“风险可控”之间寻求动态平衡。

（四）制度供给与技术发展的时滞

法律制度、会计准则、审计标准等规范性文件的制定和修订通常需要较长周期，而大数据技术发展日新月异，两者之间存在结构性时滞，进而导致多个层面的问题，比如数据权属、跨境数据流动规则、云服务商责任等关键问题缺乏明确界定，企业面临合规不确定性；数据资产的确认与计量、云计算费用的资本化与费用化区分等问题缺乏统一指引，会计处理存在较大随意性[3]。

三、大数据时代会计信息风险的防范策略

（一）构建多层次的技术防护体系

大数据时代，单一的技术防护手段已难以应对复杂多变的威胁，必须构建覆盖数据全生命周期、贯穿基础设施到应用层面的多层次技术防护体系，从数据安全、信息质量、系统连续性三方面形成纵深防御结构。

第一，在数据安全角层面，企业应建立“纵深防御”的安全架构，在网络层面部署防火墙、入侵检测 / 防御系统，对进出会计信息系统的流量进行监控与过滤；应用层面实施多因素身份认证、基于角色的权限访问控制，确保“最小权限原则”得到落实；数据层面采用传输加密与存储加密技术，即使数据被非法获取也难以解密；终端层面加强设备管理与安全审计，防止通过终端设备入侵核心系统。

第二，在信息质量层面，可以借鉴供应链管理的思路，对数据流动的每个环节把关。具体来说，在数据刚进入系统的地方设置一个质量校验节点，自动检查原始数据是不是完整、准确、格式一致；同时建立数据血缘追踪机制，记录每条数据从采集、处理到最终披露的每一步变化，方便以后追查问题；再配合持续的数据质量监控工具，一旦发现异常数据模式就立刻报警；此外，定期做一次数据质量评估，并把评估结果和相关部门或员工的绩

效考核挂钩，这样更容易引起重视。

第三，在系统连续性上，企业应建立完善的容灾备份与应急响应机制。核心财务系统应部署双活或主备架构，确保单点故障不影响业务连续性；制定系统故障应急预案，明确故障分级标准、响应时限、升级路径及业务切换流程；定期开展灾难恢复演练，验证备份数据的可用性与恢复流程的有效性。

（二）推进内控制度的数字化重构

技术防护解决的是“外力”问题，而内控制度解决的是如何制度层面防范风险，规范“人”与“系统”的交互行为。具体而言，在控制环境方面，明确数字化转型中的决策权责、审批流程与责任归属，避免因系统自动化而模糊了“谁决策、谁负责”的界限；在风险评估方面，建立针对技术风险（如系统漏洞、数据泄露）的识别与评估机制，将技术风险纳入企业整体风险评估体系；在控制活动方面，将预算控制、费用标准、信用政策等规则嵌入系统自动执行，同时设置异常交易的“熔断机制”——当系统检测到超出预设阈值的交易时，自动转入人工审核流程；在信息与沟通方面，建立跨部门的异常交易通报机制，确保财务部门、IT 部门、业务部门之间的信息共享；在监督方面，引入持续控制监控技术，对系统自动执行的规则进行再校验，防止因规则配置错误导致的系统性偏差。

（三）提升会计人员的数字素养与风险意识

技术与制度的落地，最终依赖于“人”的认知与能力。大数据时代对会计人员提出了复合型能力要求，即会计从业人员需要既要懂会计专业，也要懂数据、懂系统、懂风险。对此，企业应建立分层分类的培训体系，对于基层财务人员，侧重于系统操作技能、数据安全意识、电子凭证处理规范的培训；对于业务骨干，增加数据分析工具应用（如结构化查询语言、商业智能软件）、异常模式识别、业财融合逻辑等能力训练；对于财务管理者，则需要提升对技术风险的研判能力、数字化转型的领导力、以及跨部门协同的沟通能力。

此外，在人才引进方面，应优化财务团队的学历与专业结构，引入具有信息技术背景、数据科学背景的复合型人才，改变传统财务团队单一会计学背景的格局。在人才激励方面，应将数据质量、系统安全、合规表现纳入财务人员的绩效考核体系，引导行为导向从“完成任务”转向“守护质量”。

更重要的是，需要重塑大数据时代会计职业认同中专业判断的内涵。在大数据环境下，会计人员的角色正在发生根本性转变，他们不再是财务数据的被动记录者，而是会计信息质量的主动守护者，需要参与系统规则的设计与优化，承担异常交易信号的识别责任，同时成为技术风险防控的重要把关人，因此，会计教育体系与职业培训体系也需要进行系统性调整，以培养适应数字化时代的复合型会计人才。

（四）完善法律法规与行业标准体系

在法律法规层面，应加快明确以下问题：第一，企业存储于云端的数据，所有权归属企业还是与服务商共有，服务商在何种条件下有权访问或使用数据；第二，明确重要财务数据出境的审批程序、安全评估标准及法律责任；第三，明确服务商在数据安全事件中的赔偿责任、举证责任及监管义务；第四，统一电子发票、电子回单等无纸化凭证的技术标准与法律效力认定规则。

行业标准层面，也需要一些实际的推进动作。比如会计数据的基本标准，包括数据格式、接口规范、编码规则等，如果全行业能有一套统一的框架，不同系统之间的业财融合就会顺畅很多，技术门槛和兼容成本也会降低。再比如针对云会计服务的准入机制，目前市场上提供云会计服务的厂商资质参差不齐，有些小厂商安全能力薄弱，容易成为风险突破口。如果能够建立明确的准入门槛，要求服务商具备相应的技术能力、安全资质和服务可靠性，就能过滤掉一部分低质量的服务商。此外，在监管方式层面，应推动从“人工监管”向“数据监管”转型。监管部门可利用大数据分析技术，对企业的财务数据进行非现场监测，识别异常模式与风险信号，实现“以数据监管数据”。同时，应建立跨部门的信息共享与执法协作机制，形成监管合力。

四、结语

大数据时代，企业会计信息风险的本质是技术逻辑与会计逻辑的结构性错配。技术追求效率与实时，会计强调谨慎与可验证，二者张力在制度滞后与能力不足条件下转化为现实风险。本文提出的四位一体防范框架表明，技术是基础，制度是保障，人员是根本，监管是支撑。唯有实现从被动防御向主动治理的范式转换，让会计人员从数据记录者转变为质量守护者，方能建立与风险共存的韧性能力，使技术服务会计本质而非替代会计逻辑。

参考文献

[1] 盛玉萍 . 大数据时代企业会计信息风险与防范策略分析 [J]. 市场周刊 ,2024,37(36):119-122.

[2] 孙远林 . 也谈大数据时代下企业会计信息管理 [J]. 商业观察 ,2021,(36):83-85.

[3] 钟安琦 . 大数据环境下建筑企业会计信息风险应对策略探析 [J]. 现代企业文化 ,2025,(06):50-52.

