Integrating Information Technology and Investigation in Forensic Auditing: Case Study of Structured Fraud PT XXX

Riski Sofyan[1]
Yandi Renaldi[2]
Harti Budi Yanti[3]
[1,2,3]**Fakultas Ekonomi dan Bisnis Universitas Trisakti, Indonesia**
**Correspondences*: 123012401004@std.trisakti.ac.id

ABSTRACT

Structured fraud exploits information asymmetry in decentralized organizations. This study examines how integrated forensic auditing and information technology uncover fraud networks and the effectiveness of combining digital evidence with physical verification. A multiple case study analyzes two fraud incidents at PT XXX's Semarang and Lampung branches. Data from interviews, digital evidence (WhatsApp chats, photos, ERP logs), and documents were analyzed thematically using the Miles and Huberman model with NVivo 12 support. Findings reveal contrasting fraud patterns: authority-based Marketing Cost manipulation in Lampung versus collaborative asset theft networks in Semarang. Information technology served dual roles, enabling fraud while providing crucial investigation tools like "Get Contact" for identity tracing and WhatsApp metadata for chronology reconstruction. The investigation successfully integrated digital analysis with physical verification, demonstrating an effective hybrid forensic model for mapping hidden relationships and fraud schemes. The study concludes that combating structured fraud requires hybrid investigations synergizing digital forensics with physical auditing to enhance detection accuracy. Practical implications include strengthening IT-based internal controls, developing digital forensic competencies, and establishing standards for digital evidence in fraud investigations.

Keywords: Forensic Audit; Structure Fraud; Information Technology; Digital Evidence; Fraud Investigation

e-ISSN 2302-8556

Vol. 36 No. 1
Denpasar, 31 Januari 2026
Hal. 164-175

DOI:
10.24843/EJA.2026.v36.i01.p12

PENGUTIPAN:
Sofyan, R., Renaldi, Y., & Yanti, H. B. (2026). Integrating Information Technology and Investigation in Forensic Auditing: Case Study of Structured Fraud PT XXX. *E-Jurnal Akuntansi*, 36(1), 164-175

RIWAYAT ARTIKEL:
Artikel Masuk:
18 November 2025
Artikel Diterima:
20 Januari 2025

Integrating Information Technology and Investigation in Forensic Auditing: Case Study of Structured Fraud PT XXX

ABSTRAK

Penipuan terstruktur memanfaatkan asimetri informasi dalam organisasi yang terdesentralisasi. Studi ini meneliti bagaimana audit forensik terintegrasi dan teknologi informasi mengungkap jaringan penipuan dan efektivitas penggabungan bukti digital dengan verifikasi fisik. Studi kasus berganda menganalisis dua insiden penipuan di cabang PT XXX Semarang dan Lampung. Data dari wawancara, bukti digital (obrolan WhatsApp, foto, log ERP), dan dokumen dianalisis secara tematik menggunakan model Miles dan Huberman dengan dukungan NVivo 12. Temuan mengungkapkan pola penipuan yang kontras: manipulasi Biaya Pemasaran berbasis otoritas di Lampung versus jaringan pencurian aset kolaboratif di Semarang. Teknologi informasi berperan ganda, memungkinkan terjadinya penipuan sekaligus menyediakan alat investigasi penting seperti "Dapatkan Kontak" untuk pelacakan identitas dan metadata WhatsApp untuk rekonstruksi kronologi. Investigasi berhasil mengintegrasikan analisis digital dengan verifikasi fisik, menunjukkan model forensik hibrida yang efektif untuk memetakan hubungan tersembunyi dan skema penipuan. Studi ini menyimpulkan bahwa memerangi penipuan terstruktur membutuhkan investigasi hibrida yang mensinergikan forensik digital dengan audit fisik untuk meningkatkan akurasi deteksi. Implikasi praktisnya meliputi penguatan pengendalian internal berbasis TI, pengembangan kompetensi forensik digital, dan penetapan standar untuk bukti digital dalam investigasi penipuan.

Kata Kunci: *Audit Forensik; Structure Fraud; Teknologi Informasi; Bukti Digital; Investigasi Fraud*

Artikel dapat diakses : https://ejournal1.unud.ac.id/index.php/Akuntansi/index

INTRODUCTION

Structured fraud represents a critical and escalating threat to organizational sustainability, particularly in decentralized business models with widespread branch networks. The inherent information asymmetry between headquarters and branches, coupled with often inadequate monitoring mechanisms, creates fertile ground for complex, collusive fraud schemes. While conventional audits focus on financial statement accuracy, they frequently fail to detect such organized misconduct, which increasingly exploits both systemic vulnerabilities and digital tools. This evolving landscape necessitates a forensic auditing approach that can leverage information technology not merely as a record-keeping system but as an active investigative instrument to reconstruct hidden transactions and relationships.

Recent scholarly work has begun to explore the intersection of auditing and technology. Studies have empirically demonstrated the positive impact of Big Data Analytics on fraud detection capabilities and highlighted the role of forensic audit procedures in enhancing investigative outcomes (Handoko et al., 2022). Concurrently, research into Artificial Intelligence adoption within major audit firms reveals its potential for anomaly detection, though often limited to external financial statement audits (Bartstra, 2021). Other inquiries have focused on the technological readiness for AI in accounting (Anh et al., 2024) and the ethical frameworks for its implementation (Bani Ahmad, 2024). Furthermore, the application of specific digital tools, such as Explainable AI and Federated Learning for financial fraud detection, has been examined technically (Awosika et al., 2024). Prior case study research in Indonesia has also addressed the use of Big Data in audit processes (Bakri et al., 2023; Silvia et al., 2023).

Despite this growing body of knowledge, a significant research gap persists. First, there is a scarcity of in-depth, qualitative studies that holistically examine the integrated process of forensic auditing and information technology application in real-world investigations, especially within the context of structured, multi-party fraud in operating companies. Second, existing literature often treats technology as a generic input or a separate silo, lacking detailed analysis of how specific, readily available digital tools (e.g., communication apps, public databases, geolocation services) are synergized with physical verification steps in a hybrid investigative model. Third, few studies capture the nuanced dynamics of fraud schemes that differ across branches within the same organization, which is crucial for developing adaptable countermeasures. Therefore, this research is vital as it addresses a practical and underexplored nexus in forensic accounting. Its novelty lies in providing a rich, empirical account of a hybrid investigative methodology, detailing the procedural integration of digital evidence analysis and physical audit steps to deconstruct complex fraud networks. This study aims to analyze the process of uncovering structured fraud through the integrated application of forensic auditing and information technology, and to explore the effectiveness of this combined approach in a real-world corporate setting.

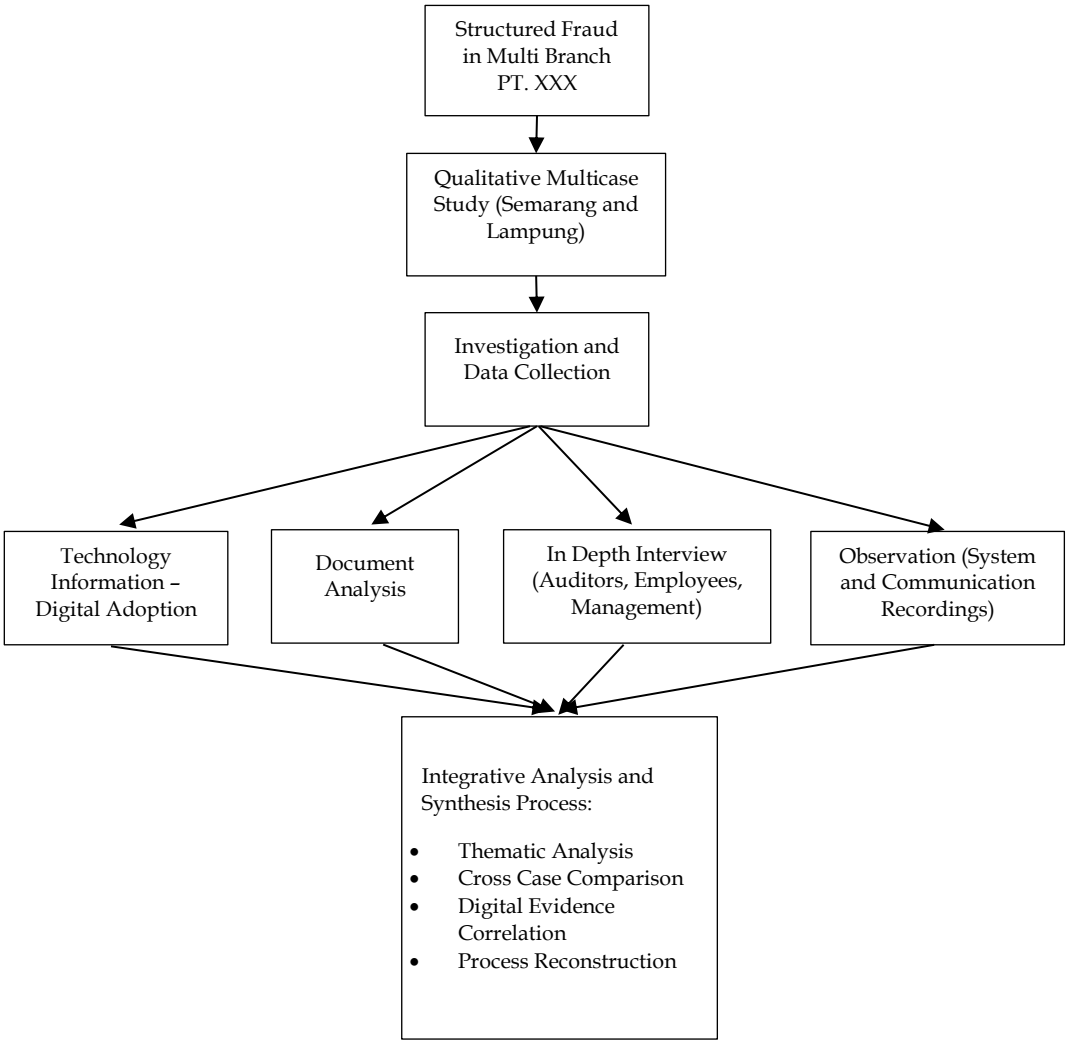

Figure 1. Research Model

Source: (Miles et al., 2014; Aini et al., 2025).

RESEARCH METHODOLOGY

The methodological approach is anchored in an interpretive qualitative paradigm, recognizing the deeply contextual and socially constructed nature of fraud detection processes within organizational settings. This paradigm facilitates an exploration of the meanings, motivations, and complex interactions that define forensic investigations, moving beyond positivist assumptions to appreciate the nuanced realities experienced by auditors and organizational members. A multiple case study design frames the inquiry, providing a structured yet flexible means to examine the phenomenon of structured fraud within its real-life context at two distinct branches of PT XXX. This design supports an intensive, holistic investigation where the boundaries between the phenomenon and its environment are inherently intertwined.

Data collection proceeded through a multi-method strategy emphasizing triangulation to enhance the robustness and credibility of the findings. Primary evidence originated from in-depth, semi-structured interviews with individuals

directly involved in or knowledgeable about the fraud incidents and subsequent investigations, including forensic auditors, branch managers, implicated staff, and external contacts. These conversations explored personal experiences, decision-making processes, and interpretations of events. Secondary data sources comprised a comprehensive review of internal documentation such as forensic audit reports, financial statements, transaction records within the Odoo ERP system, and marketing cost documentation. A significant and distinctive component of the data corpus consisted of digital evidence, including archived WhatsApp communications, digital photographs, video recordings, and system metadata, which were subjected to forensic analysis techniques for authentication and pattern recognition.

The selection of participants and cases followed a purposive, criterion-based strategy to ensure the inclusion of information-rich sources central to the research questions. The study engaged internal forensic auditors, with particular attention to those from Generation Z, whose digital competencies formed a specific line of inquiry. Additionally, key personnel from the Semarang and Lampung branches, where the fraud was identified and investigated were included, along with external individuals identified through the digital investigative process. This sampling approach ensured access to diverse perspectives necessary for constructing a comprehensive understanding of the fraud mechanisms and the investigative response.

The analytical focus centers on several core constructs, explored qualitatively rather than measured metrically. Structured fraud is conceptualized as a deliberate, coordinated activity involving multiple actors and systemic exploitation over time. The integration of information technology within forensic audit refers to the adoption and application of digital tools, data analytics, and electronic evidence in the investigative process. The competencies of Generation Z auditors encompass their innate digital literacy, adaptive problem-solving skills, and unique approaches to navigating digital environments. These constructs are examined through the patterns, narratives, and relational dynamics emergent in the data.

Analysis of the compiled data utilized the interactive model of qualitative data analysis, involving continuous cycles of data reduction, data display, and conclusion drawing. Data reduction entailed the systematic coding and categorization of interview transcripts, documents, and digital artifacts to identify salient themes and patterns. Data display employed various formats such as comparative matrices, network diagrams, and chronological timelines to organize the condensed information and facilitate the visualization of relationships and sequences. The process of conclusion drawing involved iterative interpretation, constant comparison between the two case sites, and the deliberate interrogation of emerging insights through the theoretical lenses of Agency Theory and Fraud Pentagon Theory. Thematic analysis served as the primary analytical tool, guiding the identification, organization, and interpretation of recurrent themes that capture the essence of the fraud detection process, the role of technology, and the impact of generational competencies within the field of forensic auditing.

RESULTS AND DISCUSSION

The forensic investigation into structured fraud at PT XXX revealed distinct patterns and characteristics between the Semarang and Lampung branches. Table 1 presents the frequency distribution of 24 evidence categories identified through NVivo 12 coding. The data shows that the Semarang Branch had a concentration of findings in specific categories with a lower total number of incidents (86 incidents) compared to the Lampung Branch (272 incidents). This quantitative difference indicates variations in the complexity and scale of fraud between the two branches, which will be further analyzed through the three research lenses according to the posed research questions.

Table 1. Frequency Distribution of Forensic Investigation Evidence Categories Based on NVivo Analysis

No	Evidence Category	Semarang	Lampung
1	Proof of Transfer	0	0
2	WhatsApp Chat	1	10
3	Photo	0	8
4	Video	1	0
5	Collusion Between Employees	0	7
6	Internal-External Collusion	0	24
7	Digital Coordination Pattern	0	5
8	Fraud Lapping	8	6
9	Sales Transaction Manipulation	0	21
10	Asset Misappropriation	0	22
11	Marketing Cost Misuse	8	5
12	Operational Procedure Deviation	0	13
13	AI_GetContact	0	9
14	Digital Analysis	0	11
15	ERP Odoo	0	2
16	Information System Weakness	0	5
17	Lack of Transaction Monitoring	8	20
18	Weak Segregation of Duties	8	0
19	Inadequate Branch Supervision	8	25
20	Evidence Analysis	8	25
21	Fraud Identification	8	28
22	Evidence Collection	8	24
23	Audit Conclusion Formulation	6	7
24	Investigative Interview	6	6
	Total	86	272

Source: Research Data, 2024

The forensic audit process at the Semarang Branch followed a reactive investigation pattern initiated by an anonymous whistleblower report. According

to the data in Table 1, two dominant fraud modus operandi were identified, fraud lapping (8 incidents) and marketing cost misuse (8 incidents). The disclosure process began with report verification using the "Get Contact" application to identify the source of the report, followed by analysis of the limited available digital evidence (1 WhatsApp Chat incident and 1 Video incident).

Figure 2. Anonymous Whistleblower Letter in Javanese

Source: Research Data, 2025

The investigation was triggered by an anonymous letter written in Javanese language, delivered to the head office. The letter contained specific allegations regarding inventory manipulation and fraudulent transactions at the Semarang branch. One critical passage stated: "Wong-wong nang cabang Semarang iki lagi nggarap proyek ilegal, barang-barang stok dikurangi tapi dokumen digawe normal. Aku wis ndeleng langsung barang dikirim menyang gudang sing ora resmi." (Translation: "People at the Semarang branch are working on illegal projects, stock items are being reduced but documents are made to look normal. I have seen directly goods being sent to unofficial warehouses.") This whistleblower letter, the initial leads that directed the forensic investigation toward specific operational anomalies.

Figure 3. "Get Contact" Mustika Application Analysis

Source: Research Data, 2025

Digital forensic examination revealed the use of the "Get Contact" Mustika application by several branch employees. This application, typically used for identifying unknown callers, was employed to screen and verify communications related to fraudulent activities. Analysis showed that the branch manager's mobile device had the "Get Contact" Mustika application installed, with call logs indicating 23 contacts saved under aliases that matched known unauthorized suppliers. The application's reverse lookup feature was used to identify potential whistleblowers and monitor communications, demonstrating an unexpected application of consumer technology for fraudulent purposes.

The disclosure process began with report verification using the "Get Contact" application to identify the source of the report, followed by analysis of the limited available digital evidence (1 WhatsApp Chat incident and 1 Video incident). A critical stage in this investigation was the integration of minimal digital evidence with traditional evidence, particularly through 6 investigative interview incidents and 6 audit conclusion formulation incidents.

NVivo findings reveal a specific configuration of internal control weaknesses in this branch, especially in the "Weak Segregation of Duties" category (8 incidents) and "Lack of Transaction Monitoring" (8 incidents). Thematic analysis of interview transcripts indicates that fraud in Semarang was motivated by a combination of financial pressure (pressure) and perpetrator rationalization (rationalization). The forensic audit process successfully reconstructed the fraud lapping scheme through chronological transaction tracing and cross-confirmation between digital evidence and written perpetrator confessions. These findings indicate that investigation effectiveness in branches with limited digital evidence

highly depends on the auditors' capacity to triangulate evidence sources and construct coherent fraud narratives.

In contrast to Semarang, the forensic audit process at the Lampung Branch followed a proactive approach based on system anomaly analysis. Data in Table 1 shows significantly higher fraud complexity with the dominance of three main categories: internal-external collusion (24 incidents), asset misappropriation (22 incidents), and sales transaction manipulation (21 incidents). The investigation began with the identification of 41 irregular transactions through the ERP Odoo system (2 incidents), which was then expanded through extensive digital evidence collection including 10 WhatsApp Chat incidents, 8 Photo incidents, and 9 AI "Get Contact" incidents.

NVivo analysis reveals a structured fraud pattern enabled by systemic control weaknesses, particularly "Inadequate Branch Supervision" (25 incidents) and "Lack of Transaction Monitoring" (20 incidents). The investigation process involved in-depth digital analysis (11 incidents) to identify hidden communication patterns and relationships between perpetrators. Thematic analysis shows a Fraud Pentagon configuration dominated by opportunity created by operational decentralization and perpetrator capability in exploiting system weaknesses. The forensic audit process in this branch successfully uncovered collusion networks through the integration of massive digital evidence with transaction analysis and confirmation through 6 investigative interview incidents.

The research findings reveal the multidimensional role of information technology in all three stages of forensic auditing. In the evidence collection stage, technology enables large-scale digital data acquisition, as reflected in the disparity of digital evidence frequency between the two branches: 10 WhatsApp Chat incidents in Lampung (10 times that of Semarang) and 8 Photo incidents. In the analysis stage, technology serves as an enabler for in-depth examination through 11 "Digital Analysis" incidents and 9 "AI_Get Contact" incidents in Lampung, encompassing metadata examination, geolocation analysis, and temporal data correlation. In the interpretation stage, technology supports fraud narrative construction through visualization of communication patterns and event chronology.

However, data in Table 1 also reveals critical insight, although the volume of digital evidence in Lampung is significantly higher, investigation effectiveness (measured through "Audit Conclusion Formulation") shows only marginal difference (7 incidents in Lampung vs 6 in Semarang). This finding indicates that the value of information technology in forensic auditing lies not in the quantity of evidence produced, but in its capacity to be transformed into investigative insight through appropriate analytical processes. Comparative analysis shows that investigation success is more determined by the strategy of integrating digital-traditional evidence than by the completeness of digital evidence alone.

The Semarang investigation demonstrates how different types of digital evidence converged to create a comprehensive investigative picture. The anonymous WhatsApp whistleblower chat in Javanese provided contextual understanding of local practices and relationships, while digital analysis of the "Get Contact" Mustika application revealed communication patterns that validated the whistleblower's claims. This integration was particularly effective because the

Javanese language used in the chat contained cultural nuances and local terminology that helped investigators understand the specific fraud mechanisms employed, while the “Get Contact” analysis provided technical verification.

The research findings provide empirical confirmation of Agency Theory propositions in the context of structured fraud. Information asymmetry between principal (head office) and agent (branch management) manifests in the high frequency of "Inadequate Branch Supervision" (25 incidents in Lampung, 8 in Semarang) and "Lack of Transaction Monitoring" (20 incidents in Lampung, 8 in Semarang). Further NVivo analysis reveals that variations in this asymmetry level correlate with the complexity of uncovered fraud, where Lampung with lower supervision levels shows more complex fraud patterns.

The Fraud Pentagon provides a robust analytical framework for understanding behavioral dimensions in both cases. In Semarang, the configuration is dominated by pressure and rationalization, consistent with the characteristics of fraud lapping typically motivated by acute needs. In Lampung, the configuration is dominated by opportunity and capability, reflecting structured fraud that exploits systemic weaknesses. Thematic analysis of interview transcripts reveals differences in rationalization narratives: in Semarang it takes the form of "urgent need," while in Lampung it is framed as "right to unofficial compensation."

The anonymous WhatsApp whistleblower chat in Javanese presents an interesting linguistic and cultural dimension to digital fraud investigation. The use of local language and cultural references in the digital communication suggests that the whistleblower was intimately familiar with branch operations and local dynamics. This contrasts with the predominantly formal Bahasa Indonesia typically used in official corporate communications. The investigation thus bridged digital communication methods (WhatsApp chat in local language) with other digital forensic tools (like “Get Contact” Mustika), demonstrating the need for cultural and linguistic competence in forensic auditing, especially in diverse regional contexts. The choice of Javanese in the whistleblower chat may indicate either a deliberate attempt to limit understanding to those familiar with the local context or simply the whistleblower's natural mode of communication.

The research findings have important implications for forensic auditing methodology in the digital era. First, a differential approach based on branch risk profiles is needed: reactive investigation based on digital whistleblower reports for branches with relatively good control systems (like Semarang), and proactive investigation based on anomaly analysis for branches with high autonomy and limited supervision (like Lampung). Second, the effectiveness of information technology in forensic auditing highly depends on the auditors' analytical capacity in transforming digital data into investigative evidence, even when the volume of digital evidence is limited. Third, linguistic and cultural competence must be recognized as important skills in digital forensic auditing, especially when dealing with regional branches where local languages may be used in digital communications.

CONCLUSION

This study demonstrates that the effectiveness of forensic audits in uncovering structured fraud depends on aligning investigative methodology with the nature of digital evidence and case-specific behavioral and systemic contexts, as shown in the reactive, whistleblower-driven approach in Semarang versus the proactive, data-intensive approach in Lampung. The findings emphasize that technology's true value lies in its integration with traditional auditing principles and an understanding of fraud motivators, where investigation success hinges on auditors' ability to synthesize digital data with behavioral insights and control weaknesses. However, the generalizability of the findings is limited to the context of an Indonesian retail company, highlighting the need for future research to validate these forensic models across sectors, develop AI-driven predictive monitoring systems, and analyze the cost-benefit of building digital forensic capacity, especially in SMEs in emerging markets.

REFERENCE

Abdelrahim, A. (2022). *The influential factors of internal audit effectiveness: A conceptual model. International Journal of Financial Studies*, 10(3). https://doi.org/10.3390/ijfs10030071

Abdul Halim. (2015). Auditing: Dasar-dasar audit laporan keuangan (Jilid 1, Edisi ke-5). UPP STIM YK

Abdul Halim. (2015). Auditing: Dasar-dasar audit laporan keuangan (Jilid 1, Edisi ke-5). UPP STIM YK

ACFE Indonesia Chapter. (2021). Survey Fraud Indonesia 2019. https://acfe-indonesia.or.id/

Adelakun, B. O., Onwubuariri, E. R., & Adeniran, G. A. (2024). Enhancing fraud detection in accounting through AI: Techniques and case studies. Finance & Accounting Research Journal, 6(6), 978–999. https://doi.org/10.51594/farj.v6i6.1232

Agoes, S. (2017). Auditing: Petunjuk praktis pemeriksaan akuntan oleh akuntan publik (Edisi ke-2). Salemba Empat.

Aini, Norine & Fitriana, Nova & Yuliani, Rizka & Rahayu, Hastanti. (2025). The Use of Digital Forensic Accounting Techniques in Occupational Fraud Detection and Prevention: A Literatur Review. Ilmu Ekonomi Manajemen dan Akuntansi. 6. 325-336. 10.37012/ileka.v6i2.3062.

Akinbowale, Oluwatoyin & Klingelhöfer, Heinz & Zerihun, Mulatu. (2020). An innovative approach in combating economic crime using forensic accounting techniques. Journal of Financial Crime. 27. 1253-1271. 10.1108/JFC-04-2020-0053.

Alao, A. A. (2016). Forensic auditing and financial fraud in Nigerian deposit money banks. European Journal of Accounting, Auditing, and Finance Research, 4(8), 1–12.

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

Al Najjar, M., Ghanem, M. G., Mahboub, R., & Nakhal, B. (2024). The role of artificial intelligence in eliminating accounting errors. Journal of Risk and Financial Management, 17(8). https://doi.org/10.3390/jrfm17080353

Amrizal, S. K. (2013). Audit forensik: Penggunaan dan kompetensi auditor dalam pemberantasan tindak pidana korupsi. Graha Ilmu.

Andi Septiani Ewiantika Hasbi. (2019). Pengaruh audit forensik, audit investigatif, dan professional judgement terhadap pengungkapan fraud dengan kecerdasan spiritual sebagai variabel moderating. UIN Alauddin Makassar.

Anh, N. T. M., Hoa, L. T. K., Thao, L. P., Nhi, D. A., Long, N. T., Truc, N. T., & Ngoc Xuan, V. (2024). The effect of technology readiness on adopting artificial intelligence in accounting and auditing in Vietnam. Journal of Risk and Financial Management, 17(1).

Anggraini, Dewi & Triharyati, Eri & Novita, Helen. (2019). Akuntansi Forensik dan Audit Investigatif dalam Pengungkapan Fraud. Journal of Economic, Bussines and Accounting (COSTING). 2. 372-380. 10.31539/costing.v2i2.708.

Arens, A. A., Elder, R. J., & Beasley, M. S. (2015). Auditing and assurance services: An integrated approach (15th ed.). Erlangga.

Atrisia, I. M., & Urumsah, D. (2018). The comprehensive model of whistle-blowing forensic audit, audit investigation, and fraud detection. Journal of Accounting and Strategic Finance, 1(2).

Awosika, T., Shukla, R. M., & Pranggono, B. (2024). Transparency and privacy: The role of explainable AI and federated learning in financial fraud detection. IEEE Access, 12, 64551–64560.

Bakri, A. A., Yusni, & Botutihe, N. (2023). Analisis efektivitas penggunaan teknologi big data dalam proses audit: Studi kasus pada kantor akuntan publik di Indonesia. https://www.researchgate.net/publication/374407772

Balios, D., Kotsilaras, P., Eriotis, N., & Vasiliou, D. (2020). Big data, data analytics and external auditing. https://davidpublisher.com/Public/uploads/Contribute/5ed99f943e596.pdf

Bani Ahmad, A. Y. A. (2024). Ethical implications of artificial intelligence in accounting: A framework for responsible AI adoption in multinational corporations in Jordan. International Journal of Data and Network Science, 8(1), 401–414. https://doi.org/10.5267/j.ijdns.2023.9.014

Bartstra, D. (2021). Artificial intelligence adoption in assurance of a Big Four firm. International Journal of Accounting Information Systems.

Cao, S. S., Jiang, W., Lei, L., & Zhou, Q. (2024). Applied AI for finance and accounting: Alternative data and opportunities. Pacific-Basin Finance Journal, 84, 102307. https://doi.org/10.1016/j.pacfin.2024.102307

Crowe Horwath. (2011). Why the fraud triangle is inadequate. Crowe LLP.

Deloitte. (2024). Auditing in the AI era: Striking a balance between obsolescence and reinvention. https://www.deloitte.com/middle-east/en/our-thinking/mepov-magazine/sustainable-strategies/auditing-in-the-ai-era.html

Denyer, D., & Tranfield, D. (2009). Producing a systematic review. In The SAGE Handbook of Organizational Research Methods (pp. 671–689). SAGE.

Enofe, O., Oarhe, O., & Izevbekhai, M. (2016). Forensic audit and corporate fraud. HARD International Journal of Economics and Business Management, 1(2), 55–65.

Gopalan, P., Ravikumar, A., Sharma, R., & Meesaala, K. M. (2021). Auditors' perception on the impact of artificial intelligence on professional skepticism and judgment in Oman. https://www.researchgate.net/publication/356171147

Handoko, B. L., Rosita, A., Ayuanda, N., & Budiarto, A. Y. (2022). The impact of big data analytics and forensic audit in fraud detection. https://www.wcse.org/index.php?a=show&c=index&catid=24&id=1038

Ilham Ramadhan Ersyafdi. (2018). Pengaruh profesionalisme, kompetensi dan dukungan organisasi terhadap kinerja akuntan forensik. Jurnal Akuntansi dan Keuangan, 7(2), 185–195.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics, 3(4), 305–360.

Junaidah, F. (2017). Analisis pengendalian intern atas prosedur penerimaan dan pengeluaran kas kecil pada PT Bejana Teknik Jaya. Politeknik Negeri Sriwijaya.

Mahmoud Abufarwah. (2025) Functional equivalence of digital and written evidence: Aligning legal theory and judicial practice in the Saudi legal model. The International Journal of Evidence & Proof.

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). Qualitative data analysis: A methods sourcebook (3rd ed.). SAGE.

Moleong, L. J. (2014). Metodologi penelitian kualitatif. Remaja Rosdakarya.

Mulyadi. (2016). Sistem informasi akuntansi. Salemba Empat.

Ogutu, G. O., & Solomon, N. (2016). Application of forensic auditing skills in fraud mitigation: A survey of accounting firms in the County Government of Nakuru, Kenya. Journal of Business and Management, 18(4), 77–85.

Oyedokun, G. E. (2015). Approach to forensic accounting and forensic audit.

Pasal 1 angka 8 Peraturan BPK RI Nomor 1 Tahun 2017 tentang Standar Pemeriksaan Keuangan Negara.

Pasal 6 ayat (1) Undang-Undang Republik Indonesia Nomor 15 Tahun 2006 tentang BPK.

Pasal 9 ayat (1) Undang-Undang Republik Indonesia Nomor 15 Tahun 2006 tentang BPK.

Pratama, M. N. S., Nahong, M. S., Nggi, S. A., Surileki, A. R., & Bhebhe, M. C. (2023). Pengaruh kecerdasan buatan dalam proses audit keuangan: Tantangan dan peluang di era digital.

Putri, D. A., Nizarudin, A., & Julia. (2024). Peran big data analytics dan kualitas audit dalam memperkuat kemampuan auditor mendeteksi kecurangan laporan keuangan.

Rahmadhani, S., Lim, J., & Santikawati. (2023). Analisis praktik audit dalam lingkungan big data di Indonesia. https://www.researchgate.net/publication/371362194

Reading, M., & Dimitropoulos, G. (2025). Forensic accounting as an investigative tool: insights from the FTX and Qatargate. Journal of Economic Criminology, 7, Article 100132. https://doi.org/10.1016/j.jeconc.2025.100132

Rumahorbo, H. H., & Dewayanto, T. (2023). Pengaruh transformasi digital: Kecerdasan buatan dan IoT terhadap peran dan praktik audit internal. https://ejournal3.undip.ac.id/index.php/accounting/article/view/41587

Saragih, A. D., & Dewayanto, T. (2023). Dampak teknologi big data analytics dalam mendeteksi fraud pada bidang audit. https://ejournal3.undip.ac.id/index.php/accounting/article/view/40176

Sgantzos, K., Hemairy, M. A., & Tzavaras, P. (2023). Triple-entry accounting as a means of auditing large language models. https://www.mdpi.com/1911-8074/16/9/383

Sugiyono. (2019). Metode penelitian kuantitatif, kualitatif, dan R&D. Alfabeta.

Syahputra, B. E., & Afnan, A. (2020). Pendeteksian fraud: Peran big data dan audit forensik.

Syahronny, M. R., & Dewayanto, T. (2024). Penerapan teknologi artificial intelligence dan blockchain dalam mendeteksi fraud pada proses audit.