人工智能技术在内部审计中的应用研究——以 DeepSeek 为例

王亚辉[1] 胡丽娜[2]

1 河北工程技术学院，河北石家庄，050000；

2 河北省水利规划设计研究院有限公司，河北石家庄，050000；

摘要：第三代人工智能技术的迅猛发展，给各行各业带来了深刻的影响，也极大地冲击着传统行业。内部审计，发挥着公司治理的基石的作用。通过对公司业务活动、风险管理和内部控制进行独立、客观的监督与评价，保障资产安全与财务信息真实。其不仅是防范舞弊的“防火墙”，更是推动管理优化、实现战略目标的重要保障。传统的内部审计方法主要通过手工核查的方式实现，信息化程度高度发展的今天，传统审计方式正面临前所未有的挑战。

关键词：人工智能技术；内部审计；DeepSeek；应用研究

DOI：10.64216/3080-1486.25.10.063

引言

随着生成式大语言模型的不断发展，也极大地推动者内部审计行业的变革，DeepSeek，是国内近年来比较具有代表性的大语言模型，在审计过程中能够帮助内部审计实现风险智能评估、流程合规性检查及动态监控，提升审计效率与风险覆盖度，推动审计从“事后检查”向“全周期风险管理”转型。本文以 DeepSeek 为例，分析人工智能技术对内部审计影响，探索人工智能技术在内部审计工作中的应用场景和风险，并提出了风险的应对策略。

1 DeepSeek 应用于内部审计的影响与场景

1.1 DeepSeek 对内部审计的影响

1.1.1 提升审计效率与质量

在传统的内部审计中，审计抽样能够在资源有限的情况下，用一部分样本推断总体情况，为量化审计风险提供依据。但此方法存在着一定的局限性，审计抽样带来的误受风险和误拒风险会对审计的效率和质量造成负面影响。而 DeepSeek 是生成式人工智能，在审计效率方面，DeepSeek 能自动化进行内控测试，并对全量数据进行数据分析和报告草拟，大大缩短了审计的周期。在审计质量上，DeepSeek 能够通过机器学习对全部业务数据进行扫描，不仅能精准定位传统方法难以发现的隐蔽异常模式（如关联交易舞弊），还能基于实时数据持续监控风险，实现了从事后核查到事前预警的根本性转变。

1.1.2 革新审计方法与模式

以 DeepSeek 为代表的生成式人工智能的审计，极大程度地实现了从抽样到全量、从事后监督到实时的跨越。在工作方法上，DeepSeek 能够处理海量不同类型的数据，比如结构化数据、非结构化数据和半结构化数据，并能发现这些数据背后的逻辑，使审计发现更为精准和全面，极大提升了审计工作的深度与广度。在此基础上，DeepSeek 还能够将提取数据、数据对账等任务自动化，显著提升了审计流程的效果。在工作模式上，人工智能接管技术门槛较低的自动化任务，如此一来，审计人员可将精力集中于框架设计、结果审查、复杂问题的专业判断和解决、与管理层的沟通等更高价值的战略性活动。此外，DeepSeek 能够根据一些观点和《中国内部审计准则》的要求从多种来源整合信息，并生成审计工作底稿和审计报告初稿，帮助审计人员快速确定好工作的框架。

1.1.3 重塑审计人员的角色和价值

DeepSeek 的崛起正深刻重塑着内部审计人员的角色与核心价值。在角色上，审计人员正从基础工作的执行者，转变为 AI 工具的驾驭者与复杂问题的研判者。 他们从繁琐的抽样、核对等重复劳动中解放出来，转而负责设计分析模型、解读 AI 发现的风险线索，并运用专业判断处理更具战略性的复杂问题。在价值上，其贡献重心从提供合规保障，升级为驱动业务优化与战略决策。 通过将精力聚焦于深度调查、根源分析及前瞻性风险评估，审计人员能够为管理层提供更具洞察力的建议，从确保合规的“监督者”，转型为创造价值的“战略伙伴”。

2 DeepSeek 在内部审计中的应用场景

2.1 审前调查阶段

在审前调查阶段，DeepSeek 的应用彻底颠覆了传统依赖审计人员个人经验和有限抽样的粗糙模式。它能够无缝接入企业的 ERP、财务、供应链及人事等多套业务系统，通过强大的自然语言处理与数据建模能力，对海量的结构化与非结构化数据进行全量清洗、整合与关联分析。这意味着，审计人员无需再花费数周时间进行手工数据提取与整理。更重要的是，DeepSeek 可以运行预设的或自定义的风险分析模型，例如，通过贝叶斯算法识别费用报销中的异常集群，或通过协同过滤原理发现潜在的关联方交易。系统能据此自动生成一张多维度的、可视化的风险热力图，不仅标出高风险区域，还能量化风险等级并阐述逻辑依据。这使得审计计划的制定从一种“经验艺术”转变为一门“数据科学”，审计资源可以被精确地部署到风险最高的领域，实现了真正意义上的“精准制导”审计。

2.2 审计实施阶段

在审计实施阶段，DeepSeek 扮演着一位不知疲倦、算力超群的智能分析官角色。它能够根据审前阶段锁定的高风险线索，进行深度化的自动穿透与溯源。例如，当系统提示某供应商交易存在异常时，DeepSeek 可瞬间追溯与该供应商相关的所有交易、审批流程、甚至比对招标文件与合同文本的一致性，形成完整的证据链条。在侦测复杂舞弊方面，其能力远超人类。DeepSeek 可以利用图神经网络技术，自动构建并分析实体关系网络，迅速识别出表面上毫无关联的员工、供应商股东、银行账号之间存在的隐蔽连接，从而精准定位出虚构交易、利益输送等精心掩饰的舞弊风险。同时，在内部控制测试上，它能以“秒级”速度对成千上万个控制点（如采购订单审批权限、职责分离）进行自动化合规测试，并立即标记出所有例外情况，使审计人员能从繁琐的符合性测试中脱身，将精力集中于对重大异常进行现场核实与深度访谈，极大地提升了审计工作的深度与广度。

2.3 审计报告形成阶段

在审计报告阶段，DeepSeek 的应用带来了效率的倍增与价值的升华。它能够基于审计实施阶段确认的发现，自动抽取关键信息点（如问题描述、涉及金额、违反制度、风险定性等），并按照预设的专业报告模板，快速生成一份结构严谨、论据充分、表述清晰的审计报告初稿。这直接将审计人员从大量重复性的文书工作中解放出来。此外，DeepSeek 还是一个强大的法规知识库，能够智能地将每一个审计发现与相关的内部控制条款、外部监管法规或公司政策精准关联，并引用具体条款内容，确保每一个结论都有理有据，显著提升了报告的专业性与权威性。报告定稿后，系统会自动将本次审计的所有分析模型、关键发现、审计思路及最终结论进行分类归档，形成一个持续增长、可被实时调用的审计知识资产库。这打破了以往审计经验依赖于个体人员的局限，实现了组织级审计智慧的沉淀、传承与迭代，为构建学习型审计部门奠定了坚实基础。

3 DeepSeek 在内部审计中应用的风险

3.1 数据安全与隐私泄露风险

DeepSeek 在内部审计应用中面临最直接的风险是数据安全与隐私泄露。内部审计过程涉及企业最敏感的财务数据、运营信息、客户资料、员工个人信息以及商业秘密等核心资产。当这些数据被输入 DeepSeek 系统进行处理时，可能通过多种途径造成泄露：系统可能遭受外部网络攻击导致数据被窃取；授权用户可能越权访问超出其职责范围的数据；员工在日常操作中可能无意间通过提示词泄露敏感信息。更复杂的是，大语言模型在训练过程中可能会记忆特定的敏感信息，并在后续响应中不经意地输出这些内容。如果企业使用的是云端部署的 DeepSeek 服务，数据需要传输到第三方服务器，这进一步增加了数据在传输和存储过程中被截获或滥用的可能性。一旦发生数据泄露，不仅会导致企业核心竞争力受损，还可能面临 GDPR 等数据保护法规的严厉处罚，以及对商业信誉的不可逆损害。

3.2 内部审计工作质量风险

DeepSeek 的引入可能对审计工作本身的质量构成独特威胁，主要体现在模型幻觉与算法偏见。大语言模型固有的“幻觉”特性可能导致其生成看似逻辑严密但实则完全错误的审计分析、结论或法规引用，例如虚构一笔不存在的关联交易，或错误地引用一条已废止的会计准则。如果审计人员过度信赖 AI 的输出而削弱了其职业怀疑精神，未能对关键结论进行必要的交叉验证和实质性测试，这种错误就可能在最终的审计报告中。此外，模型的输出质量高度依赖于其训练数据和预设算法，如果训练数据本身存在偏见或业务场景未被充分覆盖，其构建的风险模型就可能系统性地忽略某些特定类型的风险（如新型金融工具舞弊），导致审计程序设计存在先天缺陷，留下未被察觉的审计盲区，从而严重影响审计工作的深度与准确性。

3.3 过度依赖与审计专业能力退化风险

长期深度依赖 DeepSeek，可能导致审计团队核心专

业能力的系统性退化。当模型承担了从数据清洗、异常识别到报告草拟等关键智力任务后，审计人员便从“执行者”转变为“复核者”，这使他们面临丧失亲手执行基础工作所带来的专业直觉和判断力的风险。年轻审计人员尤其可能错过通过详细审查凭证、追踪资金流向、进行穿行测试来培养“审计嗅觉”的宝贵机会。这种依赖会削弱团队对数字异常、业务逻辑矛盾的敏感度，以及在复杂环境中进行批判性思考和创造性解决问题的能力。最终，审计团队可能演变为 AI 结论的被动确认者，一旦面临模型训练数据之外的新型商业模式舞弊或复杂的职业判断与伦理困境时，将因专业储备不足而无法有效应对，从而损害审计职能的长期健康与价值。

4 内部审计中 DeepSeek 应用风险的应对策略

4.1 建立纵深防御的数据安全体系

为应对数据安全风险，需构建多层防护体系。首先，在技术层面实施端到端加密，对上传至 DeepSeek 的审计数据和在云端存储的数据进行强加密处理，并采用动态数据脱敏技术，在数据处理过程中自动隐藏身份证号、银行账户等敏感信息。其次，在管理层面建立分级授权机制，严格遵循最小权限原则，确保审计人员仅能访问与其任务相关的数据。同时，部署数据泄露防护系统，实时监控异常数据访问和下载行为。对于核心商业秘密数据，可考虑采用 “数据不出域”的私有化部署方案，所有数据处理均在内部服务器完成。此外，定期开展数据安全审计和渗透测试，确保各项防护措施持续有效，从技术和管理两个维度构筑坚实的数据安全防线。

4.2 构建人机协同的质量控制机制

DeepSeek 的引入可能对审计工作本身的质量构成独特威胁，主要体现在模型幻觉与算法偏见。大语言模型固有的“幻觉”特性可能导致其生成看似逻辑严密但实则完全错误的审计分析、结论或法规引用，例如虚构一笔不存在的关联交易，或错误地引用一条已废止的会计准则。如果审计人员过度信赖 AI 的输出而削弱了其职业怀疑精神，未能对关键结论进行必要的交叉验证和实质性测试，这种错误就可能在最终的审计报告中。此外，模型的输出质量高度依赖于其训练数据和预设算法，如果训练数据本身存在偏见或业务场景未被充分覆盖，其构建的风险模型就可能系统性地忽略某些特定类型的风险（如新型金融工具舞弊），导致审计程序设计存在先天缺陷，留下未被察觉的审计盲区，从而严重影响审计工作的深度与准确性。

4.3 实施审计专业能力提升计划

长期深度依赖 DeepSeek，可能导致审计团队核心专业能力的系统性退化。当模型承担了从数据清洗、异常识别到报告草拟等关键智力任务后，审计人员便从“执行者”转变为“复核者”，这使他们面临丧失亲手执行基础工作所带来的专业直觉和判断力的风险。年轻审计人员尤其可能错过通过详细审查凭证、追踪资金流向、进行穿行测试来培养“审计嗅觉”的宝贵机会。这种依赖会削弱团队对数字异常、业务逻辑矛盾的敏感度，以及在复杂环境中进行批判性思考和创造性解决问题的能力。最终，审计团队可能演变为 AI 结论的被动确认者，一旦面临模型训练数据之外的新型商业模式舞弊或复杂的职业判断与伦理困境时，将因专业储备不足而无法有效应对，从而损害审计职能的长期健康与价值。

参考文献

[1]龙志能,鲍镕江,何贤杰.人工智能驱动的审计变革研究[J].审计研究.2024,(5).DOI:10.3969/j.issn.1002-4239.2024.05.016.

[2]刘树.生成式人工智能在金融审计中的应用[J].审计研究.2025,(1).DOI:10.3969/j.issn.1002-4239.2025.01.006.

作者简介：王亚辉，(1995.7-)，女，河北省石家庄市人，汉族，讲师，硕士研究生，研究方向:审计管理与咨询;

胡丽娜，(1995.9-)，女，河北省沧州市人 ，汉族，中级会计师，硕士研究生，研究方向:纳税筹划。

项目来源：河北工程技术学院校级课题 项目名称：人工智能技术在内部审计中的应用研究——以 DeepSeek 为例，项目编号：2025HG49