4.3 安全与隐私保护挑战

随着数据采集范围不断延展，数据安全及隐私保护问题愈发突显。在数据的采集、传输、存储以及使用阶段，面临泄露、篡改、滥用这类安全风险。针对个人隐私保护的法律法规逐步完善，对数据处理提出了更高水准的合规要求。如何在保障数据安全的基础上充分释放数据价值，兼顾数据利用与隐私保护，成为组织必须直面的关键课题。这不仅要求技术层面的安全保障，还需完备的管理制度及合规体系。在实际工作开展期间，应构建全流程的数据安全管理机制，以技术、管理、法律等多个层面构建全方位安全防护架构。

5 优化路径与策略

5.1 技术优化

技术优化乃提升大数据应用水平的根基。应构建统一的数据标准体系，对数据采集、存储、处理及共享的全程予以规范，增强数据质量及一致性。打造灵活的混合计算架构，融入批处理、流处理、内存计算等多种技术手段，适应不同场景下的应用需求。引入智能化算法平台，降低算法应用技术壁垒，提升分析的效率与精准度。提升边缘计算能力建设水平，达成数据的本地化即时运算，为业务决策送去更及时的支撑。在技术优化阶段中，需重视技术与业务的深度融合，保证技术方案可有效处理管理实践中的问题，增进组织整体运营效率。

5.2 管理机制改进

完善的管理机制是推进大数据应用的关键支撑。应构建完备的数据治理体系，界定数据的所有权、使用权及管理权，构建跨部门的数据协同管理机制。同步制定数据共享激励举措，消除部门间信息隔阂，实现数据资源的高效运用目标。就项目管理而言，采用敏捷开发这类灵活的管理方法，减小项目迭代周期长度，加大应用成效[4]。凭借培训及宣传，提升组织成员对数据的认知，构建数据驱动的企业价值文化体系。管理机制的改进要长期坚守，通过持续的优化及调整，保证大数据应用持续为组织创造价值。

5.3 安全保障体系建设

构筑全方位安全保障体系，是大数据应用实现可持续发展的必要条件。须在数据生命周期各环节实施严格安全办法，涉及数据加密、访问控制、操作审计等事项，保障数据的完整性及保密性。采用数据脱敏、差分隐私等技术，在数据分析进程中守护个人隐私。完善数据安全管理制度体系，界定安全责任，定期开展针对安全的评估与风险排查。强化合规管控，确保数据处理依照相关法律法规规范，抵御法律风险。安全保障体系建设需技术、管理、法律等多方面协同合作，构建起立体化的防护网络。

5.4 人才培养与团队建设

人才是大数据应用成功的核心要素。要加大复合型人才培养力度，既懂技术又懂业务的专业人才更能有效推动大数据在管理实践中的应用。构建完备的内部培训体系，始终提升员工的数据素养与技术能力[5]。同步引入外部高水平人才，带来先进理念跟技术经验。在团队建设方面，推动跨部门合作开展，构建数据驱动型创新团队，为大数据项目实施供给有力人才后盾。人才培养及团队建设属于长期过程，要求组织在战略层面给予充分重视及资源投入，经由持续努力造就一支高素质的大数据人才队伍。

6 结语

大数据技术正极大改变信息化管理面貌，为组织赋予了前所未有的发展机遇。应用过程中面临技术、管理、安全等多方面难题。利用技术优化、管理机制改进、安全保障体系建设以及人才培养与团队建设等策略，可切实提高大数据应用的水平及成效。伴随人工智能、云计算、物联网等技术持续发展，大数据会跟这些技术深度结合，生成更为智能、高效的信息化管理模式。就各类组织而言，紧跟大数据发展趋向，推进数字化转型节奏，会成为增强核心竞争力的关键路径。在此过程中，持续的创新及实践是推动大数据技术于信息化管理中深度应用的无尽驱动力。

参考文献

[1] 张波,赵福,杨竞,等.基于大数据技术的计算机信息化管理系统[J].信息与电脑(理论版),2023,35(24):100-102.

[2] 王立明,李迎,刘仕伟,等.大数据技术在城市运行管理服务信息化中的应用[J].信息记录材料,2023,24(11):201-203.

[3] 李瓒明.大数据技术在企业信息化管理中的运用研究[J].中小企业管理与科技,2022,(09):117-119.

[4] 叶萍.大数据技术在企业信息化管理中的有效应用[J].中小企业管理与科技(上旬刊),2021,(12):28-30.

[5] 尤耀华.要重视大数据技术视域下企业经营管理中信息化建设创新[J].企业观察家,2021,(07):100-102.

 DOI: https://doi.org/10.12345/bdai.v6i6.34056

Intelligent Financial Risk Prevention and Control Framework for Public Institutions Driven by Large Models

Bingmei Yao

Guangxi Zhuang Autonomous Region Intellectual Property Development Research Center, Guiping, Guangxi, 530000, China

Abstract

Against the backdrop of the "Accounting Informatization Development Plan (2023-2027)" explicitly proposing to "establish an intelligent financial risk prevention system," artificial intelligence technology is accelerating the transformation of financial management models in public institutions while presenting challenges in data security, algorithmic transparency, and talent structure. This study constructs an intelligent financial risk prevention framework for public institutions using the DeepSeek large model, integrating federated learning (for data privacy protection) with SHAP interpretability technology (to enhance algorithmic transparency and credibility). The proposed "Dynamic Budget-Three-Dimensional Risk Control Dual-Track Model" comprises three layers: a data security protection layer (combining federated learning with national cryptographic algorithms), an algorithmic transparency layer (integrating SHAP attribution with sandbox simulations), and a human-machine collaborative decision-making layer (employing job competency models and micro-certification mechanisms). Empirical analysis of 32 public institutions across six provinces and municipalities demonstrates that applying the DeepSeek model can increase accounting efficiency by 40% ($p<0.01$), achieve 92%±2.3% risk identification accuracy, and reduce labor costs by 32.7% (95% CI: 30.2%–35.1%). This case study further validates the practical effectiveness of the system in three key areas: dynamic budget forecasting (with emergency fund response times under 90 minutes), real-time risk interception (98.7% success rate in blocking abnormal payments), and final account attribution analysis (LSTM model efficiency improved sevenfold). The research provides a theoretical framework and technical roadmap for public institutions to systematically address security, efficiency, and compliance challenges during intelligent financial transformation. Based on field research, it proposes actionable phased implementation strategies and a talent development system.

Keywords

DeepSeek large model; intelligent finance; federated learning; SHAP interpretability; risk prevention matrix; dynamic budget forecasting; digital transformation of public institutions

大模型驱动的事业单位智能财务风险防控融合架构与实证研究

姚冰梅

广西壮族自治区知识产权发展研究中心，中国·广西 桂平 530000

摘　要

在《会计信息化发展规划（2023-2027年）》明确提出“构建智能化的财务风险防控体系”的背景下，人工智能技术正加速重塑事业单位财务管理模式，并带来数据安全、算法透明度及人才结构等多方面挑战。本研究基于DeepSeek大模型构建事业单位智能财务风险防控体系，结合联邦学习（实现数据隐私保护）与SHAP可解释性技术（提升算法透明度和可信度），提出“动态预算-三维风控双轨模型”。该体系涵盖数据安全防护层（联邦学习与国密算法融合）、算法透明解释层（SHAP归因与沙盒推演结合）以及人机协同决策层（岗位能力模型与微认证机制）。通过对6省市32家事业单位的实证分析表明：应用DeepSeek模型可使核算效率提升40%（$p<0.01$），风险识别准确率达92%±2.3%，人力成本降低32.7%（95% CI：30.2%–35.1%）。典型案例进一步验证了其在预算动态推演（如应急资金响应时间＜90分钟）、实时风险拦截（异常支付阻断成功率98.7%）和决算归因分析（LSTM模型效率提高7倍）等方面的实践效能。本研究为事业单位在智能财务转型中系统解决安全、效率与合规问题提供了理论框架与技术路径，并基于实际调研提出了可操作的分阶段实施策略及人才能力建设体系。

关键词

DeepSeek大模型；智能财务；联邦学习；SHAP可解释性；风险防控矩阵；预算动态推演；事业单位数字化转型

【作者简介】姚冰梅（1977–），女，中国广西桂平人，本科，会计师，从事大模型驱动的事业单位智能财务风险防控融合架构与实证研究。

1 数字化转型：事业单位财务面临的挑战与机遇

1.1 战略机遇矩阵与风险矩阵分析

当前事业单位智能财务转型呈现出效率显著提升与新型风险并存的双重特征（见表 1）。

表 1 事业单位智能财务转型战略机遇与风险矩阵

机遇维度	具体表现	挑战维度	风险表现
效率提升	1. 预算编制周期缩短 80% 2. 财务数据处理速度提升 100 倍 3. 自动化替代 65% 重复性工作 4. 7×24 小时智能响应服务	技术安全	1. 核心财务数据泄露风险 2. AI 决策不可解释导致的可靠性争议 3. 系统漏洞年均攻击增长 120% 4. 基础设施故障恢复超 4 小时
决策优化	1. 资金使用效益预测精度达 95% 2. 实时风险预警响应速度＜ 10 秒 3. 跨部门数据整合率 100% 4. 资源配置前瞻性提升	合规监管	1. 缺乏 AI 财务专项法规 2. 算法可解释性不足被审计质疑 3. 数据跨境流动合规风险 4. 多系统接口标准不统一
服务创新	1. 个性化服务覆盖 90% 业务场景 2. 智能咨询准确率 98%	人才结构	1. AI+ 财务复合人才缺口率 68% 2. 45 岁以上员工转型抵触率 32%

实证研究显示，某省教育厅借助 DeepSeek 自然语言处理引擎，将预算草案编制时间从 17.3 小时压缩至 2.1 小时（$t=9.42, p<0.01$）。然而，某市疾控中心因 OA 系统使用弱口令，遭遇支付凭证篡改，造成直接经济损失 89 万元，同时暴露灾备体系缺失问题，仅 23% 单位实现热备，远低于金融行业 70% 的标准。进一步分析发现，多数事业单位尚未建立系统性的网络安全防护体系，具体体现为未部署多因素认证、未实施权限最小化原则、缺乏实时入侵检测机制等方面。

总体来看，智能财务转型在显著提升效率的同时，也带来了技术安全、合规性及人才结构等方面的新挑战。风险挑战集中体现在：

技术安全方面，财政部 2023 年通报显示，78% 的事业单位存在数据泄露隐患，典型案例如某市疾控中心因弱口令导致支付篡改，同时灾备覆盖率过低（仅 23%）、高级持续性威胁（APT）识别率不足 40%，与 2025 年目标达到 80% 存在显著差距；

合规监管方面，2024 年某部委审计中，因算法决策过程不透明，37 项支出（涉及金额 2100 万元）遭到质疑，反映出当前算法审计标准尚未有效落地；

人才结构方面，多数单位尚未建立针对数字技能的培训体系，45 岁以上员工对智能工具存在使用障碍，而年轻员工虽具备基础操作能力但缺乏业务理解深度，形成“技术 - 业务”双短板困境。

1.2 核心矛盾的制度与技术归因

根据《2023 年财政部网络安全检查通报》（财办发〔2023〕45 号），抽样单位中 78% 存在数据安全隐患，主要体现在：

制度层面，现行《事业单位内部控制规范》尚未系统覆盖人工智能权限管理，例如某科研院所发生管理员越权访问核心数据事件；

技术层面，传统加密机制与联邦学习等隐私计算技术的适配性不足，如某社保中心因加密协议漏洞导致 20 万条个人敏感信息泄露。

制度与技术之间的协同缺失尤为明显，一方面，现有内控制度仍以传统手工流程为设计基础，未能充分考虑 AI 系统的特性；另一方面，技术供应商往往专注于算法优化而忽视合规要求，导致许多先进技术难以在事业单位现有制度框架内落地。

人才结构矛盾方面，某省 2023 年对 152 家事业单位的调研显示，传统财务人员中掌握 Python 编程的比例仅为 7%，AI 指令工程师岗位空缺率高达 81.4%±3.1%。该省调研总结的核心能力短板如表 2 所示：

表 2 智能财务转型核心能力短板分析

能力项	掌握率	转型紧迫指数	干预措施
Python 编程	7%	★★★★☆	凭证岗需 NLP 操作认证
SHAP 值解析	12%	★★★★☆	分析师必修可解释 AI 课程
联邦学习架构设计	3%	★★★★★	架构师认证纳入晋升必要条件

调研还发现，不同层级事业单位面临的人才挑战存在显著差异，省级单位主要缺乏高端算法人才，地市级单位急需既懂财务又懂数据科学的复合型分析人才，而县级单位则面临基础数字化技能普及的挑战。

应对策略需聚焦于“微认证 - 岗位适配”体系构建，实现关键岗位的能力转型。应建立“岗位 - 能力 - 认证”三联动的培养机制，首先基于岗位职责明确能力要求，然后通过微认证课程提供精准培训，最后将认证结果与绩效考核挂钩。某省财政厅试点表明，该机制可使员工数字技能掌握速度提升 2.3 倍，岗位适配度提高 45%。

2 DeepSeek 技术架构与财务适配性

2.1 核心技术优势

DeepSeek 在财务核心场景中的效能对比如表 3 所示：

关键技术创新点包括：

隐私计算框架：采用纵向联邦学习，某市民生预算误差率从 14.2% 降低至 9.8%，实现数据不出库情形下的跨部门协作；动态脱敏机制依据《数据安全法》第 31 条，对非

授权人员显示区间值。该框架创新性地将联邦学习与国密算法融合，原始数据经 SM4 加密后在本单位脱敏处理，仅输出加密后的中间特征值参与联邦建模，既满足《网络安全法》数据本地化要求，又实现跨部门数据价值挖掘。某市财政局的实践表明，该方案使跨部门数据协作效率提升 3 倍，同时完全满足等保 2.0 要求。

表 3 DeepSeek 场景化解决方案效能对比

功能	传统模式	DeepSeek 方案	实证效果	合规依据
凭证生成	手工录入 (15 分钟 / 张)	语音生成 (40 秒 / 张)	效率提升 22.5 倍	GB/T 39784
决算分析	固定模板 (滞后 30 天)	LSTM 动态归因 (实时)	某水利厅耗时 42 天降至 6 小时	《算法审计指引》
内控执行	事后抽查 (覆盖率 ≤30%)	实时阻断 (覆盖率 100%)	拦截某高校异常支付 23 笔	《内控规范》

可解释决策引擎：基于 SHAP 值的归因分析清晰呈现预算偏差成因，为审计和决策提供直观依据。例如，某单位 2024 年 Q1 会议费超支分析显示：政策因素贡献 +28.4%（$p<0.05$）、执行偏差 -12.7%（$p=0.01$）、数据错误 +5.2%（检测重复记账 3 笔）。实时合规引擎内控规则随法规动态更新，如《政府会计制度》解释公告发布后，系统在 48 小时内完成规则迭代与部署。为进一步提升可解释性，可开发审计专用可视化界面，将 SHAP 值转换为自然语言描述，并支持钻取式查询。某省审计厅测试显示，该界面使非技术背景审计人员对 AI 决策的理解度从 58% 提升至 90%，审计效率提高 40%。

2.2 场景化解决方案的效能验证

DeepSeek 在多个财务核心场景中取得显著成效：

决算分析：从固定模板滞后 30 天转变为 LSTM 动态实时归因，某省水利厅决算报告生成时间从 42 天压缩至 6 小时；

内控执行：从事后人工抽查（覆盖率 ≤30%）升级为实时智能阻断（覆盖率 100%），成功拦截某高校异常支付 23 笔；

预算调整：在应急资金场景中，系统展现出较高应用价值。当气象部门发布台风预警后，系统自动触发预算推演模型，结合历史灾害数据、物资库存信息和实时舆情热度，在 1 小时内生成资金分配方案（传统方式需 3–5 个工作日）。

3 实证研究：事业单位 DeepSeek 落地路径

3.1 四阶段实施模型

基于多家试点单位的实践，本研究提炼出以下四阶段实施路径：

阶段一：历史数据结构化

某档案馆完成 1950–2020 年纸质凭证数字化，耗时从预估 18 个月降至实际 3 个月，错误率控制在 0.8%。该阶段的关键成功因素包括：①采用渐进式数字化策略，优先处理近 10 年高频查询凭证；②开发专用校对工具，通过众包模式让退休老会计远程校核；③建立元数据标准体系，为后续 AI 训练奠定基础。该阶段虽投入较大（占项目总成本 40%），但为后续智能化应用提供了高质量数据基础，投资回报率达 270%。

阶段二：预算预测与外部变量融合

创新引入多源数据：气象数据用于修正户外工程进度；疫情指数用于生成医疗物资采购预警；舆情热度用于预测应急资金需求。某市在 Prophet 模型中添加政策影响因子，差旅费预测误差从 12.3% 降至 5.1%。外部数据融合需解决数据对齐、显著性检验和可解释性处理等关键技术问题。某市财政局通过纳入气象数据，使道路养护预算准确性提升 23%，因极端天气造成的预算调整次数减少 62%。

阶段三：系统集成与风控落地

本阶段核心任务是将前两阶段的成果（数据、模型）与单位现有财务系统（如支付、核算、资产管理系统）进行深度融合，部署并激活实时风控规则。具体实施包括：构建“资金安全 - 资产防控 - 业务合规”三维风控体系（详见 3.2 节），实现支付环节的实时人脸识别拦截、资产盘点自动化、以及内控规则的 NLP 动态解析与更新。例如，某高校在此阶段成功部署并实时拦截了 23 笔异常支付，某研究所实现了固定资产的自动盘点。

阶段四：体系化运行与持续优化

此阶段标志着系统从“可用”进入“好用”和“放心用”的成熟阶段。重点在于建立三位一体的长效防护机制（详见第 4 章），包括：①制度化运行：将数据安全策略（如国密算法加密、密钥轮换）、算法透明审查（如预算推演沙盒）、人机协同决策流程固化为标准操作规范；②能力内化：推行四级智能财务能力认证体系（见表 5），实现关键岗位人员的能力转型与认证；③持续迭代：基于系统运行反馈和外部审计要求，定期优化算法模型与风控规则，形成闭环管理。

3.2 三维风险预警与执行机制

实证案例表明，三维风控体系具有良好的实战效果：

资金安全维度：单日同一 IP 支付超过 5 次即触发人脸识别，成功拦截冒用报销 3 笔，共计 82 万元；境外 IP 访问自动切换至备用服务器，有效阻断 APT 攻击；

资产防控维度：基于 YOLOv5 的智能盘点系统在某研究所实现固定资产自动识别，效率提升 97%，发现闲置设备 47 台，价值 380 万元；

业务合规维度：通过 NLP 技术自动解析政策文件，实时更新内控规则库。如某单位在《差旅费管理办法》修订后，系统自动识别“交通费限额调整”条款，即时阻断超标报销申请 16 笔。同时，通过知识图谱技术构建政策关联网络，自动推送相关制度条款，使制度执行偏差率降低 75%。