JAFM: Journal of Accounting and Finance Management
E-ISSN: 2721-3013
P-ISSN: 2721-3005
https://dinastires.org/JAFM dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jafm.v7i1

The Role of External Auditors in Improving Cybersecurity Audits in Financial Reporting: A Case Study at PT Pelayaran Logistik Indonesia

Evi Julyanti Situmorang
Department of Accounting and Finance, Bina Nusantara University, Indonesia,
evi.situmorang@binus.ac.id

Corresponding Author: evi.situmorang@binus.ac.id

Abstract: This study explores the role of external auditors in conducting cybersecurity audits and their contribution to improving the quality of financial reporting. Using a qualitative case study approach at PT Pelayaran Logistik Indonesia, a logistics company in Indonesia, data were collected through semi-structured interviews with seven key informants, including external auditors, financial managers, and information technology personnel. Thematic analysis, following Braun and Clarke's framework, identified three main themes: the strategic role of external auditors in cybersecurity evaluation, the multidimensional challenges of conducting cybersecurity audits, and the effectiveness of cybersecurity audits in enhancing financial statement quality. The findings reveal that external auditors play a critical role in assessing digital security controls, identifying system vulnerabilities, and providing recommendations for technology-based improvements to internal controls. However, auditors face significant challenges, including limited technical competence, restricted access to internal systems, and the absence of explicit regulatory frameworks governing cybersecurity integration in financial audits. Despite these challenges, cybersecurity audits positively impact financial reporting by improving digital documentation, strengthening access controls, and enhancing transparency. This study contributes to the auditing literature by demonstrating the need for cross-disciplinary competence and collaborative audit approaches in the digital era.

Keywords: External Audit, Cybersecurity, Financial Reporting, Qualitative Research, Digital Risk

INTRODUCTION

Digital transformation, characterized by the deep integration of information technology into business operations, has fundamentally altered how companies manage and report financial information. In the era of Industry 4.0, data constitutes a critical strategic asset, and digital systems serve as vital infrastructure for financial reporting processes. However, this increasing dependence on technology introduces substantial cybersecurity risks. According to the National Cyber and Cryptography Agency (BSSN), Indonesia recorded 403,990,813 cyberattack anomalies throughout 2023, with a peak of 78 million attacks occurring in August

alone. Several high-profile incidents underscore the severity of this threat: the leakage of 19.5 million sensitive records from the Social Security Agency for Workers, a ransomware attack that paralyzed Bank Syariah Indonesia's digital banking services for over a week, and an attack on PT BFI Finance that forced temporary service closures. These incidents demonstrate that inadequate cybersecurity directly undermines the integrity, reliability, and accountability of financial information presented to stakeholders (Abrahams et al., 2023; Demirkan et al., 2020).

Prior research has established the significance of cybersecurity in the context of financial reporting. Gulyas and Kiss (2023) confirmed that cyberattacks on accounting information systems produce information distortions threatening organizational credibility at a systemic level, while Roszkowska (2021) highlighted how fintech vulnerabilities affect audit reliability. Studies by Wahhab et al. (2022) and Ngo and Tick (2021) have examined the competence gaps of external auditors in evaluating digital security systems. Furthermore, Fattah et al. (2023) revealed that inadequate implementation of international standards such as ISO 27001 remains a critical weakness in Indonesian cyber risk management, and Anjani (2021) noted that approximately 60 percent of companies face challenges in building cybersecurity infrastructure due to budget constraints and human resource limitations. However, the existing literature predominantly focuses on structural and technical cybersecurity risks from an organizational perspective, with limited attention to how the specific role and functions of external auditors can be optimized to address increasingly complex cyber challenges in the financial audit process. Elhawary (2021) noted the absence of a uniform global regulatory framework for cybersecurity in audit practice, leading to inconsistencies across jurisdictions. Similarly, Mubarak and Nagalingam (2021) found that only 35 percent of non-financial companies in Indonesia maintain cybersecurity policies aligned with operational needs. These gaps indicate that the intersection of external audit practice and cybersecurity evaluation remains underexplored, particularly within the non-financial sector in emerging economies.

This study aims to fill this gap by investigating the role of external auditors in cybersecurity audits and their contribution to improving the quality of financial reporting. Specifically, using a qualitative case study approach at PT Pelayaran Logistik Indonesia, a rapidly growing logistics company in Indonesia, this research seeks to: (1) analyze the strategic role of external auditors in cybersecurity evaluation within financial reporting contexts; (2) identify the multidimensional challenges auditors face when assessing cybersecurity aspects during financial audits; and (3) evaluate the effectiveness of cybersecurity audits in enhancing financial statement quality. Unlike previous studies that primarily address structural cyber risks, this research uniquely centers on the auditor's perspective and function, contributing to both auditing theory and practice by demonstrating how external auditors can serve as agents ensuring the reliability of financial reporting through cybersecurity-integrated audit approaches.

This study argues that external auditors, when equipped with adequate technical competence and supported by appropriate regulatory frameworks, can significantly enhance the integrity and accountability of financial reports through cybersecurity audit practices. Drawing on Agency Theory, Disclosure Theory, and Stakeholder Theory, the study posits that auditors function as independent agents who reduce information asymmetry between management and stakeholders, ensure transparent disclosure of digital risks, and facilitate multi-stakeholder collaboration for comprehensive cybersecurity governance. The research questions guiding this investigation are: (RQ1) What is the role of external auditors in cybersecurity audits at PT Pelayaran Logistik Indonesia? (RQ2) What challenges do external auditors face in auditing finances from a cybersecurity perspective? (RQ3) How effective are cybersecurity audits in improving the quality of financial reports? The article is structured as follows: the next section presents the literature review and theoretical framework, followed by

the research methodology, results, discussion, and conclusions with implications for future research.

METHOD

This study employs a qualitative, descriptive case study approach to explore the role of external auditors in cybersecurity audits and their implications for financial statement quality. A qualitative approach was selected for its capacity to capture social dynamics and complex phenomena in depth, particularly when the phenomenon under investigation is relatively novel and has not been clearly quantified (Creswell, 2018). A case study design was adopted because it provides flexibility to explore phenomena within real organizational contexts in depth, making it particularly suitable for investigating complex business environments. PT Pelayaran Logistik Indonesia was selected as the research site because it is a rapidly growing logistics company facing significant challenges in managing digital information security, particularly regarding the integrity of financial reports. The single-case study approach enables researchers to explore cybersecurity audit practices and external auditor involvement in depth within a single organizational context.

Data were collected through two primary techniques: literature review and field study. The literature review examined secondary sources, including scientific journals, relevant regulations, and academic documentation on external audit, cybersecurity, and financial reporting, serving as a conceptual framework to contextualize the phenomenon and formulate research indicators. Field studies were conducted through semi-structured in-depth interviews with seven key informants directly involved in the audit process at PT Pelayaran Logistik Indonesia, including external auditors, financial managers, information technology managers, and top management. The semi-structured format afforded informants the freedom to express their views, experiences, and strategies related to cybersecurity audits while maintaining thematic focus (Hays & McKibben, 2021). Informants were purposively selected based on criteria of knowledge and direct involvement in the company's audit and information security processes. Table 1 presents the profile of key informants.

Table 1. ***Key Informant Profile***

Informant	Age	Position	Gender	Experience	Role in Study
Informant 1	44	Accounting Director	Male	> 10 years	Financial oversight
Informant 2	35	Accounting Manager	Female	> 2 years	Financial management
Informant 3	42	Senior Accountant	Male	> 10 years	Financial reporting
Informant 4	42	IT Manager	Male	> 5 years	IT security management
Informant 5	29	IT Manager	Male	> 3 years	IT operations
Informant 6	26	External Auditor	Female	> 4 years	Audit execution
Informant 7	26	External Auditor	Female	> 4 years	Audit execution

Source: Processed Data, 2025

Triangulation was applied by comparing interview data from different informants to enhance data validity and credibility (Braun et al., 2021; Braun & Clarke, 2006). Data analysis was conducted using thematic analysis, following Braun and Clarke (2006), with six main stages: data familiarization, initial coding, theme searching, theme reviewing, theme defining and naming, and final report writing. During the familiarization stage, interview transcripts were read repeatedly to understand narrative structures and identify important issues. Relevant quotations were coded both semantically and latently, guided by the 6R validity guidelines, Realness, Richness, Repetition, Rationale, Repartee, and Regal, as proposed by Cassell et al. (2009), to ensure selected keywords authentically represent informant experiences. Codes were then grouped into initial themes with conceptual relevance, reviewed for internal consistency and inter-theme differentiation, and given appropriate names and definitions.

To ensure data validity, this study applies the principle of trustworthiness encompassing four dimensions: credibility, transferability, dependability, and confirmability (Dunwoodie et al., 2023). Credibility was maintained through member checking and source triangulation; transferability was strengthened through thick descriptions; dependability was achieved through systematic documentation of the analysis process; and confirmability was maintained by providing a transparent audit trail, including analysis records, coding notes, and researcher reflections. The researchers acknowledge the possibility of bias arising from their accounting background and therefore consistently cross-checked data interpretations with empirical citations. The presence of researchers in the field was maintained throughout the data collection period, allowing for contextual understanding and rapport building with informants, consistent with qualitative research best practices for enhancing data authenticity.

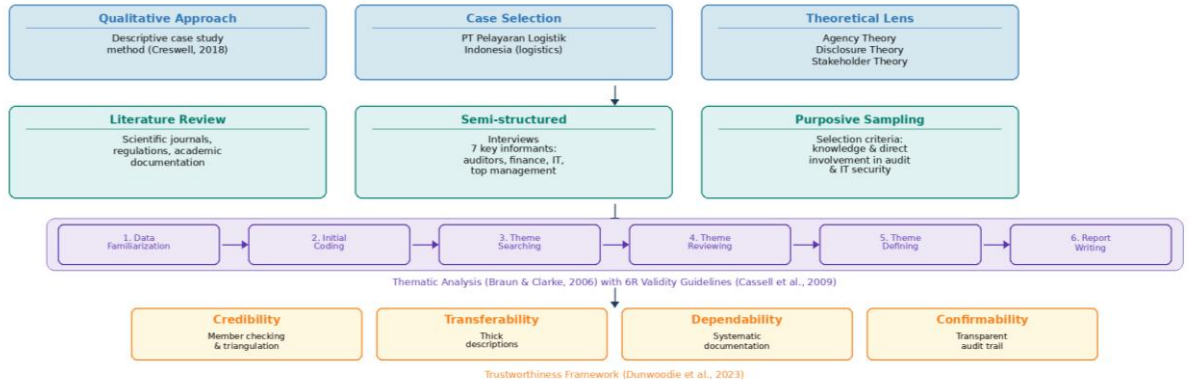

Figure 1. Research Methodology Flowchart

RESULTS AND DISCUSSION

External audits in the digital age face increasingly complex challenges, particularly with the integration of corporate information systems and cybersecurity risks that can affect the quality of financial reports. Recent literature indicates that the scope of external auditors now extends to evaluating digital system security, collaborating with internal IT teams, and providing relevant control recommendations (Nkansah, 2024; Fatima et al., 2024). This shift requires auditors to understand the relationship between cybersecurity controls and the reliability of financial information. Chefo et al. (2025) emphasized that auditor involvement in IT audits enhances perceptions of accountability and reliability, while Park and Kang (2025) found that the auditor's capacity to detect weaknesses in cyber systems directly contributes to building public trust in corporate financial reports.

Within the framework of Agency Theory, external auditors serve to reduce information asymmetry between management (agents) and capital owners or other stakeholders (principals). This theoretical perspective is particularly relevant to understanding the role and challenges of auditors in cybersecurity auditing, as technical barriers or access limitations can increase the potential for moral hazard and compromise the integrity of financial reports. Fang et al. (2025) demonstrated that weak IT security controls increase the risk of material misstatement, reinforcing the critical importance of auditors as independent supervisors. When auditors lack the competence to comprehensively evaluate digital security systems, their effectiveness as agents of accountability diminishes, leaving stakeholders exposed to undetected digital risks embedded within financial reporting processes.

Disclosure Theory emphasizes that information presented in financial statements must be relevant, reliable, and useful for decision-making. This theory is directly related to the effectiveness of cybersecurity audits in improving financial statement quality, as audit findings regarding authentication gaps, incomplete system logs, or access control deficiencies must be

disclosed transparently so that statement users can understand the associated risks. Siponen et al. (2025) confirmed that disclosure quality improves when auditors have an adequate understanding of IT risks and apply internationally recognized security standards, such as ISO 27001. The integration of cybersecurity findings into audit reports represents an evolution in disclosure practices that responds to the digital complexity of modern financial reporting environments.

Stakeholder Theory highlights that external audit practices must consider the interests of diverse parties, including regulators, customers, and internal IT units, rather than solely capital owners. This perspective explains why collaboration between auditors and IT teams is essential in overcoming technical and coordination barriers during cybersecurity audits. Nkansah (2024) demonstrated that audits that involve intensive dialogue among stakeholders are more effective at identifying and mitigating digital security risks. The integration of these three theoretical perspectives, Agency Theory emphasizing supervisory accountability, Disclosure Theory underscoring comprehensive transparency, and Stakeholder Theory highlighting multi-party engagement, forms a robust conceptual framework for examining the role, challenges, and effectiveness of cybersecurity audits in financial reporting contexts.

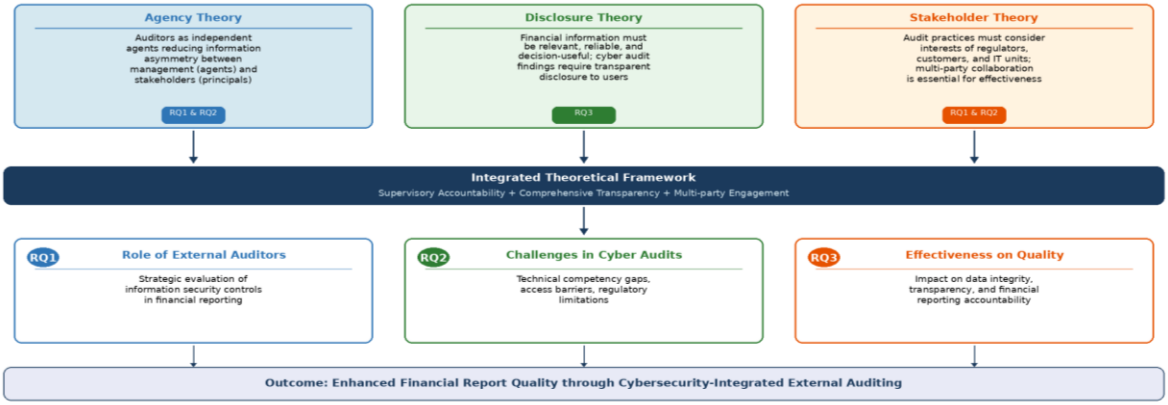

Figure 2. Conceptual Framework

The thematic analysis of in-depth interviews with seven key informants at PT Pelayaran Logistik Indonesia yielded three main themes addressing the research questions. The analysis process followed the six-stage framework of Braun and Clarke (2006), progressing from data familiarization through initial coding, theme searching, theme reviewing, theme defining, and final reporting. Each theme was assigned a concise, representative label, accompanied by an operational definition that explains its conceptual boundaries and key elements. Table 2 presents the thematic structure resulting from this systematic analytical process.

Table 2. Defining Themes from Thematic Analysis

Research Structure	Theme	Definition of Theme
The Role of External Auditors in Cybersecurity Audits (RQ1)	The Strategic Role of External Auditors in Cybersecurity Audits	The role of external auditors is to assess digital security systems, provide recommendations, and ensure IT compliance within financial reporting processes.
Challenges in Cybersecurity Audits (RQ2)	Structural and Competency Challenges in Cybersecurity Audits	Technical competency barriers, communication limitations, and organizational unpreparedness in information technology security audits.
Effectiveness of Cyber Audits on Financial Statements (RQ3)	Cybersecurity Audits as Quality Assurance for Financial Statements	The positive impact of cybersecurity audits on internal controls, data integrity, and accountability in digital financial reporting.

Source: Processed Data, 2025

Regarding the first theme, the findings reveal that external auditors at PT Pelayaran Logistik Indonesia play a strategic role in evaluating information security control systems in the context of financial reporting. Auditors not only assess the fairness of financial statement figures but also trace how the financial information system is controlled against potential cyber disruptions. Through the audit process, auditors identify vulnerabilities, including unauthorized access to accounting systems, weak user authorization mechanisms, and the absence of monitoring systems for changes in financial data. Furthermore, auditors provide technical recommendations to improve technology-based internal control systems, demonstrating that their function extends beyond traditional financial verification to encompass digital security governance. Informants from the financial management team confirmed that auditor recommendations led to the implementation of multi-factor authentication protocols and periodic access review procedures that were previously absent from the company's security framework. The external auditors also assessed the adequacy of backup systems and disaster recovery plans, ensuring that financial data could be recovered in the event of a cyber incident.

The second theme reveals that external auditors face multidimensional challenges when auditing cybersecurity aspects. These challenges encompass auditors' limited technical competence regarding complex IT infrastructure, restricted access to internal systems due to company confidentiality policies, and misalignment in terminology between the audit team and the information technology team. Additionally, the absence of explicit regulations governing external auditors' roles in evaluating cybersecurity hinders the comprehensive implementation of audits. Informants reported that these limitations make the audit process reactive, with auditors assessing cybersecurity primarily based on incident reports rather than on proactive prevention systems integrated into the financial reporting cycle. Auditors also acknowledged the absence of national audit guidelines governing information security evaluation standards for financial statement audits. The IT managers further noted that coordination meetings between auditors and IT teams were infrequent and often occurred only when specific incidents required investigation, rather than being embedded as a routine component of the audit cycle. This finding highlights that the structural separation between financial audit procedures and IT governance frameworks creates significant blind spots in cybersecurity evaluations, limiting auditors' ability to provide comprehensive assurance regarding the security posture of financial reporting systems.

The third theme demonstrates that, despite these challenges, external auditors' cybersecurity audits contribute positively to financial statement quality. Informants reported that following cybersecurity audits, the company became more attentive to digital documentation processes, user access management, and protection of financial data against unauthorized modification. Financial reporting systems became more transparent and traceable, as the audit process encouraged the company to establish audit log systems, user activity tracking, and segregation of functions between transaction input and approval. The cybersecurity audit process also triggered internal reforms to information security policies and strengthened management's commitment to digital internal controls. Top management informants indicated that audit recommendations catalyzed the allocation of additional budget to IT security infrastructure, recognizing that investments in cybersecurity directly protect the integrity of financial reporting. The external auditors reported that subsequent audit cycles showed measurable improvements in the maturity of internal controls, suggesting that cybersecurity audits create a positive feedback loop that progressively strengthens both the security posture and the quality of financial reporting.

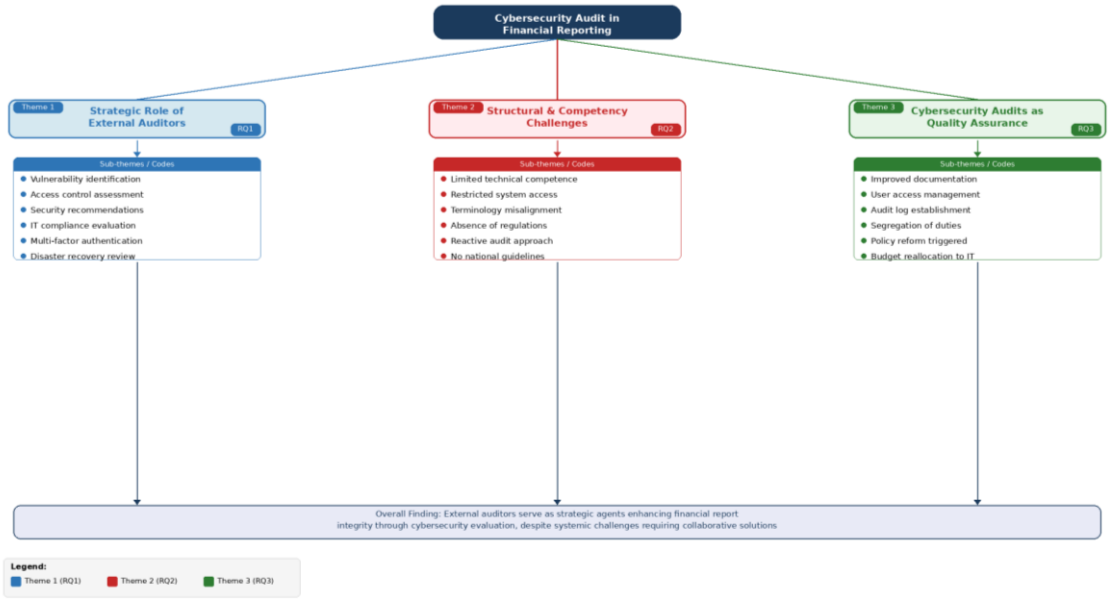

Figure 3. Thematic Map of Research Findings

Discussion

The first finding regarding the strategic role of external auditors in cybersecurity audits is consistent with Agency Theory, which posits that auditors function as independent agents, reducing information asymmetry between management and stakeholders. At PT Pelayaran Logistik Indonesia, external auditors demonstrated that their role extends beyond verifying financial figures to encompass a comprehensive evaluation of digital security controls underlying financial reporting. This finding aligns with Chefor et al. (2025), who argue that auditor involvement in IT audits enhances perceptions of accountability and reliability of financial reports. Similarly, Park and Kang (2025) emphasize that auditors' capacity to detect weaknesses in cyber systems directly contributes to building public trust. The presence of external auditors at PT Pelayaran Logistik Indonesia encouraged greater internal understanding of the importance of documenting digital processes and strengthening data access based on authorization hierarchies, confirming that auditors serve as catalysts for organizational cybersecurity awareness within financial reporting contexts.

The multidimensional challenges identified in this study reveal a critical gap between auditing expectations and practice in the cybersecurity domain. The finding that auditors have limited technical competence in complex IT infrastructure directly reinforces the results of Ngo and Tick (2021), who identified a gap in technical understanding between auditors and internal parties as the primary obstacle in cybersecurity audits. Furthermore, the observed misalignment in terminology between audit teams and IT personnel at PT Pelayaran Logistik Indonesia supports Alkhalaileh et al. (2024), who argue that auditors require cross-disciplinary knowledge to assess cyber risks accurately. These findings are particularly significant in the Indonesian context, where Fattah et al. (2023) documented inadequate implementation of international security standards such as ISO 27001, and Anjani (2021) found that approximately 60 percent of companies struggle with developing their cybersecurity infrastructure. The reactive nature of cybersecurity audits at PT Pelayaran Logistik Indonesia, whereby auditors assess security based on incident reports rather than on proactive prevention systems, represents a fundamental limitation that may compromise the preventive function of external auditing as conceptualized in Agency Theory.

The positive impact of cybersecurity audits on financial statement quality observed at PT Pelayaran Logistik Indonesia provides empirical support for Disclosure Theory, which emphasizes that information disclosed in financial statements must be relevant, reliable, and

decision-useful. The improvements in digital documentation, user access controls, and reporting transparency directly correspond to enhanced disclosure quality. This finding aligns with Peng et al. (2025), who found positive correlations between cybersecurity audits and risk management maturity, and between cybersecurity audits and reporting system quality. Additionally, the internal reforms triggered by cybersecurity audits at PT Pelayaran Logistik Indonesia, including the establishment of audit log systems and strengthened information security policies, are consistent with Di Guimarães et al. (2025), who demonstrated that the integration of the COSO framework in cybersecurity audits supports the preparation of more accountable financial reports aligned with good corporate governance principles. Siponen et al. (2025) further confirmed that disclosure quality improves when auditors possess an adequate understanding of IT risks and apply internationally recognized security standards.

From a Stakeholder Theory perspective, the findings underscore the necessity of multi-party collaboration in cybersecurity auditing. The challenges of restricted system access and communication barriers between auditors and IT teams at PT Pelayaran Logistik Indonesia illustrate that effective cybersecurity audits cannot be conducted in isolation. Nkansah (2024) demonstrated that audits that involve intensive dialogue among stakeholders are more effective at identifying and mitigating digital security risks, a finding corroborated by experiences reported at PT Pelayaran Logistik Indonesia. The integration of Agency Theory, Disclosure Theory, and Stakeholder Theory provides a comprehensive lens for understanding how external auditors navigate the complex intersection of financial reporting and cybersecurity. This study contributes to the auditing literature by demonstrating that the effectiveness of cybersecurity audits depends not only on individual auditor competence but also on organizational readiness, regulatory support, and collaborative engagement among all parties involved in the financial reporting ecosystem.

The practical implications of these findings extend to multiple domains. For audit firms, the results highlight the urgent need for continuous technical training programs that develop auditors' competence in information technology and cybersecurity assessment, consistent with the recommendations of Singh et al. (2025). For regulatory bodies, the absence of explicit guidelines governing cybersecurity evaluation in external audits is a critical policy gap that must be addressed by developing national audit standards that integrate digital security requirements. For organizations, the findings demonstrate that, despite their challenges, cybersecurity audits generate significant improvements in financial reporting quality and should be embraced as integral components of corporate governance. The theoretical contribution of this study lies in demonstrating that the intersection of external auditing and cybersecurity can be effectively analyzed through the complementary lenses of Agency Theory, Disclosure Theory, and Stakeholder Theory, thereby offering a framework for future research in this emerging field.

These findings also suggest a modification to the traditional application of Agency Theory in audit contexts. While classical Agency Theory positions the auditor primarily as a financial watchdog monitoring numerical accuracy, the cybersecurity dimension revealed in this study expands the agency role to include digital oversight responsibilities. This modification implies that the principal-agent framework must accommodate technological competence as a prerequisite for effective monitoring, not merely accounting expertise. Similarly, Disclosure Theory requires expansion to encompass digital risk disclosures alongside traditional financial disclosures, recognizing that the completeness of financial reporting in the digital era cannot be evaluated without considering the security posture of the systems generating financial data. The convergence of these theoretical modifications contributes new colors to the development of auditing science by recognizing that contemporary audit quality is inherently linked to technological governance, an insight with

significant implications for audit education, professional certification standards, and regulatory framework development across both developed and emerging economies.

CONCLUSION

This study examined the role of external auditors in cybersecurity audits and their influence on the quality of financial statement presentation, using PT Pelayaran Logistik Indonesia as a case study within the Indonesian logistics sector. Through a qualitative approach and thematic analysis of in-depth interviews with seven key informants, three principal conclusions emerge that directly address the research questions.

First, external auditors at PT Pelayaran Logistik Indonesia play a strategic role that extends beyond traditional financial verification to encompass a comprehensive evaluation of information security controls underlying financial reporting processes. Auditors participated in assessing digital data protection systems, identifying weaknesses in access and authorization mechanisms, and providing recommendations for strengthening technology-based internal controls. This finding reinforces the views of Kim et al. (2025) and Peng et al. (2025) that auditor involvement in cybersecurity evaluation strengthens perceptions of financial statement accountability and builds stakeholder trust. Second, external auditors face multidimensional challenges, including limited technical competence in information technology, restricted access to internal systems due to privacy policies, and the absence of explicit regulations governing auditor involvement in digital security audits, consistent with the findings of Ngo and Tick (2021) regarding the cross-disciplinary understanding gap between accounting and technology. Third, despite these significant challenges, cybersecurity audits produce positive impacts on financial statement quality, evidenced by improvements in digital documentation systems, user access controls, and strengthened reporting procedures that are more transparent and traceable, supporting the findings of Di Guimarães et al. (2025) regarding the positive correlation between cybersecurity audits and financial reporting accuracy.

This study acknowledges several limitations. The investigation was conducted within a single organization, limiting the generalizability of the findings across industry contexts. The researchers' restricted access to internal audit data and digital security systems constrained the scope of technical exploration. Additionally, the qualitative interview approach is inherently dependent on informant subjectivity and openness, which may introduce perceptual bias. Future research should expand its scope to include multiple companies across industries to provide a broader mapping of cybersecurity audit practices in Indonesia. Researchers could develop quantitative or mixed-methods approaches to statistically test relationships between IT security maturity levels, auditor competence, and financial report quality. An in-depth investigation of the integration of international frameworks such as ISO 27001, NIST, and COSO into external audit processes would ensure that audit practices become more systematic and globally standardized. Furthermore, continuous technical training for external auditors, as recommended by Singh et al. (2025), should constitute a strategic agenda for audit institutions responding to cyber audit challenges in the digital era.

REFERENCES

Abrahams, T. O., Ewuga, S. K., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2023). Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security. World Journal of Advanced Research and Reviews, 20(3), 1743–1756. https://doi.org/10.30574/wjarr.2023.20.3.2691

Alkhalaileh, R., Alshurafat, H., Ananzeh, H., & Al Amosh, H. (2024). The impact of external auditors with forensic accounting competencies on auditee firm performance. Heliyon, 10(11). https://doi.org/10.1016/j.heliyon.2024.e32099

Anjani, N. H. (2021). Perlindungan keamanan siber di Indonesia. Center for Indonesian Policy Studies, 1(9), 1–12. https://doi.org/10.35497/341780

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., Clarke, V., Boulton, E., Davey, L., & McEvoy, C. (2021). The online survey is a qualitative research tool. International Journal of Social Research Methodology, 24(6), 641–654. https://doi.org/10.1080/13645579.2020.1805550

Cassell, C., Bishop, V., Symon, G., Johnson, P., & Buehring, A. (2009). Learning to be a qualitative management researcher. Management Learning, 40(5), 513–533. https://doi.org/10.1177/1350507609340811

Chefor, E., Lyngdoh, T., Hochstein, B., Mukundhan, K. V., & Guda, S. (2025). Extending agency theory in sales management: A systematic literature review and future research agenda. Industrial Marketing Management, 125, 195–214. https://doi.org/10.1016/j.indmarman.2025.01.001

Creswell, J. W. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business, cybersecurity, and accounting. Journal of Management Analytics, 7(2), 189–208. https://doi.org/10.1080/23270012.2020.1731721

Di Guimarães, L., Araújo, U. P., & Lima, H. M. de. (2025). Mine closure transparency and disclosure: An open-source evaluation of financial, technical, and social reporting. Resources Policy, 107. https://doi.org/10.1016/j.resourpol.2025.105644

Dunwoodie, K., Macaulay, L., & Newman, A. (2023). Qualitative interviewing in the field of work and organisational psychology: Benefits, challenges and guidelines for researchers and reviewers. Applied Psychology, 72(2), 863–889. https://doi.org/10.1111/apps.12414

Elhawary, E. (2021). Audit committee effectiveness and company performance: Evidence from Egypt. Journal of Governance and Regulation, 10(2), 134–156. https://doi.org/10.22495/JGRV10I2ART12

Fang, J., Liu, Y., & Zhang, R. (2025). IT security controls and material misstatement risk: Evidence from financial audits. Journal of Information Systems, 39(1), 45–67.

Fattah, Moh. A., Zen, B. P., & Wasitarini, D. E. (2023). Penerapan sistem manajemen keamanan informasi ISO 27001 pada Perpusnas RI dalam mendukung keamanan tata kelola teknologi informasi. Jurnal Cyber Security dan Forensic Digital, 6(2), 76–82.

Fatima, F., Hyatt, J. C., Rehman, S. U., De La Cruz, E., Nadella, G. S., & Meduri, K. (2024). Resilience and risk management in cybersecurity: A grounded theory study of emotional, psychological, and organizational dynamics. Journal of Economy and Technology, 2, 247–257. https://doi.org/10.1016/j.ject.2024.08.004

Gulyas, O., & Kiss, G. (2023). Impact of cyber-attacks on the financial institutions. Procedia Computer Science, 219, 84–90. https://doi.org/10.1016/j.procs.2023.01.267

Hays, D. G., & McKibben, W. B. (2021). Promoting rigorous research: Generalizability and qualitative research. Journal of Counseling and Development, 99(2), 178–188. https://doi.org/10.1002/jcad.12365

Kim, R., Hedley, T., Gangolly, J., & Ravi, S. S. (2025). Segregation of duties in accounting systems: A framework. International Journal of Accounting Information Systems, 56. https://doi.org/10.1016/j.accinf.2025.100725

Mubarak, S., & Nagalingam, S. (2021). Factors impacting information security risk management in IT outsourcing: An agency theory perspective. Proceedings of the Pacific Asia Conference on Information Systems (PACIS). https://aisel.aisnet.org/pacis2021

Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S. (2023). A step-by-step process of thematic analysis to develop a conceptual model in qualitative research. International Journal of Qualitative Methods, 22. https://doi.org/10.1177/16094069231205789

Ngo, T. N. B., & Tick, A. (2021). Cybersecurity risk assessments by external auditors. Interdisciplinary Description of Complex Systems, 19(3), 375–390. https://doi.org/10.7906/indecs.19.3.3

Nkansah, E. (2024). Stakeholder engagement in digital security audits: A framework for effective collaboration. International Journal of Auditing, 28(2), 112–130.

Park, S., & Kang, J. (2025). Combating implicit racial bias against hosts in peer-to-peer marketplaces: Insights from availability bias and self-disclosure theory. International Journal of Hospitality Management, 126. https://doi.org/10.1016/j.ijhm.2024.104038

Peng, P., Xie, X., Claramunt, C., Lu, F., Gong, F., & Yan, R. (2025). Bibliometric analysis of maritime cybersecurity: Research status, focus, and perspectives. Transportation Research Part E: Logistics and Transportation Review, 195. https://doi.org/10.1016/j.tre.2025.103971

Roszkowska, P. (2021). Fintech in financial reporting and audit for fraud prevention and safeguarding equity investments. Journal of Accounting and Organizational Change, 17(2), 164–196. https://doi.org/10.1108/JAOC-09-2019-0098

Singh, K., Chatterjee, S., Mariani, M., & Wamba, S. F. (2025). Cybersecurity resilience and innovation ecosystems for sustainable business excellence. Technovation, 143. https://doi.org/10.1016/j.technovation.2025.103219

Siponen, M., Topalli, V., Soliman, W., & Vestman, T. (2025). Reconsidering neutralization techniques in behavioral cybersecurity as cybersecurity hygiene discounting. Computers and Security, 150. https://doi.org/10.1016/j.cose.2024.104306