Universal Library of Business and Economics Research Article

ISSN: 3064-9951 | Volume 2, Issue 1

Open Access | PP: 49-53

DOI: https://doi.org/10.70315/uloap.ulbec.2025.0201009

Peculiarities of Auditing Small and Medium-Sized Enterprises in the Context of Digitalization

Viktoriia Lezhanina

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

Abstract

This article provides a comprehensive examination of audit practices in small and medium-sized enterprises (SMEs) undergoing digital transformation. Drawing on contemporary research and industry insights, it explores how cloud-based systems, artificial intelligence, and automation tools reshape auditors' roles, methodological approaches, and risk management strategies. The discussion highlights critical cybersecurity concerns, risks of data misrepresentation in cloud environments, and evolving expectations for transparency and reliability in financial reporting. In addressing these challenges, the paper underscores the importance of robust internal controls, enhanced staff competencies, and a continuous monitoring approach. Additionally, it identifies prospective mechanisms for improvement, such as deeper adoption of analytics dashboards, maturity models tailored to digital auditing, and strategic collaborations with technology providers. Overall, the findings illuminate the pathways by which SMEs and their auditors can harmonize technological progress with the core principles of thorough, ethical, and high-quality assurance.

Keywords: *Auditing; Small and Medium-Sized Enterprises; Digital Transformation; Cybersecurity; AI-Driven Audit; Cloud Computing; Internal Controls; Audit Risk Management.*

INTRODUCTION

The small and medium-sized enterprise (SME) sector plays a fundamental role in national and regional economies, given its capacity to generate employment, foster innovation, and drive local development [1]. In many countries, SMEs account for the majority share of businesses, resulting in a significant impact on the overall economic output. Recent research indicates that the digital transformation (or "digitalization") of SMEs can further amplify their economic contributions by enhancing operational efficiency and strengthening competitiveness [1, 8]. Consequently, policymakers and practitioners increasingly emphasize the integration of advanced digital technologies and data-driven processes into the audit and financial reporting frameworks of these enterprises.

With the advent of artificial intelligence (AI), cloud computing, and other Fourth Industrial Revolution (Industry 4.0) technologies, auditing has undergone substantial reconfiguration [6]. SMEs, in particular, are faced with both the benefits of automation and the challenges posed by increased reliance on digitized systems for recordkeeping, risk assessment, and compliance. On the one hand, these technologies can expand the scope of audit procedures, yielding more robust real-time analyses and fraud detection. On the other, auditors must contend with new sources of risk, including cybersecurity threats, algorithmic biases in AI-driven applications, and the complexities of managing large volumes of digital evidence [3, 4].

Research efforts have reflected these emerging complexities. Studies on the European context, for example, indicate that digital maturity among SMEs is highly uneven, particularly in fields such as cloud adoption, automated invoice processing, and AI-based analytics [1, 8]. Scholars underscore a pressing need to adapt audit methodologies and develop clearer standards that address the specificities of smaller entities operating within digitalized environments [5, 7]. Likewise, organizational readiness, employees' digital competencies, and corporate leadership support appear to be critical drivers determining whether SMEs can fully capitalize on technological advancements [2, 4].

Against this backdrop, the present study aims to examine the evolving nature of SME audits under conditions of digital transformation. The chief goals are to:

Citation: Viktoriia Lezhanina, "Peculiarities of Auditing Small and Medium-Sized Enterprises in the Context of Digitalization", Universal Library of Business and Economics, 2025; 2(1): 49-53. DOI: https://doi.org/10.70315/uloap.ulbec.2025.0201009.

1. Identify the key challenges and opportunities arising from the integration of digital tools within SME accounting and audit processes.
2. Analyze specific risks, including cybersecurity and data integrity issues, as well as the strategic potential of automated solutions.
3. Propose directions for future development in the regulatory and methodological landscape of SME audits.

Such an inquiry is especially relevant as digital transformation deepens and regulatory bodies place heightened emphasis on transparency, timeliness, and reliability of reported information [8]. By focusing on both technological advancements and organizational capacities, this work intends to illuminate a path toward more resilient, data-driven audit frameworks that serve the varied needs of SMEs.

Methodologically, this article is grounded in a synthesis of existing theoretical and empirical studies, aiming to bridge insights from auditing standards, digital technology adoption, and SME-specific concerns. First, a literature review was performed to gather background information on the current state of auditing in digitally advanced contexts. Particular emphasis was placed on academic and professional publications analyzing audit risks, AI-driven procedures, and the role of digital maturity [1, 6]. Subsequently, the paper synthesizes findings from comparative analyses on how SMEs address regulatory, operational, and technological issues in pursuit of more efficient, transparent audits.

Transformation of the Auditing Practice in the Context of Digitalization

The pervasive shift toward digital systems—encompassing information management tools, electronic documentation flows, and process automation—has profoundly altered the business landscape for small and medium-sized enterprises (SMEs) [1]. In the past, many SMEs relied on paper-based records and labor-intensive administrative tasks, an approach that not only demanded substantial human input but also introduced greater potential for clerical errors. Today, widespread adoption of electronic invoicing, enterprise resource planning (ERP) systems, and integrated financial software has enabled SMEs to execute transactions swiftly, maintain updated records, and rapidly generate essential data for audit purposes [8]. These transformations, although beneficial, also mandate more robust controls to ensure the integrity of financial and operational information.

The push for heightened transparency and reliability in financial disclosures emerges as a direct outcome of digital tools integrated into SMEs' day-to-day functions [8]. Stakeholders—including investors, banks, and regulatory bodies—expect faster validation of reported figures, particularly given that software automation can capture and summarize extensive financial data in near real time. Concurrently, auditors are asked to perform more extensive checks to confirm that no material misstatements occur within these automated processes [7]. Enhanced real-time visibility also amplifies expectations related to fraud detection and error identification. Thus, auditors have had to recalibrate their traditional sampling-based techniques to incorporate continuous data analysis, which further underscores the necessity for auditors to be proficient in handling computerized workflows [3].

Underpinning this evolution are clear advantages and parallel challenges. On the positive side, the adoption of automated processes frequently yields operational efficiency, cost savings, and quicker turnaround in financial reporting [1]. Automated invoice matching and algorithmic cost allocations can reduce clerical labor, allowing SMEs to direct resources toward higher-level strategic planning. At the same time, new threats become evident. Cybersecurity risks and vulnerabilities in networked accounting systems pose significant dangers, particularly for smaller enterprises less equipped with formalized IT security frameworks [6]. Another potential pitfall involves the possibility of overreliance on software-driven outputs without adequate internal controls, raising the risk of unintentional misstatements if automated processes operate on incorrect assumptions or flawed data [4]. Consequently, while digital integration can streamline data processing and bolster the trustworthiness of financial reporting, it must be accompanied by rigorous internal control mechanisms and tailored governance structures.

Table 1. Key distinctions in auditing practices before and after digital transformation [1, 4, 6, 8]

Aspect	Pre-digital	Post-digital
Data management	Paper-based, manual data entry	Automated systems, real-time transaction logs
Audit evidence	Physical invoices, receipts	E-invoices, electronic documents
Error detection	Sampling-based, labor-intensive tests	Continuous monitoring, exception reports
Cybersecurity concerns	Minimal (local records)	High (networked systems, online threats)
Auditor skill requirements	Primarily accounting-focused	Accounting + IT + data analytics expertise
Speed of reporting	Slower, periodic	Faster, often near real time

As shown in Table 1, the transition from paper-based, manual environments to tech-driven ecosystems entails both improved efficiency and the necessity for advanced security protocols. Although these shifts facilitate a more streamlined audit process, the inherent complexities of networked software call for refined controls. SMEs—and the auditors that serve them—must, therefore, adjust their respective strategies and systems to maintain dependable and verified financial data.

Central to the reconfiguration of modern audits is the deployment of sophisticated software platforms, particularly those employing artificial intelligence (AI) for automated transaction validation and risk assessment [6]. Certain AI-enabled algorithms can detect anomalous entries, inconsistencies in general ledgers, and patterns indicative of irregular transactions with a speed and accuracy previously unattainable via conventional sampling methods. This enhancement does not eliminate the professional judgment of auditors, but rather complements and augments their ability to assess control environments [7]. AI-based auditing tools also provide suggestions for in-depth reviews, enabling auditors to better allocate their time and expertise.

Beyond AI, cloud computing solutions, automated analytics, and Big Data platforms serve as vital components in modern audit procedures [2]. Cloud-based file-sharing services, for instance, expedite the gathering of necessary evidence, which can be uploaded and reviewed from multiple locations. Advanced analytics offer real-time insights into key performance indicators and risk hotspots, and they can flag variances that exceed predefined thresholds. This agility is particularly advantageous for SMEs in dynamic markets where operational and financial parameters frequently change, thereby necessitating up-to-date and continuous auditing coverage [3]. Still, leveraging cloud and analytics tools demands rigorous data protection measures to prevent unauthorized access and ensure compliance with data privacy regulations.

In parallel with these technological trends, the skill set required of auditors has broadened significantly. Proficiency in accounting standards remains indispensable, yet the capacity to interpret outputs from machine learning models, configure automated transaction workflows, and analyze large unstructured datasets is now of near-equal importance [4, 6]. Audit teams, particularly those working with SMEs, must acquire capabilities that bridge finance, IT, and risk management, an aspect often referred to as the "hybridization" of auditor expertise [3]. A more interdisciplinary educational background—encompassing data analytics, business intelligence, and cybersecurity principles—will likely become standard practice in contemporary auditing courses and professional certifications.

In summary, auditing in the digital era is driven by a confluence of evolving technologies and shifting SME priorities. Tools that harness AI, cloud platforms, and comprehensive Big Data solutions position auditors to deliver a deeper evaluation of an organization's financial health, but also impose demanding new responsibilities. For SME audits, the essential challenge lies in assembling an adequately skilled workforce, establishing robust digital infrastructures, and embedding cybersecurity measures commensurate with the sophistication of the employed technologies.

Auditing SMEs: Risks, Prospects, and Mechanisms of Improvement in the Era of Digital Transformation

A central challenge facing small and medium-sized enterprises (SMEs) in the digital era is the heightened risk profile associated with interconnected systems, cloud-based recordkeeping, and automated data flows [1]. Cybersecurity and data protection risks become particularly acute when sensitive financial information is stored or transmitted via remote servers, given the potential for unauthorized access, data leakage, and deliberate manipulation. Even when encryption measures are in place, smaller organizations may lack specialized IT departments, thereby complicating the prompt detection and remediation of breaches. This gap underscores the importance of proactive cybersecurity frameworks, such as periodic penetration testing and robust network monitoring.

Beyond immediate security considerations, the use of cloud-based infrastructures and automated accounting software raises concerns regarding unintentional data distortion [8]. Instances of incorrect parameter settings or incompatible software modules can propagate systemic errors throughout financial statements. For example, an automated process that classifies revenues into the wrong account could significantly impact earnings reporting. SMEs frequently adopt standardized or cost-effective "off-the-shelf" solutions that, while convenient, do not always account for unique business transactions or multi-jurisdictional tax rules. Auditors, therefore, must verify that client systems are both well-configured and periodically updated, mitigating the likelihood of misclassifications and incomplete transaction logs.

Integral to addressing these challenges is the maturation of internal controls and procedures aimed at ensuring data reliability [6]. The conventional approach of relying on end-of-period reconciliations is insufficient under real-time reporting conditions, where errors can spread rapidly. Instead, continuous control mechanisms—ranging from automated discrepancy flags to real-time audit trails—are increasingly vital. These processes, although largely system-driven, require thorough human oversight. Indeed, staff training in red-flag identification, systematic data review, and incident reporting is indispensable to sustaining confidence in the information produced by digital platforms. Failure to invest in such competencies can hinder the reliability of even the most advanced automation tools.

Table 2. Predominant risk categories in digital auditing of SMEs and recommended controls source [1, 6, 8]

Risk category	Description	Recommended control measures
Cybersecurity	Unauthorized access, data breaches, malware attacks	Use multi-factor authentication, encrypt data, conduct regular penetration tests

Systemic data distortion	Automation errors, incorrect parameter settings	Implement real-time dashboards, schedule system checks, ensure software compatibility
Cloud vulnerabilities	Service interruptions, misconfiguration of cloud platforms	Verify service-level agreements, monitor system updates, maintain backup protocols
Fraud and manipulation	Intentional data tampering or suspicious transactions	Activate anomaly detection modules, adopt continuous control-based audits
Inadequate staff expertise	Errors arising from insufficient digital literacy	Provide specialized training, establish clear escalation policies

As illustrated in Table 2, the key risk categories largely mirror the increasingly digital context of SME accounting. Effective management hinges upon both technical and organizational measures, ranging from access protocols to ongoing staff development. Ultimately, maintaining robust data accuracy in automated environments depends on the synergy of well-designed systems, systematic risk assessments, and human competencies.

Under the impetus of technological innovation, SMEs and their auditors increasingly leverage analytic dashboards, visualization tools, and real-time performance trackers [2]. With these digital interfaces, auditors can expedite the review of both financial and nonfinancial indicators, thereby transitioning from periodic sampling to more continuous monitoring. Notably, customizable interfaces allow the integration of cash-flow metrics, operational ratios, and compliance data on a single screen. This real-time perspective assists in detecting unusual trends promptly—such as a sudden spike in accounts payable or delayed inventory turnover—and prompts auditors to delve deeper.

Alongside these practices, evolving maturity models illuminate how organizations progress through stages of "digital readiness" in audits [2]. Initially, enterprises might adopt basic electronic recordkeeping, while advanced phases feature complex data analytics and high-level automation. Some methodologies assess digital maturity along multiple dimensions, including data governance, process integration, and staff competency in data analysis. In practice, these frameworks guide both SMEs and their auditors in pinpointing shortcomings—such as incomplete data capture or insufficient transparency—and inform subsequent investments in software upgrades or specialized training.

Furthermore, collaborative partnerships with technology providers constitute a promising avenue for strengthening digital audits. Vendors routinely offer specialized auditing modules or integrated solutions that automatically update relevant data for multiple stakeholders [1]. Similarly, forging alliances with IT consultants can yield tailored toolsets for real-time data validation and predictive analytics. In turn, external collaboration can be combined with in-house efforts to reinforce auditors' technical skills. For instance, specialized training programs often center on data security protocols, systems configuration, or advanced analytics, which are critical in environments where digital instruments handle voluminous or complex transactions [8].

Over the longer term, the strategic integration of digital capabilities into the auditing workflow promises deeper insights, enhanced reliability of client systems, and faster identification of irregularities [6]. However, auditors must also adapt their foundational methods, ensuring that professional skepticism is not diminished by an overreliance on automated alerts. The increasing volume of data and the capacity for analytics are beneficial only if personnel can interpret the outputs effectively. Herein lies the future direction for SME auditing in a digital context: synergy between technological innovation, upskilling of staff, and rigorous adherence to emerging best practices that reconcile automation with sound professional judgment.

CONCLUSION

In the modern landscape, small and medium-sized enterprises stand at the forefront of economic activity, while simultaneously contending with an increasingly complex, digitally driven environment. The analysis undertaken here indicates that the digitalization of SME operations, though highly beneficial, elevates both the sophistication and scope of audit practices. Robust internal control systems, supplemented by continuous monitoring and backed by specialized IT competencies, emerge as critical determinants of audit accuracy and credibility. Cybersecurity threats, data leakage risks, and potential algorithmic distortions in accounting platforms call for a paradigm shift: auditors must now possess not only deep accounting knowledge but also a strong grounding in information technologies and data analysis.

Furthermore, the transition to cloud-based platforms and advanced analytics redefines what stakeholders expect in terms of transparency and the timeliness of reported information. By proactively integrating AI applications for anomaly detection and real-time data validation, auditors can respond more effectively to vulnerabilities and adapt to dynamic regulatory standards. Still, vigilance in areas such as data privacy, organizational training, and objective oversight remains indispensable to mitigating novel risks.

Looking ahead, strategic partnerships between auditors, technology vendors, and SMEs themselves will be instrumental in creating specialized solutions that can address the complexities of modern financial reporting. These collaborative frameworks, in conjunction with maturity models designed to evaluate digital readiness and employee competencies, promise a sustainable trajectory for enhancing the robustness of audits in increasingly digitalized

contexts. Overall, striking a balance between innovative automation and professional skepticism will remain pivotal to preserving trust, integrity, and excellence in SME auditing procedures.

REFERENCES

1. 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.
2. Broccardo, L., & Tenucci, A. (2024). Steering digitalization and management control maturity in small and medium enterprises (SMEs). Technological Forecasting & Social Change, 204, 123446.
3. ICAEW. (2018). Artificial intelligence and the future of accountancy. Institute of Chartered Accountants in England and Wales.
4. Kokina, J., & Davenport, T. H. (2017). The emergence of artificial intelligence: How automation is changing auditing. Journal of Emerging Technologies in Accounting, 14(1), 115–122.
5. Raphael, J. (2015). How artificial intelligence is changing auditing. CPA Journal, 85(10), 10–12.
6. 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(4), 323–336.
7. Sun, T. (2019). A conceptual framework for applying deep learning in auditing. International Journal of Accounting Information Systems, 33(2), 12–25.
8. 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.