EJDER
European Journal of Digital Economy Research
e-ISSN : 2717-9230

Volume : 6
Issue : 1
Year : 2025
Pages : 23-36

DIGITAL TRANSFORMATION IN INTERNAL AUDIT: PARADIGM SHIFTS, EMERGING RISKS, AND STRATEGIC RESILIENCE

Hayrettin USUL[a], Bekir Yusuf ALPAY[b]

[a] Prof. Dr., İzmir Kâtip Çelebi University, Faculty of Economics and Administrative Sciences, Business Administration hayrettin.usul@ikcu.edu.tr, https://orcid.org/0000-0002-3930-0866

[b] yusuf.alpay@yahoo.com, https://orcid.org/0009-0002-3038-7894

ABSTRACT :

Digital transformation is fundamentally reshaping internal audit practices, transitioning traditional manual processes into technology-driven methodologies and redefining the role of auditors. This study explores how advancements in artificial intelligence (AI), blockchain, robotic process automation (RPA), and data analytics are revolutionizing audit paradigms, enabling real-time transaction analysis, continuous monitoring, and enhanced detection of anomalies. While these innovations improve efficiency, accuracy, and strategic value, they introduce multifaceted risks, including sophisticated cybersecurity threats, algorithmic biases, and vulnerabilities in data privacy. For instance, AI-driven audits risk perpetuating systemic inequities if trained on flawed datasets, while cloud adoption amplifies exposure to ransomware and supply chain attacks. Concurrently, auditors face a significant skills gap, with many lacking proficiency in advanced technologies despite widespread recognition of their necessity, underscoring the urgent need for upskilling initiatives. The research emphasizes the evolving dual responsibilities of internal auditors, who must now balance assurance roles with advisory functions—guiding organizations through digital adoption while ensuring ethical AI governance and compliance with dynamic regulations. Sector-specific challenges, such as auditing decentralized ledgers in supply chains or safeguarding sensitive health records, highlight the need for tailored solutions. Persistent barriers include resistance to automation, resource disparities between firms, and regulatory ambiguities surrounding emerging technologies. To navigate this transformation, the study advocates for hybrid skill development, ethical frameworks to ensure AI transparency, and collaborative efforts to democratize access to digital tools. By addressing these challenges, internal audit functions can harness digitalization to strengthen governance, foster stakeholder trust, and enhance organizational resilience in an increasingly complex risk landscape.

Keywords : Internal Audit, Digital Transformation, Ethical AI, Blockchain Technology, Robotic Process Automation.

RECEIVED: 14 March 2025 **ACCEPTED:** 22 May 2025

DOI:
https://doi.org/10.5281/zenodo.15660150

CITE
Usul, H., Alpay, B. Y., (2025). Digital transformation in internal audit: Paradigm shifts, emerging risks, and strategic resilience. *European Journal of Digital Economy Research, 6*(1), 23-36. https://doi.org/10.5281/zenodo.15660150

Review Paper

1. INTRODUCTION

The advent of digital technologies has catalyzed a seismic shift across industries, redefining operational paradigms and stakeholder expectations. Within the audit sector, this transformation is particularly profound, as organizations transition from manual, document-centric processes to dynamic, data-driven methodologies (PwC, 2023). Digitalization—encompassing artificial intelligence (AI), blockchain, robotic process automation (RPA), and advanced analytics—has emerged as both a disruptor and an enabler, compelling internal audit functions to evolve beyond traditional compliance roles into strategic partners capable of navigating complex risk landscapes (IIA, 2024). This evolution is not merely technological but cultural. Auditors are no longer confined to retrospective evaluations of financial records; they are now pivotal in real-time risk governance, ethical AI oversight, and cybersecurity resilience (ACFE, 2023). For instance, AI-powered tools enable auditors to analyze entire datasets instantaneously, uncovering anomalies that manual sampling might overlook (Sewpersadh, 2025). Similarly, blockchain's immutable ledgers are transforming supply chain audits by ensuring transactional transparency (Deloitte, 2024). Yet, these advancements coexist with escalating risks—algorithmic biases, data privacy breaches, and regulatory ambiguities—that demand auditors to balance innovation with vigilance (KPMG, 2022).

Technological innovations such as AI and machine learning (ML) are redefining audit efficiency and precision. Algorithms trained on historical data can predict fraud patterns, assess credit risks, and automate repetitive tasks such as invoice matching (Boritz & Stratopoulos, 2023). For example, banks now deploy AI to scrutinize millions of transactions for suspicious activities, reducing false positives compared to rule-based systems (Deloitte, 2024). However, the "black-box" nature of AI models raises ethical concerns, particularly when biased training data perpetuates systemic inequities in loan approvals or hiring practices (Floridi et al., 2018). Blockchain's decentralized architecture, meanwhile, offers unparalleled transparency in transactional audits. Smart contracts automate compliance checks, while distributed ledgers provide tamper-proof records for supply chain and ESG audits (IBM, 2023). Walmart's blockchain initiative, for instance, reduced food traceability time from days to seconds, enhancing audit reliability (Sharma & Kumar, 2021). Robotic process automation (RPA) further streamlines workflows by automating tasks like data entry and reconciliation. A recent survey found that RPA reduced audit cycle times in manufacturing sectors significantly (Protiviti, 2022). However, over-reliance on automation risks deskilling auditors and obscuring nuanced anomalies detectable only through human judgment (Barr-Pulliam et al., 2023). Advanced analytics tools like Tableau and Power BI enable continuous, real-time auditing, shifting from periodic reviews to proactive risk management. Siemens' AI-driven analytics platform, for example, reduced operational risks through predictive maintenance alerts (Shamim, 2025).

These innovations, however, coexist with emerging risks. Digital audits rely on vast data ecosystems, amplifying exposure to cyber threats. Recent reports reveal that financial sectors are frequent targets of breaches, often exploiting vulnerabilities in third-party cloud platforms (Verizon, 2023). High-profile ransomware attacks, such as the 2023 MGM Resorts incident, underscore the need for robust encryption and zero-trust architectures (CISA, 2023). Algorithmic bias further complicates accountability. Studies demonstrate that AI models used in credit scoring disproportionately penalize low-income applicants due to biased training data (Umeaduma & Adedapo, 2025). Auditors must now evaluate not only financial risks but also the ethical implications of AI deployments, necessitating frameworks like Explainable AI (XAI) (Floridi et al., 2018). Regulatory frameworks, meanwhile, struggle to keep pace with technological innovation. The EU's Digital Operational Resilience Act (DORA) mandates stringent IT risk protocols, yet gaps persist in auditing decentralized finance (DeFi) platforms (European Commission, 2023). Similarly, proposed AI audit standards remain under debate, leaving firms navigating uncharted territory (PCAOB, 2023). Compounding these challenges is a widening skills gap. Reports highlight that many audit teams lack proficiency in AI and data analytics, jeopardizing their ability to assess emerging risks (ISACA, 2023). Concurrently, automation threatens to displace routine audit

roles, necessitating reskilling initiatives (World Economic Forum, 2023).

Amid these shifts, the role of internal auditors is evolving from "watchdogs" to strategic advisors. They now collaborate with IT departments to evaluate cloud migration risks, guide AI ethics committees, and design blockchain governance protocols (KPMG, 2022). Auditors at institutions like JPMorgan Chase, for instance, advise on AI model validation to ensure compliance with fair lending laws (JPMorgan, 2023). This transformation demands hybrid competencies—technical fluency in tools like Python or SQL, coupled with soft skills like ethical reasoning and stakeholder communication (ACCA, 2023).

This study examines how digitalization reshapes internal audit practices, focusing on three interconnected dimensions: technological drivers, emerging risks, and strategic adaptations. Through case studies—such as healthcare's use of AI to anonymize electronic health records (EHRs) and blockchain's role in supply chain transparency—the paper synthesizes academic and industry insights to propose actionable strategies. These include upskilling auditors in digital tools, advocating for ethical AI governance frameworks, and fostering public-private partnerships to democratize access to advanced technologies. By addressing these imperatives, internal audit functions can harness digitalization to enhance governance, fortify stakeholder trust, and navigate the complexities of an increasingly digitized risk landscape.

2. INTERNAL AUDIT PRACTICES

Internal audit practices form the cornerstone of organizational governance, risk management, and control frameworks. As defined by the Institute of Internal Auditors (IIA, 2024), internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. This function systematically evaluates whether business processes are efficient, risks are appropriately managed, and governance mechanisms align with strategic objectives (Deloitte, 2024). However, the scope and execution of internal audit practices have evolved significantly in response to digital transformation, regulatory complexity, and stakeholder demands for transparency (PwC, 2023). Internal audit serves three primary purposes: assurance, consulting, and strategic insight. Assurance involves providing objective assessments of risk management, control, and governance processes, while consulting focuses on advising management on process improvements and compliance (IIA, 2024). Strategic insight, a more recent addition, emphasizes foresight on emerging risks such as cybersecurity threats or ESG (Environmental, Social, Governance) compliance gaps (ACFE, 2023). The effectiveness of internal audit hinges on adherence to the International Professional Practices Framework (IPPF) by the IIA, which mandates independence, objectivity, and proficiency (IIA, 2024). Independence ensures auditors operate free from managerial influence, while objectivity requires unbiased evaluations. For example, auditors at Siemens AG adhere to a strict rotation policy to prevent conflicts of interest, ensuring fresh perspectives during risk assessments (Harvard Business Review, 2023).

Modern internal audit practices prioritize risk-based approaches, tailoring audits to an organization's most critical vulnerabilities. The COSO ERM Framework (2017) guides auditors in aligning audits with enterprise risk appetite. A multinational corporation might prioritize supply chain audits during geopolitical instability, while a fintech firm focuses on cybersecurity resilience (COSO, 2017). Tools like heat maps and risk matrices visually prioritize risks, enabling auditors to allocate resources effectively (PwC, 2023). Advances in data analytics have shifted audits from periodic reviews to real-time oversight through continuous auditing. This approach leverages AI and robotic process automation (RPA) to analyze transactions as they occur. For instance, JPMorgan Chase uses machine learning algorithms to monitor billions of daily transactions, flagging anomalies such as duplicate payments or unauthorized access (JPMorgan, 2023). Such proactive methods reduce fraud losses by up to 35% compared to traditional approaches (ACFE, 2023). Agile methodologies, borrowed from software development, further enhance audit flexibility. Auditors at Toyota, for example, conduct "sprint-based" audits, delivering incremental findings to management every two weeks instead of annual reports (Protiviti, 2022). This iterative process accelerates remediation and aligns audits with dynamic business needs.

Key components of effective internal audit practices include independence, competency, and technology integration. Internal audit functions must operate independently from management to

maintain credibility. Best practices include reporting directly to the Audit Committee of the board of directors and securing budgetary autonomy to avoid conflicts of interest (KPMG, 2022). At Coca-Cola, the internal audit team's budget is approved by the Audit Committee, insulating it from operational pressures (Marr, 2023). Competency development is equally critical, requiring hybrid skills that blend technical expertise (e.g., data analytics, cybersecurity) with soft skills like communication and ethical judgment. The IIA's Global Skills Framework (2024) identifies competencies such as technical acumen, critical thinking, and stakeholder engagement. Firms like EY now mandate certifications such as Certified Internal Auditor (CIA) and Certified Information Systems Auditor (CISA) for promotions (EY, 2023). Technology integration has become indispensable, with tools like AI-powered analytics detecting patterns in unstructured data, blockchain validating transactional integrity, and RPA automating repetitive tasks (Deloitte, 2024). Unilever's internal audit team, for example, reduced invoice processing errors using RPA bots (Marionne, 2024).

Challenges in modern internal audit practices are multifaceted. Cybersecurity and data privacy risks escalate as audits increasingly rely on digital platforms. The 2023 IBM Cost of a Data Breach Report found that 83% of financial institutions experienced breaches via third-party vendors (IBM, 2023). After the SolarWinds hack, Microsoft's audit team mandated multi-factor authentication for all third-party software providers (Verge, 2024). Regulatory complexity further complicates audits, with global frameworks like the EU's General Data Protection Regulation (GDPR) and Digital Operational Resilience Act (DORA) creating overlapping compliance demands. A 2023 survey by Thomson Reuters found that 67% of audit teams struggle to keep pace with regulatory updates (Thomson Reuters, 2023). Ethical dilemmas also arise with AI adoption, such as biased algorithms in hiring audits. Auditors must adopt frameworks like Explainable AI (XAI) to ensure transparency. Talent shortages compound these challenges, with a 40% gap in auditors skilled in AI and blockchain (ISACA, 2024). Firms like KPMG address this through partnerships with universities for specialized training programs (KPMG, 2022).

Case studies illustrate the practical application of modern audit practices. Walmart implemented blockchain to track food provenance across 25,000 suppliers, reducing audit cycle times by 90% and improving recall accuracy (Sharma & Kumar, 2021). HSBC's AI-driven platform, AML Accelerate, analyzes 300 million transactions monthly, cutting false positives by 60% and saving $200 million annually (HSBC, 2024). Nestlé adopted agile auditing to address ESG risks in its cocoa supply chain, using monthly sprints to reduce child labor incidents by 45% (UNICEF, 2020). These examples underscore the transformative potential of integrating technology with audit methodologies.

Looking ahead, internal audit must prioritize upskilling initiatives to bridge talent gaps, fostering hybrid competencies through training programs that merge AI literacy with ethical reasoning (IIA, 2024). Public-private collaboration is essential to standardize digital audit protocols, leveraging bodies like the Global Internal Audit Common Body of Knowledge (CBOK) (ACCA, 2023). Ethical AI frameworks, such as the EU's Ethics Guidelines for Trustworthy AI (European Commission, 2023), should guide auditors in evaluating algorithmic fairness. By addressing these imperatives, internal audit functions can enhance governance, fortify stakeholder trust, and navigate the complexities of a digitized risk landscape.

3. THE IMPACT OF DIGITALIZATION ON INTERNAL AUDIT PRACTICES

The integration of digital technologies into internal audit practices represents a paradigm shift in the profession, driven by advancements in artificial intelligence (AI), blockchain, robotic process automation (RPA), data analytics, and other emerging tools. This transformation has redefined traditional audit methodologies, risk assessment frameworks, data collection processes, and the overall role of auditors in organizational governance (Usul & Alpay, 2024). Digitalization enables auditors to transcend conventional limitations, such as reliance on sampling methods, by leveraging technologies capable of analyzing entire datasets in real time. For example, automation and AI allow auditors to scrutinize all transactions of an audited entity, eliminating sampling risks and enhancing the likelihood of detecting anomalies, errors, or fraudulent activities (Alexander, 2021). This shift not only improves efficiency but also elevates the quality of audit outcomes, as auditors gain access to comprehensive insights derived from continuous monitoring and advanced analytical tools (Moffitt

et al., 2018). The ability to process vast volumes of structured and unstructured data—ranging from financial records to IoT device outputs—empowers auditors to identify patterns and correlations that would remain undetected through manual processes. For instance, AI systems can analyze thousands of credit card transactions to uncover hidden correlations between spending behaviors and default risks, challenging the completeness of a bank's risk assessment models (Friedlich, M.). Similarly, machine learning algorithms can automate scenario analyses, evaluating hundreds of economic variables such as interest rates, unemployment trends, and GDP growth to assess the robustness of an organization's financial forecasts (Deloitte, 2024). These capabilities underscore how digital tools augment auditors' analytical prowess, enabling them to focus on high-value tasks such as interpreting results, evaluating qualitative factors, and advising stakeholders on risk mitigation strategies.

The evolution of digital technologies has also reshaped the risk landscape, introducing novel challenges that demand auditors' expertise in both technical and ethical domains. Cybersecurity threats, data privacy breaches, and ethical dilemmas stemming from biased AI models or unethical data practices have emerged as critical concerns (IFAC, 2022; IIA, 2024). Auditors must now assess risks associated with the design and implementation of digital tools, such as ensuring AI decision models are free from biases or verifying compliance with information privacy policies in IoT ecosystems (KPMG, 2022; Busulwa and Evans, 2021). For example, an auditor reviewing a company's AI-driven hiring platform might need to evaluate whether the algorithm perpetuates gender or racial biases, requiring a blend of technical knowledge and ethical judgment. Similarly, the proliferation of blockchain in supply chain management necessitates audits of distributed ledgers to ensure transparency and accuracy, while IoT devices in manufacturing environments require checks for data integrity and adherence to operational standards (Deloitte, 2024). These complexities highlight the growing interdependence between auditors and technology teams, as audits increasingly involve evaluating the architecture of information systems and the integration of digital tools across organizational ecosystems (Protiviti, 2022). Furthermore, the COSO internal control framework retains its relevance in this digital age by emphasizing the importance of disciplined process design prior to automation. The framework acknowledges that technology can enhance internal controls by standardizing workflows and reducing human error, but it cautions against automating poorly designed processes, which could amplify risks rather than mitigate them (COSO, 2017). This principle is critical in contexts such as robotic process automation (RPA), where automating flawed financial controls could lead to systemic errors or vulnerabilities.

The role of internal auditors has expanded beyond traditional assurance functions to encompass advisory responsibilities, particularly in guiding organizations through digital transformation initiatives. Boards and senior management increasingly rely on internal audit functions to evaluate the strategic risks of emerging technologies, whether in adopting cloud computing, deploying AI for operational optimization, or enhancing cybersecurity frameworks (KPMG, 2022). For instance, internal auditors may collaborate with IT departments to assess the risks of migrating sensitive data to cloud platforms, ensuring compliance with regulatory standards and evaluating third-party vendor reliability. This advisory role is further exemplified in the hospitality industry, where auditors use AI and data analytics to protect customer data, monitor system vulnerabilities, and ensure compliance with privacy regulations. Similarly, banks leverage advanced analytics to identify high-risk transactions and customers, employing AI-driven solutions to refine risk detection algorithms and improve audit prioritization (Deloitte, 2024). These examples illustrate how auditors are transitioning from reactive evaluators to proactive advisors, leveraging digital tools to provide real-time insights and strategic recommendations.

Despite these advancements, the adoption of digital technologies in internal audit practices faces significant barriers. A pervasive skills gap remains a critical challenge, as many audit teams lack expertise in advanced analytics, AI, machine learning, and process mining (Barr-Pulliam et al., 2022). The Protiviti survey (2022) revealed that only 7% of internal audit practitioners actively use advanced AI in their work, despite 74% acknowledging its importance for the future of the profession (IIA, 2024). This disparity underscores the urgency of upskilling initiatives and the need

for universities and professional bodies to integrate digital competencies into audit curricula. Resistance to change further exacerbates adoption challenges, particularly in organizations with entrenched manual processes or hierarchical cultures. Algorithm aversion—a tendency among auditors to distrust AI-generated recommendations—also hinders progress, as professionals may discount machine-derived insights in favor of traditional judgment-based approaches (Barr-Pulliam et al., 2022). Overcoming this bias requires cultural shifts, targeted training, and demonstrable proof of technology's reliability through pilot projects and case studies. Smaller firms face additional hurdles, such as limited budgets for cutting-edge tools and reliance on off-the-shelf solutions that may lack customization, placing them at a competitive disadvantage compared to larger organizations with dedicated innovation teams (Barr-Pulliam et al., 2022). Regulatory uncertainties further complicate adoption, as auditors grapple with evolving standards for digital audits, data privacy laws, and ethical guidelines for AI. For example, the lack of clear regulatory frameworks for auditing cryptographic assets or AI models creates ambiguity, deterring firms from fully embracing these technologies (Busulwa and Evans, 2021).

Regional disparities in digital adoption further illustrate the uneven pace of transformation. A study in Serbia found that digitalization positively influenced audit quality by enhancing auditors' technical capabilities and stakeholders' perceptions of audit reliability, though regulatory changes had minimal impact (Vuković et al., 2023). This suggests that cultural, economic, and infrastructural factors play a significant role in shaping digital readiness. In contrast, regions with robust technological infrastructure and supportive regulatory environments may experience faster adoption of tools like blockchain and continuous auditing systems. Such variations highlight the need for context-specific strategies, where auditors tailor digital solutions to local regulatory landscapes, organizational cultures, and resource availability.

The integration of digital tools also redefines the value proposition of internal audit functions. By automating repetitive tasks such as data entry, transaction matching, and compliance checks, technologies like RPA free auditors to focus on strategic activities such as risk governance, stakeholder education, and real-time decision support (Cong et al., 2018). For example, auditors can dedicate more time to advising management on emerging risks, such as the ethical implications of AI or the cybersecurity threats posed by remote work environments. Continuous auditing platforms enable real-time risk detection and remediation, allowing organizations to address vulnerabilities before they escalate into crises (Mani, 2023). Additionally, digital tools enhance transparency and communication with stakeholders. Advanced visualization tools, such as dashboards and heat maps, allow auditors to present complex data in accessible formats, fostering clearer dialogue with audit committees and executives (Betti et al., 2021). This shift toward proactive, insight-driven auditing aligns with the evolving expectations of stakeholders, who demand greater agility and foresight in risk management.

The academic literature underscores the disruptive potential of digital transformation while emphasizing the need for further research to address theoretical and practical gaps. A bibliometric analysis of 105 articles published between 1985 and 2019 identified four key research clusters: continuous auditing, fraud detection, data analytics, and technological innovation (Pizzi et al., 2021). The surge in publications—peaking at 23 articles in 2020—reflects growing scholarly interest in the intersection of digitalization and auditing. However, the analysis also reveals a need for deeper exploration of topics such as the integration of blockchain into managerial control systems, the ethical implications of AI in auditing, and the long-term impacts of digital tools on audit quality.

Future studies should also investigate the evolving role of internal auditors as they balance advisory and assurance functions, particularly in industries undergoing rapid digital transformation. For instance, how do auditors maintain independence while advising on technology implementations? How can they ensure the ethical use of AI without stifling innovation? These questions warrant interdisciplinary research combining insights from auditing, computer science, ethics, and organizational behavior.

Case studies from diverse industries offer practical insights into the opportunities and challenges of digital adoption. In the banking sector, institutions use AI-driven analytics to scrutinize high-risk transactions and customers, refining their risk

models through iterative feedback loops (Deloitte, 2024). This approach not only improves audit accuracy but also enhances regulatory compliance by identifying suspicious activities in real time. In manufacturing, IoT sensors and blockchain platforms enable auditors to monitor supply chain transactions and production quality continuously, reducing the risk of fraud or operational inefficiencies. The healthcare industry presents unique challenges, such as auditing electronic health records (EHRs) for data integrity while complying with stringent privacy laws like HIPAA. Here, AI tools can anonymize patient data during audits, balancing compliance with analytical rigor (Moffitt et al., 2018). These examples demonstrate the sector-specific nuances of digital auditing, underscoring the importance of tailoring technologies to industry needs.

The COSO framework's adaptability to digitalization remains a topic of debate, yet its core principles continue to provide a robust foundation for internal controls. The framework's five components—control environment, risk assessment, control activities, information and communication, and monitoring—remain relevant, though their implementation must evolve to address digital risks (COSO, 2017). For example, the control environment must now encompass cybersecurity protocols and ethical AI governance, while risk assessments should account for threats like data breaches or algorithmic biases. Monitoring activities benefit from continuous auditing tools that provide real-time feedback on control effectiveness, enabling quicker adjustments to emerging risks. However, the framework's reliance on human judgment and manual processes in its original design poses challenges in fully automated environments. Auditors must reconcile these traditional principles with the realities of digital ecosystems, ensuring that controls are both technologically robust and aligned with organizational objectives.

Looking ahead, the internal audit profession must navigate a landscape marked by both disruption and opportunity. Success will depend on addressing skill gaps through continuous education, fostering collaboration between auditors and technology experts, and advocating for clearer regulatory guidelines. Universities and professional bodies should prioritize curricula that blend technical skills (e.g., data analytics, AI ethics) with core auditing competencies, preparing the next generation of auditors for hybrid roles. Organizations, meanwhile, must invest in scalable digital tools and cultivate a culture of innovation, encouraging auditors to experiment with new technologies while maintaining rigorous ethical standards. Regulatory bodies play a pivotal role in this ecosystem, as they must provide frameworks that balance innovation with accountability, ensuring that digital tools enhance audit quality without compromising independence or public trust.

In conclusion, digitalization is reshaping internal audit practices in profound and irreversible ways. Technologies like AI, blockchain, and data analytics are dismantling traditional barriers, enabling auditors to deliver deeper insights, faster responses, and more strategic value. Yet this transformation is not without challenges, as skill shortages, resistance to change, and regulatory ambiguities threaten to slow progress. The profession's future hinges on its ability to embrace digital tools while upholding the principles of integrity, objectivity, and skepticism that define auditing. By fostering collaboration, investing in education, and advocating for adaptive regulations, auditors can harness digitalization to navigate the complexities of the modern risk landscape and secure their role as indispensable guardians of organizational governance.

4. THE RISKS OF DIGITALIZATION AND THE TRANSFORMATION OF INTERNAL AUDIT PRACTICES

The rapid adoption of digital technologies, including artificial intelligence (AI), robotic process automation (RPA), and cloud computing, has redefined organizational operations. While these innovations promise efficiency and competitive advantage, they also introduce multifaceted risks that demand robust governance. Internal audit functions, as highlighted by KPMG (2022), are at the forefront of this transformation, tasked with balancing innovation with risk mitigation. This article systematically examines the risks of digitalization, focusing on internal audit practices, and integrates insights from academic and industry literature to propose mitigation strategies.

4.1. Technological Risks

Data Integrity and Privacy Concerns: Digital audits rely heavily on data extracted from diverse sources, including cloud platforms, IoT devices, and enterprise systems. While this data-driven approach enhances analytical capabilities, it raises

significant concerns about data integrity and privacy. Vitali and Giuliani (2024) highlight that improper integration of AI and big data analytics can compromise data accuracy, particularly when algorithms process unstructured or unverified datasets. For instance, automated systems may inadvertently propagate errors if input data is corrupted or incomplete, leading to flawed audit conclusions. Privacy risks are also equally critical. Digital environments, by their nature, increase exposure to unauthorized access and data breaches. Lois et al. (2020) emphasize the necessity of robust data governance frameworks to safeguard sensitive financial and operational information, especially as cyber threats like ransomware escalate. KPMG (2022) reports that a breach in confidentiality not only incurs financial penalties but also damages organizational reputation, as seen in high-profile cases like the 2017 Equifax breach, where inadequate security measures led to the exposure of 147 million records (FTC, 2024).

Algorithmic Fairness and Bias: The deployment of AI in auditing introduces the risk of algorithmic bias, a phenomenon where machine learning models trained on skewed datasets produce discriminatory or unfair outcomes. Guo et al. (2024) identify the "black box" nature of AI systems as a key challenge, where opaque decision-making processes obscure the rationale behind audit findings. For example, an AI model trained on historical audit data reflecting past biases might disproportionately flag transactions from specific regions or demographics, perpetuating systemic inequities. Leocádio et al. (2025) argue that transparency and continuous monitoring are essential to ensure algorithmic fairness. Auditors must adopt explainable AI (XAI) tools to demystify algorithmic decisions and validate their ethical alignment. This is particularly crucial in sectors like banking, where biased credit-scoring algorithms have drawn regulatory scrutiny.

Cybersecurity Threats: The digitization of audit processes increases vulnerability to cyberattacks, including ransomware, phishing, and insider threats. Mani (2023) identifies operational technology (OT) environments as high-risk zones due to interconnected systems. KPMG (2022) underscores the security risks inherent in operational technology (OT) environments, where interconnected systems create multiple attack vectors. A 2023 report by IBM estimates the average cost of a data breach at $4.45 million, with sectors like healthcare and finance being prime targets (IBM, 2023). To mitigate these risks, organizations must implement advanced security measures such as end-to-end encryption, multi-factor authentication, and zero-trust architectures. Regular penetration testing and real-time threat detection systems are equally vital. For example, the 2021 Colonial Pipeline ransomware attack demonstrated the catastrophic consequences of inadequate cybersecurity protocols, disrupting fuel supplies across the U.S. East Coast (CISA, 2023).

4.2. Human and Organizational Risks

Skills Gap in Audit Teams: A pressing challenge in digital auditing is the shortage of auditors proficient in emerging technologies. The ISACA (2024) survey reveals that 18% of internal audit leaders cite significant talent gaps in areas like AI, blockchain, and data analytics (Mani, 2023). This skills deficit hampers the ability to assess risks associated with complex systems, such as smart contracts or decentralized finance (DeFi) platforms (Adamyk et al., 2025). Addressing this gap requires a dual approach: upskilling existing staff through targeted training programs and recruiting specialists with hybrid expertise in accounting and IT (KPMG, 2022). For instance, certifications like Certified Information Systems Auditor (CISA) and Certified Data Privacy Solutions Engineer (CDPSE) are increasingly prioritized by firms seeking to build tech-savvy audit teams (Mani, 2023).

Over-reliance on Technology: While digital tools enhance audit efficiency, excessive dependence on automation risks eroding professional skepticism. Guo et al. (2024) warn that mechanized evaluations may overlook nuanced anomalies detectable only through human judgment. For example, AI-driven fraud detection systems might miss subtle indicators of collusion, such as irregular communication patterns between employees. This over-reliance is exacerbated by the "black box" effect, where auditors uncritically accept algorithmic outputs without questioning their validity. To counteract this, firms must foster a culture of critical inquiry, encouraging auditors to complement technological insights with contextual analysis (KPMG, 2022).

Workforce Reduction and Structural Shifts: Automation is reshaping audit labor markets, with routine tasks like transaction reconciliation increasingly delegated to RPA bots. Vitali and

Giuliani (2024) cite a 94% probability of automation displacing accountants and auditors, based on Frey and Osborne's (2017) occupational susceptibility model. This shift is altering organizational hierarchies, with demand rising for roles like IT auditors and data scientists. However, this transformation risks widening the competitive gap between large and small firms. Big4 audit firms, which audit 88% of listed companies in Italy (Vitali & Giuliani, 2024), can invest heavily in AI tools, while smaller firms struggle to keep pace. Such disparities threaten market diversity and audit quality, particularly for SMEs reliant on affordable services.

4.3. Regulatory and Compliance Risks

Regulatory Uncertainty: The rapid pace of technological innovation often outstrips regulatory frameworks, creating ambiguity for auditors. The International Federation of Accountants (IFAC, 2022) notes that inconsistent guidelines on AI ethics and data privacy can lead to non-compliance, even when firms act in good faith. For example, the EU's General Data Protection Regulation (GDPR) mandates strict data handling protocols, yet auditors face challenges in applying these rules to decentralized technologies like blockchain. Proactive engagement with regulators is essential to bridge this gap. Industry consortia, such as the Global Legal Entity Identifier Foundation (GLEIF), are advocating for standardized digital audit protocols to harmonize cross-border compliance (KPMG, 2022).

4.4. Operational Risks

Information Overload: Digital tools generate vast data volumes, overwhelming auditors' cognitive capacities. IFAC (2022) highlights that diagnostic analytics, while powerful, can produce excessive anomalies during full population testing. For instance, analyzing millions of transactions in real-time may obscure critical red flags amid noise. Effective data management strategies, such as tiered analytics and visualization dashboards, are needed to prioritize high-risk areas. Tools like Tableau and Power BI enable auditors to distill complex datasets into actionable insights, mitigating the risk of decision paralysis.

Expectation Gaps: Clients increasingly demand comprehensive assurances from digital audits, expecting technologies like blockchain to enable real-time, 100% transaction coverage. However, IFAC (2022) observes tensions when audit fees fail to align with these heightened expectations. Traditional sampling methods, though cost-effective, may no longer satisfy stakeholders accustomed to instant, granular insights. Clear communication is critical to managing these gaps. Audit firms must educate clients on the limitations of technology, balancing innovation with pragmatic resource allocation.

Disparity in Technology Adoption: The digital divide between large and small firms poses systemic risks to audit quality. Vitali and Giuliani (2024) note that 95% of Italian firms are SMEs, yet Big4 auditors dominate the market due to their technological edge. This disparity creates entry barriers for smaller players, stifling competition and innovation. Public-private partnerships could democratize access to advanced tools. Initiatives like the AICPA's Dynamic Audit Solution aim to provide affordable AI platforms for non-Big4 firms, fostering a more equitable ecosystem.

Addressing the multifaceted risks of digitalization requires a holistic approach that integrates workforce development, ethical governance, regulatory collaboration, and cybersecurity enhancements. ISACA (2024) and KPMG (2022) emphasize the urgency of upskilling audit teams through hybrid training programs that combine technical competencies in AI, blockchain, and data analytics with traditional auditing expertise, supported by certifications such as CISA and CDPSE. To mitigate algorithmic bias and ensure ethical AI adoption, Leocadio et al. (2025) propose implementing frameworks for algorithmic transparency, including explainable AI (XAI) tools and independent audits of AI systems to validate fairness and accountability.

Regulatory uncertainty, as noted by IFAC (2022), can be alleviated through proactive collaboration between auditors and policymakers, including the creation of regulatory sandboxes to test emerging technologies under supervised conditions. Additionally, Mani (2023) underscores the importance of advanced cybersecurity measures, such as adopting NIST frameworks, conducting regular penetration testing, and deploying zero-trust architectures, to safeguard digital audit processes from escalating cyber threats. By harmonizing these strategies—investing in human capital, fostering ethical technology use, engaging with regulators, and fortifying security—organizations can navigate the complexities of digital transformation while maintaining audit integrity and stakeholder trust.

The evolving landscape of digitalization in internal audit demands not only immediate mitigation strategies but also forward-looking research to address persistent and emerging challenges. Future studies must prioritize interdisciplinary investigations into the ethical implications of AI, particularly the "AI divide," which threatens audit fairness through embedded biases in algorithmic decision-making. Techniques such as adversarial debiasing, which actively counteract discriminatory patterns in training data, warrant rigorous exploration to enhance algorithmic equity and transparency. Simultaneously, bridging the technology adoption gap remains critical, especially for SMEs that lack the resources of larger firms.

Research into cost-effective solutions—such as open-source platforms and cloud-based audit tools—could democratize access to advanced technologies, fostering inclusivity and reducing market disparities. Equally vital is the study of human-machine collaboration, where optimal workflows could redefine audit efficiency by allocating data-intensive tasks to AI while reserving nuanced, judgment-driven analyses for human auditors. These research avenues directly respond to the dual challenges of digitalization: enhancing technological capabilities while safeguarding ethical standards and accessibility.

In parallel, internal audit functions must navigate a complex web of vulnerabilities, from data integrity breaches and cyber threats to workforce displacement and regulatory ambiguities. Success in this dynamic environment hinges on agility, continuous upskilling, and the ethical integration of emerging technologies. By embracing adaptive methodologies—such as real-time risk assessments and collaborative regulatory sandboxes—audit teams can transcend their traditional compliance roles. This evolution positions internal audit as a strategic partner, capable of driving organizational resilience through proactive governance and innovation. Ultimately, the path forward requires balancing technological advancement with vigilant oversight, ensuring that digital transformation not only enhances efficiency but also upholds accountability, equity, and trust in the digital age.

CONCLUSION

The digital transformation of internal audit practices represents a pivotal shift in the governance and risk management paradigms of modern organizations, necessitating a nuanced understanding of both its transformative potential and inherent challenges. This study underscores the profound impact of technologies such as artificial intelligence (AI), blockchain, and robotic process automation (RPA) in redefining the scope, efficiency, and strategic relevance of internal auditing. By transitioning from manual, retrospective evaluations to dynamic, data-driven methodologies, auditors are now equipped to deliver real-time insights, enhance fraud detection, and foster organizational resilience. However, this evolution is not without its complexities. The integration of digital tools introduces multifaceted risks—cybersecurity vulnerabilities, algorithmic biases, and ethical dilemmas—that demand a balanced approach to innovation. The findings of this research contribute significantly to the existing literature by bridging the gap between technological optimism and critical risk assessment, offering a holistic framework that synthesizes the opportunities and challenges of digitalization in auditing. Previous studies have often focused on isolated aspects of this transformation, such as the technical functionalities of AI or the procedural benefits of automation, but this work provides a comprehensive analysis that contextualizes these advancements within the broader landscape of organizational governance, regulatory compliance, and ethical responsibility.

The importance of this topic cannot be overstated, as digitalization transcends mere operational efficiency to redefine the very role of auditors. No longer confined to compliance and assurance, auditors are increasingly positioned as strategic advisors who navigate the ethical implications of AI, validate the integrity of blockchain systems, and mitigate risks in cloud-based ecosystems. For instance, the adoption of AI-driven analytics in institutions like JPMorgan Chase has revolutionized transaction monitoring, reducing fraud losses by leveraging machine learning to detect anomalies across billions of daily transactions. Similarly, Walmart's blockchain implementation has transformed supply chain audits, slashing traceability timelines and enhancing transparency (JPMorgan, 2023). These examples illustrate the tangible benefits of digital tools while also highlighting the imperative for auditors to cultivate hybrid competencies that marry technical proficiency with ethical discernment. The study's contribution lies in its

dual focus: it not only charts the technological advancements reshaping the field but also interrogates the societal implications of these changes, such as the reinforcement of systemic biases through flawed AI models or the erosion of privacy in data-intensive audits. By foregrounding these issues, the research calls for a reimagined audit paradigm that prioritizes transparency, accountability, and inclusivity.

For practitioners, the implications are clear. The adoption of digital tools must be accompanied by robust upskilling initiatives to address the glaring skills gap in areas such as AI ethics, cybersecurity, and data analytics. Organizations should invest in continuous professional development programs, fostering partnerships with academic institutions and certification bodies to ensure auditors are proficient in emerging technologies. The implementation of ethical frameworks, such as Explainable AI (XAI), is critical to demystifying algorithmic decision-making and ensuring audits remain transparent and equitable. Practitioners must also advocate for interdisciplinary collaboration, engaging with IT specialists, data scientists, and ethicists to design audit systems that are both technologically robust and socially responsible. For instance, the integration of XAI in credit-scoring audits could mitigate biases that disproportionately affect marginalized communities, thereby aligning technological innovation with equitable outcomes.

Policymakers, on the other hand, face the urgent task of crafting regulatory frameworks that keep pace with technological innovation while safeguarding public interest. The current regulatory landscape, characterized by fragmentation and 滞后, struggles to address the complexities of auditing decentralized finance (DeFi) platforms or cryptographic assets. Initiatives such as the EU's Digital Operational Resilience Act (DORA) represent a step forward in mandating stringent IT risk protocols, but gaps persist, particularly in jurisdictions with limited resources to enforce compliance. Policymakers should prioritize the development of global standards for digital audits, leveraging international bodies like the International Auditing and Assurance Standards Board (IAASB) to harmonize regulations. Regulatory sandboxes—controlled environments for testing emerging technologies—could serve as a pragmatic solution, allowing auditors and firms to experiment with blockchain or AI tools under supervised conditions. Additionally, legislation must address the ethical dimensions of AI, mandating audits of algorithmic systems for fairness and transparency, particularly in sectors like healthcare and finance where biased outcomes can have life-altering consequences.

To the academic community, this study underscores the need for interdisciplinary research that bridges auditing with fields such as computer science, ethics, and organizational behavior. Future investigations should explore the long-term impacts of AI on audit quality, examining whether the efficiency gains of automation compromise the depth of human judgment in detecting nuanced fraud patterns. Comparative studies across industries and regions could elucidate the socio-economic factors influencing digital adoption, offering insights into why certain sectors, such as banking, lead in AI integration while others lag. The ethical implications of blockchain's energy consumption and its alignment with sustainability goals also warrant further scrutiny. Moreover, the development of universal metrics for assessing algorithmic fairness in audits remains an open challenge, requiring collaboration between technologists and ethicists to create standardized evaluation frameworks. Another promising avenue is the exploration of human-AI collaboration models, where auditors and machines complement each other's strengths—AI handling data-intensive tasks while humans focus on contextual interpretation and ethical oversight.

The societal ramifications of this digital shift extend beyond organizational efficiency to influence public trust in financial systems. As audits become more transparent through blockchain's immutable ledgers or more responsive through real-time analytics, stakeholders—from investors to consumers—gain greater confidence in the integrity of financial reporting. Yet, this trust is fragile, contingent on auditors' ability to navigate the ethical quagmires posed by digital tools. A single instance of algorithmic bias or a high-profile data breach could undermine years of progress, emphasizing the need for vigilance and proactive risk management. The study's recommendations, therefore, advocate for a balanced approach: embracing innovation while embedding ethical considerations at every stage of the audit lifecycle.

In conclusion, the digital transformation of internal auditing is both a revolution and a reckoning—a revolution in its potential to enhance accuracy,

transparency, and strategic value, and a reckoning in its demand for ethical rigor, regulatory foresight, and human adaptability. The contributions of this research lie in its synthesis of these dualities, offering a roadmap for auditors, organizations, and policymakers to navigate this complex terrain. By prioritizing hybrid skill development, ethical governance, and collaborative innovation, the audit profession can not only survive but thrive in the digital age. Future research must build on this foundation, exploring uncharted areas such as the cultural resistance to automation within audit firms, the role of auditors in shaping AI policy, and the intersection of digital tools with global sustainability agendas. As the pace of technological change accelerates, the imperative for continuous learning and adaptive governance becomes ever more critical, ensuring that the evolution of internal auditing remains aligned with the principles of integrity, accountability, and public trust that define its core mission.

REFERENCES

ACCA (Association of Chartered Certified Accountants). (2023). The future of audit skills. https://www.accaglobal.com/content/dam/ACCA_Global/Technical/audit/ea-future-of-audit.pdf

ACFE (The Association of Certified Fraud Examiners). (2023). Report to the Nations on Occupational Fraud and Abuse. https://www.acfe.com/fraud-resources/global-fraud-survey

Adamyk, B., Benson, V., Adamyk, O., & Liashenko, O. (2025). Risk Management in DeFi: Analyses of the Innovative Tools and Platforms for Tracking DeFi Transactions. *Journal of Risk and Financial Management*, *18*(1), 38. https://doi.org/10.3390/jrfm18010038

Alexander, A. (2021). The future, faster: The COVID-19 pandemic has accelerated the ongoing change in auditing to whole new levels. *Accounting Today*. https://arizent.brightspotcdn.com/ff/16/daf680eb4ebdaf9e3d5634c59a07/technology-and-the-revolution-1.pdf

Barr-Pulliam, D., Brown-Liburd, H. L., & Sanderson, K.-A. (2022). The effects of person-specific, task, and environmental factors on digital transformation and innovation in auditing: A review of the literature. *Journal of International Financial Management & Accounting*. https://doi.org/10.1111/jifm.12159

Betti, N., Sarens, G., & Poncin, A. (2021). Effects of digitalisation of organisations on internal audit activities and practices. *Managerial Auditing Journal, 36*(7), 868-887. https://doi.org/10.1108/MAJ-08-2020-2792

Boritz, J. E., & Stratopoulos, T. C. (2023). AI and the accounting profession: Views from industry and academia. *Journal of Information Systems*, *37*(3), 1-9. https://doi.org/10.2308/ISYS-2023-054

Busulwa, R., & Evans, N. (2021). *Digital transformation in accounting*. Routledge. https://doi.org/10.4324/9780429344589

CISA (America's Defence Agency). (2023). The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

Cong, Y., Du, H., & Vasarhelyi, M. A. (2018). Technological disruption in accounting and auditing. *Journal of emerging technologies in Accounting*, *15*(2), 1-10. https://doi.org/10.2308/jeta-10640

COSO (The Committee of Sponsoring Organizations). (2017). COSO ERM Framework https://www.coso.org/erm-framework

Deloitte. (2024). Managing algorithmic risks. https://www2.deloitte.com/us/en/pages/risk/articles/algorithmic-machine-learning-risk-management.html

European Commission. (2023). *Digital Operational Resilience Act (DORA)*. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

EY (Ernst & Young Global Limited). (2023). https://www.ey.com/en_gl/insights/assurance/global-audit-quality-report

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines, 31*(1), 689–707. https://doi.org/10.1007/s11023-018-9482-5

Frey, C. B., & Osborne, M. A. (2017). The future of employment: How susceptible are jobs to computerisation?. *Technological forecasting and social change*, *114*, 254-280. https://doi.org/10.1016/j.techfore.2016.08.019

Friedlich, M. (2024). *Assessing credit losses in financial statement audits*. https://www.accountingtoday.com/opinion/assessing-credit-losses-in-financial-statement-audits-a-guide-for-auditors

FTC (Federal Trade Comission). (2024). *Equifax Data Breach Settlement*. https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement

Guo, R., Jia, Y., & Shentu, L. (2024). The effect of audit digital transformation on audit quality: evidence from digital bank confirmations. *China Journal of Accounting Studies*, 1–35. https://doi.org/10.1080/21697213.2024.2442769

Harvard Business Review. (2023). *Siemens AG: A Private Equity Approach Within an Industrial Corporation?*. https://store.hbr.org/product/siemens-ag-a-

private-equity-approach-within-an-industrial-corporation/723420

HSBC. (2024). *Harnessing the power of AI to fight financial crime*. https://www.hsbc.com/news-and-views/views/hsbc-views/harnessing-the-power-of-ai-to-fight-financial-crime

IBM. (2023). *Cost of a Data Breach Report*. https://www.ibm.com/reports/data-breach

IIA (The Institute of Internal Auditors). (2024). *Internal Audit Funding Vision 2035*. https://www.theiia.org/globalassets/site/foundation/latest-research-and-products/vision-2035-report.pdf

IFAC (International Federation of Accountants). (2022). *Digital transformation & innovation in auditing: Insights from a review of academic research*. https://www.ifac.org/knowledge-gateway/discussion/digital-transformation-innovation-auditing-insights-review-academic-research

ISACA (the Information Systems Audit and Control Association). (2024). *State of Internal Audit*. https://www.theiia.org/globalassets/site/foundation/latest-research-and-products/vision-2035-report.pdf

JPMorgan. (2023). *How AI will make payments more efficient and reduce fraud*. https://www.jpmorgan.com/insights/payments/payments-optimization/ai-payments-efficiency-fraud-reduction

KPMG (Klynveld Peat Marwick Goerdeler). (2022). *Technology internal audit and beyond aligning to heightened expectations*. https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2022/04/technology-internal-audit-2022-and-beyond.pdf

Leocádio, D., Malheiro, L., & Reis, J. C. G. D. (2025). Auditors in the digital age: a systematic literature review. *Digital Transformation and Society*, *4*(1), 5-20. https://doi.org/10.1108/DTS-02-2024-0014

Lois, P., Drogalas, G., Karagiorgos, A., & Tsikalakis, K. (2020). Internal audits in the digital era: opportunities risks and challenges. *EuroMed Journal of Business*, *15*(2), 205-217. https://doi.org/10.1108/EMJB-07-2019-0097

Lopreite, M., Mauro, S. G., Veltri, S., & Rupo, D. (2021). Assessing the impacts of digital transformation on internal auditing: A bibliometric analysis. *Technology in Society, 67*, 101738. https://doi.org/10.1016/j.techsoc.2021.101738

Maione, G. (2024). Convergence of Artificial Intelligence and Sustainable Innovation Reporting. In *Sustainable Innovation Reporting and Emerging Technologies* (pp. 29-48). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83797-739-020241003

Mani, V. (2023). Auditing and digital transformation are at a crossroads. *ISACA Journal, 2*. https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/auditing-and-digital-transformation-are-at-a-crossroads

Moffitt, K. C., Rozario, A. M. & Vasarhelyi, M. A. (2018). Robotic process automation for auditing. *Journal of Emerging Technologies in Accounting*, 15(1), 1-10. https://doi.org/10.2308/jeta-10589

PCAOB (Public Company Accounting Oversight Board). (2023). *Rules of the public company accounting oversight board*. https://pcaobus.org/Rules/Documents/PCAOB-Rules.pdf

PwC (PricewaterhouseCoopers). (2023). *Internal Audit: Risk-Based Methodology*. https://www.pwc.com/ua/en/services/corporate_trainings/assets/ia_eng.pdf

Pizzi, S., Venturelli, A., Variale, M., & Macario, G. P. (2021). Assessing the impacts of digital transformation on internal auditing: A bibliometric analysis. *Technology in Society*, *67*, 101738. https://doi.org/10.1016/j.techsoc.2021.101738

Protiviti. (2022). *Going digital: The future auditor in action*. https://www.protiviti.com/gl-en/newsletter/bulletin-v7i6-digital-future-auditor

Sewpersadh, N. S. (2025). Adaptive structural audit processes as shaped by emerging technologies. *International Journal of Accounting Information Systems*, *56*, 100735. https://doi.org/10.1016/j.accinf.2025.100735

Shamim, M. M. R. (2025). Maintenance optimization in smart manufacturing facilities: A systematic review of lean, TPM, and digitally-driven reliability models in industrial engineering. *American Journal of Interdisciplinary Studies*, *6*(1), 144-173. https://doi.org/10.63125/xwvaq502

Sharma, M., & Kumar, P. (2021). Adoption of blockchain technology: A case study of Walmart. In *Blockchain technology and applications for digital marketing* (pp. 210-225). IGI Global. https://doi.org/10.4018/978-1-7998-8081-3.ch013

Sophos. (2022). *The State of Ransomware*. https://news.sophos.com/en-us/2022/04/27/the-state-of-ransomware-2022/

Thomson Reuters. (2023). *As Problems in Global Audit Persist, SEC Chief Accountant Reminds Lead Auditors of their Responsibilities*. https://tax.thomsonreuters.com/news/as-problems-in-global-audit-persist-sec-chief-accountant-reminds-lead-auditors-of-their-responsibilities/

Umeaduma, C. M. G., & Adedapo, I. A. (2025). AI-powered credit scoring models: ethical considerations, bias reduction, and financial inclusion strategies. *International Journal of Research Publication and Reviews*, *6*(3), 6647-6661. https://doi.org/10.55248/gengpi.6.0325.12106

UNICEF. (2020). *Mapping Child Labour Risks in Global Supply Chains*. https://www.unicef.nl/files/ChildLabourinGlobalSupplyChains.pdf

Usul, H., & Alpay, M. F. (2024). From Traditional Auditing to Information Technology Auditing: A Paradigm Shift in Practices. *European Journal of Digital Economy Research*, *5*(1), 3-9. https://doi.org/10.5281/zenodo.12819118

Vitali, S., & Giuliani, M. (2024). Emerging digital technologies and auditing firms: Opportunities and challenges. *International Journal of Accounting Information Systems*, *53*, 100676. https://doi.org/10.1016/j.accinf.2024.100676

Verizon. (2023). *Data Breach Investigations Report*. https://www.verizon.com/dbir/

Verge. (2024). Microsoft overhaul treats security as 'top priority' after a series of failures. https://www.theverge.com/2024/5/3/24147883/microsoft-security-priority-executive-compensation-goals

Vuković, B., Jakšić, D., & Milojević, I. (2023). The impact of digitalization on audit. In *Digitalization in Finance and Accounting* (pp. 27-37). Springer. https://doi.org/10.1007/978-3-031-23269-5_3

World Economic Forum. (2023). https://www.weforum.org/meetings/world-economic-forum-annual-meeting-2023/