The American Journal of Management and Economics Innovations
ISSN 2693-0811 | Open Access

TYPE Original Research
PAGE NO. 45-51
DOI 10.37547/tajmei/Volume07Issue05-05

Check for updates

Internal audit issues and their impact on the quality of financial reporting

Viktoriia Lezhanina
Bookkeeper at SC LLC, FL, USA,
Auditor at Compliance Audit LTD, Ukraine

OPEN ACCESS
SUBMITED 20 March 2025
ACCEPTED 22 April 2025
PUBLISHED 12 May 2025
VOLUME Vol.07 Issue 05 2025

CITATION

Viktoriia Lezhanina. (2025). Internal audit issues and their impact on the quality of financial reporting. The American Journal of Management and Economics Innovations, 7(05), 45–51. https://doi.org/10.37547/tajmei/Volume07Issue05-05

Abstract: This paper examines the core challenges confronting internal audit functions and evaluates their implications for the quality of financial reporting. Drawing on prior research emphasizing the role of internal audits in enhancing transparency, the study situates its analysis in the context of small and medium-sized enterprises (SMEs) that experience acute resource constraints and heightened vulnerability to fraud and misstatements. Key findings reveal that methodological incoherence—evidenced by a lack of unified audit standards—coupled with incomplete adoption of advanced data-analytics tools significantly undermines the reliability of financial disclosures. Moreover, widespread digitalization introduces additional complexities, including cybersecurity threats and the need for specialized IT expertise. These deficiencies can inflate audit risk and detection failures, ultimately jeopardizing stakeholder trust. The paper concludes with targeted recommendations to refine audit procedures, integrate robust technological solutions, and foster stronger engagement of managerial and shareholder communities in sustaining high-quality financial statements.

Keywords: Internal Audit; Financial Reporting; Digitalization; Audit Risk; Small and Medium-Sized Enterprises (SMEs); Cybersecurity; Data Analytics; Control Environment.

Introduction: An increasing demand for transparency in financial reporting has amplified the impor-tance of internal auditing in organizations across various sectors [8, 9]. Stakeholders—ranging from investors to regulatory bodies—expect corporate finan-cial statements to be both accurate and reliable,

underscoring the need for robust internal audit procedures. These procedures serve as a safeguard against misstatements and fraud, ultimately supporting market confidence in reported figures [1]. Furthermore, the current wave of digital transformation, encompassing the growing application of artificial intelligence (AI) and advanced data-analytics methods, has introduced both additional opportunities and heightened complexities into internal auditing [2, 12]. While automation can significantly enhance efficiency in detecting anomalies and errors, the lack of standardized approaches for auditing AI-driven processes poses new risks to the quality of financial statements [6].

Simultaneously, small- and medium-sized enterprises (SMEs) face unique obstacles when strengthening their internal audit functions [15]. With relatively limited resources and expertise, SMEs often lag in adopting contemporary digital tools and platforms, leading to potential vulnerabilities in their audit and control environ-ment [13]. As SMEs comprise a substantial portion of many economies, ensuring that these enterprises have access to effective internal audit frameworks becomes crucial for maintaining financial stability [5].

A growing body of research highlights the transformative role of internal auditing not only in reducing fraud risk but also in contributing to strategic decision-making [3]. Studies underscore that deficiencies in internal audit methodologies—such as outdated control checklists or inadequate training in emerging technologies—can directly compromise the reliability of financial reporting [7, 10]. In addition, recent works emphasize the heightened relevance of digital risks, spanning cyber threats to shortcomings in cloud-based systems integration [3, 11]. While large corporations often have dedicated IT-audit departments, SMEs with more constrained budgets may find themselves unable to deploy strong digital safeguards [4]. Consequently, research calls for more standardized guidelines and greater investment in developing the auditing capacity to address big-data analytics, AI-based decision support, and overall cybersecurity [16].

Despite growing academic attention, notable gaps remain. For instance, many studies focus on auditing in large entities, leaving the unique challenges of SMEs relatively underexplored [14, 15]. Furthermore, the interplay between newly adopted technological tools—like AI-driven risk assessment—and conventional internal audit procedures still lacks cohesive frameworks that would allow auditors to integrate novel techniques reliably [12, 13].

In light of these considerations, the primary objective of this study is to identify the key problems currently confronting internal audit functions and to evaluate how these issues affect the quality of financial reporting. Special attention will be paid to the influences of AI, cloud computing, and cybersecurity requirements on audit procedures. Based on the findings, the paper will propose specific recommendations aimed at refining methodological and procedural aspects of internal auditing to ensure more accurate and trustworthy financial statements in both SMEs and larger entities.

1. Key issues in internal auditing

Methodological and organizational constraints, inadequate adaptation to digital technologies, and escalating cyberrisks together form a complex set of challenges that affect the effectiveness of internal auditing and, ultimately, the quality of financial reporting [4, 5, 12, 15]. Research findings indicate that the absence of unified standards often leads to duplicated procedures, incomplete testing, and a higher probability of oversight. This issue is especially acute for small and medium-sized enterprises (SMEs), where resource shortages further complicate the execution of high-quality internal audits.

In many countries, the development of detailed methodological guidelines is left to industry associations or individual firms. As a result, organizations must rely on generalized recommendations that do not always reflect specific industry features or constrained financial and human resources [15]. For instance, the classical approach to reducing overall audit risk (AR) is to consider the product of

$$IR \times CR \times DR,$$

where IR denotes inherent risk, CR represents control risk, and DR refers to detection risk [2]. However, in an environment where part of the audit sample is processed manually and procedures are inconsistently applied, IR and CR values may be miscalculated, thereby inflating DR even at the audit planning stage.

Financial and staffing constraints are particularly significant in SMEs, which, according to Brodny and Tutak (2022), make up a substantial segment of the European economy. Their vulnerability lies in limited access to advanced analytical instruments and in difficulties hiring qualified internal auditors. Consequently, several key control functions may be partially overlooked, creating gaps in examining the most risk-prone areas such as debtor–creditor relationships and intangible-asset transactions [15].

Challenges related to digitalization and technological innovations become more serious when IT systems deployed at a given enterprise are insufficiently integrated into the overall audit framework [4]. Fragmented IT infrastructure gives rise to inconsistencies in data across departments, complicating the collection of audit evidence. Likewise, a lack of expertise in big data and AI poses a dilemma: even if modern analytics platforms are available, the findings they produce may be misinterpreted [12]. The shortage of tech-savvy professionals and data analysts who can adapt big data to the specific needs of internal auditing further heightens overall audit risk [2]. Table 1 summarizes some factors that hinder the full-scale use of digital solutions in internal auditing.

Table 1. Key barriers to implementing digital technologies in internal auditing

Barrier	Description	Impact
1. Fragmented IT systems	Lack of a unified platform and inconsistent software solutions across departments	Increased risk of data loss and complications in transaction analysis
2. Skills shortages in big data and AI	Few experts capable of interpreting outputs from intelligent algorithms	Errors in risk assessment and low effectiveness in anomaly detection
3. Suboptimal data architecture	No clear procedures for data accumulation and verification	Limited reproducibility of audit tests and disruptions in control processes

Cyberrisks and information security take on critical importance given the marked increase in electronic document flows. According to Rikhardsson et al. (2022), even small companies may handle a volume of financial information comparable to that of much larger organizations. The growing number of cyberattacks and sophistication of malicious tools mean internal auditors must assess not only accounting transactions but also the overall security of IT infrastructure [4]. Neglecting these considerations can lead to situations in which data tampering or unauthorized copying goes unnoticed, ultimately distorting an enterprise's actual financial standing. This risk is particularly high in SMEs, where financial constraints often preclude the installation of comprehensive encryption systems and consistent IT security audits [5].

In sum, weak methodological foundations—especially evident in resource-limited SMEs—combined with technological challenges and cyberthreats create a multifaceted set of problems. These factors intensify classical audit risks and add new threats to the reliability of financial statements. Overcoming such barriers necessitates unified standards and an expanded range of competencies for auditors, including in-depth knowledge of digital platforms. However, implementing such measures is complicated by budget limitations and a shortage of qualified personnel at most firms. Fragmented IT infrastructure and a lack of codified procedures for secure data storage exacerbate the threat of cyberattacks, further highlighting the need for coordinated efforts between auditing and information security teams. Addressing these obstacles requires a reexamination of traditional audit methods, focusing on advanced technological support and ongoing staff training.

2. Impact of these problems on the quality of financial statements

Ongoing deficiencies in internal control, insufficient risk management practices, and the evolving complexities of digital audit techniques can significantly compromise the reliability of corporate financial reporting [4, 5, 12, 15]. A crucial aspect of mitigating such challenges lies in understanding how the absence of robust policies and procedures—further exacerbated by inadequate adoption of IT solutions—exposes an enterprise to heightened risks of misstatements and fraud.

Weak internal control environments amplify the probability of errors and fraudulent manipulations. When classical audit risk (AR) is conceptualized as

$$AR = IR \times CR \times DR$$

where IR represents inherent risk, CR stands for control risk, and DR refers to detection risk—ineffective internal controls escalate CR, thereby increasing AR overall. This relationship becomes especially precarious if limited resources force small internal audit teams to prioritize certain accounts or processes at the expense of others [15]. In such scenarios, even routine data entry mistakes or seemingly minor misclassifications can go undetected, fueling larger financial discrepancies. Table 2 exemplifies how weak internal control can interact with each component of AR, illustrating the cumulative nature of potential misstatements.

Table 2. Interaction of weak internal controls with audit risk components

Risk component	Primary issue	Consequence
Inherent risk (IR)	Complex transaction structures or high estimation uncertainty	Greater *a priori* likelihood of errors in specialized areas like intangible assets
Control risk (CR)	Deficient segregation of duties, incomplete reconciliation processes	Systemic flaws enable misstatements or fraud to remain hidden from basic checks
Detection risk (DR)	Restricted audit scope, insufficient testing procedures	Key anomalies may go unexamined, leading to unqualified opinions despite financial distortions

Equally critical is the sequence and thoroughness of audit actions. An internal audit function that frontloads data analytics or invests more resources in planning is often better equipped to spot irregularities early. Conversely, a disorganized approach—where random checks precede risk assessment—may misalign testing efforts with high-risk transactions [12]. Findings from Brodny and Tutak (2022) reinforce that smaller entities, in particular, benefit from structured, step-by-step audit plans, which ensure that all major accounts and disclosures receive proportionate scrutiny.

The importance of risk management and IT adoption becomes evident in the context of new digital platforms and data analytics. Enterprises employing big data solutions or cloud-based accounting systems often achieve more transparent recording of transactions, thus narrowing the scope for undetected misstatements [15]. However, digital platforms alone do not guarantee higher data quality. Auditors must be capable of interpreting analytics outputs, including anomaly detection flagged by AI algorithms, and then aligning these insights with the established control environment [4]. If an organization underinvests in analytical capabilities or staff training—especially around big data governance and data integrity—financial statements may not reflect actual performance, thereby increasing litigation risk and damaging stakeholder trust.

The potential for erroneous or manipulated data emphasizes the need for continuous investments in robust monitoring mechanisms. In many cases, organizations assume that once a set of control procedures is in place, ongoing oversight remains minimal [12]. This misconception frequently emerges in

smaller firms, where limited resources and cost considerations can deprioritize periodic upgrades or maintenance of IT systems. Table 3 highlights how improving internal controls and IT solutions can tangibly enhance financial statement reliability, framing these efforts as a cyclical process of reassessment and improvement.

Table 3. Key investments in control systems for enhanced financial reporting

Investment area	Action required	Expected outcome
Advanced analytics tools	Acquire or update software to capture, store, and interpret high-volume datasets	Reduced detection risk through improved anomaly spotting and predictive modeling
Continuous staff training	Regular skill development in data governance, machine learning applications, and financial audit expertise	Higher accuracy in financial statement verifications and deeper domain expertise
Integrated control frameworks	Align separate IT subsystems and create unified compliance checklists for main business processes	More coherent audit trails, boosting internal and external confidence in disclosures

Additional value in fortifying controls arises from the involvement of management and shareholders in ensuring data quality and transparency. When top executives demonstrate a visible commitment to thorough internal audit reviews, this endorsement serves as a cornerstone for a "tone at the top" environment conducive to ethical compliance [5]. In publicly traded companies, heightened shareholder scrutiny can reinforce the diligence of the board of directors, driving a culture that prioritizes robust financial disclosures. Such a culture not only instills stronger operational discipline but also heightens the sense of accountability among mid-level managers [12]. Moreover, the presence of a reliable internal audit function can attract more risk-averse investors, who seek assurance that the firm's reported earnings genuinely reflect economic reality.

Investor confidence thus thrives when organizations commit to transparent oversight frameworks [4]. Evidence from small and medium-sized enterprises indicates that even incremental upgrades—such as routine digital backups, timely reconciliations, and systematic staff training—can lower perceived investment risk [15]. In contrast, enterprises that routinely bypass internal checks risk fostering an environment where financial manipulations remain undetected, thereby undermining the trust of lenders, regulators, and capital market participants.

In sum, the interplay between strong controls, sophisticated IT-enabled methodologies, and active stakeholder involvement is paramount for delivering credible financial statements. An environment that neglects any of these dimensions—whether through weak sequential testing or limited technological investment—risks producing financial data that are both inaccurate and susceptible to fraudulent influences. Nonetheless, organizations that consistently refine their internal auditing protocols, integrate advanced digital platforms, and engage their managerial and shareholder communities build a more sustainable foundation for long-term financial integrity [12, 15].

CONCLUSION

This research underscores the pivotal relationship between internal audit efficacy and the caliber of financial disclosures. The absence of harmonized audit methodologies not only generates inconsistencies but also expands the scope for unchecked errors and fraud.

While SMEs face particularly pronounced difficulties stemming from limited finances, human capital shortages, and less sophisticated IT infrastructures, these challenges also manifest in larger entities striving to align with emerging best practices. Evidence from recent studies highlights the growing relevance of digital platforms in both detecting anomalies and broadening the range of potential misstatements. Cyberrisks further amplify the need for concerted investment in security protocols and staff training, ensuring that technological adoption does not merely introduce new vulnerabilities.

Ultimately, the results show that upgrading traditional internal audit frameworks to reflect the demands of modern, data-intensive operating environments can strengthen managerial oversight and elevate stakeholder confidence. Management teams, board members, and shareholders therefore bear collective responsibility for establishing clear procedural guidelines, investing in continuous professional development, and embracing integrated analytical tools. Such measures not only bolster audit reliability but also contribute to the stability of financial markets by promoting consistent and transparent reporting.

REFERENCES

AICPA. (2015). Reimagining auditing in a wired world: A call to action for the profession. American Institute of Certified Public Accountants.

Alles, M. G., & Gray, G. L. (2020). Will audit analytics and AI transform the audit? Current Issues in Auditing, 14(2), 9–20.

Basuony, M. A. K., Mohamed, E. K. A., Hussain, M. M., & Marie, L. (2017). The effect of internal audit function on the financial performance of small and medium enterprises: An emerging market perspective. International Journal of Accounting and Information Management, 25(2), 159–180.

Broccardo, L., Tenucci, A., Agarwal, R., & Alshibani, S. M. (2024). Steering digitalization and management control maturity in small and medium enterprises (SMEs). Technological Forecasting & Social Change, 204, 123446.

Brodny, J., & Tutak, M. (2022). Digitalization of small and medium-sized enterprises and economic growth: Evidence for the EU-27 countries. Journal of Open Innovation: Technology, Market, and Complexity, 8(2), 67.

Chan, D. K., & Kim, S. H. (2020). Emerging AI applications in auditing: Opportunities, challenges, and ethical considerations. In Proceedings of the AAA Annual Meeting (pp. 55–68). American Accounting Association.

Commerford, B. P., Dennis, S. A., Joe, J. R., & Warne, R. C. (2021). Who or what is the auditor? The influence of the nature of the auditor's work on intrinsic motivation and interactions with AI audit technology. Journal of Accounting Research, 59(5), 1536–1576.

ICAEW. (2018). Artificial Intelligence and the Future of Accountancy. Institute of Chartered Accountants in England and Wales.

IFAC. (2018). Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements. International Federation of Accountants.

Omoteso, K. (2012). The application of artificial intelligence in auditing: Looking back to the future. Expert Systems with Applications, 39(9), 8490–8495.

Raschke, R. L., Trewin, U., & Williams, P. F. (2018). A cognitive style perspective of AI usage in auditor inquiry. Journal of Information Systems, 32(3), 125–147.

Rikhardsson, P., Thórisson, K. R., Bergthorsson, G., & Batt, C. (2022). Artificial intelligence and auditing in small- and medium-sized firms: Expectations and applications. AI Magazine, 43(3), 323–336.

Sun, T., & Vasarhelyi, M. A. (2017). In digital accounting: The effects of cognitive computing on assurance and the evolution of auditing. Journal of Emerging Technologies in Accounting, 14(2), 27–43.

Sutton, S. G., Holt, M., & Arnold, V. (2016). The reports of my death were greatly exaggerated—artificial intelligence research in accounting. International Journal of Accounting Information Systems, 22, 60–73.

Tîrcovnicu, G.-I., & Hategan, C.-D. (2023). The audit risk assessment of European small- and mid-size enterprises. Journal of Risk and Financial Management, 16(3), 158.

Vasarhelyi, M. A., Sun, T., & Issa, H. (2016). Research ideas for artificial intelligence in auditing. Journal of Emerging Technologies in Accounting, 13(2), 1–20.