IT Governance, Audit and Risks Management in Banks: A Narrative Literature Review and Future Research Agenda

Paola Demartini and Flavia Cocuccioni
Roma Tre University, Italy

Paola.demartini@uniroma3.it
Fla.cocuccioni@stud.uniroma3.it

Abstract: The increasing digitalization of the banking sector has significantly reshaped institutional control mechanisms and governance structures, particularly in the realm of Information Technology (IT). This narrative literature review examines the evolving role of IT audit and governance in banks, with a specific focus on how these mechanisms contribute to risk management and regulatory compliance. Drawing upon a corpus of 26 peer-reviewed studies spanning from the early 2000s to 2025, this paper offers an integrated framework to understand the complex interrelations between IT governance, internal auditing, emerging technologies, and institutional oversight. Our literature review situates IT audit practices within broader organizational, cultural, and regulatory contexts. It explores how frameworks such as COBIT and COSO serve not only as technical guides but also as institutional artifacts that shape organizational behavior, strategic decision-making, and normative compliance. The review reveals that the role of IT audit has expanded from a purely technical function to a strategic enabler of trust, transparency, and accountability within financial institutions. Furthermore, audit committees and specialized board-level IT committees are shown to play a critical role in translating technological risks into governance priorities, thereby fostering a culture of proactive risk mitigation. Our analysis addresses the competencies of IT auditors, emphasizing the increasing demand for specialized skills in cybersecurity, data governance, and AI-integrated systems. The findings suggest that organizations with robust IT governance structures and trained audit personnel are better equipped to address technological disruptions and regulatory pressures. Moreover, the integration of Artificial Intelligence (AI) into audit processes is identified as both a transformative opportunity and a governance challenge. This paper contributes to the literature by providing a picture that connects technical auditing practices with broader sociotechnical systems. It identifies critical gaps in current audit practices, highlights the importance of organizational culture and ethics in IT governance, and proposes avenues for future research, particularly on the intersection of AI, audit methodologies, and institutional compliance.

Keywords: IT governance, Risk management, Banks, COBIT, AI

1. Introduction

The ongoing digitalization of the banking sector is reshaping operational models redefining the control systems within financial institutions. The conjunction of regulatory pressure, the diffusion of new technologies and the presence of cyber threats has led to the necessity of reinforcing IT governance to ensure security, reliability and compliance. In this landscape, IT governance takes shape in an ensemble of processes, structures and decision-making mechanisms with the purpose of generating value for the organization, while supporting the achievement of the entity's objectives maintaining acceptable levels of risk.

In particular, the introduction of Artificial Intelligence into the organizational processes poses new challenges for control design and testing. For this reason, it is essential to identify AI-integrated applications and define assessment models to guarantee this new technological dimension is properly governed. Among the latter, we deem relevant to explore the contribution of the COBIT (Control Objectives for Information and related Technology) framework in supporting digital risk management and regulatory compliance.

The research question driving our investigation is:

RQ1:What is the significance of information technology audit in reinforcing risk management and regulatory : compliance in banking?

To answer this question, we performed a narrative literature review on the role of IT audit and governance in the banking sector. Findings are based both on literature review and researchers' expertise by direct involvement in the field. The review looks at how IT audit connects with risk management and regulatory compliance, gathering insights from various studies since the early 2000s up to now. The paper digs into concepts like IT governance, internal controls, auditor independence, and compliance, creating a big-picture view that blends different research approaches.

2. A Narrative Literature Review on the Role of IT Audit and Governance in the Banking Sector

Narrative literature review is an approach used to answer broad questions and to evaluate literature from a vast point of view, including studies with heterogeneous methodologies, as stated by Baumeister e Leary (1997). A distinctive aspect of this type of review is the ability to offer a comprehensive landscape on the topic, not limiting to an exposition of results but defining as well the theoretical background of the analyzed studies, and providing a fitting way to examine the argument using a qualitative method, since the subject of this research is IT governance and IT audit, thus the predominant analysis is not quantitative. Snyder (2019) refers to narrative review as semi-systematic review and delineates the concept of meta-narratives, affirming that "the review seeks to identify and understand all potentially relevant research traditions that have implications for the studied topic and to synthesize these using meta-narratives instead of by measuring effect size" (p. 335).

Following the guidance of Baumeister and Leary (1997) and Snyder (2019), the present work uses a narrative literature review to delve into IT audit in the banking sector, between risk management and regulatory compliance, examining research to reconstruct the landscape and apply it on the case study analyzed in the last chapter. This review was conducted using academic databases like Scopus and Google Scholar, researching "IT audit" and "IT governance" as "Article title", "Abstract", "Keywords" and making use of keywords such as "information technology", "COBIT", "information system security", "cybersecurity", "Internal Control", "Internal Audit", "external audit", "auditor independence", "compliance", "risk management", "audit reports", and selecting subject areas as "Business, Management and Accounting" and "Economics, Econometrics and Finance". Lastly, although the temporal range was set from 2010 to 2025, it was then extended to include relevant contributions of the early 2000s, to incorporate foundational studies. The result of the research was equal to 178 documents: the selection of the studies was based on the discussion of the topic and the relevance of the main themes for the current research and their publication in scientific or academic journals. The exclusion criterion was built on their relevance to this investigation: articles not focusing on the financial sector and more precisely on banking were excluded or, if included, they were especially pertinent and suitable to analyze widely IT governance.

In our aim the reviewed literature should underscore the increasing significance of Information Technology (IT) audit within the landscape of risk management and regulatory compliance in the banking sector. Over the past decades, the rapid evolution of digital technologies has transformed traditional financial oversight, necessitating robust frameworks for governance, internal controls, and risk mitigation. Central to this transformation are frameworks like COBIT (1996, 2012) and COSO (1992, 2013, 2017), which integrate IT governance with broader organizational objectives. This body of research explores how IT audit functions as both a mechanism for ensuring regulatory adherence and a strategic tool for managing emerging risks inherent in digital infrastructure.

Out of all the documents retrieved, 26 articles were selected and used for the writing of this paper. Our findings unfold around the following themes:

- Evolution of IT audit and governance in Banking
- IT controls implemented into audit procedures
- Application of IT governance frameworks to strengthen internal controls
- The competence of IT auditors and the role of innovative technologies such as AI

3. Findings

3.1 Evolution of IT Audit and Governance in Banking

Several organizations maintain an internal audit function that encompasses responsibilities related to IT audit and IT governance. But what is "internal audit"? This practice has been defined as follows by the Institute of Internal Auditors (IIA):

"Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes" (Institute of Internal Auditors, n.d.).

Among other risks, it analyses technology risk and focuses on the ICT system of an enterprise, in which the performers of the procedures, the IT auditors, must be independent and objective, and must review the effectiveness of the ensemble of risk management, governance, internal controls and information system, by performing tests and investigation.

The development of Information Technology made the introduction of IT audit necessary to manage governance in institutions subject to normative requirements and risk management processes. As early as the 2000s, Moeller (2010) defined concepts that nowadays are habitual notions, treating the topic of IT audit spanning from technological evolution of processes and internal control implications, passing through information systems security, business continuity and data recovery, towards the compliance of new legislation, that at the time was the Sarbanes-Oxley Act of 2002. His discussion includes both IT general controls and IT automatic controls, reviewing various frameworks to perform the audit, such as COBIT, and underlining the newfound role of the auditor in an embryonal digital transformation environment. Merhout and Havelka (2008), not only underline the crucial role of IT audit in IT governance but also propose a relationship between auditors and managers aimed at perceiving audit practices as a value-added activity for the firm, bettering documentation and internal operations for starters, and improving overall strategic planification, risk management and governance.

To define the link between governance, risk management and IT audit, a recent research study underlined the evolution of the audit committee: from a body with supervisory and monitoring functions from the financial point of view to a risk management authority in the IT and cyber field. Chen et al. (2022) uncovered that IT experts in the audit committee lower significantly the probability of data breaches and better the enterprise's capacity to mitigate technology risk; the audit committee strengthens operational resilience and already in 2014 there was evidence of the fact that these committees had responsibilities for cyber risk management (NACD, 2014). A survey showed that only 37% of firms in the world include IT experts on the board of directors, limiting the cyber risk management (EY, 2020).

To avoid the dilution of the audit committee, causing the ineffectiveness of the body, many authors advise the creation of ad hoc technology committees at the board level, showing improvements in internal control and security of the firm overall, comprehending the disadvantage of cyberattacks just by its institution (Chen et al., 2022). Furthermore, IT committees can share their knowledge with the board of directors, instructing on complex themes and contributing to the development of a strategic approach on digital risk management, reducing the gap of expertise among managers of traditional approach and new ICT challenges (Hartmann & Carmenate, 2021).

Another research (Higgs et al., 2016) reveals that the presence of a technology committee increases the likelihood that the company will report data breaches and, more importantly, it discloses that market response proves to be better if the firm includes a technology committee, unveiling the influence and impact of this structure from a reputational standpoint. De facto this work also contributes to the signaling theory, as the presence of the committee signals to the market that IT governance is robust and enhances stakeholder confidence.

3.2 IT Controls Implemented Into Audit Procedures

While the establishment of specialized board committees illustrates the growing awareness of IT risks and cybersecurity challenges, regulatory compliance frameworks introduce requirements to ensure that IT controls are implemented into audit procedures. These findings are integrated with the obligations imposed by the Sarbanes-Oxley Act 404(b), that redefined audit on internal controls: regulatory compliance requires a precise evaluation of the period-end financial reporting process by the auditors. The so-called financial close process includes both manual and automatic controls, among other the most relevant are the IT general controls (ITGC) and the IT application controls (ITAC): a study reveals that many deficiencies occur when external auditors verify them and this limits the efficiency of the controls in ensuring security of the firm and integrity of financial data: this is the rationale for the introduction of the IT audit in the other general audit practices (Janvrin et al., 2019). The study performed by Janvrin et al. (2019) underlines the necessity to test the information technology systems in a sound manner, in fact the Public Company Accounting Oversight Board (PCAOB) (a nonprofit corporation created by the Sarbanes–Oxley Act of 2002 to oversee the audits of US-listed public companies) noted how auditors limit their activity to the entity level controls and the walkthrough tests, only a preliminary analysis to consolidate the understanding of how the firm assesses ICT risks. The same study suggests that the approach of the external auditors in integrated audits is guided by their over-reliance on internal controls information, not performing substantive testing; while, when executing financial statements

audits, they tend to use stricter techniques to give assurance on the data. This is the first reason for the increase in the competencies of both internal and external IT auditors: in fact, other researches (Hadden & Hermanson, 2003; Hadden, Hermanson & DeZoort, 2003) using a survey found the presence of the audit committee when in the board of directors there where individuals with auditing experience and acquaintance with the COBIT model, assigning the duty of IT controls to this particular committee but also highlighting its expertise on the subject. The role of board-level IT committees shows to be fundamental also in the management of data breaches, IT attacks and on increasing stakeholders' trust in the enterprise processes (Hartmann & Carmenate, 2021).

3.3 Application of IT Governance Frameworks to Strengthen Internal Controls

In recent years, many studies have underlined the importance of integrating technical competences and IT governance structures in the internal audit functions, and in general inside the organizations' governance structures, to the end of responding more effectively to IT risks. A study performed in 2025 on the adoption of IT governance frameworks by clients subject to external audit, revealed that it is positively correlated with a higher efficiency of the audit. This is connected to a better integrity of data, better risk management and advanced transparency on IT processes: the findings show clearly that regulators should incentivize the adoption of frameworks like COBIT to lower the risk of material errors and approach a progressively higher compliance with financial reporting requirements (Roustom et al., 2025). The results of this study are consistent with prior findings affirming that IT governance lowers control risk and helps define an effective audit strategy and is central to the topic of this thesis, since it implies an appropriate integration of IT risks and therefore IT controls, suggesting a more robust control environment and better risk management.

Although the study by Roustom et al. (2025) provides recent evidence of the benefits of IT governance adoption, these findings are consistent with earlier research: Huang et al. (2011), proposed a quantitative evaluation model of IT general controls, based on the integration of the principles of the Enterprise Risk Management and COBIT's best practices, already introduced in chapter 2. Their work shows that activity-level IT controls are critical for ensuring the reliability of the financial reporting systems. Some examples of these controls are data management, system security and end-user application controls. The validation of this theoretical model is enforced by a case study on a Big Four auditing firm, included in Huang et al.'s (2011) research, which demonstrates how structured risk-based IT control frameworks contribute to strengthening the internal control environment. Taken together, these articles confirm that well-designed ITGC and, more generally, solid IT governance are essential to enhance risk management practices and in accomplishing higher audit quality and regulatory compliance.

This thesis is also confirmed by Rubino et al. (2014) that emphasize the role of COBIT in reinforcing internal controls over financial reporting, integrating this framework with the COSO framework to identify, document and monitor ITGCs and ITACs. The analysis performed uses the relationship between COBIT domains and the five integrated COSO components, highlighting how this framework helps comply with regulatory requirements and supports risk management in financial reporting processes. Building upon their earlier work, Rubino et al. (2017) expanded their vision, including cultural and organizational components, and shifted their attention from a compliance-focused view to an integrated outlook: the result of the study supports the introduction of IT governance frameworks, especially COBIT, to minimize risk for the whole ITC infrastructure of the organization. They also point out that implementing IT controls has a direct impact on planning, development and support of ICT systems, in particular IT general controls contribute actively to the identification of roles and responsibilities in the organizational structure and IT application controls assure completeness and accuracy of data, influencing internal and external reporting. Because it is complex to analyze ITGC and ITAC, the authors decided to investigate the controls based on three IT dimensions: organizational controls, process controls and soft variables controls. The former category defines policies and procedures, roles and responsibilities, and the general corporate organization. The second category regulates the internal documentation and informational flows, contributing to better the quality of the data and providing clarity, efficiency and integrity, this being one of the main objectives of the COBIT framework. The latter category concentrates on organizational culture, integrity and the management's values, monitoring any update of the code of conduct and promoting ethical behavior towards the employees. These three types of controls are strictly interconnected: IT organizational controls define the rules and procedures, that alone are not enough to ensure the well-functioning of the firm, then IT process controls assure the information reliability and supervision of the way in which it is used, on the other side IT soft variables controls step in upstream, given that the definition of the controls of the other categories can be performed only when the values and the culture of the organization are clear.

The following image summarizes the aforementioned concepts:

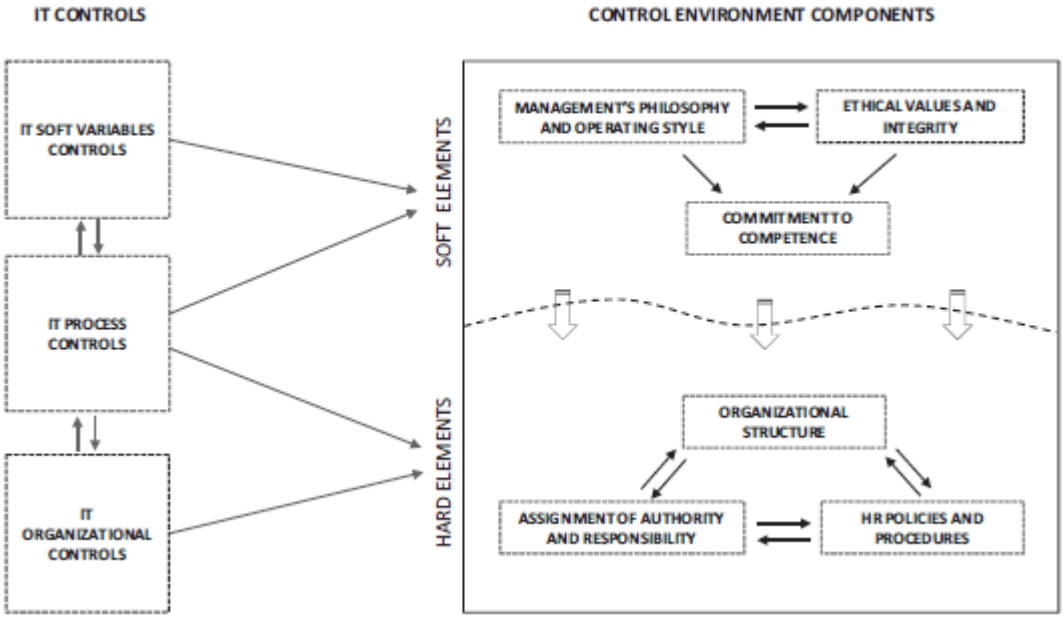

Figure 1: The role of IT controls in the control environment components

Another research (Nuijten et al., 2023) exploring the role of IT auditors compared with general auditors, both in the internal audit function, reveals that IT auditors perceive IT risks more than general auditors, and this difference of opinion is more pronounced in the so-called yellow risks, of moderate and medium gravity, than in red and green risks, respectively severe and light. This shows that the expertise of IT professionals provides more precise judgement and less biases based on personal propension of risk, and therefore it constitutes an optimal reason to introduce IT frameworks and specialized personnel inside the organization.

3.4 The Competence of IT Auditors and the Role of Innovative Technologies Such as AI

External auditors distinguish themselves from internal auditors because "…. the standards, requirements, or other audit criteria used in external audits are declined outside the organization being audited" (Gantz, 2014). The same applies to IT external auditors, specialists in information technologies.

In 2015, a study on Italian banks (D'Onza et al., 2015) underlined that the senior management expected better IT security, to prevent data breaches and system vulnerabilities, strategic support on process design and risk minimization, through the identification of emerging risks, above all in cybersecurity. The model on which the research was based arises from the classification of IT audit in three categories: IT governance, IT management and IT technical, with a specific focus on the first two areas to study the relationship between managers and IT auditors. IT governance was evaluated using the five domains defined by COBIT: strategic alignment, value delivery, resource management, risk management and performance evaluation, while IT management was assessed through the Global Technology Auditing Standard No. 17 of the Institute of Internal Auditors (IIA) and Moeller's classification (2010) defining the following seven areas: IT acquisition and development, change management, operations and maintenance, disaster recovery and business continuity, IT outsourcing, IT security, IT control over financial reporting – aligning with the compliance requirements for Italian listed banks to Law 262/2005, the equivalent of the Sarbanes-Oxley Act in Italy. This discussion serves as further groundwork to understand the role of IT auditors in the banking sector, with their weaknesses and chances for improvement.

On the topic of auditors' expertise, an article by Haislip et al. (2016) highlighted that firms with material weakness in IT controls are more likely to change their external auditor in favor of more experienced ones: this signals to the market that the management aspires to strengthen the IT governance framework, based on external knowledge. Another finding of this study is the fact that the transition to the more capable auditor

improved the company's IT performance within one year, demonstrating the fundamentality of IT knowledge in audit practices, not only for IT controls but for the entirety of internal controls, showing regulators that IT training improves financial reporting outcomes and it becomes the bridge to cover the gap between regulatory expectations and the actual efficacy of controls in organization. Finally, IT audit is shown as a key factor in regulatory compliance but also in governance and prevention of IT risks: the role of IT auditors does not stop at compliance but influences directly audit methodologies and control frameworks to mitigate this category of risks.

However, the results of a more recent study (Mahlangu & Moosa, 2023) on IT knowledge and competences of internal auditors show that their proficiency at the moment is low and the conclusion of this discussion underlines that an insufficient understanding of these procedures can lead to inability to detect IT risks, among other operational risks: this is where the role of IT auditors from external accounting firms lies. External auditors find a deficiency whenever the risk management plan lacks strategy for a specific risk and there is no control arranged to oversee it, or the control is not effective. As underlined by Spears et al. (2013), the institution of new policies and practices often results in symbolic compliance, not supported by real changes in the firm aimed at appearing sound at the external auditors' eye; the real assurance can be given when the IT risk is controlled and managed substantively and effectively.

Finally, the role of innovative technologies, such as artificial intelligence in the context of IT audit and internal control, has recently been investigated by some studies. On one hand, Tanriverdi & Taskin (2023) have performed a systematic literature review and found that some technologies, machine learning, mining and predictive analysis overall, have been implemented significantly in IT audit processes. On the other hand, Almaqtari (2024) carried out an empirical study that resulted in showing that the integration of AI in auditing processes is pandered by the IT governance structure: without an appropriate IT governance framework the adoption of advanced technologies could be critical because the organization would be exposed to major risks, while if put in place adequately becomes a enabling factor for an innovation compliant with the firm's processes.

4. Conclusions

Our narrative approach captures the broad and heterogeneous landscape of research, emphasizing the importance of theoretical integration and qualitative analysis in understanding the dynamics of IT governance and audit practices. The evolving role of audit committees from supervisory bodies to proactive risk managers in IT and cybersecurity further underscores the integration of IT and risk management strategies in contemporary organizational governance.

The findings also reveal that effective IT audit practices are rooted in adherence to standards and principles, ensuring independence, professional competence, and comprehensive evaluation of internal controls.

The central role of IT governance frameworks in managing risks, enhancing internal controls, and supporting digital transformation within organizations, particularly in the banking sector. The literature emphasizes that well-designed IT controls and frameworks like COBIT and COSO contribute significantly to regulatory compliance, risk mitigation, and audit quality.

Finally, our review highlights the importance of specialized IT auditors whose expertise allows for more precise risk assessment, especially in contexts involving moderate risks, and their role in strengthening governance and internal controls through advanced technologies like AI and machine learning.

These insights underline the interconnectedness of IT governance, risk management, and audit practices in fostering organizational resilience, regulatory compliance, and strategic innovation, making them highly relevant for discussions among social scientists focused on management and accounting in the digital age.

4.1 Future Research Avenues Related to the Implementation of Artificial Intelligence (AI) and Other new Technologies

Based on the narrative review, several avenues for future research related to the implementation of Artificial Intelligence (AI) and other new technologies within organizations can be identified:

Impact of AI on Risk Management and Internal Controls Future studies could explore how AI technologies influence the effectiveness of internal controls and risk mitigation strategies. Investigating whether AI integration leads to measurable improvements in detecting, preventing, and managing operational and financial risks would deepen understanding of AI's strategic value.

Role of AI in Enhancing IT Governance Frameworks Research could examine how AI tools support the implementation and evolution of IT governance frameworks like COBIT or COSO. This includes assessing whether AI automates compliance processes, enhances decision-making, or facilitates real-time monitoring of controls, thereby strengthening overall governance structures.

Adoption Barriers and Facilitators for AI Technologies further inquiry can focus on organizational, cultural, and regulatory factors that influence the adoption of AI in audit and risk management functions. Understanding the facilitators and barriers can inform best practices and policy recommendations for effective AI integration.

Impact on Auditor Expertise and Decision-Making future research could analyze how AI affects the decision-making processes of IT and internal auditors, especially concerning their perception of risks and controls. Exploring whether AI leads to biases or improves objectivity due to enhanced data analysis capabilities would be valuable.

AI and competency development in audit teams investigations could target the evolving skills requirements for auditors in the era of AI, identifying necessary competencies, training needs, and the influence of AI on professional judgment and independence.

Finally, ethical and regulatory challenges of AI in Audit and Governance future work could explore ethical considerations, regulatory compliance issues, and the legal implications of deploying AI in critical organizational functions, promoting the development of responsible AI frameworks aligned with governance standards.

These research directions will significantly contribute to understanding the transformative potential of AI technologies within management and accounting contexts, supporting more resilient, transparent, and efficient organizations.

Ethics statement: Ethical clearance was not required for the research

AI statement: AI tools were used to check the English language for the proofread

References

Almaqtari, F. A. (2024). The role of IT governance in the integration of AI in accounting and auditing operations. *Economies*, 12(8), 199. https://doi.org/10.3390/economies12080199

Baumeister, R. F., & Leary, M. R. (1997). Writing narrative literature reviews. *Review of General Psychology*, 1(3), 311–320.

Chen, Y., Guo, L., & Zhou, N. (2022). IT expertise in the audit committee and data breach disclosures. *Journal of Accounting Research*, 60(3), 849–893.

D'Onza, G., & Sarens, G. (2015). The relationship between internal audit and senior management: A qualitative analysis of expectations and perceptions. *International Journal of Auditing*, 19(3), 214–231.

Gantz, S. D. (2014). *The basics of IT audit: Purposes, processes, and practical information*. Elsevier. https://www.sciencedirect.com/book/9780124171596/the-basics-of-it-audit

Hadden, L. B., & Hermanson, D. R. (2003). IT considerations in audit committee responsibilities. *Journal of Information Systems*, 17(Supplement), 61–75.

Haislip, J. Z., Hogan, C. E., & Perez, R. (2016). External auditors and IT controls: Knowledge and change. *Journal of Information Systems*, 30(3), 73–96.

Hartmann, T., & Carmenate, R. (2021). Board-level IT committees and cyber risk management. *Information Systems Journal*, 31(5), 620–645.

Higgs, J. L., Pinsker, R., Smith, T. J., & Young, G. R. (2016). The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems*, 30(3), 79–98.

Huang, S.-M., Hung, W.-H., Yen, D. C., Chang, I.-C., & Jiang, D. (2011). Building the evaluation model of the IT general control for CPAs under enterprise risk management. *Decision Support Systems*, 50(3), 692–701. https://doi.org/10.1016/j.dss.2010.08.015

Institute of Internal Auditors (IIA). (n.d.). Definition of internal audit. https://www.theiia.org/en/standards/what-are-the-standards/definition-of-internal-audit/

Janvrin, D., Payne, E. A., & Byrnes, P. (2019). The effect of IT expertise on audit process and outcomes. *Journal of Information Systems*, 33(2), 23–44.

Moeller, R. R. (2010). *IT Audit, Control, and Security*. Wiley.

Mahlangu, S., & Moosa, S. (2023). Internal auditors' IT knowledge and risk detection. *Journal of Contemporary Accounting and Economics*, 19(1), 45–60.

Merhout, J. W., & Havelka, D. (2008). Information technology auditing: A value-added IT governance partnership between IT management and audit. *Communications of the Association for Information Systems*, 23(1), 26.

Nuijten, A. L. P., Keil, M., & Zwiers, B. (2023). Internal auditors' perceptions of IT risks. *Journal of Information Systems*, 37(1), 67–83. https://doi.org/10.2308/ISYS-2020-040

Roustom, Z. M., Hamwi, K., Armoush, A., & Abubakr, A. A. M. (2025). IT governance frameworks and their impact on the efficiency of external audits. *Qubahan Academic Journal*, 5(1), 640–661. https://doi.org/10.48161/qaj.v5n1a1517

Rubino, M., Vitolla, F., & Garzoni, A. (2014). The integration of COBIT and COSO frameworks for IT governance. *Management Research Review*, 37(2), 121–133.

Rubino, M., Vitolla, F., & Garzoni, A. (2017). How IT controls improve the control environment. *Management Research Review*, 40(2), 218–234. https://doi.org/10.1108/MRR-04-2016-0093

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Spears, J. L., Barki, H., & Rivard, S. (2013). Compliance vs. strategic security: Managing information security policies. *Information Systems Journal*, 23(6), 583–610.

Tanriverdi, N. S., & Taşkin, N. (2023). A systematic literature review for new technologies in IT audit. *Acta Infologica*, Advance online publication. https://doi.org/10.26650/acin.1142281