

Auditing in Egypt's Digital Banking Environment: A Critical Four-Dimensional Analytical Framework

<https://doi.org/10.56830/IJAMS07202604>

Reda Mahmoud Mohamed Abdelrehim 

Faculty of Business, Alexandria University, Egypt.

Reda.abelrahim@alexu.edu.eg

Amr Mohamed Khamis Mohamed 

Faculty of Business, Alexandria University, Egypt.

Amr.morsy@alexu.edu.eg

Received: 15 June 2026. Accepted: 17 July 2026. Published: 30 July 2026

Abstract:

This study examines external auditing in Egypt's digital banking environment through a critical four-dimensional analytical framework. It analyses how the digital transformation of commercial banks reshapes external auditors' responsibilities in relation to audit risk, electronic audit evidence, digital internal controls, and assurance services. The study is conceptual rather than empirical; it does not test statistical relationships or measure auditors' perceptions. Instead, it adopts a structured critical review and conceptual analytical approach that synthesizes international academic and professional literature on digital banking, audit digitalisation, audit risk, cybersecurity, data analytics, internal controls, and technology-enabled assurance. This literature is integrated with Egyptian regulatory and institutional documents related to digital banks, non-cash payments, financial inclusion, electronic signatures, and personal data protection. The analysis shows that digital banking creates both audit opportunities and audit risks. While digital technologies may enhance audit efficiency, expand evidence coverage, and support data-driven procedures, they also increase auditors' dependence on complex information systems, automated controls, cybersecurity arrangements, outsourced technology services, and electronically generated evidence. Based on this analysis. The study contributes to the auditing literature by linking international debates on audit digitalisation with Egypt's regulatory environment and by offering a structured framework for understanding the changing responsibilities of external auditors in digital commercial banks. It also highlights practical implications for auditors, audit firms, regulators, professional bodies, and accounting education.

Keywords: Auditing; Digital banking; Commercial banks; Audit risk; Electronic audit evidence; Digital internal controls; Assurance services; Egypt.

1. Introduction

The digital transformation of commercial banks has changed the environment in which external auditing is planned, performed, and evaluated. Banking transactions are no longer supported mainly by visible documents, manual approvals, and conventional audit trails; they are increasingly produced through integrated information systems, automated controls, digital platforms, cloud-based services, databases, cybersecurity arrangements, and outsourced technology providers. This shift changes the auditor's work from verifying isolated accounting records to assessing the reliability of the digital systems through which financial information is generated, processed, stored, and reported. Although digital accounting systems may improve information quality, decision-making, and audit efficiency, they also increase auditors' dependence on technology-based controls and electronically generated evidence. The central audit issue, therefore, is not simply whether banks adopt digital technologies, but whether external auditors can obtain sufficient appropriate evidence, reassess audit risk, and exercise professional judgement in technology-dependent financial reporting environments (Fotouh & Lorentzon, 2023); (Al-Okaily, Alghazzawi, Alkhwaldi, & Al-Okaily, 2023); (Rahman & Zirur, 2023); (Guo, Jia, & Shentu, 2024).

In Egypt, this transformation is not merely a market-driven response to technological innovation; it has become part of a wider regulatory and institutional agenda. The establishment of the National Payments Council encouraged the expansion of electronic payments and the reduction of cash-based transactions, while Law No. 18 of 2019 and its executive regulations strengthened the legal framework for non-cash payment methods. The Central Bank and Banking Sector Law No. 194 of 2020 further formalized this direction by regulating banks, payment systems operators, payment service providers, and digital banks. In parallel, the Central Bank of Egypt's Financial Inclusion Strategy 2022-2025 promotes wider access to formal financial services through digital channels, while the executive regulations of the Electronic Signature Law and the Personal Data Protection Law No. 151 of 2020 provide important legal foundations for electronic documentation, digital signatures, and electronically processed personal data. These developments make the Egyptian banking environment increasingly digital, regulated, and evidence-intensive, which directly affects the responsibilities of external auditors (Arab Republic of Egypt, 2017); (Arab Republic of Egypt, 2019); (Arab Republic of Egypt, 2020a); (Arab Republic of Egypt, 2020b); (Central Bank of Egypt, 2022); (Ministry of Communications and Information Technology, 2005); (Arab Republic of Egypt, 2020c).

The audit implications of digital banking are ambivalent. On the one hand, technologies such as data analytics, artificial intelligence, robotic process automation, digital confirmations, and automated audit tools can improve audit coverage, support risk-based procedures, and allow auditors to examine larger volumes of transactions more efficiently. Big data analytics may help auditors understand the client's environment, perform

analytical procedures, assess internal controls, and direct audit attention toward higher-risk areas. On the other hand, these benefits are not automatic. Digital banking may also intensify information technology risk, cybersecurity risk, data quality risk, outsourcing risk, and the risk of excessive reliance on automated outputs. Weak access controls, poor system configuration, unreliable data extraction, or ineffective cybersecurity arrangements may compromise the reliability of financial reporting and electronic audit evidence. For this reason, audit quality in digital banks depends not only on the availability of digital tools, but also on auditors' ability to evaluate systems, controls, data integrity, and professional scepticism in a critical manner (Barr-Pulliam, Brown-Liburd, & Sanderson, 2022); (Alrashidi, Almutairi, & Zraqat, 2022); (Huang & Vasarhelyi, 2019); (Noordin, Hussainey, & Hayek, 2022); (Adiloglu & Gungor, 2019); (Lugli & Bertacchini, 2023); (Atolo & Mukoma, 2025).

This issue is particularly important in emerging markets, where regulatory initiatives and banking innovation may advance faster than audit methodologies, professional guidance, and digital audit education. In the Egyptian context, prior evidence indicates that digital transformation is expected to affect key determinants of audit quality, especially auditors' qualifications, audit procedures, and the timing of audit reporting. This suggests that the challenge is not limited to banks' adoption of digital systems but extends to the readiness of the auditing profession to adapt its competencies and judgement to a more complex digital environment. As digital banking expands through mobile wallets, prepaid cards, electronic payment channels, digital accounts, and platform-based services, auditors must deal with larger volumes of electronically generated data while also assessing whether such data are complete, secure, traceable, and legally accessible. Thus, digitalisation reshapes the audit process itself, including client understanding, risk assessment, evidence collection, internal control evaluation, and reporting (Almaleeh, 2021).

Despite the growing body of research on digitalisation and auditing, the literature remains fragmented. Some studies examine specific technologies such as blockchain, artificial intelligence, big data analytics, or robotic process automation, while others discuss audit digitalisation in broad professional terms or in developed-market settings. These studies are useful, but they do not sufficiently explain how digital banking changes external auditors' responsibilities within Egypt's specific legal, institutional, and banking environment. More importantly, the literature often treats digital technologies as separate developments rather than as connected audit issues involving risk, evidence, controls, and assurance. This creates a research gap: there is a need for an integrated audit-focused framework that explains how Egypt's digital banking transformation affects the responsibilities of external auditors beyond the traditional financial statement audit (Liu, Wu, & Xu, 2019); (Bonsón & Bednárová, 2019); (Tiberius & Hirth, 2019); (Manita, Elommal, Baudier, & Hikkerova, 2020); (Argento, Jääskeläinen, & Rautiainen, 2025).

Based on this gap, the present study examines external auditing in Egypt's digital banking environment through a critical four-dimensional analytical framework. The study addresses the following research question: How does the digitalisation of commercial banks reshape the responsibilities, audit approach, and assurance role of external auditors in Egypt? To answer this question, the paper adopts a structured critical analytical approach that synthesizes academic literature, professional publications, and Egyptian regulatory documents. The analysis is organized around four interrelated dimensions: audit risk reassessment, electronic audit evidence evaluation, digital internal control assessment, and the expansion of assurance and advisory services. The study contributes to the auditing literature by shifting the discussion from a general description of banking digitalisation to a critical analysis of external auditors' changing responsibilities in Egypt. It also provides a conceptual basis for future empirical research and professional guidance on auditing digital commercial banks in emerging markets. The remainder of the paper is organized as follows. Section 2 explains the methodological approach. Section 3 presents the theoretical foundation. Section 4 analyses the Egyptian digital banking and regulatory context. Section 5 synthesizes the literature around the four dimensions of the framework. Section 6 presents the proposed analytical framework. Section 7 discusses the implications for practice, regulation, and education. Section 8 concludes the paper and outlines limitations, recommendations, and future research directions.

2. Methodological Approach

This study adopts a structured critical review and conceptual analytical approach. This choice is appropriate because the study does not seek to test statistical relationships or measure auditors' perceptions through field data. Its purpose is to interpret how the digital transformation of commercial banks changes the conditions under which external auditors assess risk, evaluate electronic evidence, examine digital controls, and consider broader assurance responsibilities. The review therefore serves as a method of conceptual integration: it brings together fragmented academic and professional debates and reorganizes them around an audit-focused framework relevant to Egypt's digital banking environment (Torraco, 2005); (Snyder, 2019).

The review was designed to avoid a purely descriptive account of digital banking technologies. Instead, it reads the literature critically by comparing the potential audit benefits of data analytics, artificial intelligence, robotic process automation, and digital confirmations with the risks created by system dependence, cybersecurity exposure, data integrity problems, automated controls, and electronically generated evidence. In this sense, the Egyptian context is treated as part of the analysis rather than as background information. Academic studies were used to clarify the professional implications of audit digitalisation, while Egyptian regulatory documents were used to explain how these implications become more specific under local banking, payment, electronic documentation, financial inclusion, and data protection frameworks (Huang & Vasarhelyi, 2019); (ALrashidi, Almutairi, &

Zraqat, 2022); (Fotoh & Lorentzon, 2023); (Lugli & Bertacchini, 2023); (Guo, Jia, & Shentu, 2024); (Argento, Jääskeläinen, & Rautiainen, 2025); (Arab Republic of Egypt, 2017); (Arab Republic of Egypt, 2019); (Arab Republic of Egypt, 2020a); (Arab Republic of Egypt, 2020b); (Arab Republic of Egypt, 2020c); (Central Bank of Egypt, 2022); (Ministry of Communications and Information Technology, 2005).

The source selection process was guided by the audit-focused purpose of the study. Since digital banking affects external auditing through technological, accounting, regulatory, and assurance-related channels, the review focused on studies addressing digital banking, audit digitalisation, audit quality, audit risk, electronic audit evidence, data analytics, artificial intelligence, blockchain, cybersecurity, internal controls, and assurance services. The search mainly covered recent literature from 2018 to 2026, while earlier sources were retained when they provided methodological or foundational value. Academic sources were identified through major accounting, auditing, information systems, and finance-related databases and publishers, including Emerald, ScienceDirect, Taylor & Francis, Springer, Wiley, MDPI, and Google Scholar. The search combined terms such as “digital banking,” “external audit,” “audit risk,” “electronic audit evidence,” “digital internal control,” “cybersecurity,” “data analytics,” “artificial intelligence,” “blockchain,” and “assurance services.” Sources were retained when they helped explain at least one of the four analytical dimensions of the paper: audit risk reassessment, electronic audit evidence evaluation, digital internal control assessment, or the expansion of assurance and advisory services. Egyptian regulatory and institutional documents were also included when they directly shaped the local audit environment, particularly in relation to digital banks, non-cash payments, payment service providers, financial inclusion, electronic documentation, and personal data protection. These documents were used to contextualize the international literature rather than replace it, allowing the review to connect global audit digitalisation debates with the specific regulatory conditions of Egypt’s banking sector (Tiberius & Hirth, 20196); (Manita, Elommal, Baudier, & Hikkerova, 2020); (ALrashidi, Almutairi, & Zraqat, 2022); (Rahman & Ziru, 2023); (Torraco, 2005); (Snyder, 2019); (Arab Republic of Egypt, 2019); (Arab Republic of Egypt, 2020b); (Arab Republic of Egypt, 2020c); (Central Bank of Egypt, 2022); (Ministry of Communications and Information Technology, 2005)

To maintain analytical focus, the review applied clear inclusion and exclusion criteria that kept the analysis closely connected to its audit-focused purpose. Academic studies were included when they addressed digital banking, audit digitalisation, audit quality, audit risk, electronic audit evidence, data analytics, artificial intelligence, blockchain, cybersecurity, internal controls, or assurance services. Priority was given to studies published between 2018 and 2026, as this period reflects the rapid expansion of digital banking and technology-enabled audit practices. Earlier sources were retained only when they provided methodological or foundational value for conducting a critical review or explaining broader

changes in audit practice (Torraco, 2005); (Tiberius & Hirth, 20196); (Snyder, 2019); (Manita, Elommal, Baudier, & Hikkerova, 2020).

Conversely, Sources were excluded when they discussed digital transformation in general terms without clear relevance to external auditing, banking systems, audit risk, evidence, controls, or assurance responsibilities. Studies that focused only on technological efficiency without considering professional judgement, control reliability, cybersecurity, or evidence quality were also excluded. Egyptian laws, regulations, and institutional documents were included when they directly shaped the local digital banking environment, particularly in relation to non-cash payments, digital banks, electronic documentation, personal data protection, and financial inclusion. This selection logic allowed the review to combine academic relevance with contextual relevance, so that the analysis remained grounded in both international audit literature and Egypt's regulatory setting (Arab Republic of Egypt, 2019); (Arab Republic of Egypt, 2020a); (Arab Republic of Egypt, 2020b); (Arab Republic of Egypt, 2020c); (Central Bank of Egypt, 2022); (Rahman & Ziru, 2023); (Guo, Jia, & Shentu, 2024).

The selected sources were then analysed using thematic coding rather than a chronological or technology-by-technology presentation. This approach was adopted because the paper is concerned with the audit implications of digital banking, not with describing each technology separately. The coding process grouped the literature around four audit-related themes: audit risk reassessment, electronic audit evidence evaluation, digital internal control assessment, and the expansion of assurance and advisory services. These themes made it possible to connect different technologies, including big data analytics, artificial intelligence, blockchain, robotic process automation, and digital confirmations, to the practical responsibilities of external auditors in commercial banks (Huang & Vasarhelyi, 2019); (Liu, Wu, & Xu, 2019); (ALrashidi, Almutairi, & Zraqat, 2022); (Noordin, Hussainey, & Hayek, 2022).

The synthesis followed a critical logic by comparing the benefits and limitations identified in prior studies. Literature that presents digital tools as a means of improving audit efficiency and evidence coverage was read alongside studies warning about system dependence, weak digital controls, cybersecurity exposure, data integrity problems, and overreliance on automated outputs. Egyptian regulatory documents were then used to interpret these themes within the local banking environment, particularly in relation to digital banks, non-cash payments, electronic documentation, personal data protection, and financial inclusion. This process allowed the four-dimensional framework to emerge from the interaction between international audit literature and Egypt's regulatory context, rather than from a descriptive listing of technologies (De Santis & D'Onza, 2021); (Fotoh & Lorentzon, 2023); (Lugli & Bertacchini, 2023); (Argento, Jääskeläinen, & Rautiainen, 2025); (Arab Republic of Egypt, 2020b); (Arab Republic of Egypt, 2020c); (Central Bank of Egypt, 2022).

Egyptian regulatory documents were incorporated into the analytical context of the review rather than treated merely as background material, because external auditing in digital banking is shaped by the legal and institutional conditions under which banks operate. Documents relating to non-cash payments, digital banks, financial inclusion, electronic signatures, and personal data protection were used to explain how Egypt's regulatory environment affects the four dimensions of the analytical framework: audit risk, electronic evidence, digital controls, and assurance needs. Banking and payment regulations helped interpret the risk implications of digital banks, payment systems, and service providers; the electronic signature framework clarified the legal status of electronic records and signatures; and the personal data protection framework highlighted issues related to auditors' access to customer data, privacy obligations, and secure handling of electronically processed information. This use of regulatory material prevents the analysis from applying international audit literature to Egypt in a generic way and shows how local regulation gives specific meaning to audit risk, evidence reliability, control assessment, and assurance responsibilities in Egypt's digital banking environment (Arab Republic of Egypt, 2019; Arab Republic of Egypt, 2020b; Arab Republic of Egypt, 2020c; Central Bank of Egypt, 2022; Ministry of Communications and Information Technology, 2005; (Snyder, 2019); (Almaleeh, 2021) ; (Rahman & Zirur, 2023); (Guo, Jia, & Shentu, 2024).

3. Theoretical Foundation

This study is grounded in three complementary theoretical lenses that together explain how digital banking reshapes external auditing in Egypt. The extended audit risk model explains how digitalisation expands inherent risk, control risk, and detection risk in technology-dependent banking environments. Institutional theory helps explain how regulation, professional expectations, and market pressures shape banks' digital transformation and auditors' responsibilities. The Technology-Organization-Environment perspective then connects technological systems, organizational readiness, and regulatory conditions. Together, these lenses provide the conceptual basis for the four-dimensional analytical framework developed later in the paper.

3.1 Extended Audit Risk Model

The traditional audit risk model remains a useful starting point for analysing external auditing in digital commercial banks because it links audit work to inherent risk, control risk, and detection risk. However, digital banking expands the meaning of these components. Inherent risk is no longer associated only with the complexity of banking transactions, estimates, or financial instruments; it also arises from real-time processing, digital payment channels, automated workflows, cybersecurity threats, system integration, and reliance on third-party technology providers. Control risk also becomes more technology-dependent, as key controls are increasingly embedded in access rights, application controls, automated authorization procedures, cybersecurity safeguards,

database controls, and general information technology controls. In this environment, the auditor must evaluate whether such controls are properly designed, consistently operating, and protected from unauthorized access or manipulation (Kahyaoglu & Caliyurt, 2018); (Anomah, Ayebofo, & Aduamoah, 2021); (Betti & Sarens, 2021); (Al-Khasawneh, 2022); (Atolo & Mukoma, 2025).

Detection risk is also reshaped because audit procedures increasingly depend on data extracted from digital systems. Data analytics, artificial intelligence, and automated audit tools may help auditors examine larger transaction populations and identify unusual patterns, but these tools can also create overreliance if auditors do not test data completeness, extraction logic, system reliability, and the quality of the underlying records. The extended audit risk model used in this paper therefore treats digitalisation as an expansion of traditional audit risk rather than a replacement of it. It provides the theoretical basis for the first dimension of the analytical framework: audit risk reassessment. Once digital banking changes how accounting information is generated, processed, stored, and reported, the auditor's risk assessment must also extend to information technology risk, cybersecurity risk, data integrity risk, automation risk, and outsourcing risk (Huang & Vasarhelyi, 2019); (Fotoh & Lorentzon, 2023); (ALrashidi, Almutairi, & Zraqat, 2022).

3.2 Institutional Theory

Institutional theory helps explain why digital banking in Egypt should not be analysed only as a technological choice made by individual banks. Commercial banks operate within an institutional environment shaped by regulation, professional expectations, market competition, and public policy priorities. From this perspective, the move toward digital banking reflects coercive pressures from laws and regulators, normative pressures from professional and governance expectations, and competitive pressures from financial technology developments and changing customer behaviour. This lens is useful for external auditing because auditors do not assess digital banking systems in isolation; they evaluate them within a regulated environment that defines compliance expectations, acceptable evidence, control responsibilities, and accountability requirements (DiMaggio & Powell, 1993); (Scott, 2014).

In Egypt, institutional pressure toward digital banking is reflected in the regulation of non-cash payments, the legal recognition of digital banks, financial inclusion policies, electronic documentation rules, and personal data protection requirements. These developments expand the digital environment in which banking transactions are initiated, processed, recorded, and reported, and they make audit risk, electronic evidence, digital controls, and assurance needs more dependent on regulatory context. Institutional theory therefore supports the argument that the auditor's changing responsibilities are produced by the interaction between technological development and regulatory pressure, not by technology alone. It also highlights a possible gap between the speed of banking digitalisation and the readiness of audit methodologies, professional education, and

regulatory guidance to address system reliability, cybersecurity, data governance, and professional scepticism (Arab Republic of Egypt, 2019; Arab Republic of Egypt, 2020b; Arab Republic of Egypt, 2020c; (Almaleeh, 2021) ; (Rahman & Ziru, 2023); (Argento, Jääskeläinen, & Rautiainen, 2025).

3.3 Technology–Organization–Environment Perspective

The Technology–Organization–Environment (TOE) perspective complements the audit risk and institutional lenses by showing that the audit implications of digital banking cannot be explained by technology alone. The technological dimension covers the digital platforms, payment systems, data analytics, artificial intelligence, blockchain applications, cloud services, and automated controls used by banks. These tools become audit-relevant when they affect how transactions are processed, how evidence is produced, and how risks are controlled. The organizational dimension adds another layer: the audit effect of digital banking depends on the bank's governance structure, data quality, control maturity, technology management, and ability to monitor system-based risks. In this sense, digital transformation may improve information quality and audit evidence only when it is supported by reliable systems, effective internal controls, and a clear digital governance structure (Tornatzky & Fleischer, 1990); (Manita, Elommal, Baudier, & Hikkerova, 2020); (Betti & Sarens, 2021); (Nasiri, Saunila, Ukko, & Rantala, 2022); (Rahman & Ziru, 2023).

The environmental dimension is especially important in Egypt because banks operate within a regulatory setting that encourages digital banks, non-cash payments, financial inclusion, electronic documentation, and personal data protection. These conditions shape both banks' digital strategies and auditors' responsibilities, since external auditors must evaluate technology-dependent financial reporting within a legal and institutional environment. The TOE perspective therefore supports the paper's central argument: digital banking creates audit opportunities, but these opportunities are conditional on organizational readiness, control reliability, and regulatory clarity. Where digital systems expand faster than audit skills, guidance, or control maturity, they may increase rather than reduce audit risk. This makes the TOE perspective useful for linking the four dimensions of the framework: audit risk reassessment, electronic evidence evaluation, digital internal control assessment, and the expansion of assurance responsibilities (Arab Republic of Egypt, 2019; Arab Republic of Egypt, 2020b; Arab Republic of Egypt, 2020c; Central Bank of Egypt, 2022; (Fotoh & Lorentzon, 2023); (Argento, Jääskeläinen, & Rautiainen, 2025).

4. Egyptian Digital Banking and Regulatory Context

4.1 Regulatory Drivers of Banking Digitalisation in Egypt

Banking digitalisation in Egypt is shaped by a combination of technological change, market competition, and regulatory intervention. On the market side, commercial banks increasingly rely on digital platforms, mobile banking, electronic payment channels, data

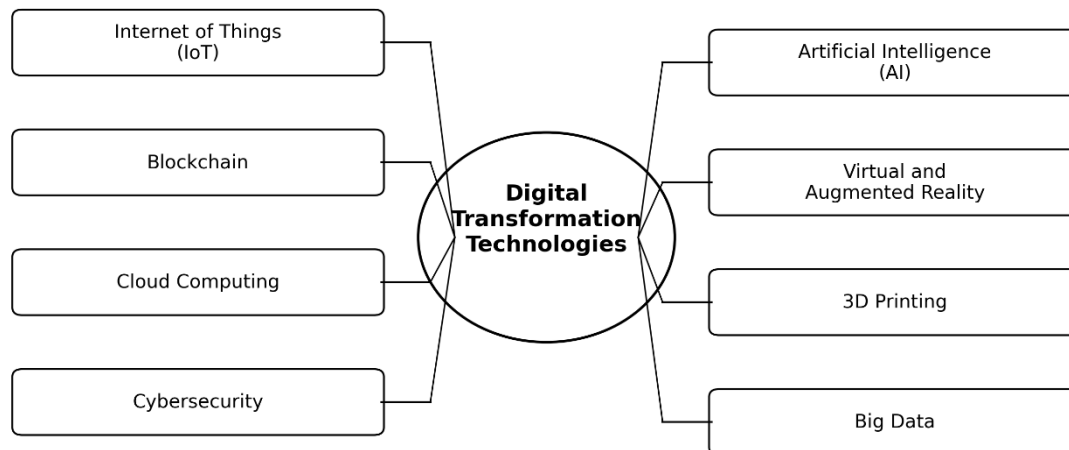
analytics, and financial technology solutions to improve service delivery, reduce transaction costs, and respond to competition from FinTech firms and non-bank financial service providers (Zohry, Fadel, & Khamis, 2021); (Al-Okaily, Alghazzawi, Alkhwalidi, & Al-Okaily, 2023); (Johri, et al., 2026). Yet the Egyptian case cannot be explained by market pressure alone. The establishment of the National Payments Council, Law No. 18 of 2019 on non-cash payment methods, its executive regulations, and the Central Bank and Banking Sector Law No. 194 of 2020 show that digital banking has become part of a wider state-led financial transformation agenda (Arab Republic of Egypt, 2017; Arab Republic of Egypt, 2019; Arab Republic of Egypt, 2020a; Arab Republic of Egypt, 2020b).

These regulatory drivers have direct audit implications. As electronic payments, digital accounts, mobile wallets, prepaid cards, and platform-based financial services expand under the Financial Inclusion Strategy 2022–2025, commercial banks generate larger volumes of digital transactions and system-based records (Central Bank of Egypt, 2022). For external auditors, this increases the importance of assessing the reliability of digital transaction flows, data integrity, cybersecurity arrangements, automated controls, and electronically generated evidence. The main professional challenge is that regulation may accelerate digital banking adoption faster than audit methodologies, technical skills, and professional guidance can adapt. As a result, digitalisation may improve audit efficiency and evidence availability, but it may also increase audit risk where auditors lack the competence or tools needed to examine complex banking systems critically (Almaleeh, 2021); (Fotoh & Lorentzon, 2023); (Rahman & Ziru, 2023); (Argento, Jääskeläinen, & Rautiainen, 2025).

4.2 Digital Banks under Egyptian Banking Law

The legal recognition of digital banks under the Central Bank and Banking Sector Law No. 194 of 2020 represents a significant institutional shift in Egypt's banking sector. The law recognizes digital banks as banks that provide banking services through digital channels or platforms using modern technologies (Arab Republic of Egypt, 2020b). This definition moves digital banking beyond the idea of traditional banks offering mobile applications or internet banking services. It indicates a banking model in which service delivery, customer interaction, transaction processing, monitoring, and control are increasingly organized through digital infrastructures. Prior literature suggests that digital banking can improve service efficiency, reduce operating costs, expand customer access, and support more flexible business models (Tjendani, Widagdo, & Muthmainah, 2018); (Al-Okaily, Alghazzawi, Alkhwalidi, & Al-Okaily, 2023); (Johri, et al., 2026). For external auditors, however, the professional issue is not whether digital banks are operationally efficient, but whether their systems generate reliable accounting information, maintain effective controls, and provide sufficient appropriate audit evidence. Figure 1 summarizes the main technologies that support this transformation and shows why digital banking should be treated as an audit-relevant environment rather than a purely operational development.

Figure 1. Key Technologies Enabling Digital Banking Transformation



Note. Adapted by the researchers based on prior literature on digital banking and audit digitalisation (Manita, Elommal, Baudier, & Hikkerova, 2020); (Wang, Sui, & Zhang, 2021); (Al-Okaily, Alghazzawi, Alkhwalidi, & Al-Okaily, 2023); (Rahman & Ziru, 2023); (Hanfy, Alakkas, & Alhumoudi, 2025).

The audit implications of digital banks arise from the technologies and infrastructures on which they depend. Cloud computing, artificial intelligence, big data analytics, blockchain-based applications, cybersecurity tools, and automated workflows may improve processing speed, scalability, and data availability, but they also create risks related to system dependence, unauthorized access, algorithmic processing, outsourcing, data integrity, and weak digital audit trails (Adiloglu & Gungor, 2019); (Abdennadher, Grassa, Abdulla, & Alfalasi, 2022); (Hanfy, Alakkas, & Alhumoudi, 2025). As a result, the auditor's work shifts from examining transactions as isolated accounting events to evaluating the digital environment in which those transactions are initiated, authorized, processed, stored, and reported. In Egypt, this shift creates a direct connection between banking law and audit responsibility: once digital banks become legally recognized banking institutions, external auditors need to integrate financial audit procedures with information systems audit procedures and assess digital risk, electronic evidence, internal control reliability, cybersecurity arrangements, and technology-enabled assurance needs (Al-Khasawneh, 2022); (Lugli & Bertacchini, 2023); (Argento, Jääskeläinen, & Rautiainen, 2025).

4.3 Electronic Evidence, Data Protection, and Cybersecurity Regulation

The expansion of digital banking in Egypt changes the nature of audit evidence because many banking transactions are now initiated, authorized, processed, stored, and retrieved electronically. In this environment, audit evidence may consist of system logs, electronic records, digital confirmations, automated reports, data extracts, and electronically signed documents. The executive regulations of the Electronic Signature Law provide a legal basis for recognizing electronic documents, electronic signatures, electronic media, and

certification mechanisms (Ministry of Communications and Information Technology, 2005). However, legal recognition does not by itself make electronic evidence sufficient or appropriate for audit purposes. External auditors still need to assess whether such evidence is authentic, complete, traceable, protected from manipulation, and supported by reliable controls over its creation, storage, transmission, and retrieval. This is particularly important in digital banks, where the reliability of audit evidence depends less on the physical existence of documents and more on the integrity of the systems that generate and preserve them (Rahman & Ziru, 2023); (Guo, Jia, & Shentu, 2024).

Data protection and cybersecurity regulation further shape the auditor's work in digital banking. The Personal Data Protection Law No. 151 of 2020 is relevant because audit procedures may require access to customer data, transaction histories, digital account records, system reports, and information processed by third-party service providers (Arab Republic of Egypt, 2020c). This creates a professional balance: auditors need sufficient appropriate evidence, but they must obtain, use, and document that evidence within legal and ethical limits relating to confidentiality, privacy, purpose limitation, and secure data handling. Cybersecurity controls are equally important because weaknesses in authentication, access rights, encryption, incident response, backup procedures, or third-party technology governance may compromise financial data and digital audit trails. For this reason, cybersecurity should not be treated as a separate technical issue, but as part of audit risk, evidence reliability, and internal control assessment in Egypt's digital banking environment (Kahyaoglu & Caliyurt, 2018); (Al-Khasawneh, 2022); (Lugli & Bertacchini, 2023); (Atolo & Mukoma, 2025).

5. Critical Literature Synthesis

This section synthesizes the literature thematically rather than descriptively. Instead of presenting digital banking technologies as separate developments, the analysis examines how these technologies reshape the external audit function. The synthesis is organized around the four dimensions of the model: audit risk reassessment, electronic audit evidence evaluation, digital internal control assessment, and the expansion of assurance and advisory services. This structure allows the discussion to move from general technological change to its professional implications for external auditors in Egyptian commercial banks.

5.1 Digitalisation as an Audit Risk Driver

Digitalisation should be treated as a direct driver of audit risk because it changes the conditions under which banking transactions are initiated, processed, authorized, recorded, and reported. In commercial banks, digital platforms, mobile applications, automated payment systems, cloud services, and data analytics may improve service delivery and provide auditors with richer data, but they also create new layers of technological complexity. Audit risk is therefore no longer limited to transaction volume, financial instruments, or accounting estimates; it also includes information technology risk,

cybersecurity risk, data integrity risk, system availability risk, automation risk, and reliance on third-party technology providers. This requires auditors to move from a mainly transaction-based understanding of risk to a system-based view that considers how digital infrastructures affect the risk of material misstatement (Jiang, Du, & Chen, 2022); (Al-Khasawneh, 2022); (Jardak & Hamad, 2022); (Atolo & Mukoma, 2025).

The literature shows that digital transformation can improve transparency, internal control quality, and audit coverage when banks operate reliable systems and strong data governance mechanisms. Yet these benefits remain conditional. Poor system configuration, weak access controls, unreliable data extraction, cyber incidents, or ineffective monitoring may increase rather than reduce audit risk, especially in banks where large volumes of transactions are processed in real time (Kahyaoglu & Caliyurt, 2018); (Fotoh & Lorentzon, 2023); (Lugli & Bertacchini, 2023); (Rahman & Zirur, 2023); (Guo, Jia, & Shentu, 2024). In Egypt, this concern is intensified by the regulatory expansion of non-cash payments, digital banks, and financial inclusion, which increases the volume of electronically generated transactions and strengthens banks' dependence on digital infrastructures. For this reason, audit risk reassessment becomes the starting point of the four-dimensional framework, as it determines how auditors subsequently evaluate electronic evidence, digital controls, and assurance needs in Egypt's digital banking environment (Arab Republic of Egypt, 2019; Arab Republic of Egypt, 2020b; Central Bank of Egypt, 2022; (Argento, Jääskeläinen, & Rautiainen, 2025).

5.2 Electronic Audit Evidence and Digital Audit Trails

Digital banking changes audit evidence not only by increasing its volume, but also by changing its form, source, and conditions of reliability. In digital commercial banks, external auditors increasingly rely on system logs, electronic records, digital confirmations, automated reconciliations, transaction metadata, data extracts, and electronically signed documents. These forms of evidence may allow wider audit coverage and more timely testing, especially when supported by data analytics and digital confirmation tools. However, electronic evidence should not be treated as reliable simply because it is generated by a system. Its audit value depends on whether the underlying data are complete, accurate, authorized, traceable, and protected from unauthorized alteration. This makes electronic evidence evaluation a more judgmental process, as auditors must assess both the evidence itself and the digital environment from which it is produced (Rahman & Zirur, 2023); (Guo, Jia, & Shentu, 2024).

Digital audit trails may also be strengthened by technologies such as blockchain, automated audit tools, and system-based verification mechanisms, but their benefits remain conditional. Blockchain and similar technologies can improve transparency and reduce manual intervention, yet they do not remove the need to evaluate system governance, access rights, data extraction procedures, and control reliability (Liu, Wu, & Xu, 2019); (Schmitz & Leoni, 2019); (Abdennadher, Grassa, Abdulla, & Alfalasi, 2022). In Egypt, the executive

regulations of the Electronic Signature Law support the legal recognition of electronic documents and signatures, while the regulation of non-cash payments and digital banks increases the volume of electronic records available for audit purposes (Ministry of Communications and Information Technology, 2005; Arab Republic of Egypt, 2019; Arab Republic of Egypt, 2020b). Legal validity, however, is not the same as audit sufficiency. External auditors must still test authenticity, completeness, security, system access, and data integrity before relying on digital evidence. For this reason, electronic audit evidence forms the second dimension of the framework, linking audit risk reassessment with digital internal control assessment and broader questions of evidence reliability in digital commercial banks (Fotoh & Lorentzon, 2023); (Hsieh & Brennan, 2022); (Lugli & Bertacchini, 2023).

5.3 Digital Internal Controls and Cybersecurity Controls

Digital internal controls are central to auditing digital commercial banks because the reliability of accounting information increasingly depends on automated processes rather than manual procedures. In this environment, traditional controls such as authorization, reconciliation, and segregation of duties remain important, but they are increasingly embedded in access permissions, application controls, automated workflows, database controls, and general information technology controls. External auditors therefore need to examine whether these controls are properly designed, consistently applied, and capable of preventing or detecting errors, unauthorized transactions, and manipulation of digital records. This requires a shift from confirming the existence of controls to evaluating their operating effectiveness within complex information systems, especially where banking transactions are processed in real time and supported by integrated digital platforms (Betti & Sarens, 2021); (Al-Khasawneh, 2022); (Rahman & Ziru, 2023).

Cybersecurity controls form a critical part of this assessment because weaknesses in authentication, user access, encryption, incident response, backup procedures, network security, or third-party technology governance may directly affect financial data and digital audit trails. A cybersecurity failure in a digital bank is not merely an operational IT problem; it may compromise transaction completeness, data accuracy, customer balances, service continuity, and the reliability of system-generated reports. Prior literature also suggests that the sophistication of digital banking systems may exceed the traditional capabilities of some audit teams, making IT specialists, data analytics, and stronger digital audit methodologies increasingly important (Kahyaoglu & Caliyurt, 2018); (Manita, Elommal, Baudier, & Hikkerova, 2020); (ALrashidi, Almutairi, & Zraqat, 2022); (Fotoh & Lorentzon, 2023); (Lugli & Bertacchini, 2023); (Argento, Jääskeläinen, & Rautiainen, 2025). In Egypt, the regulatory expansion of digital banks, non-cash payments, and financial inclusion strengthens the need for auditors to evaluate controls over system access, transaction processing, data storage, cybersecurity, and outsourced technology services, making digital internal control assessment the third dimension of the analytical framework (Arab Republic of Egypt, 2019; Arab Republic of Egypt, 2020b; Central Bank of Egypt, 2022).

5.4 Auditor Competence, Data Analytics, and Professional Scepticism

Digital banking increases the importance of auditors' technological competence because audit work now depends more heavily on understanding systems, data flows, automated controls, and technology-generated evidence. Tools such as data analytics, artificial intelligence, and robotic process automation can help auditors examine larger transaction populations, identify unusual patterns, and perform more focused risk assessment procedures. However, these tools do not reduce the need for professional judgement; they change the type of judgement required. Auditors must be able to evaluate data quality, extraction logic, system reliability, analytical assumptions, and the relevance of automated results before using them as audit evidence. Without this competence, digital tools may create a false sense of assurance and increase the risk of overreliance on management-provided reports or system outputs (Huang & Vasarhelyi, 2019); (Tušek, Ježovita, & Halar, 2021); (Jacky & Sulaiman, 2022); (Fotoh & Lorentzon, 2023); (Guo, Jia, & Shentu, 2024).

This competence challenge is especially important in emerging markets, where digital banking may develop faster than audit education, professional guidance, and firm-level technological capabilities. Evidence from Egyptian auditors indicates that digital transformation affects audit quality determinants, particularly auditors' qualifications, audit procedures, and the timing of audit reporting (Almaleeh, 2021). The issue, therefore, is not simply whether auditors use advanced technologies, but whether they can use them critically while maintaining professional scepticism. In digital commercial banks, scepticism requires auditors to question the completeness of data, the reliability of system-generated evidence, the effectiveness of automated controls, and the assumptions embedded in analytical tools. Auditor competence therefore acts as a connecting condition across the four dimensions of the framework, because weak digital skills may undermine risk reassessment, electronic evidence evaluation, digital control testing, and assurance quality (Manita, Elommal, Baudier, & Hikkerova, 2020); (Lugli & Bertacchini, 2023); (Argento, Jääskeläinen, & Rautiainen, 2025).

5.5 Assurance and Advisory Services in Digital Banking

Digital banking expands the potential scope of assurance because banks now depend heavily on digital platforms, electronic payment systems, automated controls, cybersecurity arrangements, data governance structures, and third-party technology providers. These areas may affect the reliability of financial reporting even when they fall partly outside traditional transaction testing. Prior literature suggests that emerging technologies create demand for assurance over system reliability, blockchain-based records, data analytics, cybersecurity controls, and technology-enabled reporting (Kend & Nguyen, 2020); (Manita, Elommal, Baudier, & Hikkerova, 2020); (Abdennadher, Grassa, Abdulla, & Alfalasi, 2022). In digital commercial banks, users may therefore need greater confidence not only in the

financial statements, but also in the systems and controls that produce the underlying information.

The expansion of assurance and advisory services must nevertheless be approached carefully. External auditors may be expected to provide insight into digital controls, data quality, cybersecurity weaknesses, privacy compliance, and system-based risks, but these services should not compromise independence, objectivity, or the quality of the financial statement audit. This issue is particularly relevant in Egypt, where regulation of digital banks, non-cash payments, financial inclusion, electronic documentation, and personal data protection may increase demand for assurance over digital payment controls, data governance, cybersecurity arrangements, and electronically generated records (Arab Republic of Egypt, 2019; Arab Republic of Egypt, 2020b; Arab Republic of Egypt, 2020c; Central Bank of Egypt, 2022). The fourth dimension of the framework therefore concerns the auditor's ability to respond to wider assurance needs while maintaining professional boundaries, technical competence, and sceptical judgement (Kahyaoglu & Caliyurt, 2018); (Betti & Sarens, 2021); (Rahman & Ziru, 2023); (Fotoh & Lorentzon, 2023); (Lugli & Bertacchini, 2023); (Argento, Jääskeläinen, & Rautiainen, 2025).

6. Proposed Four-Dimensional Analytical Framework

6.1 Framework Logic

The preceding analysis supports a four-dimensional analytical framework for understanding how digital banking reshapes external auditors' responsibilities in Egypt. The framework is conceptual rather than statistical; it does not test causal relationships but organizes the audit implications of digital banking into a logical sequence. It begins with audit risk reassessment, because digital platforms, automated processing, cybersecurity exposure, data dependence, and third-party technology arrangements change the conditions under which material misstatements may arise. These altered risks then affect the second dimension, electronic audit evidence evaluation, since auditors increasingly rely on system-generated records, electronic documents, data extracts, digital confirmations, and audit trails whose reliability depends on the systems that produce them (Fotoh & Lorentzon, 2023); (Al-Khasawneh, 2022); (Lugli & Bertacchini, 2023).

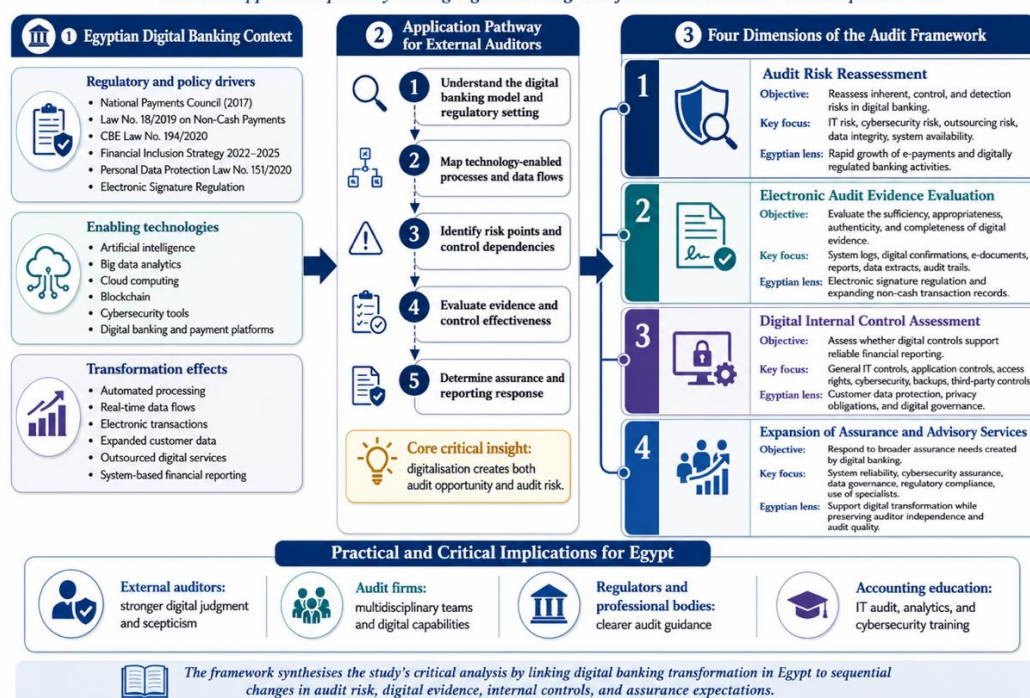
The third-dimension concerns digital internal control assessment, because electronic evidence cannot be evaluated independently from access controls, application controls, cybersecurity controls, general IT controls, and controls over outsourced technology services. The final dimension addresses the expansion of assurance and advisory services, as digital banking creates wider demand for assurance over data governance, cybersecurity, system reliability, digital payment controls, and compliance with digital regulation. In Egypt, these four dimensions are shaped by a regulatory environment that promotes non-cash payments, digital banks, financial inclusion, electronic documentation, and personal data protection. The framework therefore links technological change with audit judgement

and local regulation, showing that external auditors are not merely required to use more digital tools, but to evaluate the reliability of technology-dependent financial reporting environments more critically (Arab Republic of Egypt, 2019; Arab Republic of Egypt, 2020b; Arab Republic of Egypt, 2020c; Central Bank of Egypt, 2022; (Argento, Jääskeläinen, & Rautiainen, 2025).

Figure 2 presents the proposed four-dimensional framework and illustrates how it applies to external auditing in Egypt's digital banking environment.

Proposed Four-Dimensional Framework for Auditing Digital Commercial Banks in Egypt

A critical application pathway linking digital banking transformation to external audit responsibilities



Note. Developed by the researchers based on prior audit digitalisation literature and Egyptian regulatory documents (Manita, Elommal, Baudier, & Hikkerova, 2020); (Almaleeh, 2021) ; (Rahman & Ziru, 2023); (Guo, Jia, & Shentu, 2024); Arab Republic of Egypt, 2020b; Central Bank of Egypt, 2022).

6.2 Audit Risk Reassessment

Audit risk reassessment is the starting point of the framework because digital banking changes the conditions under which material misstatements may arise. In commercial banks, risk is no longer linked only to transaction volume, financial instruments, accounting estimates, or management judgement. It also emerges from automated processing, real-time payments, system integration, cybersecurity exposure, data quality weaknesses, cloud-based services, and reliance on third-party technology providers. These features require auditors to interpret inherent risk, control risk, and detection risk more broadly. Inherent risk may increase when digital products and payment channels generate

large volumes of transactions rapidly; control risk becomes more dependent on access controls, application controls, cybersecurity safeguards, and general IT controls; and detection risk may rise if auditors rely on data extracts or system-generated reports without testing their completeness, accuracy, and extraction logic (Anomah, Ayebofo, & Aduamoah, 2021); (Kahyaoglu & Caliyurt, 2018); (Al-Khasawneh, 2022); (Atolo & Mukoma, 2025).

This reassessment is particularly important in Egypt because the regulatory expansion of non-cash payments, digital banks, and financial inclusion increases banks' dependence on electronic transaction flows and technology-based financial reporting systems (Arab Republic of Egypt, 2019; Arab Republic of Egypt, 2020b; Central Bank of Egypt, 2022). Digitalisation may improve audit efficiency and allow wider evidence coverage, but it may also conceal weaknesses that are difficult to detect through traditional audit procedures, such as poor system configuration, unauthorized access, weak cybersecurity monitoring, unreliable data extraction, or inadequate governance of outsourced technology services. For this reason, auditors should not treat digital banking as evidence of stronger control reliability by default. They need to reassess audit risk critically before deciding how far they can rely on electronic evidence, automated controls, and technology-enabled audit procedures (Fotoh & Lorentzon, 2023); (Lugli & Bertacchini, 2023); (Rahman & Ziru, 2023); (Guo, Jia, & Shentu, 2024); (Argento, Jääskeläinen, & Rautiainen, 2025).

6.3 Electronic Audit Evidence Evaluation

Electronic audit evidence evaluation is the second dimension of the framework because digital banking changes the form, source, and reliability conditions of the evidence used by external auditors. In digital commercial banks, audit evidence may include system logs, electronic transaction records, digital confirmations, automated reports, metadata, data extracts, and electronically signed documents. These sources can improve audit coverage and allow auditors to test larger populations of transactions, but their reliability cannot be assumed merely because they are system-generated. Auditors need to evaluate whether electronic evidence is complete, accurate, authorized, traceable, securely stored, and protected from unauthorized alteration. This makes evidence evaluation more dependent on understanding the systems, interfaces, access rights, and extraction procedures through which audit data are produced (Rahman & Ziru, 2023); (Guo, Jia, & Shentu, 2024); (Hsieh & Brennan, 2022).

In Egypt, the legal recognition of electronic documents and signatures provides an important basis for using digital records in business and banking contexts, but legal validity is not equivalent to audit sufficiency. A digital document may be legally recognized while still requiring audit work to test its authenticity, completeness, security, and connection to the underlying transaction cycle. The expansion of non-cash payments, digital banks, and personal data regulation also means that auditors must balance evidence collection with

data protection, confidentiality, and secure handling of customer information (Ministry of Communications and Information Technology, 2005; Arab Republic of Egypt, 2019; Arab Republic of Egypt, 2020b; Arab Republic of Egypt, 2020c). For this reason, electronic audit evidence evaluation links the first and third dimensions of the framework: audit risk reassessment identifies where evidence risk arises, while digital internal control assessment determines whether such evidence can be relied upon for audit purposes (Fotoh & Lorentzon, 2023); (Lugli & Bertacchini, 2023).

6.4 Digital Internal Control Assessment

Digital internal control assessment is the third dimension of the framework because the reliability of electronic audit evidence depends on the controls embedded within banking information systems. In digital commercial banks, controls are no longer limited to manual authorization, reconciliation, and segregation of duties. They are increasingly built into access permissions, application controls, automated workflows, database controls, cybersecurity safeguards, and general information technology controls. External auditors therefore need to evaluate whether these controls are properly designed, effectively implemented, and capable of preventing or detecting errors, unauthorized transactions, data manipulation, and system failures. This requires audit work to move beyond documenting the existence of controls toward testing their operating effectiveness within the digital environment that produces financial information (Kahyaoglu & Caliyurt, 2018); (Betti & Sarens, 2021); (Al-Khasawneh, 2022); (Rahman & Ziru, 2023).

This assessment is especially important where banks rely on cloud services, outsourced technology providers, automated processing, and real-time payment systems. Weaknesses in user access, encryption, system configuration, incident response, backup procedures, or third-party governance may directly affect data integrity, transaction completeness, and the reliability of system-generated reports. In Egypt, the regulatory expansion of digital banks, non-cash payments, and financial inclusion increases banks' dependence on digital infrastructures, making control assessment a central part of external audit responsibility rather than a separate technical exercise (Arab Republic of Egypt, 2019; Arab Republic of Egypt, 2020b; Central Bank of Egypt, 2022). The auditor may need support from IT specialists and data analytics tools, but such support should strengthen—not replace—professional judgement over whether digital controls provide a reliable basis for audit evidence and assurance conclusions (Manita, Elommal, Baudier, & Hikkerova, 2020); (Alrashidi, Almutairi, & Zraqat, 2022); (Lugli & Bertacchini, 2023); (Argento, Jääskeläinen, & Rautiainen, 2025).

6.5 Expansion of Assurance and Advisory Services

The expansion of assurance and advisory services is the fourth dimension of the framework because digital banking creates assurance needs that extend beyond the traditional audit of financial statement balances. In digital commercial banks, financial

reporting reliability is increasingly linked to system reliability, cybersecurity arrangements, data governance, automated controls, electronic payment processes, and the performance of third-party technology providers. Users of financial information may therefore require greater confidence not only in reported figures, but also in the digital infrastructures that generate, process, and protect those figures. Prior literature indicates that emerging technologies can increase demand for assurance over blockchain-based records, data analytics, cybersecurity controls, system integrity, and technology-enabled reporting (Kend & Nguyen, 2020); (Manita, Elommal, Baudier, & Hikkerova, 2020); (Abdennadher, Grassa, Abdulla, & Alfalasi, 2022).

This expansion should be interpreted carefully, because broader assurance does not mean that external auditors should move without limits into consulting roles. Auditors may provide insights into digital controls, data quality, cybersecurity weaknesses, privacy compliance, and system-based risks, but such work must remain consistent with independence, objectivity, professional scepticism, and audit quality. In Egypt, the regulation of digital banks, non-cash payments, financial inclusion, electronic documentation, and personal data protection may increase demand for assurance over digital payment controls, data governance, cybersecurity arrangements, and electronically generated records (Arab Republic of Egypt, 2019; Arab Republic of Egypt, 2020b; Arab Republic of Egypt, 2020c; Central Bank of Egypt, 2022). The professional challenge is therefore to develop digital assurance capabilities while maintaining clear boundaries between assurance, advisory involvement, and the independent financial statement audit (Kahyaoglu & Caliyurt, 2018); (Betti & Sarens, 2021); (Rahman & Zirur, 2023); (Fotouh & Lorentzon, 2023); (Lugli & Bertacchini, 2023); (Argento, Jääskeläinen, & Rautiainen, 2025).

6.6 Framework Implications for Egypt

The proposed framework has specific implications for Egypt because digital banking is developing within a regulatory environment that actively promotes non-cash payments, digital banks, financial inclusion, electronic documentation, and personal data protection. These developments create a banking environment in which audit risk, electronic evidence, digital controls, and assurance needs are closely connected. For example, the expansion of digital payment channels increases the volume of system-generated transactions, while the legal recognition of digital banks and electronic records makes auditors more dependent on information systems and digital audit trails. The framework therefore helps translate Egypt's regulatory transformation into audit responsibilities by showing that external auditors must evaluate not only financial statement balances, but also the digital processes and controls through which those balances are produced (Arab Republic of Egypt, 2019; Arab Republic of Egypt, 2020b; Arab Republic of Egypt, 2020c; Central Bank of Egypt, 2022; Ministry of Communications and Information Technology, 2005).

The framework also highlights a professional readiness challenge for the Egyptian auditing profession. Digital banking may improve data availability, audit

coverage, and the use of analytical procedures, but these benefits depend on auditors' ability to assess system reliability, cybersecurity arrangements, data integrity, automated controls, and outsourced technology services. Without adequate digital competence, audit methodologies, and regulatory guidance, the same technologies that appear to improve audit efficiency may increase the risk of overreliance on system-generated evidence. For this reason, the framework can support audit firms, regulators, professional bodies, and accounting education providers in identifying where audit practice needs development: digital risk assessment, electronic evidence evaluation, IT control testing, cybersecurity understanding, and assurance over technology-dependent banking activities (Almaleeh, 2021); (ALrashidi, Almutairi, & Zraqat, 2022); (Rahman & Ziru, 2023); (Guo, Jia, & Shentu, 2024); (Argento, Jääskeläinen, & Rautiainen, 2025).

7. Discussion and Implications

The framework shows that commercial banks' digitalisation does not affect external auditing through a single technological channel. Rather, it reshapes the auditor's work through interconnected changes in audit risk, electronic evidence, digital internal controls, and assurance expectations. As a result, the implications of digital banking should be discussed at several levels: external auditors, audit firms, regulators and professional bodies, and accounting education.

At the level of individual external auditors, the proposed framework implies that auditors in digital commercial banks need to broaden their understanding of the audit client beyond financial statements, branches, and conventional transaction cycles. In Egypt's digital banking environment, the auditor must understand how transactions are initiated through digital channels, processed by core banking systems, authorized through automated workflows, protected by cybersecurity controls, and converted into accounting information. This requires a more system-oriented audit mindset, where audit risk assessment is linked to information technology risk, data integrity, access controls, third-party technology arrangements, and the reliability of system-generated evidence. The auditor's professional judgement therefore becomes more demanding, not less important, because digital tools may increase audit coverage while also creating risks of overreliance on automated outputs and management-provided system reports (Fotouh & Lorentzon, 2023); (Rahman & Ziru, 2023); (Guo, Jia, & Shentu, 2024).

At the practical level, traditional audit procedures in Egypt should be supported by stronger digital evidence evaluation, IT control testing, cybersecurity awareness, and data analytics competence. Auditors need to question whether electronic records are complete, accurate, traceable, securely stored, and legally accessible, especially where audit evidence includes customer data, system logs, digital confirmations, and records processed by third-party providers. This does not mean that auditors must become technology specialists, but they must be capable of directing specialist work, challenging technical explanations, and linking system weaknesses to financial reporting risk. In this sense, professional scepticism

remains central: auditors should treat digitalisation as a source of both audit opportunity and audit risk, particularly in a regulatory environment shaped by digital banks, non-cash payments, financial inclusion, electronic documentation, and personal data protection (Almaleeh, 2021); (ALrashidi, Almutairi, & Zraquat, 2022); Arab Republic of Egypt, 2020b; Arab Republic of Egypt, 2020c; Central Bank of Egypt, 2022).

The discussion then moves from individual auditor judgement to firm-level capability. Audit firms need to treat digital banking as a firm-level methodological challenge, not only as a competence issue for individual auditors. Auditing digital commercial banks requires investment in updated audit methodologies, data analytics tools, cybersecurity knowledge, information systems audit procedures, and quality control mechanisms capable of reviewing technology-dependent audit evidence. Firms also need to build multidisciplinary audit teams that combine financial audit expertise with IT audit, data analytics, cybersecurity, and banking technology knowledge. Without such firm-level support, individual auditors may be expected to evaluate complex digital systems without adequate tools, training, or specialist assistance, which may increase detection risk and weaken audit quality (Manita, Elommal, Baudier, & Hikkerova, 2020); (ALrashidi, Almutairi, & Zraquat, 2022); (Noordin, Hussainey, & Hayek, 2022); (Fotoh & Lorentzon, 2023).

This firm-level challenge is particularly important in Egypt, where digital banks, non-cash payments, financial inclusion policies, electronic documentation, and personal data protection requirements are expanding the technological complexity of banking audit engagements. Larger audit firms may be better positioned to develop specialist teams and digital audit platforms, while smaller firms may face constraints related to training costs, access to advanced tools, and the recruitment of IT audit specialists. Such differences could widen audit quality gaps unless firms develop clearer procedures for digital risk assessment, electronic evidence validation, IT control testing, cybersecurity review, and the use of external specialists. Audit firms should also manage advisory opportunities carefully, ensuring that services related to digital controls, data governance, and cybersecurity do not compromise independence or weaken the credibility of the statutory audit (Almaleeh, 2021); (Rahman & Ziru, 2023); (Lugli & Bertacchini, 2023); (Kakwani & Naidu, 2025); (Argento, Jääskeläinen, & Rautiainen, 2025).

Beyond the responsibilities of individual auditors and audit firms, the framework also points to a wider institutional role for regulators and professional bodies in Egypt. Egyptian regulation has already encouraged non-cash payments, digital banks, financial inclusion, electronic documentation, and personal data protection, but these developments also require clearer audit-related guidance on digital risk assessment, electronic audit evidence, IT controls, cybersecurity controls, data access, and third-party technology arrangements. Without such guidance, auditors may face uncertainty about how to evaluate system-generated evidence, how far they can rely on automated controls, and how to

balance evidence collection with confidentiality and data protection requirements. Regulators and professional bodies should therefore treat digital audit readiness as part of the wider development of Egypt's digital banking environment, not as a separate technical issue left only to audit firms (Arab Republic of Egypt, 2019; Arab Republic of Egypt, 2020b; Arab Republic of Egypt, 2020c; Central Bank of Egypt, 2022; Ministry of Communications and Information Technology, 2005).

Professional bodies also need to strengthen auditors' digital competence through training, continuing professional development, and practical guidance on data analytics, cybersecurity awareness, IT control testing, electronic documentation, and the use of specialists. This is particularly important because prior evidence from Egypt suggests that digital transformation affects audit quality through auditors' qualifications, audit procedures, and reporting timeliness (Almaleeh, 2021); (Kluiters, Srivastava, & Tyll, 2022). At the same time, regulators should pay attention to independence issues as demand grows for assurance and advisory services related to digital controls, data governance, cybersecurity, and compliance. The main implication is that Egypt's audit infrastructure should develop alongside its digital banking infrastructure, so that external auditors are better equipped to evaluate technology-dependent financial reporting while maintaining professional scepticism, independence, and public trust (Fotoh & Lorentzon, 2023); (Rahman & Ziru, 2023); (Guo, Jia, & Shentu, 2024); (Lugli & Bertacchini, 2023); (Argento, Jääskeläinen, & Rautiainen, 2025).

Finally, the framework has direct implications for accounting education because digital banking requires future auditors to understand more than traditional accounting standards, audit procedures, and financial statement assertions. Accounting programmes in Egypt need to integrate digital audit competencies into their curricula, including accounting information systems, data analytics, cybersecurity awareness, electronic audit evidence, IT general controls, application controls, data protection, and the audit implications of digital banking regulation. This does not mean replacing core accounting and auditing knowledge with technology training; rather, it means connecting audit concepts such as risk, evidence, internal control, materiality, and professional judgement to the digital systems through which banking transactions are now processed and reported. Without this integration, graduates may enter audit practice with strong theoretical knowledge but limited ability to evaluate technology-dependent financial reporting environments (Almaleeh, 2021); (Huang & Vasarhelyi, 2019); (ALrashidi, Almutairi, & Zraqat, 2022); (Fotoh & Lorentzon, 2023).

In addition, accounting education should also place greater emphasis on practical and interdisciplinary learning. Students need exposure to audit data analytics, system-based case studies, digital control testing, electronic documentation, cybersecurity scenarios, and the ethical challenges associated with accessing and using customer data. Collaboration between universities, audit firms, banks, regulators, and professional bodies could help reduce the gap between academic preparation and the skills required in digital banking

audits. Such education should not present digital tools as automatic solutions, because auditors must still question data quality, system outputs, management reports, and automated controls. The main educational implication is therefore to produce auditors who are technically aware, analytically capable, and professionally sceptical in digital environments, rather than auditors who merely know how to use audit software (Manita, Elommal, Baudier, & Hikkerova, 2020); (Noordin, Hussainey, & Hayek, 2022); (Rahman & Ziru, 2023); (Guo, Jia, & Shentu, 2024); (Argento, Jääskeläinen, & Rautiainen, 2025); (Thi Phuong Nguyen & Van Ninh, 2026)

8. Conclusion, Limitations, and Future Research

8.1 Conclusion

This study examined how the digitalisation of commercial banks reshapes external auditing in Egypt through a critical four-dimensional analytical framework. The analysis concludes that digital banking should not be viewed merely as an operational or technological development, but as a transformation in the audit environment itself. Digital platforms, automated processing, data analytics, electronic records, cybersecurity arrangements, and third-party technology services affect how auditors assess risk, obtain evidence, test controls, and define assurance responsibilities. Although these developments may improve audit efficiency and evidence coverage, they also increase auditors' dependence on complex information systems and system-generated evidence. The main conclusion of the study is therefore that digitalisation expands, rather than reduces, the need for professional judgement, technological awareness, and professional scepticism in external auditing.

In the Egyptian context, the proposed framework is particularly relevant because the banking sector is moving toward greater reliance on non-cash payments, digital banks, financial inclusion, electronic documentation, and personal data protection. These developments create a more technology-dependent banking environment in which audit risk, electronic evidence, digital internal controls, and assurance expectations are closely connected. The study concludes that external auditors in Egypt need to reassess audit risk, evaluate the reliability of electronic audit evidence, examine digital internal controls and cybersecurity arrangements, and respond carefully to expanding assurance and advisory needs. Overall, the study contributes by offering a structured framework for understanding the changing role of external auditors in Egypt's digital commercial banking environment and by highlighting the need for coordinated development among auditors, audit firms, regulators, professional bodies, and accounting education providers.

8.2 Limitations

This study has several limitations that should be considered when interpreting its conclusions. First, the study is conceptual and analytical rather than empirical. It develops a four-dimensional framework based on a critical synthesis of prior literature and Egyptian

regulatory documents, but it does not test the framework through surveys, interviews, case studies, or field observations involving external auditors, audit firms, banks, or regulators. As a result, the study explains how digital banking may reshape external auditors' responsibilities, but it does not measure the actual level of digital audit readiness among Egyptian auditors or the extent to which audit firms currently apply advanced digital audit procedures in practice.

Second, the study focuses specifically on Egypt's digital commercial banking environment, which may limit the direct generalizability of its conclusions to other sectors or countries with different regulatory, technological, and professional conditions. The analysis also reflects the regulatory and professional environment available at the time of writing, while digital banking, cybersecurity requirements, data protection practices, and audit technologies continue to evolve rapidly. In addition, the framework provides a structured way to understand audit implications, but it does not offer a detailed audit Programme, technical testing checklist, or quantitative model for assessing digital audit risk. These limitations do not reduce the value of the framework, but they show that it should be treated as a conceptual foundation for further empirical and professional development.

8.3 Recommendations

Based on the conclusions of this study, external auditors and audit firms in Egypt should strengthen their readiness for digital banking audits by developing clearer procedures for digital risk assessment, electronic audit evidence evaluation, IT control testing, cybersecurity review, and the use of data analytics. Audit firms should not treat digital audit tools as optional technical support, but as part of the core audit methodology for technology-dependent banking environments. This requires investment in training, specialist support, multidisciplinary audit teams, and quality control procedures capable of reviewing system-generated evidence and technology-based audit judgements. Auditors should also maintain professional scepticism when relying on automated reports, data extracts, dashboards, or digital confirmations, as the reliability of such evidence depends on the systems and controls behind it.

The study also recommends stronger coordination among regulators, professional bodies, universities, banks, and audit firms to support the development of digital audit practice in Egypt. Regulators and professional bodies should provide practical guidance on auditing digital banks, electronic evidence, cybersecurity controls, data protection, and third-party technology arrangements. Accounting education should also be updated to prepare future auditors for digital banking environments by integrating data analytics, accounting information systems, cybersecurity awareness, digital internal controls, and ethical issues related to customer data. These recommendations aim to ensure that the expansion of digital banking in Egypt is matched by a parallel development in audit competence, professional guidance, and assurance quality.

8.4 Future Research Directions

Future research can build on this study by testing the proposed four-dimensional framework empirically within the Egyptian banking sector. Surveys, interviews, and case studies could be conducted with external auditors, audit partners, IT audit specialists, bank managers, regulators, and professional bodies to examine how digital banking affects audit risk assessment, electronic evidence evaluation, digital internal control testing, and assurance services in practice. Such studies could also measure the level of digital audit readiness among Egyptian auditors and identify the main barriers that prevent audit firms from adopting advanced digital audit tools, data analytics, cybersecurity review procedures, and multidisciplinary audit teams.

Further research could also extend the framework beyond Egypt by comparing digital banking audit practices across different emerging markets or between emerging and developed economies. Longitudinal studies would be useful to examine how audit responsibilities change over time as digital banks, artificial intelligence, cloud services, cybersecurity requirements, and data protection practices continue to evolve. Future studies may also focus on specific technologies, such as blockchain, robotic process automation, artificial intelligence, or real-time auditing, to assess their direct impact on audit quality, professional scepticism, auditor independence, and assurance expectations. In addition, research on accounting education could examine how universities and professional training programmes can better prepare auditors for technology-dependent banking environments.

References

- Abdennadher, S., Grassa, R., Abdulla, H., & Alfalasi, A. (2022). The effects of blockchain technology on the accounting and assurance profession in the UAE: An exploratory study. *Journal of Financial Reporting and Accounting*, 20(1), 53–71. <https://doi.org/10.1108/JFRA-05-2020-0151>.
- Adiloglu, B., & Gungor, N. (2019). The impact of digitalization on the audit profession: A review of Turkish independent audit firms. *Journal of Economics, Finance and Accounting*, 6(4), 209–214. <https://doi.org/10.17261/Pressacademia.2019.1164>.
- Al-Khasawneh, R. O. (2022). Challenges facing external auditor while auditing banking accounting systems in the light of the use of digital technologies of fourth industrial revolution in Jordan. *American Journal of Industrial and Business Management*, 12(4), 672–698. <https://doi.org/10.4236/ajibm.2022.124035>.
- Almaleeh, N. M. (2021). The impact of digital transformation on audit quality: Exploratory findings from a Delphi study. *Scientific Journal for Commercial Research*, 8(3), 9–36. Access link: https://sjsc.journals.ekb.eg/article_189317.html.

- Al-Okaily, M., Alghazzawi, R., Alkhwaldi, A. F., & Al-Okaily, A. (2023). The effect of digital accounting systems on the decision-making quality in the banking industry sector: A mediated-moderated model. *Global Knowledge, Memory and Communication*, 72(8/9), 882–901. <https://doi.org/10.1108/GKMC-01-2022-0015>.
- ALrashidi, M., Almutairi, A., & Zraqat, O. (2022). The impact of big data analytics on audit procedures: Evidence from the Middle East. *Journal of Asian Finance, Economics and Business*, 9(2), 93–102. <https://doi.org/10.13106/jafeb.2022.vol9.no2.0093>.
- Anomah, S., Ayebofo, B., & Aduamoah, M. (2021). An audit risk model for IT audit ecosystems and digital transformation (DX) decision making. *EDPACS*, 64(2), 1–33. <https://doi.org/10.1080/07366981.2021.1930643>.
- Arab Republic of Egypt. (2017). Presidential Decree No. 89 of 2017 concerning the establishment of the National Payments Council. *Central Bank of Egypt*, Access link: <https://www.cbe.org.eg/en/financial-technology/national-payments-council>.
- Arab Republic of Egypt. (2019). Law No. 18 of 2019 regulating the use of non-cash payment methods. *Central Bank of Egypt*, Access link: <https://www.cbe.org.eg/en/about-us/laws-and-regulations/other-laws>.
- Arab Republic of Egypt. (2020a). Prime Minister Decree No. 1776 of 2020 issuing the Executive Regulations of Law No. 18 of 2019 regulating the use of non-cash payment methods. *Ministry of Finance*, Access link: <https://www.mof.gov.eg/en/archive/media-center/news/5f5f4bd372a8c900073ebc06/Prime-Minister-Decree-no-1776-for-2020-promulgating-the-Executive-Regulations-of-Law-No-18-for-2019-regulating-the-use-of-non-cash-payment-methods>.
- Arab Republic of Egypt. (2020b). Central Bank and Banking Sector Law No. 194 of 2020. *Central Bank of Egypt*, Access link: <https://www.cbe.org.eg/en/about-us/laws-and-regulations/banking-laws> Direct PDF: <https://www.cbe.org.eg/-/media/project/cbe/page-content/rich-text/laws-and-regulations/banking-laws/cbe-law-no-194-of-2020.pdf>.
- Arab Republic of Egypt. (2020c). Law No. 151 of 2020 promulgating the Personal Data Protection Law. Law. Access link: <https://www.acc.com/sites/default/files/2021-03/Data%20Protection%20Law%20-%20Egypt%20-%20EN%20-%20MBH.pdf> Alternative access link: <https://eg.andersen.com/wp-content/uploads/2021/07/Data-Protection-Law.pdf>.
- Argento, D., Jääskeläinen, A., & Rautiainen, A. (2025). Unaccounted effects of digital transformation: A critical review and future research agenda. *Accounting, Auditing & Accountability Journal*, 38(3), 765–789. <https://doi.org/10.1108/AAAJ-01-2025-7670>.

- Atolo, D. M., & Mukoma, F. K. (2025). The impact of digital technologies on the effectiveness of internal audit function in commercial banks in Kenya. *International Journal of Research and Innovation in Social Science*, 9(10), 665–680. <https://doi.org/10.47772/IJRISS.2025.910000057>.
- Barr-Pulliam, D., Brown-Liburd, H. L., & Sanderson, K. A. (2022). The effects of the internal control opinion and use of audit data analytics on perceptions of audit quality, assurance, and auditor negligence. *Auditing. A Journal of Practice & Theory*, 41(1), 25–48. <https://doi.org/10.2308/AJPT-19-064>.
- Betti, N., & Sarens, G. (2021). Understanding the internal audit function in a digitalised business environment. *Journal of Accounting & Organizational Change*, 17(2), 197–216. <https://doi.org/10.1108/JAOC-11-2019-0114>.
- Bonsón, E., & Bednárová, M. (2019). Blockchain and its implications for accounting and auditing. *Meditari Accountancy Research*, 27(5), 725–740. <https://doi.org/10.1108/MEDAR-11-2018-0406>.
- Central Bank of Egypt. (2022). Financial Inclusion Strategy 2022–2025. Access link: <https://www.cbe.org.eg/en/financial-inclusion/financial-inclusion-strategy> Direct PDF: <https://www.cbe.org.eg/-/media/project/cbe/page-content/rich-text/financial-inclusion/financial-inclusion-strategy/highlights-of-financial-inclusion-strate>.
- De Santis, F., & D’Onza, G. (2021). Big data and data analytics in auditing. *In search of legitimacy. Meditari Accountancy Research*, 29(5), 1088–1112. <https://doi.org/10.1108/MEDAR-03-2020-0838>.
- DiMaggio, P. J., & Powell, W. W. (1993). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147–160. <https://doi.org/10.2307/2095101>.
- Fotoh, L. E., & Lorentzon, J. I. (2023). Audit digitalization and its consequences on the audit expectation gap: A critical perspective. *Accounting Horizons*, 37(1), 43–69. <https://doi.org/10.2308/HORIZONS-2021-027>.
- 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. Advance online publication. <https://doi.org/10.1080/21697213.2024.2442769>.
- Hanfy, F., Alakkas, A. A., & Alhumoudi, H. (2025). Analyzing the role of digitalization and its impact on auditing. *Multimedia Tools and Applications*, 84(19), 21203–21225. <https://doi.org/10.1007/s11042-024-19729-0>.

- Hsieh, S.-F., & Brennan, G. (2022). Issues, risks, and challenges for auditing crypto asset transactions. *International Journal of Accounting Information Systems*, 46, 100569. <https://doi.org/10.1016/j.accinf.2022.100569>.
- Huang, F., & Vasarhelyi, M. A. (2019). Applying robotic process automation (RPA) in auditing: A framework. *International Journal of Accounting Information Systems*, 35, 100433. <https://doi.org/10.1016/j.accinf.2019.100433>.
- Jacky, Y., & Sulaiman, N. A. (2022). The use of data analytics in external auditing: a content analysis approach. *Asian Review of Accounting*, 30 (1): 31-58.
- Jardak, M. K., & Hamad, S. B. (2022). The effect of digital transformation on firm performance: evidence from Swedish listed companies. *The Journal of Risk Finance, (ahead-of-print)* , 23 (4): 329-348.
- Jiang, K., Du, X., & Chen, Z. (2022). Firms' digitalization and stock price crash risk. *International Review of Financial Analysis*, 102196.
- Johri, A., Sayal, A., Chong, K. M., Khoja, M., Chaithra, N., Jha, J., et al. (2026). Enhancing audit quality and reducing costs: The impact of AI in banking and financial services. *Frontiers in Artificial Intelligence*, 8, 1718854. <https://doi.org/10.3389/frai.2025.1718854>.
- Kahyaoglu, S. B., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, 33(4), 360-376. <https://doi.org/10.1108/MAJ-02-2018-1804>.
- Kakwani, D., & Naidu, K. (2025). An analytical study on impact of digitalization of retail banking on audit and compliance. *Advances in Consumer Research*, 2(2), 746-753.
- Kend, M., & Nguyen, L. A. (2020). Big data analytics and other emerging technologies: The impact on the Australian audit and assurance profession. *Australian Accounting Review*, 30(4), 269-282. <https://doi.org/10.1111/auar.12305>.
- Kluiters, L., Srivastava, M., & Tyll, L. (2022). The impact of digital trust on firm value and governance: an empirical investigation of US firms. *Society and Business Review, (ahead-of-print)*.
- Liu, M., Wu, K., & Xu, J. J. (2019). How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain. *Current Issues in Auditing*, 13(2), A19-A29. <https://doi.org/10.2308/ciia-52540>.
- Lugli, E., & Bertacchini, F. (2023). Audit quality and digitalization: Some insights from the Italian context. *Meditari Accountancy Research*, 31(4), 841-860. <https://doi.org/10.1108/MEDAR-08-2021-1399>.

- Manita, R., Elommal, N., Baudier, P., & Hikkerova, L. (2020). The digital transformation of external audit and its impact on corporate governance. *Technological Forecasting and Social Change*, 150, 119751. <https://doi.org/10.1016/j.techfore.2019.119751>.
- Ministry of Communications and Information Technology. (2005). Decree No. 109 of 2005 issuing the Executive Regulations of the Electronic Signature Law and establishing the Information Technology Industry Development Agency. *Information Technology Industry Development Agency*, Access link: <https://www.itida.gov.eg/English/AboutUs/Documents/4.pdf>.
- Nasiri, M., Saunila, M., Ukko, J., & Rantala, T. (2022). Digital orientation, digital maturity, and digital intensity: Determinants of financial success in digital transformation settings. *International Journal of Operations & Production Management*, 42(13), 274–298. <https://doi.org/10.1108/IJOPM-09-2021-0616>.
- Noordin, N. A., Hussainey, K., & Hayek, A. F. (2022). The use of artificial intelligence and audit quality: An analysis from the perspectives of external auditors in the UAE. *Journal of Risk and Financial Management*, <https://doi.org/10.3390/jrfm15080339>.
- Rahman, M. J., & Zirur, C. (2023). Clients' digitalization, audit firms' digital expertise, and audit quality: Evidence from China. *International Journal of Accounting & Information Management*, 31(2), 221–246. <https://doi.org/10.1108/IJAIM-08-2022-0170>.
- Schmitz, J., & Leoni, G. (2019). Accounting and auditing at the time of blockchain technology: a research agenda. *Australian Accounting Review*, 29(2):331-342.
- Scott, W. R. (2014). *Institutions and organizations: Ideas, interests, and identities*. (4th ed.). SAGE Publications.
- 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>.
- Thi Phuong Nguyen, T., & Van Ninh, N. (2026). Accounting and auditing in the age of digital transformation. *Digital Transformation and Society*, 1-21.
- Tiberius, V., & Hirth, S. (2019). Impacts of digitization on auditing: A Delphi study for Germany. *Journal of International Accounting, Auditing and Taxation*, 37, 100288. <https://doi.org/10.1016/j.intaccaudtax.2019.100288>.
- Tjendani, R. D., Widagdo, A. K., & Muthmainah, M. (2018). Digital banking, corporate governance, ownership structure, and intellectual capital performance: Evidence from Indonesia. *Jurnal Keuangan dan Perbankan*, 22(4): 714-733.
- Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books.

- Torraco, R. J. (2005). Writing integrative literature reviews: Guidelines and examples. *Human Resource Development Review*, 4(3), 356–367. <https://doi.org/10.1177/1534484305278283>.
- Tušek, B., Ježovita, A., & Halar, P. (2021). The importance and differences of analytical procedures' application for auditing blockchain technology between external and internal auditors in Croatia. *Economic Research-Ekonomska Istraživanja*, 34(1), 1385-1408.
- Wang, Y., Sui, X., & Zhang, Q. (2021). Can fintech improve the efficiency of commercial banks? An analysis based on big data. *Research in International Business and Finance*, 55, 101338. <https://doi.org/10.1016/j.ribaf.2020.101338>.
- Zohry, A. F., Fadel, A. M., & Khamis, A. A. (2021). The Impact of the banking digitalization indicators disclosure on the market value of banks listed on the Egyptian Stock Exchange: An Applied Study. *Journal of Contemporary Issues in Business and Government*, 27(6):1-30.