

智能化背景下电商企业内部控制优化研究

许婧淳, 常光辉, 赵叶灵

江苏大学财经学院, 江苏 镇江

收稿日期: 2025年8月12日; 录用日期: 2025年8月25日; 发布日期: 2025年9月16日

摘要

随着智能化技术的快速发展, 电商企业的内部控制体系正在面临深刻的变革。本文聚焦智能化背景下电商企业内部控制的优化问题, 指出智能化技术在推动电商企业全链路升级的同时, 也使其内部控制面临新的挑战。本文从控制环境、风险评估、控制活动、信息与沟通、内部监督五个维度展开分析, 进而提出一系列优化措施, 旨在为智能化电商企业构建适配的内部控制体系提供参考, 以实现技术赋能与风险防控的协同发展。

关键词

智能化, 电商企业, 内部控制, 优化

Research on the Optimization of Internal Control of E-Commerce Enterprises under the Background of Intelligence

Jingchun Xu, Guanghui Chang, Yeling Zhao

School of Finance and Economics, Jiangsu University, Zhenjiang Jiangsu

Received: Aug. 12th, 2025; accepted: Aug. 25th, 2025; published: Sep. 16th, 2025

Abstract

With the rapid development of intelligent technology, the internal control system of e-commerce enterprises is facing profound changes. This paper focuses on the optimization of internal control of e-commerce enterprises under the background of intelligence, and points out that intelligent technology not only promotes the full-link upgrading of e-commerce enterprises, but also faces new challenges in its internal control. This paper analyzes from five dimensions: control environment, risk assessment, control activities, information and communication, and internal supervision, and

then proposes a series of optimization measures, aiming to provide reference for intelligent e-commerce enterprises to build an adapted internal control system, so as to realize the coordinated development of technology empowerment and risk prevention and control.

Keywords

Intelligence, E-Commerce Enterprises, Internal Control, Optimization

Copyright © 2025 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

近年来, 电商行业呈现出爆发式的增长, 根据全国电子商务公共服务网显示, 2024 年我国电子商务交易额为 46.41 亿元, 同比增长 3.9%。《中国新电商发展报告(2025)》显示, 2024 年中国电商持续领跑全球, 直播电商等新兴产业成为拉动消费与外贸增长的重要力量, 用户渗透率从 2019 年的 4.9% 跃升至 2024 年的 37.8%。与此同时, 人工智能、大数据、区块链等技术在商品推荐、仓储调度、支付结算等环节得到广泛应用, 有效提升了企业运营效率, 但也暴露出数据泄露、算法歧视、系统漏洞等新风险。内部控制作为企业风险管理的核心机制, 其有效性直接影响了电商企业的合规性与盈利性。然而, 现有的内部控制体系难以应对智能化技术带来的新型风险, 企业亟需对此进行优化。

2. 电商企业智能化及内部控制的内涵

2.1. 电商企业智能化

电商企业智能化的内涵是指电商企业以人工智能、大数据、云计算等新一代信息技术为底座, 通过技术创新与业务深度融合, 重构“人-货-场”关系, 实现全链路数字化、自动化、智能化的运营模式升级。其本质是通过技术赋能, 解决传统电商在效率、体验、决策、协同等方面的痛点, 形成更高效、精准、灵活的商业生态[1]。

2.2. 电商企业内部控制

电商企业内部控制是指电商企业为保障经营目标实现、防范风险、确保财务报告可靠性及合规性, 通过制定制度、实施措施和执行程序, 对经营活动中存在的风险进行识别、评估和管控的系统化过程, 其内涵体现为以合规为底线、以风险为导向、以流程为载体、以数据为基础, 通过组织架构、权责分配、信息系统和监督机制的协同运作, 覆盖电商业务全链条尤其注重数据安全、算法合规、资金支付等数字化场景的风险防控, 并随技术迭代持续动态优化的动态管理机制[2] [3]。

3. 智能化电商企业内部控制的问题分析

3.1. 控制环境

电商企业在控制环境方面存在技术依赖度高且风险防控不足的问题。在竞争激烈的电商领域中, 电商企业的生存和发展越发依赖技术赋能所带来的核心优势[4]。一方面, 用户对电商服务的要求正经历着从“可用”到“好用”再到“智能”的跨越式升级。如今, 电商用户不仅期待平台能够提供丰富多样的商

品选择,更对服务体验提出了严苛的标准,如个性化的推荐、分钟级的配送、保姆式的售后,每一项都考验着企业的技术底气。另一方面,运营端对关键指标的极致追求进一步加剧了技术依赖,商品交易总额的突破、复购率的提升、库存周转率的优化,无一不在倒逼企业在智能技术的研发上持续加码。更有甚者,为了抢占先机,不惜压缩新系统上线前的安全测试周期,这种“重速度、轻稳妥”的做法,看似可以快速抢占市场份额,实则后续可能爆发的技术漏洞、数据风险等埋下了难以预估的后果[5]。与此同时,随着技术的不断升级,传统的风险防控能力已无法满足现实的要求。电商生态中,像用户端 APP、支付平台、仓储管理系统等不同的环节是依靠 API 接口进行连接的,任何一个节点出现问题,都有可能通过接口迅速传导至整个系统,引发连锁反应。更为棘手的是,电商智能功能的实现往往依赖多领域据技术的交叉融合,这种跨学科的技术交织大大增加了问题分析的难度。

3.2. 风险评估

智能化技术的快速发展,使得大量新型风险以更隐蔽、更复杂的姿态涌现。然而,企业当前的风险识别体系是很难跟上这种变化节奏的,最终陷入“看得见的风险在升级,看不见的风险在滋生”的被动局面。从认知层面看,新型风险往往和技术深度绑定,其本质特征、产生逻辑、影响路径都和传统风险截然不同。很多企业对这些新型风险的认知还停留在“技术故障”层面,既未深入理解其传导路径,也缺乏对技术迭代过程中潜在风险的敏锐察觉,甚至在风险已经造成损失时,仍未能准确界定风险的性质。从工具和方法层面看,传统风险的评估大多依赖历史数据的归纳分析和风控人员的经验判断,如基于历史销售数据预测库存风险[6]。而新型风险具有突发性、跨界性的特征,智能化技术的快速发展使得很多风险是首次出现,缺乏足够的历史数据积累,导致现有的评估模型难以对其进行有效捕捉。此外,企业对新型风险的重视程度也不够,大部分的精力都分配给了能快速拉动业绩增长的项目上,而对于风险防控这类需要长期投入且见效周期较长的领域,则缺乏系统性的资源保障与战略布局[7]。例如,在资金投入上大幅压缩,使得企业无法引进先进的风险检测工具、搭建智能化的风险预警模型,在人力配置上也往往将经验丰富的骨干成员抽调至一线,仅留少量人员负责基础的风险排查。

3.3. 控制活动

电商企业在控制活动中出现的自动化控制与人工监督脱节的问题,根源在于技术驱动的自动流程与人工监督未能形成有效的配合。从技术认知看,对自动化系统的过度依赖是造成脱节的根源[8]。追本溯源,这种现象的本质是技术团队陷入了“技术万能论”的误区,他们潜意识中将自动化系统的功能边界无限放大,既未清醒认知系统运行的底层逻辑局限,也在无形中弱化了人工监督的不可替代性,最终为二者的脱节埋下了认知层面的隐患。从能力适配看,智能化技术的迭代速度远超人工监督能力升级的速度。电商领域的算法模型往往能做到每月更新,但如此频繁的更新速度使得风控人员并不能及时理解新算法的底层逻辑,从而导致人工监督沦为形式化检查[9]。从组织协同看,部门壁垒与目标错位加剧了这种脱节状态。电商企业内部的技术部门的工作重点在于提高系统处理效率,业务部门则聚焦于提高转化率、降低流失率,而监督部门作为风险防控的责任主体,因缺乏跨部门协调权,既无法推动技术部门在系统中嵌入“操作留痕、逻辑透明”的协调功能,也无法要求业务部门配合执行“人工检验与系统决策交叉验证”的机制,最终形成了“技术部门重效率,业务部门重业绩”的割裂状况[10]。

3.4. 信息与沟通

电商企业在信息与沟通环节的核心问题,集中表现为“信息孤岛”现象。具体表现为各部门的数据分散存储、独立管理,订单系统、用户画像库、库存数据库、财务结算系统等如同一个个独立的信息模

块, 其中的内容无法跨系统流通, 更谈不上形成协同价值。从兼容性来看, 电商业务涉及 CRM、ERP、WMS 等多类系统, 这些系统多由不同的供应商开发, 它们在技术架构、数据格式和通信协议上存在显著差异, 这就导致系统间难以直接交互。为了解决系统集成的难题, 电商企业通常可以选择自己开发一个中间件或者购买现成的集成软件平台, 但这两种方式的投入都比较高, 以至于许多企业尤其是中小电商, 选择放弃主动整合, 任由各系统独立运行, 最终造成了数据割裂的局面。从管理层来看, 部分管理者过于关注短期业绩, 将数据打通视为“见效慢的非紧急事项”, 既未将其纳入企业长期战略规划, 导致数据战略与业务目标脱节, 又因投入产出比不直观而削减相关预算。这种管理认知上的偏差, 直接导致企业在面对“信息孤岛”的问题时, 常常采取拖延的方法, 而非从根源上解决问题。同时, 传统管理思维下, 管理者习惯按部门职能划分权责, 对数据驱动模式认知不足, 且对新技术接受度低, 不愿尝试通过技术手段打破壁垒。

3.5. 内部监督

电商企业内部监督环节存在因技术手段不足导致审计的问题, 这一问题的背后是资源投入失衡、业务与技术协同脱节、专业人才缺失多重因素共同作用的结果。具体来看, 企业在资源的分配上存在明显的倾向性, 往往将核心资源优先投向能够直接创造营收的前端业务, 比如用户增长、渠道拓展等环节, 而内部审计监督环节则被视为“非核心成本中心”, 资源投入被严重压缩, 这直接导致审计工作大量依赖人工抽检、Excel 对账等传统方式, 样本量不足且容易受到审计人员的主观影响。与此同时, 电商业务的快速迭代, 以及企业内部多系统的割裂状态, 让本就不足的审计手段更难跟上业务节奏, 导致监督漏洞被进一步扩大。一方面, 新业务产生的大量非结构化数据难以被传统审计系统识别, 另一方面, 企业内部的订单系统、支付系统、仓储系统等工具, 往往来自不同的厂商, 数据格式和接口标准各不相同, 若审计技术缺乏跨系统的数据整合能力, 就无法实现全链路关联校验, 进而形成审计盲区[11]。更重要的是, 电商企业内部极度缺乏复合型人才, 这使得企业即便引进了先进的审计工具, 也难以充分发挥其效能[12]。所谓复合型人才, 指的是那些既对电商全链路业务有着透彻理解, 能精准识别交易流程中的风险节点, 又掌握大数据分析技术、AI 算法等审计技术, 能从海量数据中挖掘出异常关联并搭建或优化审计模型的人才。

4. 智能化电商企业内部控制和优化措施

4.1. 化解控制环境困境

电商企业为化解控制环境中技术依赖度高且风险防控能力不足的困境, 首要任务是实现技术迭代与安全测试的动态平衡。这意味着企业在追求技术赋能的同时, 也要为新系统上线前的安全测试划定不可逾越的最低安全测试周期, 通过刚性约束来消除市场上为抢占先机而擅自压缩安全验证环节的短视行为, 让技术创新的步伐始终与安全保障的节奏保持同频。在此基础上, 针对系统互联与技术融合所催生的风险传导问题, 企业应着力强化跨系统协同防控能力。一方面, 企业要搭建覆盖全业务链条的系统接口监控机制, 对用户端 APP、支付平台、仓储管理系统等通过 API 接口产生的数据交互进行实时记录与异常预警, 确保任一环节出现漏洞时能快速锁定源头并切断传导路径; 另一方面, 需组建跨领域技术分析小组, 针对智能功能背后的多领域技术的融合原理展开深入研究, 系统梳理技术交织过程中可能存在的风险节点, 并基于历史案例与模拟推演, 明确每个节点的处罚条件、影响范围及对应的处置预案, 从根本上降低问题分析的复杂度。通过上述措施, 企业既能以刚性约束保障技术迭代的安全底线, 避免因追求速度而牺牲稳定性; 又能通过跨系统监控与融合风险预判阻断风险传到链条, 降低复杂技术环境下的问题分析难度与影响范围, 最终为电商企业的长期稳定发展提供坚实保障(见图 1)。

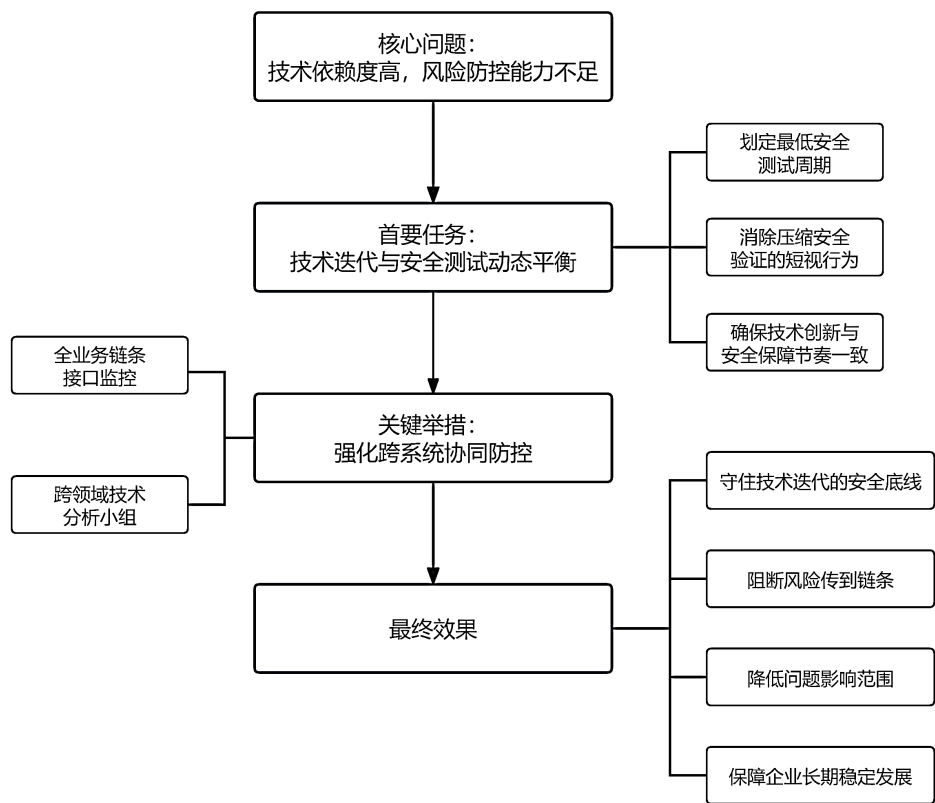


Figure 1. Control environment optimization measures
图 1. 控制环境优化措施

4.2. 构建风险评估体系

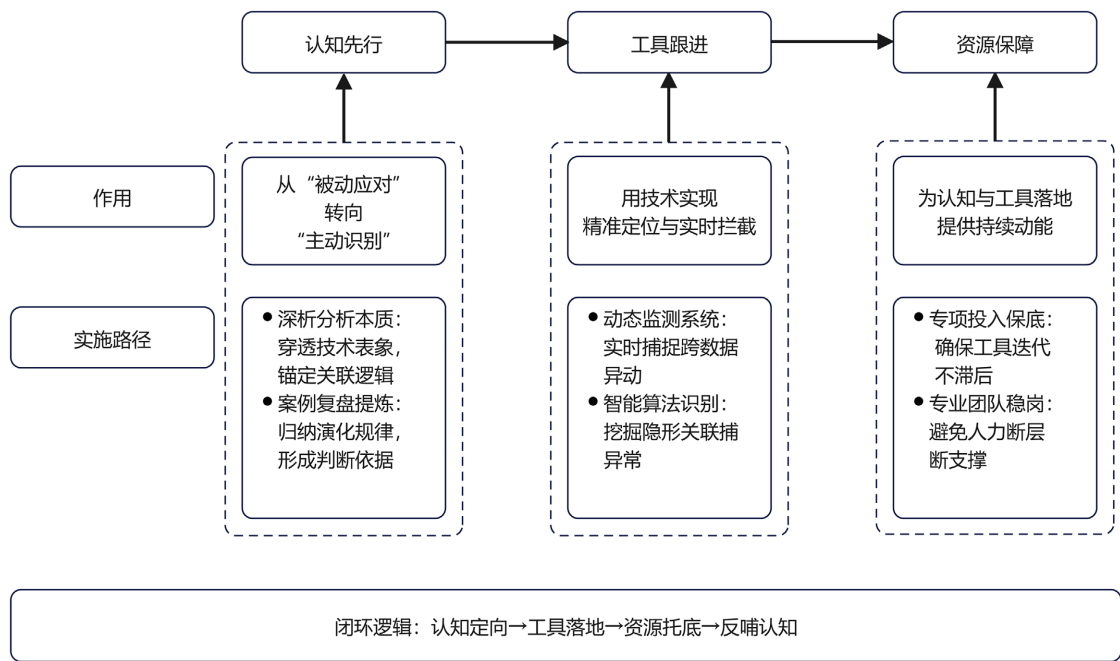


Figure 2. Risk assessment optimization measures
图 2. 风险评估优化措施

智能化技术的快速发展催生了大量的新型风险，电商企业需要从认知深化、工具升级、及资源分配三个维度展开系统性优化。在认知层面，电商企业应深化对新型风险的理解，从“技术故障”的浅层认知向深层认知转变，具体可通过组织常态化新型风险案例复盘，并邀请技术专家深度解读风险与技术的绑定逻辑及其传导路径，以此培养团队对新型风险的敏锐洞察力，确保在风险初现或造成损失时，能快速界定其性质与影响范围。在工具与方法层面，企业需要构建适配新型风险特征的评估体系。鉴于新型风险突发性、跨界性强且历史数据不足的特点，企业应引入基于实时数据的动态评估模型，利用机器学习算法的优势，对不同领域的数据进行关联分析，以捕捉传统模型难以识别的异常信号[13]。最后，企业需要强化风险防控的资源保障与战略定位，摒弃过去“重短期业绩增长，轻长期风险防控”的倾向，合理调整资源分配的结构，不再压缩风险防控的投入，预留专项资金用于引进先进的检测工具和搭建智能化预警模型[14]，在人力配置上保留经验丰富的骨干而非尽数抽调至一线，将风险防控纳入企业长期战略布局，确保其与业务同步推进[15]。综上，通过这三个维度的优化，电商企业能够对新型风险形成全方位的防控，在智能化技术驱动的市场竞争中保持优势(见图 2)。

4.3. 弥合控制活动间隙

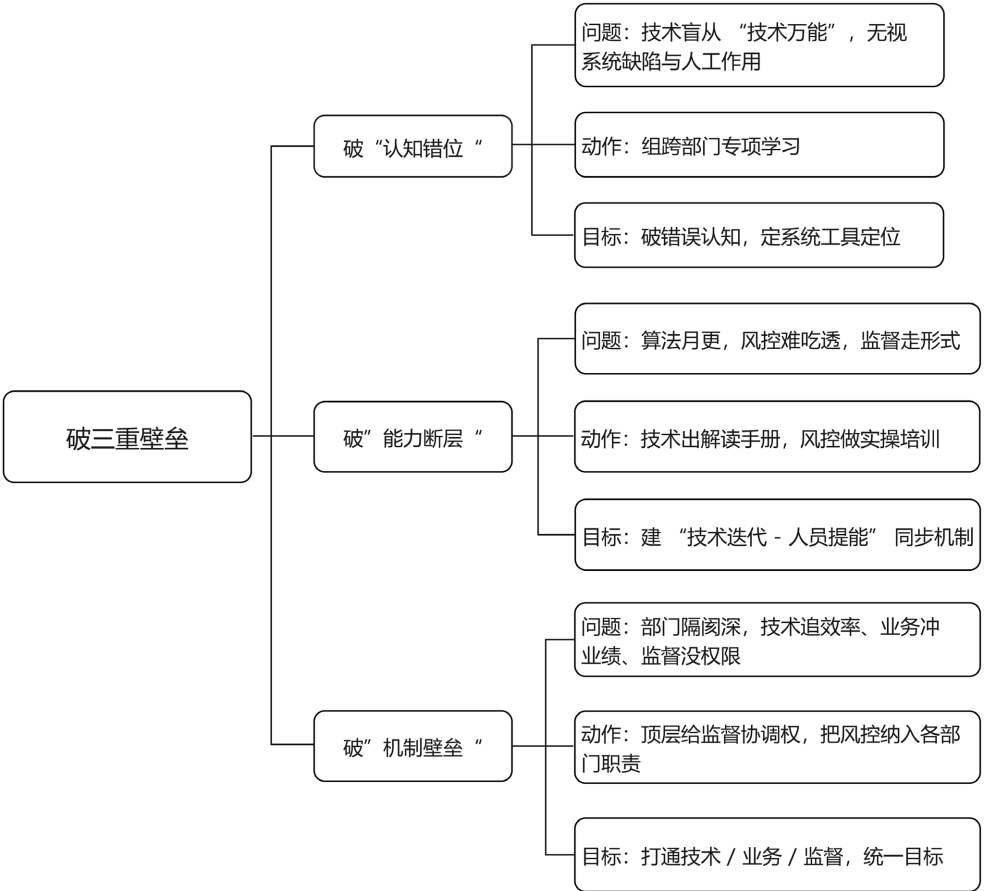


Figure 3. Control activity optimization measures
图 3. 控制活动优化措施

电商企业控制活动环节中自动化控制与人工监督脱节的问题，可以从纠正技术认知偏差、提高能力适配性、打破组织协同壁垒三个方面实施优化措施。在技术认知层面，应先破除技术团队“技术万能论”

的误区，通过组织电商企业内部技术、风控、业务等相关人员，开展一场聚焦“自动化系统技术短板”的专项学习活动，让技术团队清醒认识到自动化系统的局限性，主动重视人工监督的价值，从根源上避免自动化与人工监督脱节，为后续自动化与人工监督的协同打下基础。在能力适配层面，需建立一套让技术升级与人员能力提升保持同步的机制。具体来说，就是要求技术部门在每月对算法模型进行更新时，不能仅完成技术层面的迭代工作，还需要同步编制并输出一份说明书，用通俗易懂的语言来解释新模型的底层判断逻辑和可能存在的局限性，并组织风控人员开展专项培训，通过实操加深对系统的理解。在组织协同层面，企业需从顶层设计入手重构部门目标与权责体系，通过赋予监督部门跨部门协调权，调整业务部门和技术部门的目标，让他们不再局限于追求业绩和效率，而是将风险协同防控纳入所有部门的核心职责，最终实现技术流程、业务操作与监督工作的深度衔接。通过这三方面的优化，既能让自动化控制的效率优势得到充分发挥，又能使人工监督真正起到补位作用，从根本上解决两者脱节的问题(见图 3)。

4.4. 打通信息交流孤岛

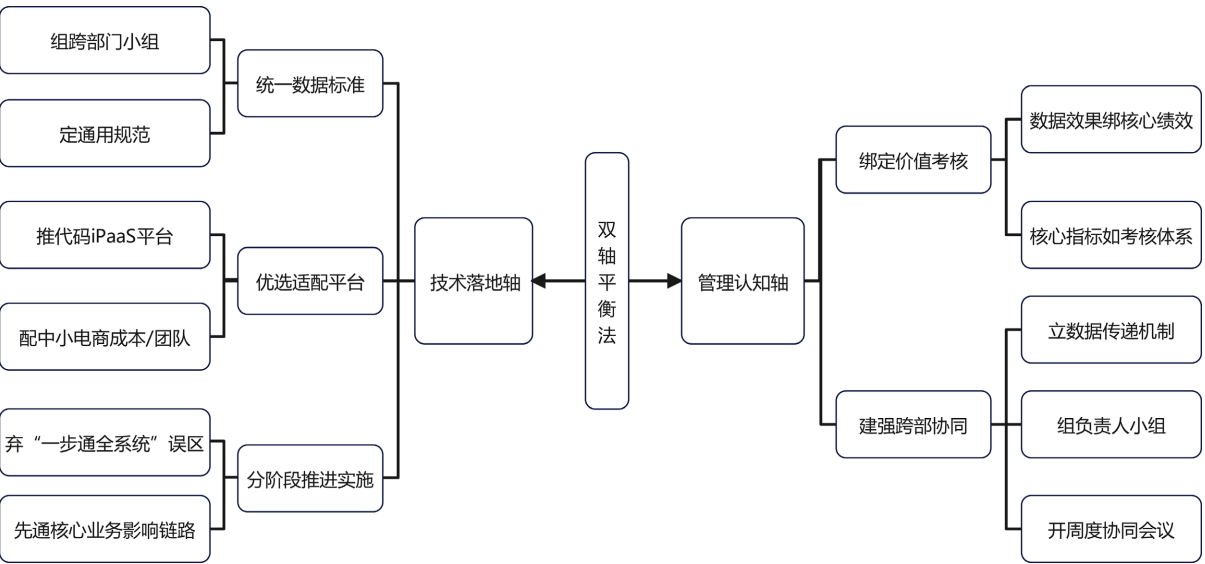


Figure 4. Information and communication optimization measures
图 4. 信息与沟通优化措施

电商企业信息与沟通环节的“信息孤岛”问题，需要从技术落地与管理机制两方面双管齐下。在技术落地层面，企业可牵头成立由技术、运营、财务、库存等多部门人员共同参与的跨部门数据标准小组，其核心任务是针对电商业务中高频使用的数据，制定统一的字段定义与格式规范，从根源上解决不同系统因数据规则差异而无法互通的问题。与此同时，考虑到中小电商的成本承受能力和技术团队规模，可以优先选择低代码 iPaaS 平台。在具体实施过程中，要避免追求“一步打通所有系统”的错误认知，而是采取分阶段的推进策略，优先处理对业务影响最大的链路。在管理机制层面，一方面要将数据打通效果与核心业务绩效深度绑定，以扭转管理层“短期导向”认知，并推动管理层把一些核心指标纳入考核体系，明确数据打通后的具体优化标准，这样才能直观地感受到数据打通的实际价值[16]。另一方面，企业需建立跨部门数据协同机制，让数据能按业务需求在部门间顺畅传递[17]。其次，成立由多部门负责人组成的跨部门数据协同小组，每周召开一次数据协同会议，这样既能避免单一部门决策导致数据规则不贴合其他部门需求，也能让各部门从“被动应对”转向“主动参与”。唯有通过技术和管理协同发力，才能改善“数据孤岛”现象。让信息真正成为驱动电商业务增长的核心动力(见图 4)。

4.5. 升级内部监督能力

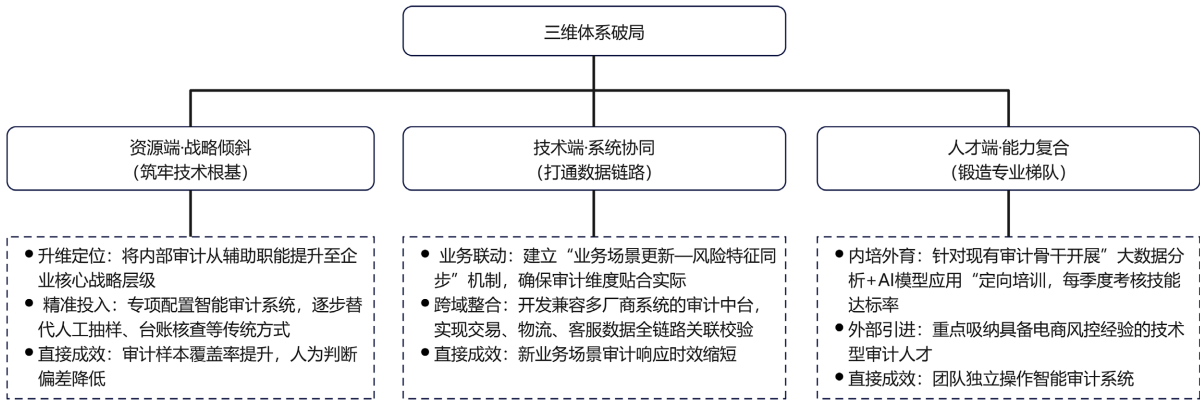


Figure 5. Internal supervision optimization measures
图 5. 内部监督优化措施

电商企业内部监督环节因技术手段不足导致的审计问题，需从资源分配、技术整合、人才建设三个角度构建一套系统性的优化方案。在资源分配层面，企业必须扭转“重前端业务、轻审计监督”的固有思维，将内部审计能力建设提升至核心战略层面，改变其“边缘职能”定位，通过适度增加专项投入引入智能化工具，以逐步替代依赖人工的传统审计方法，以此扩大审计样本的覆盖广度与深度，减少人为判断的主观偏差，让技术工具成为支撑审计精准度与效率的核心引擎。在技术整合层面，应推动业务与技术的深度协同，避免审计手段落后于业务迭代。针对新业务场景下涌现的多样化数据形态与多系统割裂的现状，建立跨部门协作机制，业务端实时更新业务场景的风险特征，技术端据此开发针对性的审计功能。由于企业初期所使用的系统来自不同的厂商，所以存在兼容性的问题。这就要求开发的审计系统要具备跨系统整合数据的能力，以实现全链路的关联校验。在人才培育层面，着力构建“业务 + 技术”双通的复合型人才梯队，通过内部选拔业务骨干进行大数据分析、AI 算法等审计技术定向培养，同时引进具备电商行业经验的技术型审计人才，形成互补型团队结构[18]。综上，通过三方面措施的协同落地，从根本上提升审计技术的系统性与适配性，让内部监督不再落后于业务(见图 5)。

5. 结语

智能化浪潮为电商企业带来了运营效率与商业生态的革新，但也对内部控制体系的适应性与前瞻性提出了更高要求。本文通过分析智能化电商企业在控制环境、风险评估、控制活动、信息与沟通及内部监督环节存在的核心问题，揭示出技术赋能与风险防控之间的深层矛盾。未来，随着人工智能、大数据等技术的进一步渗透，电商企业内部控制的优化将是一个持续动态的过程。企业需以全链路风险防控为核心，以数据协同为纽带，不断迭代内部控制机制，才能在激烈的市场竞争中实现合规经营与可持续发展的双重目标。

参考文献

[1] 王文佼. 新经济时代电商企业财务管理优化[J]. 财会学习, 2024(9): 37-39.
[2] 张发新. 数字化转型背景下科技企业内部控制路径研究[J]. 现代营销, 2025(7): 121-123.
[3] 陈双超. 数字化转型背景下企业内部控制优化研究[J]. 商讯, 2025(3): 76-79.
[4] 姜蕾, 张蕾. AI 助推电子商务领域新质生产力发展[J]. 企业科技与发展, 2024(12): 26-30.
[5] 王琳煜. 信息化背景下跨境出口电商企业风险管理策略研究[J]. 天津经济, 2024(9): 98-100.

-
- [6] 丁佩瑶. 大数据背景下企业内部控制的优化措施探讨[J]. 市场周刊, 2024, 37(18): 9-12.
 - [7] 张美婵. 数字化转型背景下电商企业内部控制挑战与对策[J]. 纳税, 2024, 18(36): 1-3.
 - [8] 贺存德. 电商企业内部控制问题分析及优化建议[J]. 全国流通经济, 2018(25): 11-12.
 - [9] 李丰华. 数智化时代企业内部控制挑战和优化路径探讨[J]. 投资与创业, 2025, 36(14): 164-166.
 - [10] 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(28): 164-166.
 - [11] 陆箐箐. 基于内部控制视角的企业内部审计优化策略探讨[J]. 理财, 2025(3): 23-25.
 - [12] 黎好. 企业会计信息化对内部控制的影响与优化策略研究[J]. 天津经济, 2025(1): 104-106.
 - [13] 许志勇, 管威. 数智时代企业内部控制优化策略探究[J]. 财会通讯, 2024(2): 128-133.
 - [14] 马静. 新经济形势下企业财务会计内部控制优化研究[J]. 商业经济, 2025(3): 157-160.
 - [15] 常成. 基于风险管理的企业内部控制体系构建策略[J]. 财会学习, 2022(34): 152-154.
 - [16] 赵基全. 企业内部控制优化“三步式”方法探究[J]. 会计之友, 2020(12): 84-88.
 - [17] 王志林. 基于风险管理的企业内部控制探析[J]. 国际商务财会, 2022(7): 60-62+68.
 - [18] 聂飞. 数字化转型下企业内部控制优化探究[J]. 现代营销, 2024(34): 115-117.