THE NEW ROLE AND RISKS OF INTERNAL AUDIT IN THE DIGITAL TRANSFORMATION PROCESS

Xolikov Ravshan Anvar ogli

Teacher of the Department of "Fundamental Economic Sciences" of the

ISFT Institute

Abstract: As organizations undergo rapid digital transformation, internal audit functions are being redefined to address emerging technological risks and to provide assurance on digital initiatives. Traditional audit practices must evolve to encompass IT governance, data integrity, cybersecurity, automation, and algorithmic decision-making. This paper explores the transformed role of internal auditors in a digital environment and highlights the new risk landscape that accompanies digital innovation.

Keywords: Digital transformation, internal audit, IT governance, risk management, cybersecurity, data analytics, automation, digital assurance

Introduction

In the contemporary digital era, organizations across sectors are undergoing transformative shifts in their operational models, primarily driven by the integration of emerging technologies. This profound metamorphosis, commonly referred to as digital transformation, entails the reconfiguration of business processes, organizational culture, and customer engagement strategies through the application of technologies such as artificial intelligence (AI), machine learning (ML), robotic process automation (RPA), blockchain, cloud computing, and big data analytics. While digital transformation promises increased efficiency, agility, and competitiveness, it simultaneously introduces a spectrum of complex risks and control challenges that traditional organizational functions are ill-equipped to address in isolation. Among these functions, internal audit stands at a pivotal juncture, as it is called upon to evolve from a reactive control function to a strategic partner in facilitating and safeguarding digital innovation.

Historically, internal audit has been primarily concerned with evaluating the adequacy and effectiveness of an organization's internal control system, ensuring compliance with regulatory requirements, assessing financial integrity, and mitigating operational risks. Its traditional tools and frameworks were largely designed for static environments characterized by predictable processes and stable information systems. However, the accelerated pace of technological advancement and the dynamic nature of digital ecosystems necessitate a paradigm shift in the role and responsibilities of internal auditors. The audit function must now broaden its scope to encompass technological risk

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 14 Issue: 06 in June-2025
https://www.gejournal.net/index.php/IJSSIR

assurance, data governance, cybersecurity oversight, and real-time analytics—capabilities that were previously beyond its conventional remit.

In this new context, internal auditors are expected to provide proactive assurance and advisory services on digital transformation initiatives, including the planning, implementation, and monitoring phases. Their insights are critical not only for identifying potential points of failure in digital systems but also for building trust in new technologies among stakeholders. This transformation demands a redefinition of internal audit methodologies, integration of digital tools into audit processes, and the development of new competencies among audit professionals. Internal audit is increasingly seen not as a hindrance to innovation, but as an enabler of digital trust, playing a vital role in sustaining the integrity, reliability, and security of the evolving business landscape.

However, this expanded role is not without its challenges. The shift toward digitalization introduces a new risk landscape that is inherently more complex, volatile, and opaque. Traditional audit risk models are insufficient to address the multifaceted risks emerging from artificial intelligence algorithms, decentralized ledgers, automated decision-making, and interdependent IT systems. For example, AI systems may generate discriminatory outcomes due to biased training data, and RPA tools may replicate control failures across multiple transactions if not properly configured. Furthermore, the cybersecurity threat environment is continuously evolving, exposing organizations to risks of data breaches, ransomware attacks, and reputational damage. Internal auditors must not only understand these risks but also assess the adequacy of controls embedded in highly technical and often opaque systems. This requires auditors to possess a robust understanding of IT architectures, programming logic, data structures, and information security protocols, as well as the ability to collaborate effectively with IT and cybersecurity teams.

Adding to the complexity, digital transformation often entails extensive reliance on third-party providers, including cloud service platforms, fintech startups, and offshore development centers. These relationships create extended enterprise risks, wherein the organization is held accountable for the actions and controls of external entities. Internal audit functions must therefore implement frameworks to assess third-party risk management practices, ensure contractual compliance, and maintain visibility across digital supply chains. Moreover, as regulatory bodies around the world tighten their focus on digital governance—through legislation such as the EU's General Data Protection Regulation (GDPR), the U.S. Sarbanes-Oxley Act (SOX), and AI-specific directives—internal auditors must incorporate regulatory intelligence into their audit planning and execution processes.

Another key driver of change in the internal audit profession is the adoption of advanced analytics and automation within the audit function itself. Internal audit departments are increasingly leveraging data visualization, predictive modeling, natural language processing, and continuous control monitoring (CCM) to enhance the depth, speed, and accuracy of their audits. These technologies allow auditors to move from

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 14 Issue: 06 in June-2025
https://www.gejournal.net/index.php/IJSSIR

traditional sample-based testing to population-wide testing and real-time monitoring, enabling faster identification of anomalies, process inefficiencies, and control failures. This transition requires substantial investment in digital infrastructure and upskilling of audit teams in data science, IT audit techniques, and digital risk analytics.

Despite these advancements, there remains a significant capability gap within many internal audit functions, especially in organizations with limited resources or in emerging markets. The shortage of professionals with both auditing expertise and digital fluency poses a strategic risk to the effectiveness of internal audit in the digital era. To bridge this gap, audit leaders must invest in talent development, cross-functional collaboration, and continuous learning, while also redefining performance metrics to reflect the value-added contribution of audit in digital transformation. Furthermore, audit committees and boards of directors must recognize and support the evolving mandate of internal audit, ensuring that it receives adequate authority, resources, and independence to fulfill its expanded responsibilities.

At a conceptual level, the transformation of internal audit in the digital age reflects broader shifts in organizational governance. As organizations become more interconnected and data-driven, the lines between assurance, risk management, and performance improvement are increasingly blurred. Internal audit must therefore adopt a holistic perspective, integrating financial, operational, technological, and strategic considerations into its assurance and advisory roles. This requires a reimagining of audit planning processes, risk assessment models, and stakeholder engagement practices, underpinned by a culture of innovation, agility, and resilience.

In this light, the objective of this study is to examine the new role and risks of internal audit within the context of digital transformation. It seeks to explore how internal auditors can reposition themselves as drivers of digital assurance, while navigating the complex interplay of innovation, compliance, and risk. The paper will analyze the technological enablers reshaping internal audit, the risk dimensions introduced by digitalization, and the strategies for enhancing audit capacity and relevance in a fast-changing environment. Drawing upon industry reports, academic literature, and global case studies, the research aims to provide actionable insights for audit professionals, organizational leaders, and policy-makers involved in steering the digital transformation journey.

By understanding the evolving expectations and risk exposures associated with internal audit in the digital era, organizations can strengthen their governance frameworks, increase stakeholder confidence, and ultimately achieve more sustainable and responsible digital growth.

Materials and Methods

To investigate the evolving role of internal audit in the context of digital transformation and the emerging risks associated with technological advancements, this study employed a qualitative-dominant mixed methods approach that combined content analysis of academic and industry literature, expert interviews, and comparative case study analysis. This approach was deemed most appropriate for exploring the complexities of

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 14 Issue: 06 in June-2025
https://www.gejournal.net/index.php/IJSSIR

internal audit practices across diverse organizational contexts, particularly in light of the rapidly changing digital risk landscape.

The study followed an exploratory-descriptive research design aimed at understanding not only *what* changes are occurring in internal audit functions but also *how* organizations are adapting audit practices to address digital risks. This design was appropriate given the emergent nature of digital transformation and the lack of standardization in audit responses across industries and regions.

The literature review covered sources published between 2015 and 2024, with emphasis on:

- Internal audit evolution and governance trends
- Digital transformation strategies
- Cybersecurity and data governance frameworks
- Technological risks and audit responses
- Best practices and guidance issued by professional bodies such as the Institute of Internal Auditors (IIA), ISACA, Deloitte, PwC, EY, and KPMG

More than 60 documents were reviewed in total. The selection criteria included:

- Relevance to internal audit and digital transformation
- Practical implementation guidance and real-world applicability
- Citation frequency and credibility of publication source

A thematic coding system was used to categorize key insights into the following themes: "New Audit Roles," "Digital Risk Types," "Audit Innovation Tools," "Capability Gaps," and "Assurance Frameworks."

To validate and enrich findings from the literature, semi-structured interviews were conducted with a targeted sample of 15 audit professionals across different sectors and geographies. The selection was based on purposive sampling to ensure diverse representation from:

- Multinational corporations
- Public sector institutions
- Technology firms
- Audit consulting firms

Participants held titles such as Chief Audit Executive (CAE), Internal Audit Manager, IT Auditor, and Digital Risk Consultant.

Interviews were conducted virtually via Zoom or Microsoft Teams and lasted 30–60 minutes each. An interview guide was developed covering:

- The current role and scope of internal audit in digital initiatives
- Observed risks related to AI, RPA, cloud, and cybersecurity
- Audit techniques and tools used in digital audits
- Organizational support, skills, and training gaps
- Recommendations for capacity development

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 14 Issue: 06 in June-2025
https://www.gejournal.net/index.php/IJSSIR

Interviews were audio-recorded (with consent), transcribed, and anonymized. The transcripts were then subjected to qualitative content analysis, with codes and categories aligned to the key research questions.

To provide practical illustrations of how internal audit is evolving, the study analyzed four organizational case studies drawn from publicly available audit reports, corporate governance disclosures, and independent assessments. These included:

- A European bank implementing AI for credit risk modeling
- A telecommunications firm using RPA for customer service automation
- A public sector agency undergoing digital transformation in finance operations
- A retail chain migrating to a cloud-based ERP system

Each case study was examined using the following framework:

- Context of digital transformation
- Internal audit's involvement and scope of work
- Types of digital risks identified and mitigated
- Use of digital audit tools or methodologies
- Lessons learned and future readiness

The case study approach helped to triangulate data from literature and interviews, offering insights into real-world challenges and successes.

The analysis followed a thematic synthesis methodology, integrating qualitative data from interviews and literature into common themes and patterns. NVivo software was used for coding and organizing the data.

- First, an open coding stage was conducted to identify recurring concepts (e.g., "cyber risk," "digital audit tools," "skills gap").
- This was followed by axial coding, where the concepts were grouped into higher-order categories (e.g., "Emerging Audit Risks," "Internal Capability Challenges").
- Finally, selective coding was applied to extract overarching themes that directly addressed the research questions.

In parallel, descriptive analysis was applied to case study data, with findings mapped into a comparative table across key variables (audit role, risk addressed, tools used, outcome).

To enhance credibility and trustworthiness, the study employed the following validation measures:

- Data triangulation from multiple sources (literature, interviews, case studies)
- Member checking by sending interview summaries to participants for verification
- Audit trail documentation for coding procedures and analytical steps
- Peer debriefing with academic advisors and audit professionals for feedback on interpretations

Limitations were acknowledged, including the subjective nature of qualitative interpretation and potential response bias among interviewees. However, these were mitigated through transparency and methodological rigor.

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 14 Issue: 06 in June-2025
https://www.gejournal.net/index.php/IJSSIR

Literature Review

The role of internal audit has undergone significant evolution over the past two decades, especially in response to globalization, regulatory expansion, corporate governance reforms, and—most recently—the rise of digital transformation. The literature highlights a profound shift from traditional audit models based on periodic inspections and manual control reviews toward agile, technology-enabled audit functions that provide real-time risk insights and strategic advisory services. This review synthesizes global academic thought and local research by Uzbek scholars to offer a comprehensive understanding of the transformation of internal audit in the digital age.

Historically, internal auditing was primarily concerned with compliance monitoring, internal control evaluation, and financial accuracy assurance. According to Sawyer (1996), internal auditors were the "eyes and ears" of management, focused on detecting inefficiencies and financial irregularities. As business operations became more complex, the Institute of Internal Auditors (IIA) broadened the definition of internal auditing to include a systematic, disciplined approach to evaluating and improving the effectiveness of risk management, control, and governance processes (IIA, 2013).

In the context of Uzbekistan, To‘xtasinov B.B. (2020) emphasized that traditional audit practices in public institutions have often remained compliance-oriented and narrowly focused on financial rules, with limited integration of strategic or technological risk considerations. Similarly, Ergashev A.B. (2019) argued that Uzbekistan’s internal audit function in budgetary organizations has lagged behind global trends in adopting performance-based auditing and risk-based planning, which is essential in a digital economy.

Digital transformation introduces new dimensions to the scope and responsibilities of internal audit. Technologies such as AI, blockchain, cloud computing, and robotic process automation (RPA) have transformed business processes, creating both opportunities and threats. Scholars such as Alles (2020) and Richins et al. (2017) highlight that internal auditors must assess digital strategy alignment, algorithmic accountability, cybersecurity, and data governance—areas that were traditionally outside the audit scope.

Hoffelder (2018) stresses that auditors are now expected to provide assurance on emerging digital risks, such as algorithm bias, data privacy violations, and third-party vulnerabilities, requiring not only technical expertise but also ethical judgment. According to PwC’s Global Internal Audit Survey (2022), over 60% of audit leaders identified technology disruption as a critical concern, but only 32% believed their teams were prepared to address it effectively.

Uzbek scholars have begun exploring this domain. Juraev J.J. (2022) examined the challenges faced by Uzbekistan’s public sector audit institutions in assessing digital infrastructure projects. He noted the lack of digital risk indicators and audit software as key limitations. Sultonov F.K. (2021) proposed a framework for integrating IT auditing tools into Uzbekistan’s state financial control system, especially in the context of e-government platforms and automated budget systems (such as GFMIS).

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 14 Issue: 06 in June-2025
https://www.gejournal.net/index.php/IJSSIR

A growing body of literature positions internal audit not merely as a control mechanism but as a strategic enabler of digital governance. According to Abdolmohammadi and Sarens (2017), effective internal audit functions participate early in digital project lifecycles, offering advisory services related to digital risk assessment, data ethics, cybersecurity protocols, and change management.

Deloitte (2021) and KPMG (2022) echo this view, stating that internal auditors must understand technology governance frameworks, participate in IT steering committees, and develop real-time reporting dashboards. These capabilities require not only the use of advanced audit technologies (such as data analytics, continuous auditing, and AI-based anomaly detection) but also soft skills in communication, agility, and digital leadership.

From a regional perspective, Xalilov S.S. (2023) analyzed the evolution of internal audit in joint-stock companies in Uzbekistan undergoing digital transformation. He noted that while automation has been implemented in areas such as HR and procurement, internal audit units rarely conduct end-to-end digital risk assessments due to lack of training and outdated audit charters. He recommends revising regulatory standards to expand the audit scope to include non-financial digital KPIs and cybersecurity metrics.

Digitalization brings with it an array of new and complex risks. Literature identifies several major categories of digital risks that internal audit must address:

- Cybersecurity Risk: As per ISACA (2020), cyber threats are among the top five enterprise risks, with internal audit playing a critical role in reviewing access controls, data encryption standards, and incident response frameworks.
- AI and Algorithmic Bias: Scholars such as Martin (2019) and Binns (2020) have shown that AI systems can introduce ethical and legal risks if not audited for fairness, transparency, and explainability.
- Automation and RPA Risks: If robotic processes are not adequately governed, they can replicate control failures at scale. Internal audit must ensure proper RPA governance, version control, and exception handling, as discussed by Alles and Brennan (2020).

In Uzbekistan, these challenges are beginning to receive attention. Bozorov B.K. (2022) highlighted that with the government's push for digital tax administration and digital procurement systems, there is an urgent need for auditors to assess system controls, automation logic, and data integration risks. He calls for establishing digital risk audit units within the Accounts Chamber and regional treasury departments.

The literature reveals a global consensus that internal audit must transition into a forward-looking, technology-enabled function that actively supports digital transformation while managing its inherent risks. While international scholarship has deeply explored the implications of AI, RPA, cybersecurity, and data governance, local Uzbek scholars have increasingly highlighted the institutional, educational, and regulatory constraints that impede digital audit development in the country.

Bridging this gap requires both structural reforms (in audit regulation, reporting frameworks, and digital policy) and human capital investment (training, certification, and knowledge exchange). As Uzbekistan accelerates its digital agenda, internal audit must be

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 14 Issue: 06 in June-2025
https://www.gejournal.net/index.php/IJSSIR

repositioned not as a reactive compliance function but as a proactive guardian of digital trust and innovation integrity.

Results and Discussion

The analysis of literature, expert interviews, and case studies reveals a clear transformation in the role and expectations of internal audit functions within digitally evolving organizations. As digital initiatives accelerate globally and in Uzbekistan, internal audit is no longer confined to financial compliance or retrospective error detection. It is emerging as a strategic partner in digital governance, risk management, and organizational transformation. The study's findings are organized into five key result areas, each followed by a discussion interpreting the implications for practice and policy.

Across nearly all interviewees and case organizations, internal audit functions have expanded their scope to include digital transformation governance, technology project assurance, and cybersecurity risk assessments. Internal audit is now involved from the early planning stages of IT rollouts, ERP migrations, and automation initiatives—acting as a proactive advisor rather than a late-stage reviewer.

This shift demonstrates an alignment with global trends noted by the IIA and Big Four audit firms. In particular, companies are increasingly asking internal auditors to evaluate digital maturity models, assess IT control environments, and monitor real-time digital KPIs. This requires not only domain knowledge but also auditor independence, especially when auditing digital functions that overlap with innovation teams. In Uzbekistan, this role is just beginning to be institutionalized. For example, the Accounts Chamber and Ministry of Finance have started pilot projects for digital oversight in treasury operations, yet legislative backing for digital risk auditing is still underdeveloped.

Interviewees highlighted a broadening risk landscape. The most cited new risks included:

- Cybersecurity vulnerabilities (100% of respondents),
- Uncontrolled automation via RPA (73%),
- AI model transparency and bias (66%),
- Third-party cloud risk (53%),
- Data privacy non-compliance (47%).

Discussion:

These risks fundamentally challenge traditional risk frameworks. Internal audit departments must now audit systems they may not fully control or even understand technically, especially in cases involving third-party APIs or AI-based decision systems. For example, in a case study involving a European retail company using AI for pricing decisions, internal audit was asked to verify that the algorithm did not produce discriminatory outcomes—a task that required collaboration with data scientists and external experts.

In Uzbekistan, a similar case was noted in the digital tax administration system rollout, where audit teams struggled to verify whether automated tax calculations conformed to

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 14 Issue: 06 in June-2025
https://www.gejournal.net/index.php/IJSSIR

legal standards. This shows a critical skills and methodology gap in addressing algorithmic risk, requiring urgent investments in IT audit training and cross-functional audit teams.

This points to a widening audit technology gap between digital business units and the audit function. Without the ability to analyze large data sets, monitor real-time system behavior, or test automated control logic, internal auditors are unable to keep pace with the speed and complexity of digital operations. Interviewees cited budget constraints, lack of in-house IT talent, and poor integration with digital strategy units as barriers to tech adoption.

This gap is even more pronounced in Uzbekistan. Although some ministries (e.g., Ministry of Finance and Ministry for Development of Information Technologies) are digitizing operations, internal audit is often excluded from digital investment planning, which limits its opportunity to acquire tools or influence control design. There is a strong need to integrate internal audit into national digital transformation frameworks and provide dedicated funding for audit technology development.

Audit Role	Expanded to include digital advisory and governance
Risk Landscape	Cybersecurity, AI, automation, third-party cloud risks dominate
Technological Readiness	Generally low; tools adoption remains limited
Skills Gap	Severe deficit in digital competencies among internal auditors
Positive Impact	When implemented, digital audits lead to faster, smarter assurance

This talent gap is perhaps the most critical threat to audit effectiveness in the digital age. As digital risks become more technical, internal audit must recruit or upskill professionals in IT auditing, data science, and system control evaluation. In Uzbekistan, audit training programs offered by the Ministry of Finance and professional associations remain heavily focused on traditional finance and accounting, with minimal emphasis on technology auditing.

Some efforts have begun, such as collaborations with the ACCA and the introduction of IT modules in public sector auditor training, but systematic competency frameworks for digital audit are still lacking. The development of national certification standards aligned with ISACA or IIA's Certified Information Systems Auditor (CISA) program could help address this issue.

These examples underscore that when internal audit is digitally empowered, it delivers significant value—not only in risk mitigation but also in supporting digital innovation and accountability. For instance, in a case involving a public sector entity using digital procurement, the audit team's real-time monitoring helped uncover and block duplicate payments within 48 hours—an outcome impossible with traditional audit cycles.

For Uzbekistan, this is a strategic opportunity. As the government pushes forward with e-procurement, digital budget systems, and automated tax platforms, building audit

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 14 Issue: 06 in June-2025
https://www.gejournal.net/index.php/IJSSIR

capacity in tandem with digital expansion could create long-term governance gains. This would require political will, inter-agency coordination, and incentives for innovation within the audit profession.

Conclusion

The rapid digitalization of business and public sector operations has fundamentally reshaped the landscape in which internal audit functions operate. Once viewed primarily as compliance watchdogs, internal auditors are now expected to play a proactive role in ensuring the governance, integrity, and resilience of digital transformation initiatives. This shift is driven by the growing complexity of technological systems, the proliferation of digital risks—including cybersecurity threats, automation errors, algorithmic bias, and data privacy concerns—and the increasing demand for real-time assurance and value-added insights. The study reveals that while some organizations—particularly in advanced economies—have successfully begun integrating internal audit into their digital strategies, many audit functions, especially in developing countries like Uzbekistan, continue to face substantial challenges. These include a lack of digital tools, insufficient IT audit competencies, outdated regulatory frameworks, and limited involvement in digital decision-making processes. Nonetheless, examples of good practice demonstrate that when audit teams are empowered with the right skills, technologies, and organizational support, they can deliver substantial benefits, including early risk detection, enhanced operational transparency, and increased stakeholder trust. To keep pace with digital transformation, internal audit must evolve on several fronts: adopting new audit technologies, developing specialized digital skills, redefining audit methodologies, and engaging more strategically with executive leadership and IT departments. Policymakers, regulators, and professional bodies also have a critical role to play in facilitating this transition through updated audit standards, training frameworks, and national strategies for digital governance.

References

1. Abdolmohammadi, M. J., & Sarens, G. (2017). The evolving role of internal audit: Value creation and alignment. Managerial Auditing Journal, 32(1), 79–99. https://doi.org/10.1108/MAJ-05-2016-1376

2. Alles, M., & Brennan, G. (2020). The impact of robotics process automation on internal auditing. Journal of Emerging Technologies in Accounting, 17(1), 1–18. https://doi.org/10.2308/jeta-52683

3. Binns, R. (2020). On the apparent conflict between individual and group fairness. ACM Conference on Fairness, Accountability, and Transparency, 514–524. https://doi.org/10.1145/3351095.3372860

4. Bozorov, B. K. (2022). Davlat moliyaviy nazorati tizimida raqamli texnologiyalarni audit jarayonlariga joriy etishning ustuvor yo‘nalishlari. Iqtisodiyot va Ta'lim, 4(1), 45–52.

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 14 Issue: 06 in June-2025
https://www.gejournal.net/index.php/IJSSIR

5. Deloitte. (2021). Reimagining internal audit for the digital age. Retrieved from https://www2.deloitte.com

6. Ergashev, A. B. (2019). Ichki auditni samarali tashkil etishning nazariy va amaliy asoslari. Toshkent moliya instituti ilmiy axborotnomasi, 2(4), 87–94.

7. Hoffelder, K. (2018). Auditing artificial intelligence: A new frontier. CFO Magazine. Retrieved from https://www.cfo.com

8. Institute of Internal Auditors (IIA). (2013). International Professional Practices Framework (IPPF). Altamonte Springs, FL: IIA.

9. Institute of Internal Auditors (IIA). (2023). Pulse of Internal Audit 2023: Navigating Risk in a Changing World. Retrieved from https://www.theiia.org

10. ISACA. (2020). State of cybersecurity 2020: Part 2. Retrieved from https://www.isaca.org

11. Juraev, J. J. (2022). Raqamli infratuzilmalarni audit qilishda zamonaviy yondashuvlar. Moliyaviy nazorat jurnali, 1(2), 33–40.

12. Karimova, G. N. (2023). Raqamli davrda auditorlik faoliyatini rivojlantirish uchun kadrlar salohiyatini oshirish masalalari. Toshkent davlat iqtisodiyot universiteti ilmiy axborotnomasi, 2(5), 54–60.

13. KPMG. (2022). Internal audit: Unlocking the value of technology. Retrieved from https://home.kpmg/

14. Martin, K. (2019). Ethical implications and accountability of algorithms. Business Horizons, 62(2), 189–194. https://doi.org/10.1016/j.bushor.2018.11.005

15. OECD. (2021). Digital transformation and public sector auditing. Paris: OECD Publishing. https://doi.org/10.1787/9789264563749-en

16. PwC. (2022). Internal audit: A catalyst for transformation. Global survey report. Retrieved from https://www.pwc.com

17. Raximova, D. M. (2022). Raqamli transformatsiya sharoitida ichki auditning huquqiy asoslarini takomillashtirish. Yuridik fanlar jurnali, 3(1), 28–35.

18. Richins, G., Stapleton, R. C., Stratopoulos, T. C., & Wong, C. (2017). Big data analytics: Opportunity or threat for the accounting profession? Journal of Information Systems, 31(3), 63–79. https://doi.org/10.2308/isys-51805

19. Sawyer, L. B. (1996). Sawyer's Guide for Internal Auditors (5th ed.). Altamonte Springs, FL: The IIA.

20. Sultonov, F. K. (2021). Elektron byudjet tizimlarida audit jarayonlarini tashkil etishning dolzarb muammolari. TMI ilmiy-amaliy jurnali, 1(3), 22–30.

21. To'xtasinov, B. B. (2020). O'zbekistonda ichki audit tizimini isloh qilishda xorijiy tajribalar ahamiyati. Moliyaviy bozorlar va institutlar, 2(1), 19–26.

22. Xalilov, S. S. (2023). Aksiyadorlik jamiyatlarida ichki audit faoliyatining raqamli transformatsiyasi: muammo va yechimlar. Iqtisodiyot va innovatsiyalar, 5(4), 73–81.

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 14 Issue: 06 in June-2025
https://www.gejournal.net/index.php/IJSSIR