Proceedings of the International Conference on Education, Economics, Business, Entrepreneurship, and Finance (ICEBEF)
Volume 4 (2026)

ENHANCING DIGITAL INTEGRITY THROUGH INVESTIGATIVE AND CYBERSECURITY AUDITING

Millicent Boadi[1], Silas Twum[2], Denny Andriana[3], and R Nelly Nur Apandi[4]
[1,2,3,4]Faculty of Economics and Business Education, Universitas Pendidikan Indonesia
Email: millb1301@upi.edu; twum.s90@upi.edu; denny.andriana@upi.edu; nelly.nna@upi.edu

ABSTRACT
In the era of digital transformation, organizations increasingly rely on technology-driven systems for governance, financial management, and service delivery. Although these advancements improve efficiency, they also increase the risk of digital corruption, making digital integrity essential for maintaining public trust and institutional accountability. This study examines how the integration of investigative auditing and cybersecurity auditing can strengthen digital integrity and combat digital corruption within organizations. The study uses a comprehensive literature review and case studies from public institutions implementing investigative and cybersecurity audit practices. Data were analyzed thematically to identify key patterns, challenges, and strategies for improving audit effectiveness in digital environments. The findings indicate that integrating investigative and cybersecurity auditing strengthens digital integrity by addressing both technological and behavioral factors. The study concludes that while cybersecurity protects digital systems, ethical awareness, fairness, and organizational trust remain critical determinants in preventing digital corruption effectively.

Key Words: Digital Integrity; Investigative Auditing; Cybersecurity Auditing; Digital Corruption; Accountability

INTRODUCTION

In today's digital era, organizations increasingly rely on information technology systems to manage data, finances, and service delivery. While digitalization enhances efficiency, it also exposes institutions to emerging risks such as data breaches, cyber fraud, and unauthorized access (Erondu & Erondu, 2023), which collectively undermine digital integrity. Maintaining digital integrity, which encompasses the accuracy, reliability, and trustworthiness of digital systems, has therefore become essential for effective governance and accountability (Ajiga et al., 2024). Within this context, investigative auditing and cybersecurity auditing play critical roles. Investigative auditing focuses on uncovering irregularities, detecting fraud, and ensuring compliance, while cybersecurity auditing safeguards information systems against digital threats. Integrating these two approaches can strengthen institutional capacity to prevent, detect, and mitigate digital corruption (Iipumbu et al., 2023).

While digital auditing has gained increasing attention in recent years, most existing studies have examined financial, internal, or compliance auditing (Alzeban, 2019); (Hegazy & Farghaly, 2021); (Chang et al., 2019), without adequately exploring how investigative auditing and cybersecurity auditing can be integrated to enhance digital integrity. Current literature tends to focus either on the technical aspects of cybersecurity, such as threat detection and data protection, or on the forensic dimension of investigative auditing (Henriques et al., 2024); (Serketzis et al., 2019), but rarely on the intersection between the two. Moreover, few studies have analyzed how behavioural factors, such as auditor motivation, ethical judgment, and organizational culture, influence the effectiveness of these digital auditing processes. This gap limits understanding of how institutions can holistically prevent and manage digital corruption through coordinated auditing frameworks.

Therefore, this research addresses the gap by examining the synergistic role of investigative and cybersecurity auditing in promoting digital integrity, guided by Behavioural Agency Theory (Pepper & Gomez-Mejia, 2015). These theories explain how incentives, risk perceptions, and monitoring mechanisms influence decision-making and accountability, offering a useful framework to explore the alignment between human behaviour, auditing practices, and digital integrity.

Accordingly, this study seeks to answer the following research questions: (1) How do investigative and cybersecurity auditing contribute to enhancing digital integrity within organizations? (2) In what ways can the integration of these audit approaches reduce digital corruption and improve accountability? (3) How do behavioural and organizational factor influence the effectiveness of digital auditing practices? These questions will guide the exploration of both the technical and human elements that underpin effective digital governance.

The scope of this study focuses on public sector institutions where digital transformation is expanding, but the risk of corruption and data manipulation remains prevalent (Sarker et al., 2018); (Otia & Bracci, 2022). The research will rely on case analyses of documented digital fraud and audit incidents, complemented by a systematic literature review of scholarly and institutional sources on investigative and

cybersecurity auditing. This approach will enable a comprehensive understanding of both practical experiences and theoretical perspectives. Geographically, the study emphasizes developing economies, where challenges such as limited digital infrastructure, weak enforcement mechanisms, and evolving audit systems influence the effectiveness of digital integrity measures. By examining these contexts, the study aims to generate insights that are both contextually relevant for policymakers and practitioners and theoretically significant for advancing knowledge on the integrated digital auditing framework.

METHOD

The study adopted a qualitative research design combining case analyses with systematic literature review. Data were collected from documented digital fraud cases in Indonesian public institutions, including audit reports, cyber incident reports, and official publications from anti-corruption agencies. A systematic literature review following PRISMA guidelines examined peer-reviewed articles, policy papers, and technical reports published between 2015-2025 from databases including Scopus, ScienceDirect, and Google Scholar.

Thematic analysis was employed to identify recurring patterns across case studies and literature sources. The analysis involved familiarization, initial coding, theme development, and interpretation through the lens of Behavioural Agency Theory. Validity was ensured through triangulation between case data and literature findings, with transparent documentation of selection criteria and coding procedures.

RESULTS AND DISCUSSION

The analysis employed a qualitative thematic approach, integrating a systematic literature review (2015–2025) with documented case evidence from public sector institutions in developing economies. The central focus was the intersection of investigative and cybersecurity auditing in promoting digital integrity. Four major themes emerged from the data:

Investigative Auditing and Digital Integrity

Investigative auditing serves as a post-incident accountability mechanism, uncovering root causes of digital fraud and identifying control weaknesses. In Indonesian public-sector cases, investigative audits revealed data falsification, unauthorized access, and procurement manipulation in digital systems. Under Behavioural Agency Theory, effectiveness depends not only on technical capacity but also on ethical climate and organizational culture supporting audit legitimacy.

Cybersecurity Auditing and Data Assurance

Cybersecurity auditing provides preventive protection through system monitoring, vulnerability

assessment, encryption, access controls, and compliance verification. Strong cybersecurity frameworks significantly reduce data breaches and unauthorized access incidents. However, implementation challenges persist in developing economies, including limited technical capacity and infrastructure constraints.

Synergy Between Audit Types

The integration creates a holistic ecosystem addressing both preventive and corrective dimensions. Cybersecurity auditing identifies vulnerabilities proactively, while investigative auditing responds reactively to anomalies. Combined, they create a closed feedback loop continuously strengthening system integrity. Insights from cybersecurity audits inform investigative processes, while investigative outcomes refine cybersecurity protocols.

Behavioural and Organizational Influences

Three critical behavioural factors emerged: (1) Ethical perception and trust in auditing systems - when audits are perceived as fair and legitimate, compliance increases; (2) Incentive structures and risk awareness - employees comply when perceiving higher potential losses from noncompliance; (3) Organizational support and technological readiness - management commitment, training, and resource allocation determine implementation success.

Case-Based Insights from Public Sector Institutions

Analysis of Indonesia's 2024 National Data Centre ransomware attack, Tokopedia data breach, South Jakarta data leak, and e-procurement fraud revealed that digital corruption stems from human behaviour as much as technical vulnerabilities. Each incident demonstrated how lapses in vigilance, ethical conduct, and accountability preceded technical failures. When auditing systems became transparent and fair, behavioural compliance improved significantly.

The Indonesian experience illustrates that integrity emerges from convergence of technical systems, ethical awareness, and behavioural accountability. Integrated auditing not only detects and prevents digital corruption but cultivates psychological and moral conditions necessary for sustained compliance.

CONCLUSION

This study demonstrates that digital corruption is not merely technological failure but a product of human behaviour, organizational culture, and ethical perception. Investigative and cybersecurity auditing, when

effectively integrated, create a holistic system preventing and detecting digital irregularities while promoting accountability and transparency.

Evidence from Indonesian digital fraud cases confirms that when auditing systems are fair, transparent, and behaviourally sensitive, they strengthen compliance and ethical commitment. Conversely, when perceived as punitive or biased, they trigger concealment and defensive behaviour.

Digital integrity emerges at the intersection of technology and behaviour. Cybersecurity systems provide technical protection, but human judgment, ethical awareness, and organizational trust determine effectiveness. This synergy is essential for countries navigating rapid digital transformation, especially in public sectors where trust and transparency are critical to governance.

REFERENCES

Ajiga, D., Okeleke, P. A., Folorunsho, S. O., & Ezeigweneme, C. (2024). Designing cybersecurity measures for enterprise software applications to protect data integrity. *Computer Science & IT Research Journal*, *5*(8), 1920–1941.

Alzeban, A. (2019). An examination of the impact of compliance with internal audit standards on financial reporting quality: Evidence from Saudi Arabia. *Journal of Financial Reporting and Accounting*, *17*(3), 498–518.

Chang, Y.-T., Chen, H., Cheng, R. K., & Chi, W. (2019). The impact of internal audit attributes on the effectiveness of internal control over operations and compliance. *Journal of Contemporary Accounting & Economics*, *15*(1), 1–19.

Erondu, C. I., & Erondu, U. I. (2023). The role of cyber security in a digitalizing economy: A development perspective. *International Journal of Research and Innovation in Social Science*, *7*(11), 1558–1570.

Hegazy, M. A., & Farghaly, M. (2021). External and internal auditors perceptions on compliance with internal audit standards and practices: Spirit vs letters? *Corporate Ownership & Control Journal*, *18*(3), 31–45.

Henriques, J., Caldeira, F., Cruz, T., & Simões, P. (2024). A survey on forensics and compliance auditing for critical infrastructure protection. *IEEE Access*, *12*, 2409–2444.

Iipumbu, E., Nhamu, I., & Chitauro, M. (2023). A Comparative Analysis of Information Systems Audit and Digital Forensics Processes. *Available at SSRN 4648699*.

Otia, J. E., & Bracci, E. (2022). Digital transformation and the public sector auditing: The SAI's perspective. *Financial Accountability & Management*, *38*(2), 252–280.

Sarker, M. N. I., Wu, M., & Hossin, M. A. (2018). Smart governance through bigdata: Digital transformation of public agencies. *2018 International Conference on Artificial Intelligence and Big Data (ICAIBD)*, 62–70.

Serketzis, N., Katos, V., Ilioudis, C., Baltatzis, D., & Pangalos, G. (2019). Improving forensic triage efficiency through cyber threat intelligence. *Future Internet*, *11*(7), 162.

Suhardjo, S., Suharti, S., Suyono, S., Mukhsin, M., & Hadi, S. (2023). Digital Internal Controls: Safeguarding Data Integrity and Compliance in a Technologically Evolving Landscape. *International Conference on Business Management and Accounting*, *2*(1), 306–311.