

STRENGTHENING PUBLIC TRUST THROUGH DIGITAL FORENSIC AUDIT: A STUDY OF EMERGING PUBLIC SECTOR ACCOUNTABILITY

Adonia Anita Batkunde*¹

Jurusan Akuntansi, Universitas Pattimura, Indonesia
Email: mejiagayofa02@gmail.com

Theresia Febiengry Sitanala

Jurusan Akuntansi, Universitas Pattimura, Indonesia
Email: theresiasitanala1011@gmail.com

Abstract

This study aims to examine the role of digital forensic audits in strengthening public trust by improving public sector accountability. In the digital era, various public financial management and administration practices are increasingly vulnerable to potential misuse, data manipulation, and fraud that are difficult to detect using traditional audit methods. The advent of digital forensic audits offers a technology-based approach that enables more effective, transparent, and accurate fraud detection, investigation, and prevention. This study employed a literature review method, examining various academic sources, regulations, and best practices across relevant jurisdictions. The results indicate that digital forensic audits can serve as a strategic instrument in building transparency, strengthening oversight mechanisms, and increasing the accountability of state officials in the eyes of the public. However, challenges such as limited competent human resources, uneven technological infrastructure, and a still-developing regulatory framework are major obstacles to widespread implementation. These findings emphasize the importance of strengthening the capacity of public institutions, investing in technology, and harmonizing regulations to ensure the effectiveness of digital forensic audits as a means of strengthening public trust in the public sector.

Keywords: Digital forensic audit, public sector accountability, public trust, transparency

INTRODUCTION

This research is motivated by increasing public expectations for transparency, accountability, and integrity in the increasingly complex public sector in the digital era. Rapid social, economic, and political changes have

¹ Correspondence author

made the public more critical in assessing the performance of government and public institutions. Cases of corruption, financial reporting manipulation, and abuse of authority uncovered in recent decades have led to a crisis of public trust in state institutions. This situation creates an urgent need for a stronger, more modern, and technology-based oversight system to mitigate potential irregularities and restore the government's legitimacy in the eyes of the public. Audits, as an instrument of public accountability, need to evolve with the times, functioning not only as routine audits but also as a means of building trust through deeper, data-driven transparency (Darwin, 2024a).

Amidst the rapid development of information technology, digital forensic audits have emerged as a breakthrough in modern audit practice. This technology enables auditors to trace digital footprints, analyze transaction patterns, and identify anomalies undetectable by traditional audit methods (Tariq, 2025). Digital forensic audits are not limited to post-fraud investigations but can also serve as a preventative system by increasing the effectiveness of internal oversight (Edet & Christopher, 2025a). Through the use of digital forensic technology, public auditors are able to provide a more objective, transparent, and digitally verifiable picture, thereby strengthening accountability and increasing public trust in public financial reports. This transformation is a crucial part of the modernization of public sector accounting systems, which must adapt to the digital era.

However, the implementation of digital forensic audits in the public sector is not without challenges. Unequal technological infrastructure, limited auditor competency in digital forensic techniques, and lagging regulations are real obstacles. In many developing countries, the implementation of digital-based audits is still seen as a novelty requiring significant investment, both in terms of human resources and supporting software and hardware (AL-Raggad & AL-Raggad, 2024a). Furthermore, legal and ethical aspects are also crucial factors that must be considered to ensure that forensic audit results are accepted legally and publicly. These challenges demonstrate that the implementation of digital forensic audits cannot be viewed solely as a technical aspect but must be part of a comprehensive strategy for building clean, transparent, and sustainable governance (Shakir & Abbas, 2020).

On the other hand, the opportunities offered by digital forensic audits for the public sector are enormous. With its ability to trace digital footprints in real time, this technology can help detect indications of misuse of public funds early (Sari & Muslim, 2023). Furthermore, digital forensic audits can also improve the efficiency of the audit process by leveraging big data analytics, allowing

auditors to analyze millions of transactions quickly. This not only strengthens the oversight function but also accelerates the process of making more accurate, data-driven decisions. Successful implementation of digital forensic audits has the potential to create a more accountable, efficient, and integrated bureaucratic culture, thereby directly restoring and strengthening public trust in the government sector (Omar et al., n.d.).

Against this backdrop, this study seeks to examine how digital forensic auditing can contribute to strengthening public trust by enhancing accountability in the developing public sector. This research emphasizes the analysis of literature that discusses the relevance, benefits, and challenges of implementing digital forensic technology in public sector audits. Furthermore, this research is expected to provide a comprehensive understanding of the urgency of integrating digital forensic auditing into modern public oversight systems, while also providing an academic and practical foundation for policymakers in creating a more transparent, innovative, and trustworthy governance framework. Thus, this study not only contributes to the development of scientific literature but also provides concrete recommendations for realizing a public sector capable of responding to the challenges of the times and meeting the increasingly complex demands of society.

RESEARCH METHOD

The research method used in this study is a literature review, using a descriptive-analytical approach to various academic sources and professional practices relevant to the topic of digital forensic auditing in the public sector context. This research collected, identified, and analyzed scientific articles, books, policy reports, and previous research documents that discuss the link between digital forensic auditing and improving public sector accountability. The review process was conducted by searching international and national scientific databases to identify the latest literature related to the issues of transparency, accountability, and public trust. All collected sources were then critically analyzed to identify patterns, knowledge gaps, and emerging trends in strengthening public sector governance through the implementation of digital forensic auditing.

The literature analysis phase was conducted by emphasizing the relevance and contribution of each source to understanding the relationship between digital forensic auditing and public trust. Secondary data obtained from the literature were compared and synthesized to develop a conceptual

framework that supports an understanding of how digital forensic auditing can strengthen public sector accountability and ultimately increase public trust. This approach enabled the research to produce a comprehensive theoretical mapping and provide conceptual recommendations that can be used as a foundation for developing further empirical research and policies that support more transparent and accountable public governance.

RESULT AND DISCUSSION

Digital Forensic Audit as an Instrument for Fraud Detection, Prevention, and Action in the Public Sector

The rapid development of digital technology has transformed work patterns in various fields, including public sector governance, which is required to be more transparent, accountable, and efficient (Wahyuandari, 2025). On the other hand, this development also presents new challenges in the form of an increased potential for fraudulent activities using information technology. Fraud in the public sector not only causes financial losses to the state but also undermines public trust in government institutions. In this context, digital forensic auditing emerges as a crucial instrument capable of detecting, preventing, and taking action against various forms of irregularities by utilizing sophisticated digital forensic technology. Digital forensic auditing is not simply a conventional examination technique, but rather a comprehensive approach that combines aspects of accounting, information technology, law, and investigation to uncover valid and accurate evidence.

Fraud detection in the public sector has often been hampered by data complexity, electronic document manipulation, and the limitations of traditional audit methods in tracing digital footprints (Najih, 2025). Digital forensic audits can address this challenge by providing more sophisticated electronic data analysis methods, ranging from tracing suspicious financial transactions and analyzing system logs to recovering intentionally deleted data (Kaur et al., 2023). Through specialized software and digital investigative techniques, auditors can identify unusual transaction patterns, identify perpetrators through digital footprints, and uncover the *modus operandi*. The primary advantage of digital forensic audits is their ability to provide legally admissible electronic evidence, allowing findings to be used not only in administrative contexts but also in litigation.

Beyond functioning as a detection tool, digital forensic audits also play a crucial role in fraud prevention in the public sector. This prevention is achieved through the implementation of technology-based internal control systems

equipped with real-time monitoring mechanisms (Edet & Christopher, 2025b). For example, government financial systems can be integrated with forensic audit software that automatically flags anomalous transactions, sends early warnings, and reports directly to authorities. This way, potential losses can be minimized before they reach a more detrimental stage. Furthermore, the existence of digital forensic audits encourages the development of a culture of integrity within the bureaucracy, as state officials recognize that their every action can be traced digitally and leaves an electronic trail that is difficult to erase. This preventative effect is crucial in creating a cleaner and more integrity-driven public sector environment.

The fraud-fighting function within the context of digital forensic audits is equally crucial. When fraud has already occurred, digital forensic audits provide concrete evidence that can be used in the investigation and law enforcement process. For example, digital traces in the form of system access logs, file metadata, or electronic transaction records can serve as strong evidence that clarifies the chronology of events (Gunasegaran et al., 2023). Digital evidence generated by forensic processes has advantages over physical evidence because it can reconstruct the perpetrator's actions in detail, even down to the time and device used. This not only makes it easier for law enforcement officials to prove corruption or abuse of authority but also expedites the case resolution process, thus providing a deterrent effect for other perpetrators. In other words, digital forensic audits serve as a bridge between internal audits and the broader legal process.

The implementation of digital forensic audits in the public sector is also closely linked to improving good governance. Transparency and accountability can be better maintained when audit systems utilize digital technologies that are difficult to manipulate (Oyerogba, 2021). In this context, the use of technologies such as big data analytics, artificial intelligence, and blockchain further strengthens the position of digital forensic audits as a key instrument for public financial oversight. For example, blockchain can guarantee the authenticity and integrity of transaction data, making it more difficult to falsify documents or manipulate budgets. Meanwhile, artificial intelligence can assist auditors in analyzing transaction patterns more quickly and accurately. The integration of these technologies demonstrates that digital forensic audits are not simply a response to fraud that has already occurred but also part of a long-term strategy to build a sustainable oversight system.

Despite its significant potential, implementing digital forensic audits in the public sector is not without challenges. Limited human resources with expertise

in digital forensics, high technology investment costs, and bureaucratic resistance to change are real obstacles that must be overcome. Therefore, the implementation strategy must be accompanied by increased auditor capacity through ongoing training, the development of adequate technological infrastructure, and the enforcement of regulations supporting the use of digital evidence in court. Furthermore, collaboration between auditors, IT experts, law enforcement, and regulators is key to ensuring the effectiveness of digital forensic audits. This synergy enables a more comprehensive investigation process, from evidence collection and analysis to decisive legal action.

Overall, digital forensic audits can be viewed as a strategic instrument in realizing a public sector free from fraudulent practices. Their detection, prevention, and enforcement functions complement each other to form a comprehensive oversight system. With the use of digital technology, the audit process is no longer limited to examining physical documents but can drill down to previously unattainable levels of detail. This makes digital forensic audits not merely a technical tool but also a symbol of the government's commitment to maintaining integrity, increasing transparency, and strengthening public trust. Going forward, the role of digital forensic audits will become increasingly important as the complexity of the state financial system and the sophistication of fraud methods increases. The transformation towards modern and integrity-based public sector governance will not be achieved without the presence of digital forensic instruments as a key pillar in monitoring and enforcing accountability.

The Transformation of Conventional Audits to Digital Technology-Based Audits

The development of digital technology over the past two decades has transformed various aspects of human life, including accounting and auditing (Azizi et al., 2024). Audits, previously synonymous with manual approaches based on physical documents and direct observation, are now undergoing a significant transformation toward audit models that rely on digital systems, big data, and artificial intelligence. This transformation is driven not only by advances in information technology, but also by the demands of an increasingly complex business environment, the need for transparency, and public expectations for greater accountability. The shift from conventional audits to digital technology-based audits cannot be viewed simply as a technical phenomenon, but also as a paradigm shift that has revolutionized the way

auditors work, interact with data, and present audit results to stakeholders (Amalia et al., 2025).

Conventional audits essentially focus on gathering audit evidence through sampling, examining physical documents, interviews, and direct field observation (Barr-Pulliam et al., n.d.). This process is often time-consuming, expensive, and limited in its ability to reach the entire data population. Furthermore, conventional audits are prone to delays in detecting anomalies or fraud due to their retrospective nature, which involves reviewing past transactions. This results in audit results sometimes being less relevant in the context of decision-making that demands speed. This limitation underlies the need for a transformation to digital-based audits, which can provide faster, more accurate, and more comprehensive analysis.

Digital technology-based audits are born from the use of integrated accounting information systems, big data analytics, cloud computing, blockchain, and artificial intelligence (Wijesooriya & Basnayake, 2024). This technology enables auditors to access, process, and analyze large amounts of data in real time, so that the audit process is no longer limited to samples but can encompass the entire transaction data set. With this approach, auditors act not only as evidence collectors but also as analysts capable of assessing transaction patterns, detecting anomalies early, and providing more in-depth data-driven recommendations. The auditor's role is shifting from being merely a "compliance guard" to a "strategic partner" in organizational decision-making.

One of the most crucial aspects of this transformation is the use of big data analytics in the audit process. While conventional audits can only examine a small subset of data, big data technology allows auditors to analyze an entity's entire transaction data, including relevant external data, such as market trends or consumer behavior. This type of analysis provides added value by detecting unusual patterns or fraud risks more quickly and accurately. Furthermore, the application of machine learning in audits allows the system to learn from previous transaction patterns, thus improving the accuracy of fraud detection over time (Yoon, 2020).

Digital transformation has also brought significant changes to data storage and security. Cloud computing technology, for example, allows auditors to access company data from any location without having to carry physical files or hard copy documents. This increases work efficiency and reduces the risk of document loss. Furthermore, the use of blockchain technology in auditing promises a higher level of transparency and data

integrity due to its immutable nature and verifiability by all relevant parties. With blockchain, auditors have greater confidence in the authenticity of transaction data, thereby ensuring audit quality (Lajoie & Gendron, n.d.).

However, the transformation to digital-based auditing also presents new challenges. Auditors are required to possess robust information technology competencies to operate analytical tools and understand the digital systems used. This change requires significant investment in training, capacity building, and the adoption of modern audit software. Another challenge lies in cybersecurity, where the vulnerability of digital data to hacker attacks or data leaks requires the implementation of robust protection systems. Furthermore, audit regulations and standards need to adapt to technological developments to ensure digital audit practices remain within a clear legal and ethical framework.

This transformation also impacts the auditor-client relationship. In conventional audits, face-to-face interactions, interviews, and site visits are integral parts of the process. However, in digital-based audits, these interactions are reduced as auditors rely more heavily on digital data. This raises questions about how to maintain the quality of communication, understanding the business context, and sensitivity to non-financial aspects that may not be fully captured in digital data. Auditors need to develop soft skills, such as communication, organizational understanding, and professional integrity, so that digital transformation does not diminish the humanistic values of the audit profession itself.

The transformation from conventional audits to digital technology-based audits is not simply a replacement of work tools, but also a cultural shift within the audit profession. Auditors accustomed to manual methods need to adapt to a new mindset that is more data-driven, with speed and accuracy of analysis. Professional organizations, regulators, and educational institutions play a significant role in driving this transformation by providing technology-based curricula, formulating digital audit standards, and creating a supportive regulatory ecosystem. If this transformation can be managed well, audit results in the digital era will have far greater added value, not only as a verification tool but also as a strategic instrument for improving governance, transparency, and accountability in both the public and private sectors (Udrescu, 2024).

Thus, the transformation from conventional audits to digital technology-based audits can be understood as a necessity born of the times. The audit process can no longer be carried out using slow and limited traditional methods; it must adopt technology to meet the challenges of an increasingly

dynamic and complex business environment. Challenges in the form of competence, security, and regulation do exist, but the potential benefits offered, such as efficiency, accuracy, and improved accountability, make this transformation inevitable. Audits in the digital era are not only a means of assessing the accuracy of financial reports but also a foundation for public trust in the integrity of an organization. Ultimately, the success of this transformation will be determined by the audit profession's ability to maintain a balance between technology and the fundamental values of the profession.

Challenges of Implementing Digital Forensic Audits in the Public Sector, Including Limited Human Resources, Regulations, and Infrastructure

The increasingly rapid development of digital technology has encouraged the public sector to adopt new approaches to governance, accountability, and transparency. One important innovation in state financial oversight and auditing is the implementation of digital forensic audits. Digital-based forensic audits are considered a strategic instrument for detecting, preventing, and prosecuting fraud, corruption, and abuse of authority within the government bureaucracy (Elumilade et al., 2021). However, despite its increasing urgency, the implementation of digital forensic audits in the public sector faces a variety of complex challenges. These challenges stem from limited human resources, regulatory gaps or weaknesses, and limited supporting infrastructure that is not yet fully ready to support the successful digital transformation of audits.

Human resources are a major obstacle to the implementation of digital forensic audits in the public sector. Essentially, digital forensic audits require auditors with multiple skills, including understanding accounting, forensic investigation, and technical skills in information technology (lipumbu et al., 2023). Required competencies include data analysis skills, mastery of forensic software, and the ability to interpret complex digital evidence. Unfortunately, in many public sector institutions, the availability of qualified human resources with these cross-disciplinary competencies remains very limited. Conventional auditors are generally trained only to conduct document-based audits or traditional financial reports, while the demands of the digital era require them to be able to trace digital traces hidden in information systems, network devices, and large databases. This limitation results in a significant competency gap between technological demands and the actual capacity of auditors in the public sector. Furthermore, the need for ongoing training and international certification in digital forensics has not been prioritized in many government

institutions, slowing the adaptation of human resources to the changing audit paradigm (J. Henriques et al., 2024).

In addition to limited human resources, regulations are also a determining factor that still poses significant challenges to the implementation of digital forensic auditing in the public sector. Legislation governing forensic auditing, particularly digital-based auditing, remains minimal and has not been well integrated into the applicable legal system. For example, regulations regarding the validity of digital evidence in court, standard procedures for handling forensic data, and governance of the use of forensic audit software often lack a clear and firm legal framework. Consequently, even if auditors successfully discover evidence of digital-based fraud, its legal validity is often questioned and vulnerable to counter-suits by the parties being audited. Furthermore, several regulations regarding data and privacy actually limit auditors' ability to access necessary data, creating a dilemma between investigative interests and protecting the rights of individuals or institutions. This situation demonstrates that although digital forensic auditing has significant potential to increase public accountability, regulatory ambiguity actually hinders its optimal implementation in the field (Otia & Bracci, n.d.).

Infrastructure limitations are also crucial in influencing the effectiveness of digital forensic audits in the public sector. The information technology infrastructure of government institutions across regions remains uneven. Institutions located in urban centers may have access to adequate hardware, software, and networks, but in areas with limited resources, the infrastructure capacity to support digital forensic audits is far from ideal (Otia & Bracci, n.d.). The lack of high-capacity servers, poor internet network quality, and limited availability of cybersecurity systems make digital audit processes less effective and vulnerable to disruption. Furthermore, internationally licensed forensic audit software is very expensive, making it difficult for all public sector institutions to invest. As a result, a technological gap exists between institutions, ultimately impacting the unequal quality of digital forensic audits across the public sector as a whole.

Furthermore, organizational culture within public sector bureaucracies also exacerbates the challenges of implementing digital forensic audits. The adoption of digital technology in forensic audits is often perceived as a threat by some, particularly individuals or groups who believe its presence could reduce the scope for fraudulent practices. As a result, resistance to digital forensic audit innovation often emerges, either in the form of implicit rejection, delays in budget allocation, or minimal support from agency leaders. A work

culture still tied to conventional patterns also makes auditors reluctant to update work methods, as change is perceived as an additional burden requiring significant adaptation (Illési, 2025). In this context, the challenges are not only technical but also psychological and sociological, requiring a managerial approach to create a supportive environment for digital-based audit implementation.

Furthermore, challenges also arise in terms of system integration between institutions. The public sector consists of various ministries, agencies, and local governments, each with its own distinct information systems. The lack of standardization in public data management makes digital forensic audits difficult to conduct across institutions. Furthermore, fraud and deception cases in the public sector often involve more than one institution, necessitating strong system interoperability to ensure smooth investigations. Without proper integration, digital forensic audits risk fragmentation, with auditors only able to access specific pieces of data without being able to see the entire pattern of the crime. This not only slows investigations but also weakens the effectiveness of fraud prevention, which should be the primary goal of implementing digital-based audits (J. P. M. Henriques, 2024).

Overall, the challenges of implementing digital forensic audits in the public sector are multidimensional and interrelated. Limited human resources create competency gaps that slow technology adoption, regulatory weaknesses create legal uncertainty in the use of digital evidence, while infrastructure limitations create technical barriers that disrupt smooth investigations. These three aspects are exacerbated by organizational cultural resistance and weak system integration between institutions, preventing digital forensic audits from reaching their full potential. Therefore, efforts to implement digital forensic audits in the public sector must be viewed not only from a technological perspective but also require a comprehensive approach that includes strengthening human resource capacity, regulatory reform, equitable infrastructure development, and changing organizational culture toward more transparent, accountable, and responsive work patterns to the challenges of the digital era. With good synergy between these aspects, digital forensic audits can be a crucial instrument in strengthening the integrity of the public sector and encouraging increased public trust in governance.

The Relationship between the Implementation of Digital Forensic Audits and the Enhanced Accountability of Government Institutions

The relationship between the implementation of digital forensic audits and the enhanced accountability of government institutions is becoming increasingly significant in the context of modern public sector governance (Darwin, 2024b). Digital forensic audits, essentially a form of investigative auditing based on information technology, enable auditors to systematically search, analyze, and uncover digital evidence to detect fraudulent practices or abuse of authority. With the increasing complexity of government information systems and the increasing volume of managed data, traditional audit methods are no longer adequate to address the challenges of transparency and accountability. The advent of digital forensic audits bridges this need by providing a more precise, objective, and measurable instrument for building public trust in the performance of government institutions (Putra & Riyanta, 2025).

In practice, the accountability of government institutions is often measured by their ability to account for budget use, program implementation, and results achieved to the public. However, issues such as corruption, data manipulation, and substandard financial reporting remain serious obstacles. The implementation of digital forensic audits offers a solution to strengthen oversight and investigation functions. By utilizing technologies such as data analytics, artificial intelligence, and digital tracking systems, auditors can uncover suspicious transaction patterns that were previously difficult to detect. This directly supports increased accountability because every bureaucratic action can be traced and verified through digital evidence that is not easily manipulated.

Furthermore, digital forensic audits play a role in narrowing the scope for fraudulent practices in the public sector. A digital forensic-based audit system enables the creation of both preventative and repressive control mechanisms. From a preventive perspective, the existence of a digital audit system capable of monitoring bureaucratic transactions and communications in real time encourages officials to be more careful in carrying out their duties. Government officials become aware that their every action is recorded in a digital footprint that can be examined at any time. From a repressive perspective, when indications of misuse are detected, auditors have the ability to trace the flow of funds, documents, and related electronic communications, enabling more effective investigations. Thus, the close relationship between digital forensic

audits and government accountability is evident in how these audits enhance both prevention and enforcement of fraud.

On the other hand, the implementation of digital forensic audits also strengthens accountability in the context of public information transparency. The public, as primary stakeholders, has the right to receive accurate and reliable reports on government performance. Through the use of digital forensic audits, financial reports and data on government agency activities are more verified and their integrity is guaranteed. This not only increases public trust in the government but also encourages public participation in oversight. Accountability is no longer understood solely as an internal obligation of the bureaucracy, but rather as a form of openness that involves the wider community in ensuring that the government operates according to established rules and objectives (Netshifhefhe et al., 2024).

The relationship between digital forensic audits and government accountability is also evident in the realm of public policy (Simbolon et al., 2024). The implementation of digital technology-based audits requires clear regulations regarding data governance, audit standards, and legal protection for both auditors and audited institutions. These regulations create a stronger accountability ecosystem, as governments are not only required to comply with public accounting standards but are also required to integrate digital forensic aspects into the audit process. Consequently, government institutions are encouraged to be more disciplined in managing data and information, thereby improving reporting quality and minimizing the scope for irregularities. Regulations that support digital forensic audits ultimately reinforce the state's commitment to realizing clean and accountable governance.

Furthermore, this relationship also relates to the efficiency and effectiveness of oversight. Manual audits are often time-consuming, labor-intensive, and risk missing important details. With digital forensic audits, the audit process is faster, more accurate, and based on robust digital evidence. This enables government institutions to respond more quickly to suspected violations while saving resources. This efficiency has a direct impact on increased accountability, as the government can promptly take corrective action on identified issues. Furthermore, the effectiveness of digital forensic audits also strengthens the auditor's position as an independent party capable of providing objective, data-based recommendations, thus increasing the credibility of audit results.

However, it is also important to note that this positive relationship is not without challenges in its implementation. The implementation of digital

forensic audits requires competent human resources in information technology and forensic auditing, as well as adequate digital infrastructure. Without this support, the effectiveness of digital forensic audits in improving the accountability of government institutions will be less than optimal. However, if these challenges can be overcome through investment in auditor capacity building, strengthening regulations, and developing reliable information systems, digital forensic audits will become a crucial instrument for bureaucratic reform (AL-Raggad & Al-Raggad, 2024b).

Ultimately, the implementation of digital forensic audits and the increased accountability of government institutions have a mutually reinforcing relationship. Digital forensic audits provide a foundation for creating more transparent, accurate, and fraud-free governance. Conversely, the need to achieve accountability is driving government institutions to adopt modern audit methods that can address the challenges of the digital era. This reciprocal relationship reflects that accountability is not merely an end in itself, but also a process that continues to evolve alongside the use of technology in the public sector. Thus, digital forensic audits can be seen as a crucial catalyst in the journey to realizing a clean, professional, and trustworthy government.

CONCLUSION

The conclusions of this study indicate that digital forensic audits play a crucial role in strengthening public trust in the public sector. With the increasing complexity of government-managed financial and information systems, the use of digital technology in forensic audits ensures transparency, accuracy, and the ability to detect potential fraud more quickly and efficiently. This makes digital forensic audits a strategic instrument for creating accountable public governance amidst the dynamics of technological development and public demands for transparency.

Furthermore, the study's findings confirm that the adoption of digital forensic audits can provide added value within the evolving public sector accountability framework. The existence of technology-based audit mechanisms serves not only as a supervisory tool but also as a preventative measure that encourages state administrators to be more careful in managing public resources. This further strengthens the legitimacy of public institutions in the eyes of the public by ensuring legal certainty, fiscal transparency, and integrity in the financial management process.

Overall, this study confirms that digital forensic audits are a crucial pillar in strengthening public trust and establishing a public sector accountability

system that is adaptive to changing times. By integrating digital audit technology with the ethical commitment of public officials, the public sector can be more responsive to public demands for transparency, efficiency, and accountability. Going forward, the implementation of digital forensic audits is expected to not only improve the quality of oversight but also lay the foundation for cleaner, more modern, and more competitive governance.

REFERENCES

- AL-Raggad, A. K., & Al-Raggad, M. (2024a). Analyzing trends: A bibliometric study of administrative law and forensic accounting in the digital age. *Heliyon*, 10(18). <https://doi.org/10.1016/j.heliyon.2024.e37462>
- AL-Raggad, A. K., & Al-Raggad, M. (2024b). Analyzing trends: A bibliometric study of administrative law and forensic accounting in the digital age. *Heliyon*, 10(18). <https://doi.org/10.1016/j.heliyon.2024.e37462>
- Amalia, D. P., Nurwahyuni, Hasbah, I., & Muchran, M. (2025). The Role of Technology-Based Audits (Digital Audits) in Improving Audit Quality in Accounting Firms Public in the Industrial Era 4.0. *IECON: International Economics and Business Conference*, 3(1), 161–169.
- Azizi, M., Hakimi, M., Amiri, F., & Shahidzay, A. K. (2024). The Role of IT (Information Technology) Audit in Digital Transformation: Opportunities and Challenges. *Open Access Indonesia Journal of Social Sciences*, 7(2), 1473–1482. <https://doi.org/10.37275/oaijss.v7i2.230>
- Barr-Pulliam, D., Brown-Liburd, H. L., & Munoko, I. (n.d.). *The effects of person-specific, task, and environmental factors on digital transformation and innovation in auditing: A review of the literature*. <https://doi.org/10.1111/jifm.12148>
- Darwin, K. (2024a). Strengthening Public and Private Accountability through Digital Forensic Accounting. *Sinergi International Journal of Accounting and Taxation*, 2(4), 225–238. <https://doi.org/10.61194/ijat.v2i4.717>
- Darwin, K. (2024b). Strengthening Public and Private Accountability through Digital Forensic Accounting. *Sinergi International Journal of Accounting and Taxation*, 2(4), 225–238. <https://doi.org/10.61194/ijat.v2i4.717>
- Edet, P., & Christopher, D. (2025a). *Forensic Accounting and Financial Integrity in the Nigerian Public Sector*. 11(3).
- Edet, P., & Christopher, D. (2025b). *Forensic Accounting and Financial Integrity in the Nigerian Public Sector*. 11(3).
- Elumilade, O. O., Ogundeji, I. A., Achumie, G. O., Omokhoa, H. E., & Omowole, B. M. (2021). Enhancing fraud detection and forensic auditing through data-driven techniques for financial integrity and security. *Journal of Advanced Education and Sciences*, 1(2), 55–63. <https://doi.org/10.54660/JAES.2021.1.2.55-63>

- Gunasegaran, M., Basiruddin, R., & Mohd Rizal, A. (2023). Detecting and Preventing Fraud in e-procurement of Public Sector: A Review, Synthesis and Opportunities for Future Research. *International Journal of Academic Research in Business and Social Sciences*, 13(1), Pages 1444-1463. <https://doi.org/10.6007/IJARBSS/v13-i1/15970>
- 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. <https://doi.org/10.1109/ACCESS.2023.3348552>
- Henriques, J. P. M. (2024, May 3). Audit Compliance and Forensics Frameworks for Improved Critical Infrastructure Protection. *Audit Compliance and Forensics Frameworks for Improved Critical Infrastructure Protection*. Audit Compliance and Forensics Frameworks for Improved Critical Infrastructure Protection. <https://estudogeral.uc.pt/handle/10316/115446>
- lipumbu, E., Nhamu, I., & Chitauru, M. (2023). A Comparative Analysis of Information Systems Audit and Digital Forensics Processes (SSRN Scholarly Paper No. 4648699). Social Science Research Network. <https://doi.org/10.2139/ssrn.4648699>
- Illési, Z. (2025). Digital Evidence Management for Organizational Legal Compliance. *Interdisciplinary Description of Complex Systems: INDECS*, 23(3), 217–229. <https://doi.org/10.7906/indecs.23.3.3>
- Kaur, B., Sood, K., & Grima, S. (2023). A systematic review on forensic accounting and its contribution towards fraud detection and prevention. *Journal of Financial Regulation and Compliance*, 31(1), 60–95. <https://doi.org/10.1108/JFRC-02-2022-0015>
- Lajoie, P.-L., & Gendron, Y. (n.d.). *Contemporary Accounting Research* | CAAA Journal | Wiley Online Library. Retrieved September 24, 2025, from <https://onlinelibrary.wiley.com/doi/10.1111/1911-3846.70002>
- Najih, M. K. F. (2025). Forensic Auditing in Fraud Detection and Prevention: Integration of Technology, Internal Audit, and Anti-Fraud Regulation. *Fairness*, 1(1), 47–63. [https://doi.org/10.70764/gdpu-fr.2025.1\(1\)-04](https://doi.org/10.70764/gdpu-fr.2025.1(1)-04)
- Netshifhefhe, K., Netshifhefhe, M. V., Mupa, M. N., & Murapa, K. A. (2024). The Role of Forensic Audits in Strengthening Corporate Governance and Mitigating Compliance Risks. 8(4).
- Omar, S. S., Nayef, J. M., Qasim, N. H., Kawad, R. T., & Kalenychenko, R. (n.d.). THE ROLE OF DIGITALIZATION IN IMPROVING ACCOUNTABILITY AND EFFICIENCY IN PUBLIC SERVICES.
- Otia, J. E., & Bracci, E. (n.d.). *Digital transformation and the public sector auditing: The SAI's perspective*. <https://doi.org/10.1111/faam.12317>
- Oyerogba, E. O. (2021). Forensic auditing mechanism and fraud detection: The case of Nigerian public sector. *Journal of Accounting in Emerging Economies*, 11(5), 752–775. <https://doi.org/10.1108/JAEE-04-2020-0072>

- Putra, S. D., & Riyanta, S. (2025). Digital Forensic Governance Strategy in Indonesia to Realize The Credibility of Accountable and Efficient Public Law Enforcement Agencies. *Journal of Social Research*, 4(7), 1316–1327. <https://doi.org/10.55324/josr.v4i7.2600>
- Sari, R., & Muslim, M. (2023). Accountability and Transparency in Public Sector Accounting: A Systematic Review. *Amkop Management Accounting Review (AMAR)*, 3(2), 90–106. <https://doi.org/10.37531/amar.v3i2.1440>
- Shakir, S., & Abbas, G. (2020). Role of Forensic Auditing in Enhancing the Efficiency of Public Sector Organization: Role of Forensic Auditing. *Reviews of Management Sciences*, 2(2), 40–59. <https://doi.org/10.53909/rms.02.02.030>
- Simbolon, R., Adriana, N., Rustam, A., Sulistyowati, N. W., & Rewa, K. A. (2024). The Impact of Forensic Accounting on Financial Fraud Prevention: A Comparative Analysis Across Countries. *The Journal of Academic Science*, 1(8), 1074–1084. <https://doi.org/10.59613/m6jrt421>
- Tariq, M. U. (2025). Digital Accountability: Revolutionizing Public Sector Transparency and Service Delivery. In *Enhancing Public Sector Accountability and Services Through Digital Innovation* (pp. 129–154). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3693-9251-5.ch004>
- Udrescu, L.-M. (2024). The Evolution and Impact of Digital Transformation on Internal Audit and Managerial Control in Public Institutions. *Proceedings of the ... International Conference on Economics and Social Sciences.*, 6(1), 187–198.
- Wahyuandari, W. (2025). The Role of Forensic Auditing in Detecting and Preventing Financial Fraud in Organizations. *The Journal of Academic Science*, 2(1), 212–221. <https://doi.org/10.59613/1hay7432>
- Wijesooriya, C., & Basnayake, R. (2024). Digital Transformation in Redefining the Role of the Finance and Audit Professional of the Future. In A. Perdana & T. Wang (Eds.), *Digital Transformation in Accounting and Auditing: Navigating Technological Advances for the Future* (pp. 61–104). Springer International Publishing. https://doi.org/10.1007/978-3-031-46209-2_3
- Yoon, S. (2020). A Study on the Transformation of Accounting Based on New Technologies: Evidence from Korea. *Sustainability*, 12(20), 8669. <https://doi.org/10.3390/su12208669>