Vol. 5 No. 1 (2026)
e-ISSN: 2963-7589
Economic and Business Journal | ECBIS
https://ecbis.net/index.php/go/index

EVALUATION OF THE EFFECTIVENESS OF INVESTIGATIVE AUDIT AND DIGITAL FORENSICS: UNCOVERING THE MODUS OPERANDI OF FINANCIAL FRAUD IN PUBLIC SECTOR FINANCIAL INSTITUTIONS

Masnawaty Sangkala

Accounting, Faculty of Economics and Business, Universitas Negeri Makassar, Indonesia
E-mail: masnawaty.s@unm.ac.id

Submitted:	Revised:	Accepted:
29 September 2026	27 October 2026	05 November 2026

Abstract

Digitization of transactions increases the complexity of financial fraud investigations in financial institutions owned, managed, or carrying out public sector mandates. This study evaluates the effectiveness of investigative audits and digital forensics in uncovering fraud modus operandi, as well as identifying the prerequisites for the integration of the two. The study uses a qualitative approach in the form of a structured narrative literature review and document analysis, with the conceptual locus of public sector financial institutions in Indonesia. The study materials include scientific articles published in 2022–2026 as well as official documents from BPK, OJK, NIST, IIA, ACFE, and GAO. The synthesis findings show that investigative audits play a role in reconstructing fund flows, authorization irregularities, related party relationships, and losses, while digital forensics helps examine log trails, metadata, communications, and integrity of electronic evidence. Traceable modes include fictitious transactions, document manipulation, misuse of access, repeated payments, and procurement collusion, but the available evidence does not allow calculation of the combined success rate of the two approaches. Evaluative effectiveness depends on data quality, evidence traceability, examiner independence, multidisciplinary competence, and institutional follow-up. This study offers a matrix of effectiveness indicators and investigative integration flows that can be used as the basis for subsequent empirical evaluations.

Keywords: *Investigative Audit, Digital Forensics, Financial Fraud, Public Financial Institutions, Integrity of Evidence*

1. INTRODUCTION

Financial accountability is a key prerequisite for institutions that manage public funds to maintain public legitimacy and trust. Fraud in this environment not only reduces the efficiency of resource use, but can also disrupt financial services, customer protection, and development functions. The report of the Association of Certified Fraud Examiners (2024) shows that reporting or tips are a prominent detection mechanism in cases of organizational fraud, while the study by Maharani and Utomo (2026) links weak internal control to the risk of public sector fraud. Therefore, the ability to detect transaction patterns while building traceable evidence is a fundamental need for public financial governance.

Technological changes have expanded transaction channels and accelerated the movement of funds, so that paper-based audits are no longer adequate. Electronic records are scattered across payment systems, accounting applications, emails, work devices, and storage services that can be managed by different managers. Susanto et al. (2022) describe the shift in forensic accounting towards the integration of big data and artificial intelligence, while Fernanda and Habiburrochman (2025) identify anomaly analysis, text, and relational network applications as directions for strengthening forensic audits. These advances provide broader investigative opportunities, but also demand stricter digital evidence governance and access control.

Investigative audits have a special function to delve into indications of irregularities and establish a sequence of events that can be accounted for. The approach departs from allegations or risk signals and then examines documents, confirmations of related parties, and the economic relationship behind a transaction. The Institute of Internal Auditors (2024b) guidelines place fraud risk assessment in organizational governance and risk management, while the report of the Audit Board of the Republic of Indonesia (2024) shows the role of investigative audits and the calculation of state losses in supporting the handling of alleged criminal acts. Thus, investigative audits need to be understood as an evidence-based audit process that is different from the routine assessment of the fairness of financial statements.

Digital forensics complements investigative examinations with techniques for identifying, obtaining, preserving, examining, and interpreting electronic evidence. Log traces can show the timing of data changes, accounts used, and a series of activities that are not always visible in the final report. NIST through Guttman et al. (2022) affirms the specific challenges in the preservation of digital evidence, while Fernanda and Habiburrochman (2025) emphasize the importance of audit trails and clarity of the analytical process. The evidentiary value of electronic evidence is therefore determined not only by its ability to display anomalies, but also by its integrity and documentation of origin.

Fraud in the public financial sector can involve a single actor or a network of internal and external parties. Irregularities can potentially be in the form of transfer of funds, fictitious bills or payments, approval engineering, manipulation of recipient data, and conflicts of interest with partners. The Association of Certified Fraud Examiners (2024) shows a high proportion of corruption cases in the sample of government organizations it researches, while the U.S. Government Accountability Office (2025) documents how organized groups leverage program and technology knowledge to exploit public systems. These two sources cannot be directly equated with the prevalence in Indonesian public financial institutions, but provide a risk typology that is useful for the preparation of investigative procedures.

In Indonesia, strengthening the anti-fraud framework is becoming increasingly relevant along with the expansion of technology-based financial services. The Financial

Services Authority established POJK Number 12 of 2024 regarding the implementation of anti-fraud strategies in financial services institutions, including the pillars of investigation, reporting, and sanctions (OJK, 2024). At the same time, The Institute of Internal Auditors (2024a) emphasizes independence, objectivity, competence, and communication of results and follow-up as elements of internal audit standards. Both frameworks provide an institutional basis for assessing whether investigations result in system improvements, not just individual case findings.

One of the obstacles to investigations is the gap between accounting information that indicates irregularities and technical data that can explain how irregularities were committed. Proof of payment can lead to suspicious transactions, but determining who changed the account number or approved the payment requires tracing of access rights and system activity. Guttman et al. (2022) explain the need to maintain the quality of digital evidence during storage, while Susanto et al. (2022) highlight the need for organizational competence and ethical governance to support technology-based forensics. Without the integration of the two, investigations risk identifying financial consequences without being able to fully explain the mechanism of action.

Previous research provides conceptual support on the benefits of technology in fraud detection, but the measurements are still mixed. Maharani and Utomo (2026) synthesize research on technology, driving factors, and prevention of public sector fraud, while Fernanda and Habiburrochman (2025) focus on the application of AI in cross-context forensic audits. Suryani and Syahrudin (2025) identify the limitations of studies that specifically discuss investigative audit practices compared to fraud detection in general. These differences in focus show an opportunity to link the technical outputs of investigations with measures of effectiveness that can be tested in public financial institutions.

The effectiveness of an audit is not sufficiently assessed by the number of transactions declared anomalous or the magnitude of the initial alleged loss. Investigation results need to be evaluated through the accuracy of mode identification, the strength of evidence support, the clarity of perpetrators and fund flows, and the impact of recommendations on recurrence prevention. The Institute of Internal Auditors guidelines (2024a) link audit quality to the implementation of assignments and monitoring of corrective actions, while the U.S. Government Accountability Office (2026) emphasizes the use of analytics, transparency, and fraud risk assessment in public programs. With this perspective, effectiveness measurement needs to include technical, procedural, and institutional aspects in an integrated manner.

Based on this description, there is still a need for an evaluation framework that links investigative and digital forensic audits in a more operational manner in an effort to uncover the mode of financial fraud. This study takes public sector financial institutions in Indonesia as a conceptual locus, without claiming to conduct an audit of specific entities or cases. The

main focus is directed at the functions of both approaches, the variety of modes that can be traced, and indicators that can be used to evaluate their effectiveness. Thus, this article seeks to formulate a synthesis that can be the basis for field testing and improvement of investigative practices.

2. LITERATURE REVIEW

Financial Fraud and Modus Operandi in the Public Sector

Financial fraud encompasses deliberate acts of obtaining unauthorized benefits through abuse of authority, assets, procedures, or information. In financial institutions that manage public funds, the consequences do not stop at potential monetary losses, but extend to accountability, affordability of services, and trust in the institution. The Association of Certified Fraud Examiners (2024) groups various patterns of employment fraud, while the U.S. Government Accountability Office (2025) documents the risks of organized crime on public programs. Both sources point to the importance of checks that are able to reconstruct actions, perpetrators, and benefit streams, rather than simply identifying irregularities in the number of transactions.

Modus operandi is examined as a series of actions that allow irregularities, ranging from transaction formation, change of authorization, manipulation of evidence, to disguise of beneficiaries. In the digital context, one mode can cross accounting applications, payment systems, vendor management, and internal communication. Relevant analytical categories include fictitious payments, transaction breakdown to avoid approval thresholds, supplier account changes, duplicate bills, and misuse of user identities. This category is a potential mechanism based on the literature and governance practices, rather than a list of proven cases in one particular institution (Suryani & Syahrudin, 2025; Financial Services Authority, 2024).

Investigative Audit: Transaction Reconstruction and Evidentiary Reasoning

Investigative audits differ from routine audits of financial statements in that they are directed at specific allegations and the preparation of a chronology of events that can be retested. Auditors need to assess the origin of information, develop a hypothesis of deviation, trace transaction flows, confirm documents with independent parties, and test alternative explanations. The Institute of Internal Auditors (2024b) places the handling of fraud risks as a shared responsibility, while its professional standards emphasize objectivity, competence, adequacy of evidence, and follow-up on results (The Institute of Internal Auditors, 2024a). Thus, the success of an investigation should not be equated with the number of anomalies detected.

Suryani and Syahrudin (2025) map investigative audit research through systematic and bibliometric reviews, and show the gap between the study of initial indicators of fraud and the implementation of specific investigative audits. This study strengthens the reasons for examining separately the stages of risk identification, transaction tracing, evidence testing, and presentation of findings. Conceptually, the quality of the investigation depends on the ability to connect who approves, when changes are made, which documents are the basis for, and where the financial benefits ultimately flow.

Digital Forensics: Acquisition, Integrity, and Interpretation of Electronic Evidence

Digital forensics focuses on the handling of electronic evidence through documented identification, preservation, acquisition, examination, analysis, and reporting procedures. The value of evidence is determined not only by the contents of the file, but also by its origin, integrity, timing, and handling history. Guttman et al. (2022) describe the typical preservation considerations in digital media and objects, including the need for copy safeguarding as well as long-term management. In financial investigations, potential evidence can be access logs, records of master data changes, document metadata, authorization records, official emails, and payment traces obtained through lawful procedures.

Electronic traces need to be read alongside business documents because logs showing account activity do not in themselves prove the identity of the person operating the account. Differences in server time, shared account usage, short log retention, and data changes after an incident can weaken inference. Therefore, quality control needs to include retrieval documentation, hash verification when relevant, access restriction, securing working copies, and chain of custody records. The role of digital forensics does not replace investigative audits, but rather provides additional evidence to verify or refute financial reconstruction (Guttman et al., 2022; Susanto et al., 2022).

Auditor Competencies, Fraud Analytics, and Technology Integration

Susanto et al. (2022) examined 150 BPK investigative auditors and reported that auditor competence and digital forensic support were positively and significantly related to the quality of investigative audits. This finding is important because it empirically proves, in the context of the Indonesian audit institutions studied, that technology needs to be present with the capabilities of auditors. However, the survey did not directly measure the level of loss recovery or the ability to prove each mode in all public financial institutions. Therefore, the results support the relevance of integration, not provide a success rate for this study model.

Fernanda and Habiburrochman (2025) through a systematic review examined the potential of artificial intelligence for forensic audits, including in anomaly screening, text processing, and linkage patterns. Maharani and Utomo (2026) combine the dimensions of technology, driving factors, and prevention of public sector fraud; their review emphasizes that technology must still be accompanied by internal controls and good governance. This combination leads to the need for a work model that maintains a separation between automated risk signals, professional examinations, and legitimate proof. Algorithmic alarms should be understood as priority indicators, not final proof of error.

Anti-Fraud Governance and Characteristics of Public Sector Financial Institutions

In financial services institutions in Indonesia, Financial Services Authority Regulation Number 12 of 2024 frames an anti-fraud strategy through four pillars, namely prevention; detection; investigation, reporting, and sanctions; and monitoring, evaluation, and follow-up. These pillars show that case proof must be related to process improvement and supervision after investigation. At the level of internal audit practice, the Global Internal Audit Standards link the quality of work with independence, competence, risk-based planning, communication, and monitoring of action plans (The Institute of Internal Auditors, 2024a). The relevance of regulations for each entity must still be determined according to its legal status and scope of supervision.

The U.S. Government Accountability Office (2026) emphasizes that programs with inter-agency funding flows and the involvement of recipients and service providers can face various vulnerabilities. Therefore, fraud disclosure in institutions that carry out public mandates also requires clarity on information access rights, interfunctional coordination, reporting mechanisms, and follow-up responsibilities. A good digital investigative and forensic audit model needs to be compatible with organizational control and applicable authority restrictions.

Synthesis of Previous Research and Research Gap

The literature reviewed shows three groups of knowledge that are not yet fully connected. First, investigative research highlights auditor quality and red flag identification, but often has not independently assessed the continuity of evidence from transactions to system logs (Susanto et al., 2022; Suryani & Syahrudin, 2025). Second, technology studies highlight analytical, AI, and digitalization capabilities, but the measure of success can stop at the speed of detection or the ability

to find patterns, rather than the quality of proof and case control after an audit (Fernanda & Habiburrochman, 2025; Maharani & Utomo, 2026). Third, professional and regulatory standards establish responsibilities and processes, but do not directly provide a universal empirical index of the effectiveness of integrating investigative and digital forensic audits (The Institute of Internal Auditors, 2024a; Financial Services Authority, 2024).

The gap that this article aims at is not the absence of all studies on digital forensics or investigative audits, but rather the limitation of integration between detection quality, evidence strength, reconstruction mode, institutional capability, and follow-up in one evaluation design. Widodo et al. (2026) also show that public sector accounting fraud research still has areas that need development. Therefore, the contribution of this article is in the form of a proposal for an indicator framework that is transparent and can be tested through case studies or evaluations of several entities, not claims that the causal effectiveness of both approaches has been proven in a specific sample of institutions.

Conceptual Framework for Effectiveness Evaluation

Based on the above synthesis, the effectiveness of integration is understood as the quality of the process and the results of disclosure that allow the alleged mode to be examined in a responsible manner. The proposed relationship starts from the indication of fraud risk, followed by the determination of the scope of investigation and early preservation of digital evidence, then cross-testing of transactions and electronic traces, before reporting and follow-up of recommendations. Auditor competence, data integrity, access governance, and auditor independence are positioned as cross-stage prerequisites. The output measure includes the accuracy of reconstruction and completeness of evidence, while institutional results are assessed through the implementation of recommendations and the reduction of the repetition of the mode in the next observation.

This conceptual framework is evaluative and has not been tested using primary data. Inter-dimensional relationships are not presented as statistical influences; each indicator needs to be translated into operational definitions, measurement scales, sources of evidence, and quality assurance procedures before being used in quantitative research. The emphasis on process traceability and evidence is aligned with NIST's guidance on digital evidence preservation, the IIA principles on audit quality, and the OJK anti-fraud framework (Guttman et al., 2022; The Institute of Internal Auditors, 2024a; Financial Services Authority, 2024).

Table 1. Summary of previous research and its contribution to the study framework

Source	Focus/type of evidence	Relevance and limitations
Susanto et al. (2022)	Survey of 150 BPK investigative auditors; competence and digital forensics	Empirical support of audit quality; does not measure the success of case disclosure per institution
Suryani & Syahrudin (2025)	SLR and bibliometrics of investigative / fraud audits	Demonstrate the gap between red flag identification and investigative practice
Fernanda & Habiburrochman (2025)	SLR utilization of AI for forensic audits	Explain the potential of analytics; not the evaluation of the chain of custody in public institutions
Maharani & Utomo (2026)	Scoping review 10 public sector fraud articles	Connecting technologies, drivers, and prevention; has not yet tested audit-forensic integration models

Widodo et al. (2026)	Public Sector Accounting Fraud	Showing research agendas and gaps in context; not testing instruments for integration effectiveness
Guttman et al. (2022)	NIST guidelines for the preservation of digital evidence	Standardizing evidence-keeping processes; not organizational impact studies

Source: *Proceed Data, 2026*

3. RESEARCH METHOD

This research uses a qualitative approach in the form of a structured narrative literature review and policy document analysis. The design was chosen because the purpose of the research is to evaluate the mechanisms, prerequisites, and indicators of effectiveness of investigative audits and digital forensics, not to calculate the success of cases in certain institutions. The conceptual locus of the research is financial institutions that have ownership, functions, or mandates of the public sector in Indonesia, including the relevance of financial supervision and management of public funds. The units of analysis are in the form of ideas, previous research results, professional guidelines, as well as rules and official reports, not individual respondents. The sources examined in a targeted manner include relevant scientific articles for the 2024–2026 period as well as standard sources and reports from the OJK, BPK, IIA, NIST, ACFE, and GAO. The search was conducted based on a combination of the terms investigative audit, digital forensics, forensic accounting, fraud detection, public sector, evidence integrity, and anti-fraud; The source was chosen because of the relevance of the substance and affordability of the document. Therefore, this article is not claimed to be a systematic literature review that reports on the PRISMA process or as an effectiveness evaluation based on primary data (Maharani & Utomo, 2026; Suryani & Syahrudin, 2025).

Material collection was carried out through a literature study on summaries and available sections of scientific publications, regulatory provisions, professional standards, and institutional reports that can be accessed online. The analysis instrument was in the form of a conceptual extraction matrix containing the type of source, audit focus, type of trace or evidence, suspected mode, supporting factors, obstacles, and outcome indicators. The analysis was carried out through content reduction, thematic grouping, and comparative synthesis to answer three problem formulations, with an explicit separation between evidence directly supported by the source and the indicators proposed by the author. The evaluation criteria were grouped into the accuracy of the transaction reconstruction, the scope of the digital footprint, the integrity and traceability of evidence, the speed of handling, collaboration between functions, and the quality of follow-up. The principles of electronic evidence management are referenced from Guttman et al. (2022), while the audit governance dimension uses The Institute of Internal Auditors (2024a) and the Financial Services

Authority (2024). Because there are no case files, transaction logs, investigator interviews, or confidential audit reports available, this study does not estimate the sensitivity of detection, the rate of loss recovery, or the causal impact of the application of the technology.

4. RESULTS AND DISCUSSION

Functions of Investigative Audits in Reconstruction Mode

The BPK document on the Overview of Audit Results for the First Semester of 2024 reports one investigative audit report on SOEs with an indicative value of state losses of IDR 371.83 billion. This figure is an institutional finding within the scope of BPK, not a measure of losses found by this study (BPK, 2024). The Association of Certified Fraud Examiners report (2024) identifies the categories of corruption, billing, payroll, and payment misuse in fraud cases in government organizations that are studied globally. Both sources show the variety of information needed in an investigative audit, namely the chronology of authorizations, supporting documents, beneficiaries, and fund transfers.

The Function of Digital Forensics in Electronic Fingerprint Disclosure

NIST documented specific considerations in the preservation of digital evidence, including the need to maintain the integrity and context of evidence during handling (Guttman et al., 2022). The study by Fernanda and Habiburrochman (2025) grouped the use of forensic AI in transaction anomaly detection, text analysis, and relationship network analysis. Susanto et al. (2022) found a positive relationship between digital forensic support and investigative audit quality in a survey of BPK auditors. At the document level, the three sources support a complementary function between the analysis of transaction content and the search for related metadata, logs, or communications.

Synthesis of Integration Effectiveness Indicators

The Institute of Internal Auditors standards (2024a) contain the principles of competence, professional prudence, communication of results, and follow-up monitoring. POJK Number 12 of 2024 formulates four pillars of anti-fraud strategies, namely prevention, detection, investigation/reporting/sanctions, and monitoring/evaluation/follow-up (OJK, 2024). The selected literature adds aspects of analytical quality, the ability to understand relationships, and auditable evidence (Fernanda & Habiburrochman, 2025; Maharani & Utomo, 2026). Based on the similarity of these elements, the following conceptual indicator matrix was prepared as a proposed evaluation, not as the result of instrument validation tests.

Table 2. Conceptual evaluation matrix of the effectiveness of digital investigative and forensic audits

Dimensions	Proposed indicators	Support resources
Reconstruction precision	Payment chronology, party relations, suitability of document evidence with fund flow	BPK, 2024; IIA, 2024a
Coverage of electronic evidence	Log trails, metadata, messages, change history, links between accounts	Guttman et al., 2022; Fernanda & Habiburrochman, 2025
Integrity of evidence	Acquisition logging, access control, checksum/hash, chain of custody	Guttman et al., 2022
Detection accuracy	Risk signals can be verified; the proportion of findings is true to the alerts examined	Fernanda & Habiburrochman, 2025
Follow-up	Recommendations are acted upon, control loopholes are closed, re-event monitoring	IIA, 2024a; OJK, 2024
Governance and competence	Independence, multidisciplinary proficiency, legal access, decision documentation	IIA, 2024a; Wulandari et al., 2026

Source: *Proceed Data, 2026*

Discussion

Reconstruction of Modes through Investigative Audits

The contribution of an investigative audit lies in its ability to transform irregular signals into an auditable flow of events. For example, the alleged double payment is not sufficiently ascertained from identical nominals; the auditor needs to examine contracts, invoice numbers, proof of acceptance of employment, identity of the recipient, and payment authorization. In cases involving collusion, relationships between employees, vendors, and account owners can be key components of evidence. This pattern is in line with The Institute of Internal Auditors' (2024b) emphasis on fraud risk assessment and with the Association of Certified Fraud Examiners' (2024) exposure to the diversity of government fraud schemes. The use of the term modus operandi in this article refers to potential categories and mechanisms based on documents, rather than the findings of real cases proven by the authors.

Institutionally, investigative audits also have consequences for the clarity of reporting channels and coordination between auditors, compliance, risk management, and authorities. The report of the Audit Board of the Republic of Indonesia (2024) shows that there are investigative audit outputs and state loss calculations used for the case handling process. However, these administrative outputs do not automatically prove that all indications end up being criminal judgments or asset recovery. Therefore, effectiveness evaluation needs to distinguish between indication identification, finding confirmation, legal process, and recovery, each with an appropriate size and denominator.

Digital Forensics as an Evidentiary Amplifier

Digital forensics deepens evidence by associating accounting events with events on the information system. Vendor master change records can shed light on when account details were changed, whose account made the change, and whether the change occurred in close proximity to the execution of the payment. This relationship requires cross-testing with independent evidence because one system account can be shared together, logs can be incomplete, and server hours can be out of sync. Guttman et al. (2022) emphasize the importance of preserving evidence; therefore acquisition logging, hashing, access restrictions, and chain of custody should be treated as core parts of the quality of proof, not technical attachments.

The use of analytical and AI models can speed up data screening and help prioritize risky cases, but automatic alerts are not final evidence. Fernanda and Habiburrochman (2025) highlight transaction, text, and network analytics, while Susanto et al. (2022) point out the importance of technical support and auditor competence to the quality of investigations. Models that produce a lot of false positives can burden the investigation team; conversely, models that do not detect new schemes can build a false sense of security. Therefore, effectiveness needs to be assessed through the quality of human verification, the clarity of alarm reasons, and the suitability of data acquisition and processing with legal and privacy authorities.

Integration and Effectiveness Framework

The proposed integration starts from the receipt of indications and risk assessments, followed by the early preservation of digital evidence, traceability of transactions and party relationships, cross-testing of electronic and physical evidence, formulation of findings, and recommendations and monitoring. This sequence prevents the possibility of data changing before the examiner obtains evidence, while maintaining a focus on audit questions. POJK Number 12 of 2024 and the Global Internal Audit Standards provide the basis for the detection mechanism not to stop at the report of findings, but to be connected to the improvement of control and follow-up (OJK, 2024; IIA, 2024a). This integration is an analytical design, not a protocol that has been tested in a particular institution.

Effectiveness needs to be distinguished from efficiency. A rapid investigation is not necessarily effective if it misattributes the perpetrator, while an investigation with complete

evidence does not automatically reduce the next fraud without a change in control. A multi-level evaluation can use output measures (cases examined, documents verified), quality measures (completeness of evidence and false positives), intermediate outcomes (recommendations implemented), and long-term outcomes (recurrence of modes and loss recovery). The documentary evidence in this article supports the need for these dimensions, but they are not sufficient to provide quantitative weight or a specific threshold of success (GAO, 2026; Maharani & Utomo, 2026).

Implications and Limitations

For financial institutions that carry out public sector mandates, the main implication of the study is the need for cooperation in audit functions, information technology, law, risk, and compliance in dealing with suspected fraud. Log retention policies, auditor access, investigation technique training, and follow-up monitoring systems are practical prerequisites that can be evaluated periodically. However, not all public entities are subject to the same OJK regulatory regime; the implementation of POJK 12/2024 needs to be ensured based on institutional status and regulatory coverage. This study also does not include primary case measurement, auditor interviews, forensic device testing, or statistical validation of indicators, so the generalization of effectiveness must be limited.

4. CONCLUSION

The document synthesis shows that investigative audits help explain the chronology of transactions, deviations of authority, party relations, and possible losses, while digital forensics functions to uncover electronic traces and strengthen evidence traceability. The two complement each other in describing potential modes such as fictitious transactions, changes in account data, misuse of access, and payment collusion. The effectiveness of integration cannot be determined as a percentage of success from the literature reviewed, but rather needs to be tested through the accuracy of reconstruction, data coverage, integrity of evidence, quality of verification, competence, and follow-up. The contribution of this article is a conceptual evaluation framework that links the technical outputs of the audit with the quality of proof and governance improvement.

REFERENCES

Association of Certified Fraud Examiners. (2024). Occupational fraud 2024: A report to the nations. https://www.acfe.com/fraud-resources/report-to-the-nations-archive

Audit Board of the Republic of Indonesia. (2024). Overview of the results of the audit for the first semester of 2024. https://jateng.bpk.go.id/wp-content/uploads/2024/10/CompressedIHPS-I-2024_compressed.pdf

Fernanda, I. A., & Habiburrochman, H. (2025). The role of artificial intelligence (AI) in improving forensic audits to detect fraud: A systematic literature review. Owner: Research and Journal of Accounting, 9(4), 3430–3442. https://doi.org/10.33395/owner.v9i4.2825

Guttman, B., White, D. R., Williams, S., & Walraven, T. (2022). Digital evidence preservation: Considerations for evidence handlers (NISTIR 8387). National Institute of Standards and Technology. https://www.nist.gov/publications/digital-evidence-preservation-considerations-evidence-handlers

Maharani, M., & Utomo, D. C. (2026). Technology, drivers, and fraud prevention in the public sector: A scoping review. MAXIMUM: Media Accounting University of Muhammadiyah Semarang, 16(1), 1–13. https://jurnal.unimus.ac.id/index.php/MAX/article/view/16944

Financial Services Authority. (2024). Financial Services Authority Regulation Number 12 of 2024 concerning the implementation of anti-fraud strategies for financial services institutions. https://ojk.go.id/en/regulasi/Pages/12-Tahun-2024-Penerapan-Strategi-Anti-Fraud-bagi-Lembaga-Jasa-Keuangan.aspx

Suryani, I., & Syahrudin, M. (2025). Investigative auditing and fraud: A systematic literature review through a theoretical and bibliometric lens. Asia Pacific Fraud Journal, 10(1), 139–151. https://doi.org/10.21532/apfjournal.v10i1.400

Susanto, H., Mulyani, S., Sukmadilaga, C., & Ghani, E. K. (2022). Sustaining investigative audit quality through auditor competency and digital forensic support: A consensus study. Sustainability, 14(22), 15141. https://doi.org/10.3390/su142215141

The Institute of Internal Auditors. (2024a). Global internal audit standards. https://www.theiia.org/en/content/standards/complete-global-internal-audit-standards/

The Institute of Internal Auditors. (2024b). Internal auditing and fraud (3rd ed.). https://www.theiia.org/en/content/guidance/recommended/supplemental/practice-guides/global-practice-guide-internal-auditing-and-fraud/

U.S. Government Accountability Office. (2025). Fraud risk in federal programs: Continuing threat from organized groups since COVID-19 (GAO-25-107508). https://www.gao.gov/products/gao-25-107508

U.S. Government Accountability Office. (2026). Combating fraud: Managing risks in federally funded, state-administered programs (GAO-26-109100). https://www.gao.gov/products/gao-26-109100

Widodo, S., Handono, W. D., & Purnama, H. (2026). Public sector accounting fraud: What do we know, what is missing, and where to go next? A systematic review. MUQADDIMAH: Journal of Economics, Management, Accounting and Business, 4(2), 291–307. https://doi.org/10.59246/muqaddimah.v4i2.1947