

数字经济时代会计信息系统安全风险防范

郭梓萌

澳大利亚莫纳什大学, 澳大利亚·墨尔本 3000

【摘要】随着数字经济的发展, 会计信息系统已成为企业财务管理的核心支撑, 其安全性对数据的真实性与完整性具有决定性影响。本文围绕数字经济背景下会计信息系统面临的安全风险, 系统分析了企业在信息化建设过程中存在的薄弱环节与防护短板, 提出构建多层次、智能化防护体系的关键路径。文章重点从网络安全架构设计、动态风险预警机制、权限与流程管理优化、数据备份与灾难恢复方案、以及人员信息安全素养提升五个维度展开深入探讨, 强调技术手段与管理机制协同的重要性。通过案例化分析和策略细化, 希望为企业提升系统安全性能、应对复杂网络威胁提供了可操作的思路, 具有较强的现实指导意义与推广价值, 助力企业实现财务信息系统的稳健运行与可持续发展目标。

【关键词】数字经济时代; 会计信息系统; 安全风险防范

引言

在2023年8月, 财政部会同国家网信办和工信部联合发布了《关于加快推进企业会计信息化建设的指导意见》, 明确指出要“强化会计信息系统安全防护, 防范数据泄露和网络攻击风险”。随着数字经济的迅猛发展, 会计信息系统已逐步演变为企业财务管理的核心基础, 其安全性能的高低, 直接影响到财务数据的真实性、完整性与可用性^[1]。正因如此, 在政策推动与技术革新双重驱动下, 企业亟需构建起多层次、智能化的安全防护体系, 以切实应对当前财务管理面临的各类挑战。

1 会计信息系统是数字经济时代企业核心管理工具, 数据安全成为关键竞争力

在数字经济飞速发展的背景下, 会计信息系统已逐渐成为推动企业财务管理智能化、经营决策科学化的核心技术支撑平台^[2]。该系统通过高效整合财务、业务及数据资源, 为企业预算管理、成本控制和财务分析等关键流程提供了实时支撑。然而, 随着数据资产在企业价值链中的战略地位日益上升, 信息系统面临的安全风险也随之加剧, 已成为影响企业平稳运行与可持续发展的重要隐患之一。从黑客攻击到数据泄露、从系统故障到权限滥用, 各类安全威胁频繁出现, 一旦爆发, 不仅可能导致财务信息失真, 还可能引发经营风险, 甚至触发法律与合规问题^[3]。因此, 构建健全的信息安全防控体系, 全面强化会计信息系统的安全管理, 正日益成为企业数字化转型进程中提升核心竞争

力的关键所在。

2 加强会计信息系统安全风险防范的必要性

2.1 数字化转型对信息安全提出更高要求

在数字经济时代, 企业全面加速数字化转型, 会计信息系统也由传统的账务处理工具逐步演化为融合财务、业务与战略管理于一体的智能化平台^[4]。系统所处理的财务数据不仅种类繁多、结构复杂, 而且对数据的时效性与准确性有着极高的要求。一旦发生数据异常或系统宕机, 便可能对企业资金调度、成本核算乃至利润分析等核心管理环节造成严重干扰。因此, 构建与数字化程度相匹配的信息安全体系已成为必然选择。唯有通过加强权限管理、健全数据备份机制, 并引入加密技术与审计手段, 才能确保系统运行的稳定性与信息安全。

2.2 防范数据泄露与网络攻击刻不容缓

随着企业会计信息系统不断融合云计算、大数据、物联网等前沿技术, 系统的外延逐渐拓展, 随之而来的外部攻击与数据泄露风险也日趋严峻^[5]。不法分子利用钓鱼邮件、恶意程序、远程入侵等手段, 窃取企业的财务信息、客户数据乃至敏感资料, 严重冲击企业的信誉与合规体系。同时, 来自内部员工的不当操作或权限滥用, 同样可能引发数据失控等隐患。若缺乏有效防护机制, 企业不仅面临巨额经济损失, 还可能承担相应法律责任。因此, 建立完善的信息安全防护体系尤为关键。例如, 企业应部署防火墙、入侵检测系统 (IDS)、数据加密与多因素身份认证等

技术手段，以增强系统的防御能力。

2.3 保障企业财务信息真实性与完整性

随着会计信息系统在企业日常运营中的依赖程度持续加深，系统承载的数据量急剧上升，覆盖收入、成本、资产、预算等关键财务领域。一旦系统遭遇数据篡改、删除或伪造等风险操作，将直接影响财务报表的准确性，进而误导企业战略判断，损害投资者、监管机构及其他利益相关方的信任与预期。因此，建立完善的信息系统安全防护机制，是保障数据真实性的关键所在。例如，在财务处理环节中，应通过设定操作权限、加强数据录入校验及建立定期审计追踪机制，防止未经授权的数据更改操作。与此同时，还需引入区块链、防篡改数据库等前沿技术，实现账务数据的全过程记录与防篡改，确保信息链条封闭可追溯，为企业应对财务监管和外部审计提供坚实的数据支撑，从根本上夯实信息安全防线。

3 会计信息系统安全风险防范的关键路径

3.1 构建多层次网络安全防护体系

健全的网络安全防护体系，是保障会计信息系统稳定、高效运行的根本支撑。企业管理层应高度重视信息安全工作，将其作为数字化战略的核心组成部分，持续推进技术防护与制度建设的同步优化。首先，应构建覆盖物理安全、网络安全、主机安全、应用安全和数据安全五大层级的多层次防护体系，形成系统性的纵深防御架构。其次，必须强化员工的信息安全意识，结合网络安全培训、安全演练与应急流程宣导等方式，提升员工对潜在风险的识别和防范能力。例如，企业可定期邀请信息安全专家开展专题讲座，深入讲解常见攻击方式、防御技术与管理规范，明确各类岗位在系统运行中的职责与操作边界，激发员工主动防护意识^[6]。同时，还应结合实际业务特征，细化关键岗位的安全职责，强化对系统管理员、数据管理员等关键角色的权限控制与操作审计，确保职责分明、相互制衡，全面构建起由管理、技术与人员三位一体的多环节联动防护格局。

3.2 建立动态化风险评估与预警机制

风险识别与评价：在数字经济环境下，会计信息系统所面临的安全威胁不断演变，企业应建立动态化的风险识别

与评价机制，全面覆盖来自网络攻击、系统漏洞、数据泄露、权限滥用等方面的安全隐患。采用定性分析与定量建模相结合的方式，对各类风险因素进行识别与分类，并依据其可能造成的影响程度与发生概率进行评估。例如，可借助大数据分析技术构建风险评估矩阵模型，对历史安全事件、用户行为日志等数据进行深度挖掘，实现对系统潜在威胁的前瞻性识别，为风险管理工作提供数据支撑。

风险应对策略拟定：基于评估结果，应制定科学、分级的应对策略，实现对不同类型风险的差异化管理。对于高概率、高影响的系统性风险，可通过升级安全防护系统、引入零信任架构等方式予以规避或缓释；对于低概率但高影响的突发风险，可配置应急响应机制并建立备用系统，以增强抗压能力；而对一些日常操作中可能存在的非恶意风险，应通过优化流程管理、加强员工安全培训等手段降低其发生可能性与影响范围。比如，对于系统权限设置问题，可引入最小权限原则并实施定期复核制度，防止权限滥用及越权操作，最大限度减少人为风险因素。

3.3 优化信息系统权限管理与流程控制

在数字经济加速演进的背景下，会计信息系统操作流程日益复杂，权限管理已成为系统安全保障的核心环节。企业应依据岗位职责，科学设定权限等级，实现权限的最小化配置与动态调整，确保用户仅能访问与其职责相关的数据与功能。通过引入身份验证机制、多因素认证技术及定期权限审查制度，可有效防范因权限滥用、账户共享或越权操作所引发的数据泄露与安全事件。

针对会计信息系统运行中所涉关键业务流程，应推进流程再设计，并强化监控机制，确保操作高效与安全并重。通过对数据录入、审批、报表生成等核心模块实施自动化配置，嵌入流程追踪及异常预警功能，可实现流程的闭环控制。以费用报销系统为例，可设置标准化的审批路径与审批条件，明确报销金额限制、审批层级及时效要求，防止违规报销行为；同时启用日志审计功能，对操作全过程进行留痕与分析，为后续审计与责任追溯提供依据，全面提升系统运行的合规性与透明度。

3.4 完善数据备份与灾难恢复方案

备份机制建设：构建完善的数据备份机制，是保障会计

信息系统数据安全与业务连续性的基础。企业应根据系统重要程度和数据敏感级别,制定分层次、多频率的备份策略,确保核心财务数据在任何情况下都能实现快速还原与有效保护。具体可采取本地备份与异地灾备相结合的方式,增强备份系统的抗风险能力。例如,对财务总账、预算数据、报表资料等关键性数据进行每日增量备份与每周全量备份,并定期进行数据恢复演练,检验备份可用性与恢复时效性。

灾难恢复体系应用:同时,要建立系统性的灾难恢复体系,使其与业务连续性管理、信息安全策略紧密衔接,确保在遭遇系统故障、自然灾害或网络攻击等突发事件时,企业能够快速启动应急响应,恢复正常运行。对恢复过程中暴露出的漏洞和问题要及时修复,并将恢复流程与员工操作规范相结合,形成制度化管理。比如,在遭遇勒索病毒攻击造成系统瘫痪的情况下,可立即启用离线备份系统恢复数据,最大程度减少财务信息系统的停机时间与业务损失,切实提升企业应对突发风险的能力与恢复效率。

3.5 提升会计人员信息安全素养与技能

专业培训及学习:为切实提升会计人员在数字经济环境下的信息安全意识与防护能力,企业应定期组织信息安全培训与学习活动,促使员工不断更新知识体系、增强实操能力。培训内容应涵盖网络安全基础、系统使用规范、数据加密与备份方法、权限管理原则,以及常见网络攻击方式与应对策略等。例如,可为会计人员开设信息安全专题课程,系统讲解钓鱼邮件识别、勒索软件处理等内容,确保员工在日常操作中遵循规范、有效规避风险。同时,还应加强新技术相关培训,如区块链、云计算与智能审计系统,帮助员工适应信息化财务环境,持续提升系统应用与安全防护水平。

职业道德教育:在提升技术能力的同时,应同步强化会计人员在信息伦理与职业操守方面的教育。通过强调数据保密责任、信息安全义务及职业规范,引导员工在处理敏感信息时严守底线、规范操作。例如,可定期举办“信息安全与职业道德”专题讲座,结合典型违规案例,强化员工对数据泄露与信息滥用严重性的认识,提升其责任感与自我约束力。可探索建立“安全诚信档案”,将违规行为记录与绩效评估挂钩,激发员工主动维护信息安全的积极性。

定期考核与激励:为推动会计人员在信息安全领域持续

进步,企业应建立常态化考核机制,对系统操作规范性、数据处理安全性与应急响应能力等方面进行综合评价。通过设定量化指标,如系统登录合规率、数据录入准确率、异常事件响应时间等,对员工实际表现进行全面检验。考核结果应与绩效评定、晋升激励等挂钩,对表现优秀者予以表彰奖励,推动先进典型引领作用;对考核不达标人员,应安排针对性培训与辅导,协助其提升专业能力。为保障考核的公平性,还应设立申诉机制与反馈渠道。同时,为促进其长期发展,可搭建信息化学习平台,提供在线课程、安全资讯与技术资源,鼓励其自主学习与行业交流,不断提升自身的技术能力和安全素养,助力企业构建全面的信息安全管理人才体系。

4 结语

在数字经济蓬勃发展的背景下,会计信息系统作为企业财务管理的重要载体,其安全性直接关系到企业数据资产的完整性与经营决策的科学性。面对日益严峻的信息安全风险,企业必须高度重视系统安全管理,从技术防护、制度建设到人员素养多方面协同发力,构建全方位、多层次的风险防控体系。通过加强网络安全防护、完善权限控制机制、健全数据备份与灾难恢复方案,提升会计人员的信息安全意识与应对能力,企业才能在复杂多变的数字环境中立于不败之地,实现高质量、可持续的发展目标。

参考文献:

- [1]肖璐.会计信息系统在企业财务管理中的运用探析[J].乡镇企业导报,2024(18):123-125.
- [2]韩银双.基于业财融合的企业管理会计信息系统的构建策略探讨[J].财经界,2023(16):98-100.
- [3]文勇.云计算下财务管理信息化建设路径研究——基于珠三角中小企业的调研[J].会计之友,2020(9):31-37.
- [4]郭玉龙.人工智能视角下智能化会计信息系统对企业内部控制的改进研究[J].企业研究,2025(01):22-26.
- [5]李海玲,裴晓芸,董雪松.基于大数据技术的企业环境会计信息系统设计与实施[J].中国管理信息化,2024,27(23):50-55.
- [6]孙曦冉.电子商务企业会计信息系统风险及控制论述[J].老字号品牌营销,2024(21):139-141.