

数智化驱动的中小型企业轻量级内控体系构建研究

丁一

中国国际工程咨询有限公司, 北京 100048

DOI: 10.61369/SE.2025020021

摘要： 随着数字经济深度发展与监管合规要求日益严格，中小型企业面临转型升级与风险防控的双重压力。传统内控体系因其复杂性、高成本与资源需求，与中小型企业资源禀赋不匹配。本文结合数智化技术发展趋势，系统构建“数智化轻量级内控”概念，探索低成本、高效能的内控创新方案。

关键词： 中小型企业；轻量级内控；数智化；内控创新；风险预警

Research on the Construction of Lightweight Internal Control System for Small and Medium Enterprises Driven by Digital Intelligence

Ding Yi

International Engineering Consulting Corporation, Beijing 100048

Abstract： With the deep development of the digital economy and increasingly stringent regulatory compliance requirements, small and medium-sized enterprises face dual pressures of transformation and risk prevention. Traditional internal control systems, due to their complexity, high costs, and resource demands, are mismatched with the resource endowments of small and medium-sized enterprises. This paper systematically constructs the concept of "digitally intelligent lightweight internal control" by integrating digital intelligence technology development trends, exploring low-cost, high-efficiency internal control innovation solutions.

Keywords： small and medium-sized enterprises; lightweight internal control; digital intelligence; internal control innovation; risk early warning

一、中小型企业内控现状与数智化挑战

(一) 中小型企业内控建设典型问题

1. 许多中小型企业为满足外部监管或融资需求，简单照搬大企业内控模板或咨询公司标准化方案，导致“纸上内控”与实际业务脱节。表现为：制度过于复杂，员工理解困难，执行成本高；制度与业务需求不匹配，员工抵触心理强，存在变相规避行为；内控沦为摆设，内控活动多在外部审计或检查前临时开展，未能真正发挥风险防控作用。

2. 动态适应性不足

中小型企业处于成长阶段，业务模式和组织结构经常调整，而传统内控体系修订周期长、调整成本高，难以适应快速变化的业务需求，容易形成管理阻碍。同时，风险形态也在不断演变，特别是数字化时代的信息安全、数据合规、算法公平性等新型风险，传统内控框架往往反应滞后、应对不足，中小型企业对新型风险的覆盖存在明显短板。

3. 技术应用水平低

中小型企业信息化基础普遍薄弱，内控工作仍主要依靠人工执行与监督，效率低下且易出错。具体表现为：技术投入不足，内控无法实现自动化，增加了运行成本；数据分析能力不足，无法利用数据进行风险预警，降低了内控的有效性；内控信息化与业务系统割裂，很少企业实现了内控与业务系统的集

成，造成内控执行与业务流程的“两张皮”现象。

(二) 数智化时代给中小型企业内控带来了新的挑战：

1. 数据安全与隐私保护风险

随着数字化转型，中小型企业积累了大量业务数据和客户信息，但数据安全意识和技术防护能力普遍不足。只有少数中小型企业制定了数据分类分级管理制度，部分企业曾发生过数据泄露事件。《数据安全法》^[1]《个人信息保护法》^[2]《网络安全法》^[3]等法规对数据治理提出更高要求，加大违规处罚力度，也增加了中小型企业合规压力。同时，随着数据要素市场化，如何平衡数据价值挖掘与合规使用成为新课题，多数中小型企业缺乏专业指导和实操方案。

2. 信息系统依赖与稳定性风险

数字化程度提升使中小型企业对信息系统的依赖度显著增强，企业一旦系统瘫痪，业务将无法开展。然而，中小型企业IT基础设施建设和运维能力普遍薄弱：IT人员比例低，IT预算有限，多数企业未建立完善的业务连续性计划。系统安全事件可能造成数天的业务中断和直接经济损失，风险暴露明显^[4]。

3. 第三方服务风险

中小型企业数字化转型多依赖第三方云服务、SaaS平台等，这引入了供应商管理、服务连续性、数据权属等新型风险，多数企业未与供应商签署数据安全和水平保障协议，也未制定供应商退出机制和数据迁移等应急方案。实践中，第三方服务终止

或数据迁移困难导致业务中断案例，造成运营影响和经济损失^[6]。

4. 数字能力差距

数智化背景下，内控工作需要数据分析、信息安全、隐私计算、API 治理等新型能力，而中小型企业在这些领域存在明显能力差距。大多数中小型企业缺乏数据分析人才，也很少开展信息安全培训，企业管理层对新兴数字技术理解有限。数字化转型速度与内控能力提升不同步，形成“数字鸿沟”，中小型企业数字化业务发展超出了风险管控能力的情况在增加，风险敞口持续扩大^[6]。

二、数智化驱动的轻量级内控体系构建

（一）数智化轻量级内控的概念与特征

“数智化轻量级内控”是指在数字技术支持下，中小型企业以最小必要的控制措施实现对重大风险的有效管控，通过数据驱动和智能分析替代传统的人工控制和繁复流程，实现内控体系的精准、高效与动态优化。其核心特征包括：

1. 风险聚焦：区别于传统内控“全覆盖”思路，数智化轻量级内控遵循“二八法则”和“风险导向”原则，聚焦影响企业生存发展的关键风险，优先配置有限资源；实践验证，对中小型企业而言，聚焦管控核心风险比追求全面覆盖更具成本效益。

2. 数据驱动：从“经验判断”转向“数据决策”，基于业务数据实现风险的自动识别与预警，替代传统的人工控制点；内控决策建立在数据分析基础上，而非主观经验，提高了风险识别的准确性和预警的及时性。

3. 技术支撑：利用云计算、移动应用、自动化工具等低成本、易部署的数字工具降低内控实施门槛和运行成本；通过技术手段弥补人力资源不足，降低内控对专业人才的依赖。

4. 智能监控：利用规则引擎、异常检测算法等技术，实现对异常交易和风险行为的自动识别、实时监测与主动预警；从“事后稽核”转向“实时监控”和“预测预防”，提高内控的时效性。

5. 弹性适配：内控措施根据业务特性、发展阶段和风险变化动态调整，确保控制强度与风险水平、业务需求相匹配；避免过度控制或控制不足，保持内控与业务的协调发展。

6. 过程融合：将控制点嵌入业务流程，实现“无感控制”，降低执行阻力；内控由“独立系统”转变为“业务基因”，融入日常经营活动^[7]。

（二）数智化轻量级内控实施模型

本文提出“风险画像 - 数字赋能 - 智能监控 - 闭环优化”的数智化轻量级内控实施模型：

1. 风险画像：精准识别关键风险

数智化背景下，中小型企业可通过数据分析实现风险的精准识别。企业可分析业务数据发现应收账款异常增长、库存周转率下降、盈利率波动等风险信号，同时建立结构化风险数据库积累内外部风险事件信息，分析历史风险模式识别前兆信号。此外，利用可视化技术绘制风险关联图谱，可清晰展现业务流程中的风险关联点和扩散路径，形成完整的风险传导链视图。

风险量化与排序是中小型企业风险管理的关键环节。企业可

采用简化的5×5风险矩阵，基于历史数据计算风险发生概率和影响程度，生成直观的风险热力图。通过ABC分类法将风险分为高危、中度和低危三级，使企业能够聚焦资源优先应对“高频+高影响”的A类风险。同时，计算风险调整后收益率，可客观评估各业务活动的风险收益比，为资源配置提供数据支持。

情景模拟与压力测试为中小型企业提供风险预判能力。企业可利用简易模拟工具，测试客户违约、供应商断供、原材料价格波动等关键风险事件对现金流和运营的实际影响，明确风险承受能力边界。通过设计“生存测试”，企业能评估在极端不利情况下的生存能力和必要的资源储备水平。基于压力测试结果，企业可确定适当的控制措施和预警阈值，制定有针对性的应急预案，增强企业面对突发风险的韧性。

2. 数字赋能：降低内控实施门槛

数智化时代，中小型企业可利用低成本技术工具降低内控实施门槛：

中小型企业可通过低成本数字工具实现内控数字化转型。利用钉钉、企业微信等协同平台的流程审批功能，企业能够将传统纸质审批转为线上操作，不仅留下完整审批痕迹，还能显著提高审批效率。采用财务云、采购云、合同云等SaaS服务模式，企业可以月租形式替代大额一次性投入，既降低了技术门槛，又减少了后期维护成本，大幅节约总拥有成本。此外，借助Excel+宏或免费分析工具开发简易监测模板，实现基础数据的常态化监控，这类工具学习曲线平缓，普通员工经过短期培训即可掌握应用。

移动端优先策略为中小型企业内控赋予时空灵活性。通过开发轻量级移动审批应用，管理人员可随时随地进行业务审批，有效加快决策流程，将传统审批时间大幅缩短。设计移动端风险预警功能，实现异常情况的即时推送通知，使风险响应时间从小时级缩短至分钟级，极大提升风险处置的时效性。此外，利用移动端进行远程监督和数据采集，如外勤签到、现场检查 and 图像证据收集，既降低了传统现场监督的人力成本，又提高了数据的真实性和完整性。

流程数字化与自动化是中小型企业内控转型的关键环节。首先梳理销售订单、采购付款、费用报销等关键业务流程，设计标准化数字流程表单，实现业务全流程可视化和可追溯，增强过程管控能力。对常规重复性内控任务实施自动化处理，如自动对账、异常交易标记和额度控制等，减少人工干预和错误率。同时，构建包含电子签名、操作日志和审批记录在内的完整电子证据链，不仅降低了合规举证成本，还能有效减少业务争议的解决时间和处理成本，提升内控的有效性和可靠性。

3. 智能监控：实现风险预警与异常识别

数智化背景下，中小型企业可突破传统人工监督局限，构建智能化风险监控体系：

智能预警机制是中小型企业数智化内控的核心环节。企业可针对盈利率、资产负债率、客户账期等关键业务指标设置预警阈值，建立“红黄绿”三级预警体系，实现业务异常的提前发现。同时，构建包括交易频次、审批时间、授权范围等多维度异常监测模型，全方位捕捉风险信号。通过分级预警响应机制，企业能

够根据风险等级触发不同层级的审查和处置流程，确保低风险事件在基层得到及时处理，让管理层聚焦于高风险事件的决策与干预，优化管理资源配置。

行为分析与异常识别为内控体系提供深层防护能力。通过分析用户日常操作行为，企业能够建立正常行为为基线，从而识别非常规时间登录、批量数据导出、异常权限使用等可疑操作模式。对重要业务数据变更建立全面审计跟踪，记录“谁在什么时候做了什么”的完整证据链，确保数据管理的全程可追溯，增强责任认定的精准性。借助简单规则引擎，企业还可自动识别拆分采购规避审批、关联交易隐匿等异常业务模式，及时发现并阻断潜在的合规风险和舞弊行为。

可视化监控与决策支持工具使内控管理更加直观高效。企业可建立风险监控数字看板，直观展示风险分布、发展趋势和重点关注事项，提高风险识别效率和沟通清晰度。通过设计风险趋势分析报告，展示关键风险指标的变化趋势和预测结果，为管理层提供数据支持，增强决策准确性。同时，构建内控健康状况仪表盘，实时展示控制执行率、风险预警数量、异常事件处理率等关键指标，提高管理层对内控状况的关注度和风险意识，促进内控管理从被动应对向主动防控转变，形成全员参与的风险管理文化。

4. 闭环优化：实现内控体系持续改进

在数智化背景下，中小型企业可通过闭环优化实现内控体系的持续改进。首先，企业应建立包含异常交易识别率、风险事件防范率等关键绩效指标的评估体系，收集执行数据识别“高成本低效益”与“低成本高效益”的控制措施，评估成本效益比以优化资源配置。其次，建立内控弹性调整机制，根据业务变化和风险状况动态调整控制强度，设置例外处理流程平衡控制与效率，定期复盘执行痛点并收集一线反馈优化设计。最后，通过分析失效案例识别系统性缺陷建立防范机制，收集员工反馈优化用户体验提高执行效率，并持续追踪业务创新及时识别新风险点更新控制措施，确保内控与业务创新同步发展，形成数据驱动的内控持续改进机制^[8]。

三、研究建议

基于研究，本文对中小型企业提出几点建议，中小型企业应

构建数智化轻量级内控体系时，应重点关注以下几个方面：

首先，企业需彻底摒弃“大而全”的传统内控思维，转而采用“轻量级+数智化”策略，精准聚焦关键风险领域。具体而言，应通过风险评估识别对企业生存和发展影响最大的前20%风险点，集中80%的内控资源进行管控；针对不同风险等级采用差异化控制策略，对高风险领域设置严格控制点，对中低风险领域适当简化控制流程；同时，避免机械照搬大型企业内控体系，结合自身业务特点和组织架构，设计符合企业实际的内控措施，确保内控资源投入产出最大化。

其次，中小型企业应充分利用云服务、移动应用等低成本数字工具，降低内控实施门槛。可考虑采用SaaS服务替代自建系统，降低前期投入和维护成本；积极运用移动办公工具实现审批、监督和预警的移动化，提升内控效率；开发轻量级内控组件，实现与业务系统的无缝集成；探索运用开源软件和免费工具搭建基础内控平台，通过“小投入、快见效”的方式逐步提升数字化内控能力^[9]。

第三，企业需建立内控与业务的深度融合机制，避免内控成为业务的“绊脚石”。关键举措包括：在业务流程设计阶段即嵌入内控要素，实现“流程内控一体化”；开展内控体验优化，简化操作步骤，减少冗余环节，降低用户操作成本；设计弹性审批机制，对不同风险级别业务应用差异化审批流程，实现“风险适配”；建立内控协调机制，在业务部门设置内控协调员，促进业务与内控的日常沟通；定期组织内控与业务部门共同发现内控痛点并优化解决方案，培养“内控即服务”的理念，使内控从“管控者”转变为“创造者”^[10]。

最后，中小型企业应加强数字化能力建设，培养既懂业务又懂技术的复合型内控人才。可通过制定数字化人才发展计划，明确关键岗位的数字化能力要求；开展系统的数字技能培训，包括数据分析、流程自动化、风险识别等方面的实操技能；组建跨部门内控数字化工作小组，促进IT、业务和内控人员的知识交流与协作；同时，可灵活运用外部资源，如聘请专业机构提供数字化内控顾问服务，或采用众包方式解决特定内控技术难题。企业还应建立激励机制，鼓励员工积极探索和应用数字技术创新内控方法，形成持续学习与创新的组织文化。

参考文献

- [1] 全国人民代表大会常务委员会. 数据安全法 [Z]. 2021.
- [2] 全国人民代表大会常务委员会. 个人信息保护法 [Z]. 2021.
- [3] 全国人民代表大会常务委员会. 网络安全法 [Z]. 2016.
- [4] 陈可欣. 数智化转型背景下深化企业内部控制建设研究 [J]. 审计与理财, 2023, No.427(02):57-58.
- [5] 王智平. 数智化背景下企业会计数据治理研究 [D]. 中国财政科学研究院, 2022. DOI: 10.26975/d.cnki.gccks.2022.000198.
- [6] 王晓钊, 沈海燕. 数智化时代风险评估与内部控制评价体系研究 [J]. 工信财经科技, 2024, No.24(06):80-91.
- [7] 刘玉. 数智化时代下企业内控管理模式的探讨 [J]. 中国电子商情, 2024, No.1163(22):69-71.
- [8] 王建文. 数智化风控手段在企业内部控制中的应用探究 [J]. 财会学习, 2024, No.417(28):164-166.
- [9] 财政部, 证监会, 审计署, 银监会, 保监会. 企业内部控制基本规范 (财会 [2008] 7号) [Z]. 2008.
- [10] 财政部, 证监会, 审计署, 银监会, 保监会. 关于印发企业内部控制配套指引的通知 (财会 [2010] 11号) [Z]. 2010.