Review Paper

European Journal of Digital Economy Research
2024 Vol.5 Issue.1 pp.3-9

FROM TRADITIONAL AUDITING TO INFORMATION TECHNOLOGY AUDITING: A PARADIGM SHIFT IN PRACTICES

Hayrettin USUL*

Mustafa Furkan ALPAY**

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

* Corresponding Author, IT Auditor, furkanalpay94@hotmail.com, https://orcid.org/0009-0003-5575-8652.

ABSTRACT

The digitalization of information systems has led to fundamental shifts in auditing practices, replacing traditional manual processes with advanced digital auditing methodologies. This transformation has been accelerated by innovations in cloud technology, enhancing the efficiency and effectiveness of auditing operations. Concurrently, the evolution from document-based to transaction-based audits has redefined the auditing landscape, emphasizing real-time transaction monitoring over static record documentation. This paper explores these transformative trends within both internal and external auditing, with a specific focus on IT audit practices. It provides an in-depth analysis of the distinct objectives and methodologies inherent to IT audits, illustrating their adaptation to the digital era. The study examines the implications of these changes on audit processes, highlighting the paradigm shift towards more dynamic and data-driven auditing approaches. By synthesizing theoretical insights with practical implications, this research contributes to a comprehensive understanding of how digitalization is reshaping auditing practices. It underscores the importance of integrating advanced technologies such as AI, blockchain, and IoT in audit frameworks to enhance accuracy, reliability, and compliance in financial reporting.

Keywords: *Internal Audit, External Audit, IT Audit, Digitalization.*

1. INTRODUCTION

The rapid evolution of information technologies is fundamentally reshaping business operations. Notably, the swift advancements in cloud technology have revolutionized audit methodologies. Traditional document-centric review processes have given way to data-driven approaches, where virtual environments generate and store data in integrated modules. This transformation has led to the digitization of accounting records, rendering traditional books and documents obsolete.

These shifts necessitate corresponding changes in accounting audit practices. The transition from manual to transactional media in accounting transactions has catalyzed a paradigm shift in how accounting is recorded and classified. Consequently, the field of accounting auditing has undergone substantial transformations, prominently highlighted by the ascendance of IT auditing.

IT auditing emerges at the intersection of internal and external audit methodologies, leveraging computer-aided audit techniques and analytical procedures to gather electronic audit evidence. This approach aims to evaluate the accuracy and reliability of information systems without reliance on physical documentation (Doekhi, 2023).

The adoption of IT auditing methodologies offers manifold benefits to businesses, encompassing aspects such as impact, effectiveness, integrity, efficiency, and cost. A primary objective of IT audits is to furnish management with assurance that automated systems and processes align with their intended objectives. Special emphasis is placed on management's responsibilities in overseeing computer-based information assets and processes, guided by standards set

forth by professional organizations (Talebnia & Dehkordi, 2012).

To execute an efficient and effective IT audit, firms must meticulously determine the audit scope, allocate appropriate resources (including personnel and computer-automated audit tools), outline tasks and activities, and select suitable methods and techniques. These decisions are pivotal in optimizing audit quality and minimizing costs relative to specific IT audit objectives (Stoel, et al., 2012). The subsequent section will delve into these considerations within the contexts of internal and external audits.

2. IT AUDIT AND INTERNAL AUDIT

Internal audit serves as a critical mechanism ensuring the effective operation of an organization's internal control system. These controls are designed to provide reasonable assurance regarding the achievement of operational, reporting, and compliance objectives (COSO, 2013). As businesses increasingly rely on Information Technology (IT), there has been a noticeable shift from manual, document-based internal audits to digital processes. This transformation is significantly reshaping how internal audits are conducted.

However, this transition is not without its challenges. Internal auditors now face the task of auditing high-risk AI decision models and tools to detect potential errors or biases (The Institute of Internal Auditors [IIA], 2018). Additionally, the audit scope may include evaluating Internet of Things (IoT) devices, platforms, and associated workflows for compliance with information privacy regulations and digital ethics policies.

While IT auditing enhances the effectiveness and efficiency of internal audits, it can also lead to increased audit costs. Establishing and maintaining Internal Control over Financial Reporting (ICFR) and conducting annual audits require substantial financial and time investments. ICFR ensures that adequate internal controls are in place to achieve reliable financial reporting, providing assurance to stakeholders (Center for Audit Quality, 2019).

Despite these challenges, integrating IT audit into internal audit practices offers significant benefits. IT auditing enables auditors to utilize advanced tools and techniques for comprehensive data analysis, enhancing the accuracy and depth of audits. It improves the identification and mitigation of IT-related risks, such as cybersecurity threats and data breaches. Moreover, IT audits contribute to informed decision-making by management through detailed evaluations of IT systems (Boer, et al., 2023).

The internal control system of an organization typically comprises two distinct components: preventive controls and detective controls. Preventive controls are measures implemented to preemptively address potential issues before they manifest. Their objective is to identify and mitigate risks before they materialize, thereby facilitating the implementation of corrective measures. Preventive controls involve tasks such as defining authorizations, approvals, verifications, and restricting access to resources.

On the other hand, detective controls focus on identifying undesirable events and alerting management to these occurrences. They involve activities such as reconciling accounting records with corresponding assets, establishing performance indicators, and monitoring access to records.

In this framework, IT auditing plays a crucial role in ensuring the availability, continuity, and integrity of systems, thereby supporting the implementation of both preventive and detective controls (Otero, 2018). For instance, preventive controls in IT auditing may include access regulations and setting limits on payment approvals above specific thresholds. Detective controls, on the other hand, might involve reconciling outputs from different databases, which can serve as a manual control complemented by IT systems.

Additionally, IT auditing encompasses corrective controls, such as timely patch

updates to mitigate security vulnerabilities. These measures contribute to maintaining the security and functionality of IT systems, thereby reinforcing the overall effectiveness of the organization's internal control environment.

To effectively fulfill its intended functions, an organization's internal control system must undergo rigorous monitoring. Within the framework of COSO (Committee of Sponsoring Organizations of the Treadway Commission), monitoring is highlighted as a critical component of an internal control system. It serves to detect deficiencies in service performance and identify potential threats in real-time. During monitoring, auditors evaluate the system's effectiveness while assessing the security posture of virtual machines, networks, storage, data services, and applications. This proactive approach enables auditors to prioritize and address security vulnerabilities promptly.

The field of information technology (IT) audit encompasses a broad spectrum of activities focused on assessing and enhancing an enterprise's information system infrastructure. Key areas typically included in an IT audit are:

Access Controls: Reviewing authorizations granted to individuals accessing the system.

Backup Procedures: Ensuring the existence and adequacy of backups for critical transactions.

Compliance: Evaluating adherence to relevant laws and regulations.

Policy Adherence: Assessing alignment of transactions with the organization's internal policies and procedures.

In addition to these fundamental areas, specific aspects of IT systems are also subject to audit scrutiny:

Timeliness of Updates: Assessing the promptness of updates to the information system.

Response to External Attacks: Evaluating the effectiveness of measures taken against external threats.

Encryption Practices: Reviewing the use of protocol encryption for SSH and RDP sessions.

Security of VPN Applications: Ensuring the security and proper configuration of internet connection securing (VPN) applications.

Data Protection: Verifying the use of HTTPS for REST API calls and TLS for data protection between services.

To execute these assessments effectively, IT auditors employ a diverse range of audit techniques tailored to the specific objectives of the internal audit. Statistical methods play a crucial role in this process, facilitating accurate assessment through methods such as defining the population, determining standard deviations, estimating sample sizes, and calculating necessary samples.

Information technology (IT) controls are implemented across all levels of an organization and vary in their relationships and applications. At the entity level, IT access management focuses on establishing policies and procedures governing access to organizational resources. This ensures that access rights are appropriately defined and managed across the entire enterprise (Putters, et al., 2023).

At the process level, IT access management addresses specific functions or departments within the system, determining and managing decision-making privileges.

Among the most critical IT controls are Information Technology General Controls (ITGC), which encompass controls applied to both information systems and infrastructure. Application controls are tailored to specific applications and include measures like authorization matrices defining user rights, approval workflows for payments, and automated matching of purchases. These controls ensure that transactions are processed accurately and securely within individual applications.

General controls, on the other hand, are overarching controls that apply to system components such as databases, operating

systems, and networks. Their purpose is to oversee and regulate the processes occurring within and around the information systems. Key ITGCs include:

Logical Access Security: Managing access permissions to systems and data to ensure only authorized personnel have access.

Program Change Management: Governing the process of implementing changes to IT systems to maintain integrity and security.

IT Security: Implementing measures to protect systems and data from unauthorized access, breaches, and cyber threats.

Backup and Recovery: Establishing procedures for secure data storage and ensuring data recovery capabilities in case of data loss or system failure.

System Development: Evaluating the need for and managing changes to IT systems to meet organizational requirements and improve functionality.

Computer Operations: Configuring and installing IT systems and ensuring their ongoing operational efficiency.

These IT controls are essential for mitigating risks associated with IT operations, enhancing data security, and ensuring the reliability and continuity of business processes. Effective implementation and monitoring of these controls are critical to safeguarding organizational assets and achieving compliance with regulatory requirements.

Information Technology General Controls (ITGCs) are foundational components of any control system, designed to assess the effectiveness and functionality of controls over an extended period. They are crucial for ensuring that user controls and application controls operate reliably throughout the control period. In cases where segregation of duties and ITGCs are inadequate, it becomes challenging to provide reasonable assurance of control reliability. In such instances, firms may resort to data-driven controls, using data analysis to detect deviations that occurred during the specified period (Doekhi, 2023). If no deviations or irregular data patterns are found in the sampled data population, it suggests that risks did not materialize during that period, thereby indicating minimal likelihood of significant errors in the process. Based on the company's risk analysis, appropriate IT controls are integrated into the organization's Internal Control over Financial Reporting (ICFR) framework (ISACA, 2022).

The implementation of IT controls is detailed in work programs that are based on objective and risk analyses. These programs include annual assessments to evaluate the effectiveness of the established controls. IT auditors play a pivotal role in conducting testing at both the application and infrastructure levels. Within the ICFR context, this framework involves identifying and assessing potential risks, ensuring that financial reporting is prepared in accordance with relevant reporting standards such as IFRS or GAAP. This process may also entail issuing a letter of representation, affirming the accuracy and completeness of the financial statements (KPMG, 2018).

3. IT AUDIT AND INDEPENDENT AUDIT

Given these transformations, it is imperative for independent auditors to integrate IT audits alongside traditional audits of client companies. While IT audit is typically internal, external auditors also employ it, adhering to established auditing standards. External auditors must assess the effectiveness and reliability of the client's accounting information system (Iliescu, 2020; Kassa, 2016).

Various technologies, including blockchain technology (BT), robotic process automation (RPA), artificial intelligence (AI), and machine learning, are accelerating the digital transformation of accounting practices. These tools streamline transaction processing, reduce resource requirements, and automate repetitive tasks such as aggregating financial data and compliance reporting (Busulwa & Evans, 2021).

This digital shift challenges traditional auditing practices centered on document

review. Auditing standards are evolving, replacing document review with transaction review as accounting moves towards a transaction-based approach. Digitalized accounting enables auditors to access new data sources like big data, IoT data, and social media feeds, and to enhance access to existing data through automated text analysis in legal contracts and emails.

Digitalization also transforms auditing processes, enabling real-time audits of digital accounting systems. Automation and AI allow auditors to examine all transactions without sampling, rendering traditional document verification unnecessary and establishing transaction review as the norm.

To conduct effective IT audits, auditors follow a structured approach:

Understanding Industry and Business Context: Auditors should grasp the industry's value chain and the client's business model to align audits with governance needs.

Organizational Structure and IT Oversight: Identify governance structures, strategy committees, and IT overseers responsible for the accounting information system's security and development.

Policies and Procedures: Define and evaluate policies governing IT systems, including security protocols and data privacy measures.

Risk Assessment: Assess IT risks using appropriate techniques to develop audit plans and determine the audit scope.

Internal Control Testing: Evaluate the effectiveness of internal controls to ensure compliance and mitigate risks.

Audit Planning: Develop an audit strategy, define objectives, allocate resources, and prepare audit plans and working papers.

Auditors face challenges due to rapid technological advancements, including increased risks such as cyber threats, bias in AI models, and ethical concerns in data handling. These developments complicate the assessment of "material misstatement" risks in financial statements. Auditors must adapt by understanding emerging risks, refining assessment methodologies, and recommending effective controls to safeguard financial integrity.

As digital technologies reshape accounting practices, IT auditing becomes indispensable for ensuring the reliability and security of financial reporting. Auditors must continuously evolve their approaches to effectively manage new risks and maintain the credibility of financial audits in a digital age.

4. CONCLUSION

The profound impact of digitalization on accounting and auditing practices cannot be overstated. With businesses transitioning from document-centric to transaction-centric recording systems, the auditing profession has undergone significant transformations. These changes challenge traditional auditing practices and emphasize the critical role of IT audits in ensuring the accuracy and security of financial information.

Internally, the role of auditors extends beyond mere compliance to actively safeguarding organizational objectives through robust internal control systems. Historically reliant on manual methods, modern internal audits increasingly incorporate IT audits to comprehensively assess controls and mitigate risks associated with digital technologies such as AI, IoT, and blockchain. This shift not only enhances the efficiency of audits but also addresses emerging risks in real-time.

Externally, auditors play a pivotal role in verifying the integrity of financial reports. By conducting thorough IT audits, they scrutinize the entity's internal control framework to detect potential misstatements and ensure adherence to regulatory standards. This proactive approach is essential in an era where digital advancements introduce complexities like cybersecurity threats and data privacy concerns.

The integration of IT audits into both internal and external audit practices signifies a paradigm shift towards data-driven auditing methodologies. This transformation eliminates the limitations of traditional

sampling methods, allowing auditors to analyze entire datasets and identify anomalies with greater precision. Moreover, IT audits facilitate continuous monitoring of critical systems, enabling auditors to promptly address emerging risks and vulnerabilities.

In conclusion, as information systems continue to evolve, auditing practices must adapt to keep pace with technological advancements. The digitalization of accounting practices has underscored the importance of proactive auditing methodologies that integrate advanced technologies like AI, blockchain, and IoT. IT audits have become indispensable for ensuring the reliability, integrity, and security of financial information in today's complex business landscape.

Looking forward, several promising research avenues emerge for auditors and researchers alike. Firstly, exploring the efficacy of AI-driven audit techniques and their integration into traditional audit processes could yield insights into improving audit efficiency and accuracy. Secondly, investigating the impact of blockchain technology on audit trail transparency and data integrity presents opportunities to enhance audit reliability in decentralized systems.

Furthermore, the evolving regulatory landscape and its intersection with digital auditing practices warrant investigation. Research focusing on how auditors navigate regulatory compliance in the era of digital transformation can provide guidance for developing robust audit frameworks. Additionally, studies on the ethical implications of AI and automated auditing tools in decision-making processes could inform best practices and ethical guidelines for auditors.

Lastly, as cyber threats continue to evolve, research into cybersecurity frameworks and their integration with audit practices is crucial. Understanding how auditors can effectively assess and mitigate cybersecurity risks within organizations will be essential for maintaining trust and security in financial reporting.

In sum, the future of auditing lies in embracing technological innovations while upholding audit standards and ethical practices. By addressing these research gaps, auditors and researchers can contribute to advancing audit methodologies and ensuring the continued relevance and effectiveness of auditing practices in a digital age.

REFERENCES

Boer, A., de Beer, L., & van Praat, F. (2023). Algorithm assurance: Auditing applications of artificial intelligence. 149-183. *Advanced Digital Auditing: Theory and Practice of Auditing Complex Information Systems and Technologies*, (Eds. Berghout, et al.), Springer.

Busulwa, R., & Evans, N. (2021). *Digital Transformation in Accounting*, Routledge.

Stoel, D., Havelka, D., & Merhout, J. W. (2012). An analysis of attributes that impact information technology audit quality: A study of IT and financial audit practitioners. *International Journal of Accounting Information Systems*, 13(1), 60-79.

Center for Audit Quality (2019). Guide to internal control over financial reporting. https://www.thecaq.org/guide-internal-control-over-financial-reporting/

COSO, https://www.coso.org/

Doekhi, R.J.M. (2023). The Intercompany Settlement Blockchain: Benefits, Risks, and Internal IT-Controls. 47-88. *Advanced Digital Auditing: Theory and Practice of Auditing Complex Information Systems and Technologies*, (Eds. Berghout, et al.), Springer.

Iliescu, F. M. (2010). Auditing IT governance. *Informatica Economica*, 14(1), 93.

ISACA Journal, 15 Feb. 2022, isaca.org/ resources / isaca-journal / issues/2022/volume-1/the-evolution-of-audit-in-the-wake-of-the-pandemic

Kassa, S. (2016). Information Systems Security Audit: An Ontological Framework. *ISACA Journal*, 5, 1-8.

KPMG (2018). *https://kpmg.com.*

Otero, A. R. (2018). *Information technology control and audit*, 5th ed., 12-17, Amsterdam University Press.

Putters, J., Hashemi, J. B., & Yavuz, A. (2023). Demystifying Public Cloud Auditing for IT Auditors. Advanced Digital Auditing, 185-235. *Advanced Digital Auditing: Theory and Practice of Auditing Complex Information Systems and Technologies*, (Eds. Berghout, et al.), Springer.

Talebnia, G., & Dehkordi, B. B. (2012). Study of relation between effectiveness audit and management audit. *GSTF Business Review (GBR)*, 2(1), 92.

The Institute of Internal Auditors [IIA] (2018). https://www.theiia.org/en/standards/