International Journal of Accounting and Economics Studies, 12 (6) (2025) 868-877

International Journal of Accounting and Economics Studies

Website: www.sciencepubco.com/index.php/IJAES
https://doi.org/10.14419/5cfj0716
Research paper

The Impact of Information Technology Audit on Audit Quality: An Empirical Study of Auditors in The Capital Market of Thailand

Metinee Messuwan [1] *, Nuttavong Poonpool [2], Salakjit Ninlaphay [2]

[1] Ph.D. Candidate, Mahasarakham Business School, Mahasarakham University, Mahasarakham Province 44150
[2] Ph.D., Associate Professor, Mahasarakham Business School, Mahasarakham University, Mahasarakham Province 44150
**Corresponding author E-mail: 64010991001@msu.ac.th*

Received: September 8, 2025, Accepted: October 14, 2025, Published: October 24, 2025

Abstract

This study investigates the impact of information technology audit on the audit quality of auditors in Thailand's capital market, with a particular focus on how information technology audit practices influence key dimensions of audit quality, including reducing audit risk and data security. A quantitative research approach was employed, using structured questionnaires distributed by mail to 365 licensed auditors in the capital market, from which 93 valid responses were collected and analyzed. The findings reveal that information technology audit significantly enhances audit quality by enhancing data security, strengthening system security, and increasing operational efficiency. These results confirm the essential role of information technology audit in reducing audit risk and maintaining standards of auditing practice. Overall, the study emphasizes the strategic importance of information technology audit as a proactive mechanism for safeguarding information and ensuring the reliability of audit processes. It also highlights the ongoing need to strengthen information technology governance frameworks and develop auditors' competencies to effectively respond to emerging digital challenges. The insights derived from this research provide valuable guidance for regulators, auditors, and stakeholders seeking to improve audit effectiveness in Thailand's capital market.

Keywords: *Information Technology Audit; Data Security; Reducing Audit Risk; Audit Quality.*

1. Introduction

Over the past decade, advances in information technology and digital innovation have profoundly reshaped the structure and operations of businesses. These developments have progressed rapidly and continuously, driving digital transformation across a wide range of industries, including accounting and auditing, where processes must adapt to new technologies to enhance efficiency and reduce costs (Igou et al., 2022). The adoption of digital technologies not only strengthens competitiveness but also enables organizations to develop new operational processes (Osmundsen et al., 2018). Many organizations now regard information technology as a core strategy for creating business advantages and simplifying complex workflows (Klos & Spieth, 2020). Moreover, digital technologies have become a critical driver of organizational performance and sustainable growth by integrating processes with automation, big data analytics, and strategic decision-making tools (Schneider & Kokshagina, 2021).

Thailand has placed strong emphasis on the development and utilization of technology as a driver of national progress and an instrument for enhancing public services. The government has sought to establish new service systems by leveraging digital data to stimulate and support the country's advancement. In 2019, the National Cybersecurity Agency was designated as the authority responsible for providing protection, monitoring, surveillance, risk mitigation, and recovery in response to cyber threats (Gazette, 2023). However, the rapid growth of digital technologies has also given rise to increasingly complex cybersecurity threats that significantly affect accounting and auditing practices (Thottoli et al., 2022). Organizations now face risks such as cyberattacks, data breaches, software vulnerabilities, hardware failures, and human errors, often stemming from overreliance on technology and insufficient governance. These issues undermine the integrity and security of data (Hall, 2011). These issues also undermine stakeholder confidence, highlighting the need for a robust cybersecurity framework to maintain data integrity and confidentiality (Kafi & Akter, 2023).

Furthermore, during the COVID-19 pandemic, a 2020 report from the United States revealed a sharp increase in unauthorized data access, particularly through virtual private networks (VPNs) used for remote work, which became prime targets for cybercriminals (Gaurav, 2020). This led to operational disruptions and reflected the growing scope and complexity of cybercrime (Such-Pyrgiel et al., 2022). Hence, to ensure the appropriateness and security of information technology usage, information technology audit plays a crucial role in evaluating and overseeing the effectiveness and safety of information systems (The Securities and Exchange Commission, Thailand, 2019). This

Copyright © Metinee Messuwan et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

includes technology controls, risk management, and cybersecurity measures (ISACA, 2020), which collectively enhance operational efficiency, ensure data accuracy, and strengthen reliability (KPMG, 2020; Devale & Kulkarni, 2012). Accordingly, auditors must assess the adequacy of information technology controls to minimize losses resulting from system failures, inaccurate information, or operational disruptions (Agoes, 2012).

In general, auditors provide assurance services that encompass financial statement audits, operational audits, and compliance audits to enhance stakeholder confidence. However, in today's environment, where technology plays a crucial role in the processing and presentation of organizational information, the accuracy and reliability of data may be compromised in the absence of proper controls (Wu et al., 2023). This has led to growing calls for stricter information technology audits. Effective IT controls are therefore essential to ensuring business continuity (Saeed et al., 2023). These challenges have heightened the importance of integrated auditing practices. KPMG (2009) therefore emphasized that information technology audits are a critical component of overall audit activities and should be incorporated into financial statement audits, operational audits, and compliance audits (Devale & Kulkarni, 2012; Tingliao, 2016). Information technology audits not only focus on assessing risks associated with the use of information systems and the related controls to mitigate risks to data accuracy and reliability, but also strengthen information assurance by safeguarding data and reducing technology-related risks. Strengthening effective controls can help minimize the risk of misreporting caused by errors or fraud (Lorentzon, 2023). Such processes provide auditors with sufficient and accurate information for decision-making, promote objectivity in expressing opinions, and reduce the likelihood of overlooking indicators or flawed assumptions during evidence collection and evaluation (Federation of Accounting Professions, 2010). Majdalawieh and Zaghloul (2009) also argued that information technology audit should be an integral part of auditing practices, as the information systems environment directly influences organizational economic data, efficiency, effectiveness, and productivity (Salihu & Hoti, 2019). Adopting this new approach to auditing not only improves the quality of financial and compliance audits but also enhances stakeholder confidence. Nonetheless, although research in the field of information technology auditing has been conducted (Aditya et al., 2018), important issues remain underexplored, particularly in the context of Thailand's capital market, where there is still a lack of empirical evidence regarding the impact of information technology audit on audit quality. This study, therefore, seeks to address this gap by examining the effects of information technology audit and contributing to the advancement of auditing practices in this area.

2. Literature Review

This discussion employs two theories to explain the research relationships: the legitimacy theory by Suchman (1995) and the defense-in-depth theory by Smith C.L. (2003).

Legitimacy theory

Legitimacy theory (Suchman, 1995) states that an organization's actions and activities are shaped by societal expectations. Companies derive their rights and authority from society to utilize natural and human resources, and if they operate in line with these expectations, they fulfill a form of social contract (Gray, Kouhy & Lavers, 1995). Organizations that perceive themselves as part of society strive to meet these expectations, recognizing that failure to do so may result in social disapproval, which could hinder their success. To ensure long-term prosperity, management must continuously assess whether its operations align with societal demands. In this context, legitimacy theory helps explain the necessity of information technology audit, particularly given the growing reliance on digital technologies. Firms leveraging advances in digital innovation aim to maintain their competitive advantage in rapidly changing markets (Klos & Spieth, 2020). However, the ongoing expansion of digital technologies has introduced increasingly complex security threats to information systems. These risks, arising from greater dependence on IT and inadequate governance, can compromise data integrity and security (Hall, 2011) while undermining stakeholder trust. This underscores the need for robust cybersecurity frameworks to preserve the confidentiality and integrity of information (Kafi & Akter, 2023), fostering greater awareness of information technology security and highlighting the importance of effective information technology controls (Saeed et al., 2023).

Defense-in-depth theory

Defense-in-depth theory (Smith, 2003) is a key concept in information system security, emphasizing the establishment of multiple layers of protection to prevent unauthorized access or attacks on systems. Each layer serves a distinct purpose and employs different methods, such as physical controls, access rights management, data encryption, system monitoring, and backup processes. This multilayered approach reduces risks and enhances the resilience of systems against potential threats. With the rapid advancement of information technology and the emergence of new threats, organizations that adopt information technology appropriately can enhance operational efficiency. However, implementing defense-in-depth strategies further minimizes anomalies and strengthens confidence in data security. Information security experts widely acknowledge this theory as a fundamental mechanism for data protection. Carroll and Merwe (2009) highlighted that the increasing reliance on information technology over the past two to three decades has transformed auditing practices, with current approaches focusing on ensuring that IT systems are properly controlled, secure, and effective. In this regard, information technology audit has incorporated standards such as ISO 27001 and COBIT, which provide frameworks for IT governance and security enhancement. The effective application of these standards helps safeguard information systems, reduce risks, and prevent unauthorized access, thereby increasing the reliability of processed and stored data (Riad, 2015). Reliable data enables auditors to work more effectively and with greater confidence, which directly contributes to overall audit quality.

Auditors must be prepared to adapt to evolving business environments. Given the growing influence of information technology on audit complexity, resulting from both challenges and opportunities, auditors require extensive knowledge and skills to assess risks associated with technological changes (Rosario, 2013; Juiz, 2015). Consequently, information technology audit has become critical, reinforcing the importance of integrated audit practices that combine financial audits, operational audits, and compliance audits (Devale & Kulkarni, 2012; Tingliao, 2016). In other words, information technology audits should be conducted alongside other audit activities to support audit functions while enhancing independence and objectivity (Tingliao, 2016).

Nevertheless, practical information technology audit still faces limitations due to the lack of comprehensive and standardized guidelines addressing all dimensions of information security controls. Scholarly literature on information technology audit and its impact on audit quality remains insufficient and underexplored in empirical studies (Chou, 2015). This highlights the need for research into current information technology audit practices, particularly considering escalating threats. Accordingly, this study investigates whether auditors in Thailand have adopted information technology audit practices to enhance the efficiency and effectiveness of accounting practices. It further identifies gaps in academic research concerning information technology audit practices, information technology governance, and related issues, offering theoretical insights into whether such practices influence audit effectiveness and quality. The study develops a conceptual framework to examine the impact of information technology audit on audit quality among auditors in the Thai capital market, as illustrated in Figure 1.

Recent developments in digital auditing have underscored the transformative influence of emerging technologies such as Artificial Intelligence (AI) and blockchain on information technology auditing. AI-driven systems have become integral to modern audit practices by enabling real-time data analysis, predictive risk assessment, and enhanced decision-making. Al-Omush et al. (2025) revealed that AI-based auditing tools significantly enhance audit quality by increasing accuracy, efficiency, and risk evaluation while minimizing human error, thereby reshaping traditional assurance practices.

In parallel, blockchain technology has emerged as a pivotal innovation that redefines data integrity and transparency in auditing. Liu et al. (2024) found that blockchain improves traceability, accountability, and reliability of financial information by providing tamper-proof, verifiable records that reduce manual workloads and enhance reporting precision. Building on this, Andoko et al. (2025) demonstrated that blockchain integration significantly strengthens audit quality through immutable and transparent ledgers that mitigate human error and fraud, while automation of data collection and near-instantaneous verification improve audit timeliness. Moreover, the cryptographic and verifiable nature of blockchain-supported records establishes a single source of truth that minimizes estimation bias and earnings manipulation, contributing to more trustworthy financial reporting. Collectively, these studies highlight that integrating AI and blockchain into information technology audit frameworks can substantially enhance audit transparency, cybersecurity, and organizational trust, laying a foundation for more robust and sustainable audit quality in the digital era.

While global studies have increasingly focused on advanced digital auditing practices, particularly the integration of AI and blockchain technologies into IT governance frameworks, such adoption in Thailand remains limited. Many Thai auditing firms are still in the early stages of implementing digital audit tools, facing challenges related to technological readiness, cybersecurity infrastructure, and professional skill development. Compared with mature economies where audit automation is well established, Thai auditors often rely more on manual verification and less standardized IT control frameworks. This contextual distinction underscores the importance of examining how information technology audits operate within Thailand's capital market, where varying levels of digital maturity may influence audit quality and data security outcomes.

Building upon these technological advancements, this study develops a conceptual framework that integrates the multidimensional aspects of information technology audit: financial statement audit, operational audit, compliance audit, and information technology control with key audit quality outcomes. The framework also incorporates the mediating roles of risk reduction and data security to explain how technology-driven auditing practices enhance overall audit performance. By synthesizing insights from recent studies on AI and blockchain, this model reflects the evolving nature of digital assurance and provides a theoretical foundation for examining information technology audit effectiveness in Thailand's capital market context.

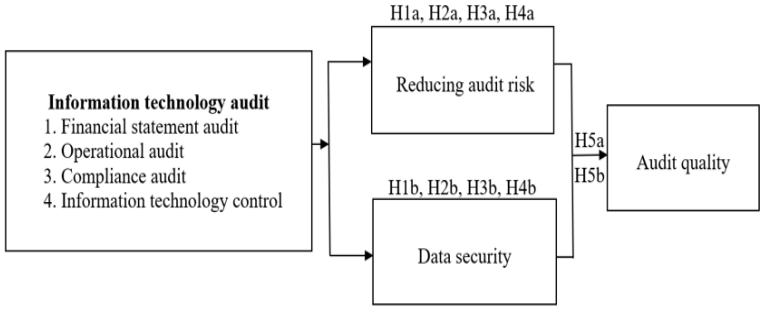

Fig. 1: Conceptual Framework

Figure 1 illustrates the conceptual framework developed for this study. It depicts the relationships between four dimensions of information technology audit: financial statement audit, operational audit, compliance audit, and information technology control, and their combined influence on audit quality through two mediating constructs: reducing audit risk and enhancing data security. Specifically, hypotheses H1a–H4a represent the effects of each audit dimension on reducing audit risk, while H1b–H4b capture their impact on data security. Subsequently, H5a and H5b examine how both reducing audit risk and data security contribute to improving audit quality. The framework highlights the integrative role of information technology audit within the broader auditing process, emphasizing that effective information technology governance and control mechanisms are essential to maintaining high audit quality in the context of Thailand's capital market.

Information technology audit is concerned with the governance, performance evaluation, and management of information technology, encompassing security controls, risk management, and the overall assurance of information technology processes (ISACA, 2013). The primary objective is to ensure that information remains secure, complete, and accurate. Since reliance on data alone cannot guarantee appropriateness and adequacy, auditing provides an assurance service that extends beyond financial audits to include operational and compliance audits, thereby strengthening stakeholder confidence. In the current environment, technology plays a critical role in the processing and presentation of organizational information. However, without appropriate controls, the accuracy and reliability of such information may be compromised (Wu et al., 2023). Thus, effective IT controls and assurance mechanisms are necessary to ensure the correctness, security, and reliability of data processing. A synthesis of prior research reveals that, over the past decade, information technology audit has evolved into a key component of organizational quality assurance, with its growth significantly influenced by technological innovations (Yeghaneh, 2015). Majdalawieh and Zaghloul (2009) further emphasized that information technology audit should be integrated into overall audit practices, meaning that information technology audits can and should be conducted alongside financial, operational, and other forms of auditing. Accordingly, an information technology audit consists of the following key components:

2.1. Financial statement audit

A financial statement audit refers to the process of examining accounting records and financial reporting to assess their completeness, reliability, and compliance with established standards. This process is grounded in fundamental principles, including the Code of Ethics for Professional Accountants, generally accepted auditing standards, and the exercise of professional judgment in observing and questioning potential misconduct. The primary objective of a financial statement audit is to enhance the credibility of audit outcomes and thereby strengthen stakeholders' confidence in financial reporting (Federation of Accounting Professions, 2010). Albrecht et al. (2015) suggested that auditors may fail to detect fraud in high-risk environments, creating gaps in fraud detection capabilities and increasing audit risk. Similarly, Watts and Zimmerman (1986) emphasized that auditing plays a vital role in reducing information asymmetry between managers and stakeholders by ensuring the reliability of reported figures. This view is consistent with Asare et al. (1994), who noted that auditors'

ability to evaluate the probability of misstatements in specific areas of the financial statements helps reduce audit risk by identifying issues requiring detailed examination. Furthermore, Rosati et al. (2020) found that if auditors devote sufficient effort to substantive testing and audit procedures, information security incidents do not negatively affect audit quality. This finding highlights the importance of a thorough financial statement audit not only in ensuring the reliability of financial information but also in safeguarding data security. Hence, the following hypotheses are proposed:
H1a: Financial statement audit has a positive effect on reducing audit risk.
H1b: A Financial statement audit has a positive effect on data security.

2.2. Operational audit

Operational audit procedures and practices play a crucial role in ensuring that organizational processes are carried out effectively, thereby reducing auditors' exposure to audit risk and minimizing the likelihood of inappropriate opinions on financial reports (Robson et al., 2007; Curtis & Turley, 2007; Peecher et al., 2007). Power (1997), however, argued that operational auditing primarily focuses on operational efficiency rather than the control of financial reporting, thus limiting its influence in reducing audit risk. Nonetheless, Gupta (2020) demonstrated that operational audit not only emphasizes areas for efficiency improvements but also fosters better compliance with operational procedures, which reduces the likelihood of errors and positively impacts audit risk. Research further suggests that operational audits assist in identifying weaknesses in internal control systems (Sawyer et al., 2014). Consistent with these findings, Arens et al. (2017) and Kinney & Shepardson (2011) highlighted that effective operational audits mitigate the chances of errors or fraud in financial reporting, thereby lowering overall audit risk. Therefore, the following hypothesis is proposed:
H2a: Operational audit has a positive effect on reducing audit risk.
H2b: Operational audit has a positive effect on data security.

2.3. Compliance audit

Compliance auditing is essential for ensuring that organizations operate in accordance with established standards. However, its ability to reduce audit risk remains limited, as compliance audits typically focus on adherence to regulatory requirements rather than the accuracy of financial information, while devoting relatively little attention to fraud detection. As a result, compliance audit may not significantly reduce audit risk because it does not comprehensively address all factors that contribute to material misstatements in financial reporting. Kinney and Shepardson (2011) emphasized that regulatory-driven audits may overlook complex financial misrepresentations, thereby restricting their effectiveness in mitigating audit risk. Similarly, Bazerman et al. (1997) noted that time pressures associated with regulatory compliance can lead to superficial audits, undermining their overall effectiveness. Nevertheless, research by Chen et al. (2015) revealed that organizations subject to rigorous compliance audits tend to achieve better compliance with regulations, indirectly supporting the reliability of financial reports and reducing the likelihood of material misstatements. In addition, Gantz (2014) argued that compliance with legal and industry standards enhances data security while mitigating risks related to errors, fraud, and adverse incidents. Consistent with this perspective, Messier et al. (2016) highlighted that regular compliance audits enable organizations to remain aligned with evolving standards and technologies, thereby promoting continuous improvement in security practices. Such a proactive approach strengthens organizational adaptability and resilience against risks. Based on the above, the following hypotheses are proposed:
H3a: Compliance audit has a positive effect on reducing audit risk.
H3b: Compliance audit has a positive effect on data security.

2.4. Information technology control

Information technology control refers to the management of information technology systems and processes, which can be broadly classified into two main categories (Arens et al., 2017). The first category is 'general controls', which apply across all information technology functions and encompass information technology governance, system development, physical and cyber security, data backup planning, contingency planning, and hardware management. The second category is 'application controls', which focus on procedures within application systems to ensure that transactions are authorized, recorded, and processed completely, accurately, and on a timely basis, thereby enhancing the reliability of information.
Effective information technology controls enable auditors to accurately assess risks, produce reliable reports, and draw reasonable conclusions from their audits. High-quality and sufficient information supports professional judgment, reducing the likelihood of overlooking critical issues or forming flawed assumptions during evidence collection and evaluation (Petter Lovaas, 2012). In line with this, Bhattacharjee et al. (2017) argued that when auditors confirm that organizations have implemented effective information technology controls, they can adjust audit procedures, lower detection risk, and enhance overall audit efficiency. However, Hall and Singleton (2018) emphasized that the complexity of modern information technology systems poses significant challenges for auditors, as comprehensive evaluations of information technology controls may be difficult without specialized expertise, thereby increasing audit risk. Based on the above, the following hypotheses are proposed:
H4a: Information technology control has a positive effect on reducing audit risk.
H4b: Information technology control has a positive effect on data security.

2.5. Reducing audit risk and data security

Information technology audit plays a critical role in safeguarding data, ensuring the accuracy and completeness of information, and preventing fraud within information systems. Moreover, it provides essential recommendations for risk reduction (Beridze, 2017), thereby lowering information technology-related audit risks while simultaneously protecting data and systems. Information technology audit minimizes errors and enables auditors to reach reasonable conclusions by providing reliable information to support their opinions (Federation of Accounting Professions, 2014). Hurtt (2011) highlighted the positive relationship between audit risk and audit quality, emphasizing the importance of obtaining sufficient and appropriate audit evidence. The application of professional judgment and skepticism allows auditors to identify suspicious circumstances and avoid reliance on flawed assumptions during evidence collection and evaluation. This approach enhances the quality of financial reporting, ultimately benefiting financial statement users (AlShaer, 2020). Reducing audit risk contributes to the accuracy and reliability of financial reporting, leading to more effective audits (Riyadi et al., 2021). Furthermore, enhanced data

security facilitates smoother audit processes by reducing disruptions caused by inconsistencies or security incidents (Rose et al., 2017). Based on the above discussion, the following hypotheses are proposed:
H5a: Reducing audit risk has a positive effect on audit quality.
H5b: Data security has a positive effect on audit quality.

2.6. Audit quality

Audit quality refers to the auditor's ability to provide reliable, independent, and ethical assurance that supports stakeholder decision-making (DeAngelo, 1981). It encompasses diligence in audit execution, the ability to detect errors, adherence to auditing standards, and transparent reporting (Arens et al., 2015; Manita et al., 2020). Key drivers include auditor competence, independence, and ethical integrity (Tandiontong, 2016). The International Federation of Accountants (2014) identified four dimensions influencing audit quality: 'inputs' (e.g., ethics and competence), 'processes' (e.g., compliance with auditing standards and internal control), 'outputs' (e.g., audit reports), and 'contextual factors' (e.g., regulation and governance). In today's digital era, Information Technology (IT) Audit plays a vital role in managing risks related to data accuracy, security, and reliability (Riad, 2015). Strong IT governance enhances the credibility of financial audits and mitigates decision-making risks (The Securities and Exchange Commission Thailand, 2022). However, the effectiveness of an IT audit depends on technological awareness, the business context, and relevant legal and regulatory frameworks.

3. Research Methodology

3.1. Sample selection and data collection

The population and sample were capital markets in Thailand (The Securities and Exchange Commission, Thailand, 2023). This database was a reliable source that provided complete addresses and listed 365 securities auditors in the capital market. The research instrument was a self-administered questionnaire that was distributed via postal services. The key informants are auditors in the capital market. A total of 365 questionnaires were mailed in mid-February 2023. After two months, to increase the response rate, a follow-up postcard was sent to auditors who had not yet responded, to remind them to fill out the questionnaire, and ask them to cooperate. A total of 93 surveys were returned, representing a response rate of 25.48 percent. According to Aaker, Kumar, and Day (2001), a 20% response rate for a postal survey is considered acceptable.
The participant characteristics of the 93 respondents are as follows: Most of the respondents were female. The age range of the respondents was 30 years or younger. Most of the respondents were single. Regarding the educational background, the majority hold a bachelor's degree. In terms of professional experience, most respondents had less than five years of auditing experience on the Thai Stock Exchange. Additionally, the majority reported an average monthly income of no more than 100,000 baht.
Additionally, this study was reviewed and approved by the Mahasarakham University Ethics Committee for Research Involving Human Subjects (Approval No.071-617/2024).

3.2. Analysis method

To establish validity, five academic experts reviewed and adjusted the measurement items in the questionnaire to achieve the best possible scale. To achieve valid results and conclusions for this study, reliability was established using Cronbach's alpha. All the scale items were defined and accepted based on the conventional guidelines proposed by Nunnally (1978). In this study, the first 30 questionnaires sent back from respondents were used to perform a pre-test of the reliability of all measurements that were used in the questionnaire. Consequently, these 30 questionnaires were included in the final data analysis for testing hypotheses and assumptions with SPSS (analysis software), including linearity, homoscedasticity, normality, and relationships among variables.

3.3. Measurements

The quantitative research setting for the empirical analysis was based on primary data obtained from a survey questionnaire. In this research, there were four sets of variables to be measured. Audit quality was the dependent variable, while information technology audits were the independent variable. The mediating variables were reduced audit risk and data security. These constructs were transformed into operational variables for true measurements. To measure each construct in the conceptual model, all variables were defined and measured using survey questions that used a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree).

4. Research Methodology

4.1. The measurement models

The study of the reflective models was conducted using SPSS. For the measure of convergent validity of the analysis, all weight values above 0.50 (factor loading) were statistically significant. The statistical tool consisted of two main components. The first involves validating the research instrument in terms of validity and reliability. To establish the content validity, five academic experts reviewed and refined the questionnaire items to ensure accurate and appropriate scale measures. The item validity scores range from 0.607 to 0.891, indicating acceptable validity (Hair et al.,2010).
Cronbach's alpha was used to ensure the instrument's reliability. All the scale items were defined and assessed according to the conventional guidelines proposed by Nunnally (1978). The results of the reliability analysis showed Cronbach's alpha values ranging from 0.710 to 0.867, all of which exceeded the minimum acceptable threshold of 0.70, indicating high internal consistency. Additionally, the item-total correlation values ranged from 0.401 to 0.782, with all items exceeding the benchmark of 0.30, demonstrating acceptable item reliability. Detailed results are presented in Table 1.

Table 1: Factor Loading, Item-Total Correlation, and Cronbach Alpha

Variables	Factor Loading	Item total correlation	Cronbach Alpha
Financial Statement audit (FAS)	0.607-0.775	0.401-0.567	0.710
Operational audit (OAU)	0.650-0.798	0.453-0.605	0.748
Compliance audit (CAU)	0.778-0.891	0.640-0.779	0.867
Information technology control (ITC)	0.675-0.758	0.491-0.579	0.746
Reducing audit risk (RAR)	0.780-0.804	0.535-0.687	0.767
Data security (DSR)	0.651-0.788	0.456-0.611	0.744
Audit quality (AUQ)	0.656-0.873	0.557-0.782	0.804

The second component involves statistical hypothesis testing based on the fundamental assumptions of regression analysis, including linearity, homoscedasticity, normal distribution, and relationships among variables (Table 2). All hypotheses were tested using regression analysis, with the corresponding equations presented below:

Equation 1: $RAR_i = \alpha_1 + \beta_1 FSA_i + \beta_2 OAU_i + \beta_3 CAU_i + \beta_4 ITC_i + \beta_5 AUS_{1i} + \beta_6 AUS_{2i} + \beta_7 AUS_{3i} + \beta_8 AUS_{4i} + \varepsilon_1$

Equation 2: $DSR_i = \alpha_2 + \beta_9 FSA_i + \beta_{10} OAU_i + \beta_{11} CAU_i + \beta_{12} ITC_i + \beta_{13} AUS_{1i} + \beta_{14} AUS_{2i} + \beta_{15} AUS_{3i} + \beta_{16} AUS_{4i} + \varepsilon_2$

Equation 3: $AUQ_i = \alpha_3 + \beta_{17} RAR_i + \beta_{18} DSR_i + \beta_{19} AUS_{1i} + \beta_{20} AUS_{2i} + \beta_{21} AUS_{3i} + \beta_{22} AUS_{4i} + \varepsilon_3$

Table 2: Correlation Matrix

Variable	FAS	OAU	CAU	ITC	RAR	DSR	AUQ	Tolerance	VIF
Financial Statement audit (FAS)	1							0.709	1.100
Operation audit (OAU)	.449*	1						0.726	1.080
Compliance audit (CAU)	.471*	.470*	1					0.879	1.138
Information technology control (ITC)	.465*	.418*	.492*	1				0.652	1.051
Reducing audit risk (RAR)	.413*	.526*	.556*	.554*	1			0.590	1.010
Data security (DSR)	.534*	.589**	.516*	.541*	.474*	1		0.862	1.040
Audit quality (AUQ)	.457*	.537*	.757**	.512*	.420*	.551*	1	-	-

Notes: * = p<0.05, ** = p<0.01.

Table 2 shows the Pearson correlation coefficients for all the variables. The results demonstrate that all dimensions of information technology audits have a significant, positive relationship with reducing audit risk ($r = .413 – .556$, $p < 0.05$), data security ($r = .474 – .589$, $p < 0.01$), and audit quality ($r = .457 – .757$, $p < 0.01$). are significantly, positively related to all dimensions of Information Technology audits. The tolerance values range between 0.590 and 0.879, and the variance inflation factor (VIF) values range between 1.010 and 1.138. Since the tolerance values are greater than 0.1 and the VIF values are less than 10, this indicates that multicollinearity among the independent variables is not a concern (James et al., 2017).

4.2. Hypothesis testing and discussion

Table 4: The Results of Regression Analysis for the Relationship Between Each Dimension of Information Technology Audit and Its Consequences

Independent Variables	Dependent Variables	
	RAR	DSR
	Eq.1	Eq.2
Financial Statement Audit (FAS)	0.180*	0.238*
	(0.085)	(0.105)
Operation audit (OAU)	0.175*	0.199*
	(0.068)	(0.080)
Compliance audit (CAU)	0.178*	0.058
	(0.079)	(0.093)
Information technology control (ITC)	0.240**	0.285**
	(0.081)	(0.095)
Control Variables:	0.054	0.079
Experience in auditing in the stock market 6-10 years (AUS_2)	(0.061)	(0.072)
Experience in auditing in the stock market 11-15 years (AUS_3)	0.039	0.139
	(0.105)	(0.124)
Experience in auditing in the stock market more than 15 years (AUS_4)	0.056	0.198*
	(0.074)	(0.088)
Adjusted R^2	0.163	0.192
Maximum VIF	1.138	1.138
Bata coefficients with standard errors in parenthesis, ** P < 0.01, * P < 0.05		

The regression analysis results from Equations 1 and 2 demonstrate the effect of each information technology audit dimension on audit risk reduction (RAR) and data security and reliability (DSR). These results support several key hypotheses, as discussed below.

First, the findings indicate that a financial statement audit (FSA) has a significant positive effect on both audit risk reduction ($\beta = 0.180$, $p < 0.05$), and data security and reliability ($\beta = 0.238$, $p < 0.05$). These results suggest that the effective auditing of financial statements enhances the accuracy, completeness, and reliability of accounting information. Because financial audits require careful planning and rigorous assessment (Alktani, 2014; Salameh, 2011), auditors are better able to evaluate and express appropriate opinions, thereby reducing audit risk. This is consistent with Riyadi et al. (2021), who emphasize that high-quality financial audits enable auditors to make well-supported judgments. Furthermore, the findings align with those of Rosati et al. (2020), who found that a thorough audit process helps prevent a decline in audit quality, even in the presence of information security incidents. Therefore, Hypotheses 1a and 1b are supported.

Second, the operational audit (OAU) shows a significant positive effect on both audit risk reduction ($\beta = 0.175$, $p < 0.05$) and data security and reliability ($\beta = 0.199$, $p < 0.05$). This suggests that evaluating operational processes helps ensure that business units follow standard procedures, which, in turn, reduces the likelihood of audit errors and improves information system efficiency. This result is consistent with

the findings of Curtis and Turley (2007) and Hall (2011), who argued that operational audits contribute to both performance efficiency and risk mitigation. Therefore, Hypotheses 2a and 2b are supported.

Third, the compliance audit (CAU) significantly influences audit risk reduction ($\beta = 0.178$, $p < 0.05$) but has no significant impact on data security and reliability ($\beta = 0.058$, $p > 0.05$). The results imply that while monitoring adherence to regulations strengthens the credibility and effectiveness of the audit process (Gantz, 2014), it does not necessarily translate into stronger data protection. Duncan and Whittington (2014) explain that organizations may be compliant with regulations but still lack comprehensive information security strategies. Hence, compliance audits alone are insufficient for ensuring data security, underscoring the need for broader IT governance. Therefore, Hypothesis 3a is supported, while Hypothesis 3b is not. This finding may reflect the traditional compliance audit practices in Thailand, where audits tend to emphasize documentary verification and regulatory conformity rather than the evaluation of real-time cybersecurity mechanisms. As a result, compliance audits may enhance procedural accountability but fail to strengthen technological safeguards for information systems. Similar conclusions were drawn by Judijanto et al. (2023), who found that compliance-driven audits often improve administrative control without necessarily improving data security resilience. This outcome highlights the necessity for Thai organizations to integrate compliance audits with IT governance and cybersecurity frameworks to achieve more comprehensive and sustainable data protection.

Fourth, the information technology control (ITC) dimension has a significantly positive impact on both audit risk reduction ($\beta = 0.240$, $p < 0.01$) and data security and reliability ($\beta = 0.285$, $p < 0.01$). These findings confirm the essential role of IT controls in mitigating technology-related risks, protecting organizational data, and enhancing audit quality. IT controls encompass a wide range of procedures, including general and application controls such as access security, system maintenance, data integrity checks, and system monitoring (Arens et al., 2017; Lovaas, 2012). Reliable information enables auditors to perform accurate assessments, reach sound conclusions, and effectively express professional judgments. Therefore, Hypotheses 4a and 4b are supported.

Regarding the control variables, auditors with over 15 years of experience (AUS4) significantly influence data security and reliability ($\beta = 0.198$, $p < 0.05$), indicating that extensive professional experience enhances auditors' capability to safeguard digital information and maintain system integrity. Senior auditors are more adept at identifying control weaknesses, implementing cybersecurity measures, and ensuring compliance with IT governance standards. This result aligns with Tinyase et al. (2025), who found that experienced auditors are better equipped to manage audit pressure and uphold audit quality under complex technological environments.

The adjusted R^2 values of 0.163 (RAR) and 0.192 (DSR) indicated a moderate model fit, while a maximum VIF of 1.281 confirmed no multicollinearity concerns.

Overall, financial audits, operational audits, and IT controls significantly strengthen audit risk management and data security. In contrast, compliance audits support regulatory assurance but have a limited impact on information security. These findings emphasize the value of a multidimensional information technology audit approach to enhance audit quality in digital environments.

Table 5: The Results of Regression Analysis for the Relationship between Reducing Audit Risk, Data Security, on Audit Quality

Independent Variables	Dependent Variables AUQ Eq.3
Reducing Audit Risk (RAR)	0.362** (0.084)
Data Security (DSR)	0.142* (0.071)
Control Variables: Experience in auditing in the stock market 6-10 years (AUS2)	0.071 (0.050)
Experience in auditing in the stock market, 11-15 years (AUS3)	0.213* (0.085)
Experience in auditing in the stock market for more than 15 years (AUS4)	0.026 (0.061)
Adjusted R^2	0.268
Maximum VIF	1.040
Bata coefficients with standard errors in parentheses, ** P < 0.01, * P < 0.05	

The regression results from Equation 3 indicate that both audit risk reduction and data security have significantly positive effects on audit quality, thus supporting Hypotheses 5a and 5b.

Audit risk reduction ($\beta = 0.362$, $p < 0.01$) significantly enhances audit quality by lowering the likelihood of material misstatements and enabling auditors to form reliable opinions. This aligns with prior studies (Hurtt, 2011; AlShaer, 2020; Riyadi et al., 2021), which emphasize the role of professional skepticism and sufficient audit evidence in improving audit outcomes.

Data security ($\beta = 0.142$, $p < 0.05$) also positively influences audit quality. Strong data protection improves data reliability, enables more accurate evidence evaluation, and reduces the risk of errors. Prior research (Westland, 2021; Vendrzyk, 2003; Lovaas, 2012) supports the view that secure and accurate data strengthen audit credibility.

Among the control variables, only auditors with 11–15 years of experience ($\beta = 0.213$, $p < 0.05$) showed a significant effect on audit quality, suggesting that mid-career auditors may offer an optimal balance of expertise and adaptability.

The model explains a moderate variance in audit quality (Adjusted $R^2 = 0.268$) with no multicollinearity issues (VIF = 1.156). Overall, the findings underscore the critical role of risk management and data security in achieving high-quality audits.

5. Conclusions, Limitations, and Further Research

5.1. Conclusions

The findings confirm that financial statement audits, operational audits, compliance audits, and information technology (IT) controls significantly contribute to reducing audit risk and enhancing data security, thereby improving audit quality. Specifically, financial and operational audits enhance information reliability and reduce audit errors through systematic verification and cautious planning (Alktani & Ghareeb, 2014; Salameh, 2011; Peecher et al., 2006). Compliance audits also play a crucial role in ensuring adherence to laws and regulations and strengthening audit quality (Gantz, 2014; Judijanto et al., 2023), although they do not necessarily enhance data security (Duncan & Whittington, 2014).

IT controls significantly reduce audit risk by protecting information assets, monitoring system processes, and ensuring data completeness and accuracy of data (Arens et al., 2017). These controls, aligned with general and applied audit standards, enable auditors to form sound professional judgments and reduce misstatements (Petter Lovaas, 2012).

Furthermore, the study confirms that reducing audit risk and improving data security directly enhances audit quality. This finding is consistent with prior research showing that professional skepticism, accurate data, and robust cybersecurity are critical for effective audit performance and reliable financial reporting (Hurtt, 2011; AlShaer, 2020; Westland, 2021).

Theoretically, this study contributes to the advancement of defense-in-depth theory by highlighting how information technology audits can reduce anomalies and strengthen data security in response to evolving technological threats. As intrusion detection becomes increasingly important, organizations must adopt robust IT governance and audit practices to ensure that security standards are upheld. The study also supports contingency theory by demonstrating how external factors, such as technological change, influence audit practices and decision-making. The expansion of information technology audits reflects a strategic response to environmental uncertainties, particularly in the digital era.

Practically, these findings provide insights for auditors in the capital market to enhance their professional competencies. The identification of key information technology audit dimensions allows the development of more reliable audit processes. By integrating information technology audit into traditional audit practices, auditors can improve data accuracy, safeguard sensitive information, and reduce the likelihood of inappropriate opinions. This contributes to greater trust in financial reporting and enhances audit effectiveness in a dynamic business environment.

In Thailand's capital market, the adoption of information technology audit remains uneven. While large audit firms and multinational corporations have begun applying digital audit tools, smaller firms often face limitations in resources, technical expertise, and regulatory guidance. Cultural tendencies toward hierarchical decision-making and limited digital literacy among senior auditors also slow adoption. Addressing these organizational and cultural constraints is crucial for strengthening Thailand's audit infrastructure.

From a policy perspective, this study highlights the need for collaboration between the National Cybersecurity Agency (NCSA) and the Securities and Exchange Commission (SEC) to establish standardized information technology audit frameworks, cybersecurity benchmarks, and certification systems for auditors. Implementing continuous professional training on data protection, digital assurance, and emerging technologies such as artificial intelligence and blockchain would help improve audit quality and align Thai practices with international standards. These policy efforts would also enhance transparency, investor confidence, and the long-term digital transformation of Thailand's auditing profession.

5.2. Conclusions

This study had certain limitations. The relatively small sample size may have reduced the statistical power and limited the generalizability of the findings beyond Thailand's capital markets. The limited number of responses (93 valid samples, representing a 25.48% response rate) may also affect the stability and representativeness of the statistical results. A smaller sample can increase the margin of error and reduce the robustness of regression estimates, particularly when examining complex variable relationships. Although the findings remain statistically significant, they should be interpreted with caution, as results might differ with a larger and more diverse sample. Expanding the dataset in future research would therefore improve the reliability, external validity, and generalizability of the conclusions. Therefore, the results should be interpreted with caution in broader or international contexts.

Future research should expand the sample size to include auditors from various regions, industries, and regulatory settings. Investigating potential moderating or mediating factors such as organizational size, audit firm characteristics, and technological maturity could further clarify the relationship between information technology audit practices and audit quality. Longitudinal or mixed-method approaches may also yield deeper insights into how digital transformation influences audit effectiveness over time. Future studies could also explore how emerging technologies such as artificial intelligence, machine learning, blockchain, and cloud-based audit analytics influence the quality and security of information technology audit practices. Comparative analyses across industries such as banking, manufacturing, and hospitality could provide deeper insights into how technological readiness, regulatory environments, and organizational culture shape the effectiveness of information technology audits in different contexts.

References

[1] Agoes, S., & Hoesada, J. (2012). Bunga Rampai Auditing. Jakarta: Salemba Empat .

[2] Albrecht, W. S., Albrecht, C., & Albrecht, C. (2015). Fraud Examination. Cengage Learning.

[3] Al-Omush, A., Almasarwah, A., & Al-Wreikat, A. (2025). Artificial intelligence in financial auditing: redefining accuracy and transparency in assurance services. EDPACS, 1–20. https://doi.org/10.1080/07366981.2025.2459490.

[4] AlShaer, H. (2020). Elevating Professional Reasoning in Auditing: Psycho-Professional Perspective. Journal of Accounting and Auditing: Research & Practice, 2020, 1–10. https://doi.org/10.5171/2020.804680.

[5] Andoko, M. P., Natalia, C., & Lindrianasari, L. (2025). Blockchain adoption in financial auditing: A global perspective on the top public companies worldwide. Edelweiss Applied Science and Technology, 9(8), 1827–1841. https://doi.org/10.55214/2576-8484.v9i8.9711.

[6] Andrew, J.L and L. S. Clifton. (2003). An Investigation into the Application of Defence in Depth Theory to Electronic Information Protection. Journal of Information Warfare. 2(2),88-96.

[7] Arens, A. A., Elder, R. J., & Beasley, M. S. (2017). Auditing and Assurance Services, Global Edition (17th Edition). In Prentice Hall eBooks. S.

[8] Asare, S., K. Hackenbrack , and W. R. Knechel. (1994). Client acceptance and continuation decisions. In Auditing Symposium XII: Proceedings of the 1994 Deloitte and Touche/University of Kansas Symposium on Auditing Problems, edited by R. P. Srivastava, 163–178 Lawrence, KS: University of Kansas.

[9] Bagranoff, N., Vendrzyk , V. (2000). The changing role of IS audit among the big five accounting firms. Information Systems Control Journal, 5 .33-7.

[10] Bazerman, M. H., Morgan, K. P., & Loewenstein, G. (1997). The Impossibility of Auditor Independence. MIT Sloan Management Review, 38(4), 89–94.

[11] Beridze, T. (2017). Information Technology Audit in Georgia. European Scientific Journal, 72. https://doi.org/10.19044/esj.2017.v13n25p72.

[12] Betti, N., & Sarens, G. (2020). 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.

[13] Bhattacharjee, S., Maletta, M. J., & Moreno, K. K. (2017). SOX Compliance and IT Controls. Journal of Information Systems.

[14] Bob Duncan & Mark Whittington. (2014). Compliance with standards, assurance and audit: Does this equal security. Conference: Security of Information and Networks. https://doi.org/10.1145/2659651.2659711

[15] Bosworth, S., & Kabay, M. E. (Eds.). (2002). Computer security handbook (4th ed.). Wiley.

[16] Carroll, M, Van Der Merwe, A and Lubbe, S. 2009. An information systems auditor's profile. Alternation: International Journal for the Study of Southern African Literature and Languages, Vol. 16(1), pp 318–355.
[17] Chen, L., Srinidhi, B., Tsang, A., & Yu, W. (2015). Audited Financial Reporting and Voluntary Disclosure of Corporate Social Re-sponsibility (CSR) Reports. Journal of Management Accounting Research, Forthcoming. https://doi.org/10.2139/ssrn.2666872.
[18] Chou, D. C. (2015). Cloud computing risk and audit issues. Computer Standards &Amp; Interfaces, 137–142. https://doi.org/10.1016/j.csi.2015.06.005.
[19] Devale , A.B., and Kulkarni ,R.V. (2012).“A review of expert system in Information System Audit”, International Journal of Computer Science and Information Technologies (IJCSIT), vol. 3, no. 5, pp.5172-5175.
[20] Federation of Accounting Professions. (2010). ISA 200: Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with Auditing Standards. Federation of Accounting Professions.
[21] Federation of Accounting Professions. (2014). International Standard on Auditing (ISA) 315 . Federation of Accounting Professions.
[22] Fiedler, F. (1972). The Effects of Leadership Training and Experience: A Contingency Model Interpretation. Administrative Science Quarterly, 17, 453-470. https://doi.org/10.2307/2393826.
[23] Gantz, S. D. (2014). The Basics of IT Audit. Elsevier.
[24] Gaurav, B. (2020). 5 Cybersecurity Threats to Be Aware of in 2020. IEEE. https://www.computer.org/ publica-tions/tech-news/trends/5-cybersecu-rity-threats-to-be-aware-of-in-2020.
[25] Genzorova, T., Corejova, T., & Stalmasekova, N. (2019). How digital transformation can influence business model, Case study for transport industry. Transportation Research Procedia, 40, 1053–1058. https://doi.org/10.1016/j.trpro.2019.07.147.
[26] Gray, R., Kouhy, R., & Lavers, S. (1995). Corporate social and environmental reporting. Accounting, Auditing & Accountability Journal, 1(1), 72-90.
[27] Gupta, K. (2020). Contemporary Auditing. Tata Mcgraw Hill Education Private Limited.
[28] Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). Multivariate data analysis (7th ed.). Pearson College Division.
[29] Hall, J. A. (2011). Information Technology Auditing and assurance (3 ed.). South-Western Cengage Learning.
[30] Hall, J. A., & Singleton, T. (2018). IT Auditing and Application Controls for Financial Reporting and SOX Compliance.
[31] Hurtt, R. K. (2011). Development of a scale to measure professional skepticism. Auditing a Journal of Practice & Theory,29(1),149–171. https://doi.org/10.2308/aud.2010.29.1.149.
[32] Igou, A., Power, D. J., Brosnan, S., & Heavin, C. (2022). Digital futures for accountants. Journal of Emerging Technologies in Accounting, 20(1), 39–57. https://doi.org/10.2308/JETA-2020-088.
[33] Information Systems Audit and Control Association. (22 October 2020). ISACA Updates IT Audit Framework (ITAF). Information Systems Audit and Control Association.
[34] Ivanov, D., Dolgui, A., & Sokolov, B. (2018). The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. International Journal of Production Research, 57(3), 829–846. https://doi.org/10.1080/00207543.2018.1488086.
[35] James, G., Witten, D., Hastie, T. and Tibshirani, R. (2021) An Introduction to Statistical Learning: With Applications in R. 2nd Edition, Springer, Berlin. https://doi.org/10.1007/978-1-0716-1418-1.
[36] Judijanto, L., Nurdiani, T. W., Ningsih, T. W., & Ryketeng, M. (2023). The effect of regulatory compliance and digital audit adoption on auditor performance and financial reporting accuracy in Indonesia. The ES Accounting and Finance, 2(01), 77–86. https://doi.org/10.58812/esaf.v2i01.154.
[37] Juiz, C. &. (2015). To govern IT, or not to govern IT? Communications of the ACM, 58-64. https://doi.org/10.1145/2656385.
[38] Kafi, M. A., & Akter, N. (2023). Securing Financial Information in the Digital realm: Case studies in Cybersecurity for Accounting Data Protection. American Journal of Trade and Policy, 10(1), 15–26. https://doi.org/10.18034/ajtp.v10i1.659.
[39] Kinney, W. R., & Shepardson, M. L. (2011). Research opportunities in internal control quality and quality assurance. Auditing: A Journal of Practice & Theory, 30(4), 1-24.
[40] Kinney, W. R., & Shepardson, R. (2011). The limits of compliance auditing: Implications for audit risk management. Journal of Accounting, Auditing & Finance, 26(3), 453–476.
[41] Klos, C., & Spieth, P. (2020). READY, STEADY, DIGITAL?! How foresight activities do (NOT) affect individual technological frames for mana-gerial sensemaking. Technological Forecasting and Social Change, 163, 120428. https://doi.org/10.1016/j.techfore.2020.120428.
[42] KPMG. (2020). Creating dynamic controls amid continuing regulatory change. KPMG LLP.
[43] Liu, C., Muravskyi, V., & Wei, W. (2024). Evolution of blockchain accounting literature from the perspective of CiteSpace (2013–2023). Heliyon, 10(11), e32097. https://doi.org/10.1016/j.heliyon.2024.e32097.
[44] Majdalawieh, M., & Zaghloul, I. (2009). Paradigm shift in information systems auditing. Managerial Auditing Journal, 24(4), 352–367. https://doi.org/10.1108/02686900910948198.
[45] Markus, M. L., & Loebbecke, C. (2013). Commoditized digital processes and business community platforms: new opportunities and challenges for digital business strategies. MIS Quarterly, 37(2), 649–654.
[46] 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. https://doi.org/10.17705/1CAIS.02326.
[47] Messier, W. F., Glover, S. M., & Prawitt, D. F. (2016). Auditing and Assurance Services.
[48] National Cyber Security Agency. (2023). Standards and Guidelines for Promoting the Development of Cyber Security Service Sys-tems.
[49] Osmundsen, K., Iden, J., & Bygstad, B. (2018). Digital Transformation: drivers, success factors, and implications. MCIS, 37. https://aisel.aisnet.org/mcis2018/37/.
[50] Peecher, M. E., Schwartz, R., & Solomon, I. (2007). It's all about audit quality: Perspectives on strategic-systems auditing. Accounting Organizations and Society, 32(4–5), 463–485. https://doi.org/10.1016/j.aos.2006.09.001.
[51] Petter Lovaas, S. C. (2012). IT Audit Challenges for Small and Medium-Sized Financial Institutions. Annual Symposium on Information Assurance and Secure Knowledge Management, 16-22.
[52] Power, M. (1997). The Audit Society: Rituals of Verification. Oxford University Press.
[53] Riad, A. (2015). ISO/IEC 27001. linkedin.
[54] Riadh Manita a, N. E. (2020). The digital transformation of external audit and its impact on corporate governance. Technological Forecasting and Social Change. https://doi.org/10.1016/j.techfore.2019.119751.
[55] Riyadi, A., Khaddafi, M., F, F., F, F., & Ilham, R. N. (2021). Internal factor of systematic risk model with information technology as intervening variables to increasing quality of government financial reports in Indonesia: Actual case from Riau Island Province. Morfai journal, 1(1), 22–35. https://doi.org/10.54443/morfai.v1i1.13.
[56] Robson, K., Humphrey, C., Khalifa, R., & Jones, J. (2007). Transforming audit technologies: Business risk audit methodologies and the audit field. Accounting Organizations and Society, 32(4–5), 409–438. https://doi.org/10.1016/j.aos.2006.09.002.
[57] Rosati, P., Gogolin, F., & Lynn, T. (2020). Cyber-Security incidents and audit quality. European Accounting Review, 31(3), 701-728. https://doi.org/10.1080/09638180.2020.1856162.
[58] Rose, A. M., J. M. Rose, K. Sanderson, and J. C. Thibodeau. 2017. When should audit firms introduce analyses of big data into the audit process. Journal of Information Systems, 31 (3): 81-99. https://doi.org/10.2308/isys-51837.
[59] Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for busi-nesses Resilience: Issues and recommendations. Sensors, 23(15), 6666. https://doi.org/10.3390/s23156666.
[60] Sagarik, D., Chansukree, P., Cho, W., & Berman, E. (2018). E-government 4.0 in Thailand: The role of central agencies. Information Polity, 23(3), 343–353. https://doi.org/10.3233/IP-180006.

[61] Salihu, A., & Hoti, X. B. (2019). The effect of IT audit on security incidents. International Journal of Scientific and Technology Research, 8(8), 1342–1347. https://www.ijstr.org/paper-references.php?ref=IJSTR-0819-21358.
[62] Sawyer, L. B., Scheiner, J. H., & Graham, J. (2014). Sawyer's Internal Auditing: Enhancing and Protecting Organizational Value. The Institute of Internal Auditors.
[63] Schneider, S., & Kokshagina, O. (2021). Digital transformation: What we have learned (thus far) and what is next. Creativity and Innovation Management, 30(2), 384–411. ttps://doi.org/10.1111/caim.12414.
[64] Smith, C. L. (2003). Principles of information security: Defense-in-depth approaches. New York, NY: Security Press.
[65] Suchman, M. C. (1995). Managing Legitimacy: strategic and institutional approaches. Academy of Management Review, 20(3), 571–610. https://doi.org/10.5465/amr.1995.9508080331.
[66] Such-Pyrgiel, M. K., Gołębiowska, A., & Prokopowicz, D. (2022). The Impact of the COVID-19 Pandemic on the Growing Importance of Cybersecurity of Data Transfer on the Internet. Polish Political Science Yearbook, (3 (51), pp.81-95. https://doi.org/10.15804/ppsy202224.
[67] Tinyase, K. O., Ocansey, E. O. N. D., & Asamoah, F. O. (2025). The moderating role of auditor experience in the relationship between audit pressure and audit quality. Archives of Business Research, 13(06), 90–108. https://doi.org/10.14738/abr.1306.18958.