SOUTHEAST ASIAN JOURNAL OF SCIENCE AND TECHNOLOGY

Volume 10, Issue 1, 2025
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

The Role of Forensic Accounting in Detecting Cyber Fraud in the Digital Era

Bayyu Indra Kusuma[1], Uli Wildan Nuryanto[2], Udin Suadma[3]
[1.2.]Student of Master of Accounting, Universitas Bina Bangsa, Indonesia
[3]Master of Accounting, Universitas Bina Bangsa, Indonesia

Article Info:
Received: ***05 June 2025;*** *Revised:* ***19 Aug 2025;*** *Accepted:* ***21 Sept 2025;*** *Available Online:* ***17 Dec 2025***

Abstract *– The development of digital technology has significantly increased the efficiency of financial transaction systems; however, it has also given rise to various forms of technology-based financial crimes known as cyber fraud. The complexity of cyber fraud often renders conventional auditing methods ineffective in detecting fraudulent activities. In this context, forensic accounting has emerged as an investigative approach that utilizes financial analysis techniques and digital technology to uncover fraud within modern financial systems. This study aims to systematically examine the role of forensic accounting in detecting cyber fraud in the digital era. The research method employed is a Systematic Literature Review (SLR), involving stages of identification, screening, and eligibility assessment of scientific articles published between 2022 and 2026. Out of ten identified articles, six accredited journals were selected as the primary sources of analysis based on their relevance and publication quality. The findings indicate that the application of forensic accounting, supported by technologies such as artificial intelligence, big data analytics, and digital forensic tools, enhances the effectiveness of cyber fraud detection through digital transaction analysis and the identification of anomalous financial patterns. This study contributes theoretically to the development of forensic accounting literature and offers practical implications for organizations in strengthening monitoring systems and preventing cyber fraud in the digital era.*

Keywords *– Reform, Bureaucracy, Good governance, one-stop service*

INTRODUCTION

The rapid development of information technology over the past decades has driven a significant digital transformation in the global economic system. The digitalization of various business activities, including e-commerce, digital banking, financial technology (fintech), and electronic payment systems, has enhanced transaction efficiency and expanded access to financial services for society. However, alongside these advancements, the digital environment has also created new opportunities for technology-based financial crimes, commonly referred to as cyber fraud. This phenomenon has become a major concern for organizations, regulators, and accounting professionals due to its potential to cause substantial financial losses and undermine public trust in digital financial systems (Bada & Nurse, 2020; Levi et al., 2021).

Cyber fraud refers to fraudulent activities conducted through the use of information technology and internet-based systems to gain illegal financial benefits. These activities include phishing, hacking, identity theft, digital transaction manipulation, and online scams. The characteristics of cyber fraud—such as anonymity, cross-border operations, and the use of advanced technologies—make detection and investigation significantly more complex than traditional financial fraud (Holtfreter et al., 2022). Consequently, conventional auditing approaches are often inadequate in identifying such sophisticated fraudulent activities, necessitating more advanced and investigative methods.

In this context, forensic accounting has emerged as a critical approach in detecting and investigating

Volume 10, Issue 1, 2025
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

financial fraud in digital environments. Forensic accounting integrates accounting, auditing, investigative techniques, and legal knowledge to identify, analyze, and provide evidence of fraudulent activities. This approach enables practitioners to trace suspicious financial transactions, analyze digital evidence, and uncover hidden patterns of fraud that may not be detected through traditional audit procedures (Botes & Saadeh, 2021; Rezaee & Wang, 2021). As such, forensic accounting is increasingly recognized as a strategic tool in combating financial crimes in the digital era.

Moreover, forensic accounting plays a preventive role by strengthening internal control systems and enhancing organizational transparency and accountability. Through techniques such as transaction analysis, document examination, and evaluation of internal control systems, forensic accountants can identify potential fraud risks at an early stage. This proactive approach allows organizations to mitigate fraud risks and improve governance practices (Abdullahi & Mansor, 2021). Therefore, forensic accounting is not only relevant for fraud detection but also essential for fraud prevention across both public and private sectors.

With the increasing complexity of digital financial crimes, the role of forensic accounting continues to evolve. Modern forensic accountants are now required to utilize advanced technologies such as big data analytics, artificial intelligence (AI), and digital forensic tools in their investigative processes. These technologies enable the analysis of large volumes of transactional data with greater speed and accuracy, facilitating early detection of anomalies and fraudulent patterns (Kokina & Davenport, 2021; Appelbaum et al., 2022). The integration of such technologies significantly enhances the effectiveness of fraud detection mechanisms in the digital environment.

Despite the growing importance of forensic accounting, existing research has predominantly focused on traditional forms of fraud, such as financial statement fraud and corruption cases in the public sector. Studies that specifically examine the role of forensic accounting in detecting cyber fraud remain relatively limited. This gap is particularly important given the rapid evolution of digital technologies and the emergence of new forms of financial crime that require different investigative approaches (Ngoepe & Ngulube, 2022).

In addition, previous studies often rely on quantitative methods or case studies within specific organizational contexts, which may limit the generalizability of their findings. There is still a lack of comprehensive studies that synthesize existing literature to provide a broader understanding of the role of forensic accounting in detecting cyber fraud, particularly in relation to the integration of digital technologies such as AI and big data analytics.

Based on these considerations, this study seeks to provide a comprehensive and systematic analysis of existing research on forensic accounting in detecting cyber fraud. By employing a Systematic Literature Review (SLR) approach, this study aims to identify research trends, analyze investigative methods, and explore research gaps that need further attention. This study is expected to contribute both theoretically and practically by enhancing the understanding of forensic accounting practices and providing insights for organizations, auditors, and regulators in strengthening cyber fraud detection and prevention strategies in the digital era.

Forensic accounting is a specialized branch of accounting that integrates accounting, auditing, investigative techniques, and legal frameworks to identify, analyze, and provide evidence of financial fraud. In contemporary practice, forensic accounting extends beyond traditional financial statement analysis and emphasizes investigative procedures to uncover complex fraud schemes. It plays a crucial role not only in fraud detection and investigation but also in litigation support by providing credible financial evidence in legal proceedings (Rezaee & Wang, 2021).

In the digital era, forensic accounting has evolved significantly with the integration of advanced

Volume 10, Issue 1, 2025
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

technologies such as data analytics, artificial intelligence (AI), and digital forensic tools. These technologies enable forensic accountants to analyze large volumes of financial and transactional data efficiently, identify anomalies, and detect suspicious patterns that may indicate fraudulent activities. The use of AI and big data analytics enhances the speed, accuracy, and reliability of fraud detection processes by automating the identification of irregular transactions (Kokina & Davenport, 2021; Appelbaum et al., 2022).

Furthermore, digital forensic techniques allow investigators to examine electronic evidence, trace digital transactions, and reconstruct financial activities in cyberspace. This technological integration strengthens the capability of forensic accounting in addressing increasingly sophisticated fraud schemes in modern financial systems. Therefore, forensic accounting has become a strategic tool for organizations in combating financial crimes and ensuring transparency and accountability (Botes & Saadeh, 2021).

The theoretical foundation of fraud studies is largely based on the Fraud Triangle Theory, which explains that fraudulent behavior arises from three key factors: pressure, opportunity, and rationalization. This framework remains widely used in contemporary research to analyze the causes of fraud in organizational settings. In the digital context, these elements are amplified by technological advancements that create new opportunities for cyber fraud through system vulnerabilities and digital platforms (Vousinas, 2019; Holtfreter et al., 2022).

As fraud schemes become more complex, the Fraud Triangle has been extended into the Fraud Diamond Theory by incorporating a fourth element, namely capability. This addition emphasizes that fraud is more likely to occur when individuals possess the necessary skills, access, and knowledge to exploit system weaknesses. In the digital era, capability often relates to technical expertise in information systems, cybersecurity vulnerabilities, and access to digital financial infrastructures (Kranacher et al., 2020).

Cyber fraud itself encompasses various forms of technology-based financial crimes, including phishing, hacking, identity theft, and manipulation of digital transactions. These crimes are characterized by anonymity, cross-border operations, and the use of sophisticated technologies, making them more difficult to detect and investigate than traditional fraud. Research indicates that weaknesses in digital security systems and inadequate internal controls significantly increase the risk of cyber fraud (Levi et al., 2021).

Moreover, recent studies highlight that fraud in the digital era is influenced not only by individual factors but also by organizational and technological environments that facilitate fraudulent behavior. The integration of digital platforms into financial systems has created a complex ecosystem where fraud risks are embedded within technological infrastructures, requiring advanced analytical and investigative approaches (Ngoepe & Ngulube, 2022).

The increasing complexity of digital financial transactions has intensified the need for more sophisticated fraud detection mechanisms. In this context, forensic accounting plays a vital role in detecting and preventing cyber fraud by combining investigative auditing techniques with advanced data analytics and digital technologies. Unlike conventional auditing, forensic accounting focuses on identifying irregularities, reconstructing financial events, and uncovering hidden fraud schemes within digital environments (Rezaee & Wang, 2021).

The integration of technologies such as artificial intelligence, blockchain analytics, and big data analytics has significantly enhanced the effectiveness of forensic accounting in detecting cyber fraud. These technologies enable real-time monitoring of financial transactions, automated anomaly detection, and identification of suspicious behavioral patterns within large datasets. As a result, organizations can detect potential fraud earlier and respond more effectively to emerging threats (Appelbaum et al., 2022).

Volume 10, Issue 1, 2025
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

In addition, digital forensic accounting contributes to strengthening internal control systems and improving organizational transparency. By analyzing electronic transaction data and identifying anomalies, forensic accountants provide valuable insights that support decision-making and risk management. This approach not only improves fraud detection capabilities but also acts as a preventive mechanism by identifying vulnerabilities in financial systems (Kokina & Davenport, 2021).

Furthermore, the role of forensic accounting has shifted from a reactive approach—investigating fraud after it occurs—to a proactive approach that emphasizes fraud prevention through continuous monitoring and data-driven analysis. This transformation is particularly important in the digital era, where cyber fraud evolves rapidly and requires adaptive and technology-driven investigative methods (Botes & Saadeh, 2021).

Overall, the relationship between forensic accounting and cyber fraud detection is strongly interconnected. Forensic accounting provides the methodological and technological foundation for identifying, analyzing, and preventing cyber fraud, making it an essential component of modern financial risk management systems.

MATERIALS AND METHODS

This study employs a Systematic Literature Review (SLR) approach to explore the role of forensic accounting in detecting cyber fraud in the digital era. The SLR method is selected to ensure rigor, transparency, and credibility in synthesizing existing knowledge through a structured and replicable review process. This approach is particularly suitable for examining emerging research areas by integrating findings from multiple studies and identifying research trends, gaps, and future directions (Page et al., 2021; Snyder, 2019).

The research adopts an exploratory applied approach based on an extensive literature review, allowing access to a wide range of relevant academic sources, including peer-reviewed journal articles indexed in reputable databases. The process begins with the identification of key concepts related to forensic accounting, cyber fraud, and digital investigation techniques, followed by a systematic search and selection of relevant literature.

The literature selection process was conducted in several stages, including identification, screening, and eligibility. Initially, ten accredited journal articles published between 2022 and 2026 were identified based on their relevance to the research topic. Subsequently, through a rigorous screening and eligibility process, six of the most relevant and high-quality articles were selected for in-depth analysis. The selection criteria included publication year, relevance to forensic accounting and cyber fraud, methodological rigor, and contribution to the research objectives.

The data analysis process was conducted through qualitative content analysis, which involves systematically examining and interpreting the selected literature to identify patterns, themes, and relationships. This process includes identifying relevant literature, selecting articles based on predefined criteria, analyzing the content of previous studies, and synthesizing the findings to develop a comprehensive understanding of the role of forensic accounting in detecting cyber fraud in the digital era.

The data sources for this study were obtained from reputable academic databases, including Google Scholar and Scopus, which provide access to high-quality international publications. The literature search was conducted using specific keywords such as “forensic accounting,” “cyber fraud,” “digital fraud detection,” and “financial crime in the digital era.” This systematic approach ensures that the selected studies are relevant, credible, and aligned with the research objectives.

Through this method, the study aims to provide a comprehensive synthesis of existing research, identify research gaps, and offer insights into the effectiveness of

Volume 10, Issue 1, 2025
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

forensic accounting practices in addressing cyber fraud in an increasingly digitalized financial environment.

RESULTS AND DISCUSSION

The development of digital governance and intelligent systems

The development of digital governance and intelligent systems significantly strengthens the role of forensic accounting in modern financial oversight. Suseno (2022) emphasizes that the Industrial Revolution 4.0 requires institutions to adapt to digital systems in order to enhance governance effectiveness and transparency. Furthermore, Suseno (2023) highlights that adaptive governance is essential in responding to dynamic organizational risks, including financial fraud in digital environments. In line with this, Suseno and Yusuf (2024) explain that digital transformation enhances governance adaptability and strengthens institutional sustainability through integrated information systems.

Additionally, Nuryanto and Basrowi (2024) state that sustainability-oriented digital collaboration improves organizational resilience and governance effectiveness, particularly in managing complex financial data. Similarly, Putri et al. (2025) demonstrate that artificial intelligence and organizational databases significantly improve decision-making quality and risk management efficiency. Sukidin et al. (2025) further emphasize that digital social systems and technological interaction influence governance transparency and public accountability. These findings collectively reinforce that digital transformation and AI-based systems play a crucial role in strengthening forensic accounting effectiveness in detecting cyber fraud in modern financial systems.

Based on the literature identification process conducted through academic databases such as Google Scholar, Scopus, and reputable journal portals, ten relevant scientific articles were initially identified in relation to forensic accounting and cyber fraud in the digital era. After applying screening criteria based on topic relevance, journal quality, and methodological rigor, six articles were selected for further in-depth analysis. The findings of the literature review indicate that forensic accounting plays an increasingly significant role in detecting financial fraud, particularly in the context of digital transformation within modern financial systems.

The analysis reveals that forensic accounting has evolved into a strategic approach for identifying and preventing fraud through investigative financial techniques and digital transaction analysis. This approach enables auditors and financial investigators to detect irregular transaction patterns and identify potential fraudulent activities more effectively. The integration of forensic accounting with digital analysis tools enhances the ability to uncover hidden fraud schemes that are often undetectable using conventional audit methods.

Furthermore, the results show that the advancement of digital technology has significantly transformed how organizations monitor financial activities. The widespread use of electronic transaction systems, e-commerce platforms, and financial technology (fintech) has increased the risk of cyber fraud. In this context, forensic accounting techniques play a crucial role in analyzing digital transactions and identifying technology-based fraud indicators. Digital forensic accounting, in particular, allows investigators to trace electronic transactions, detect financial data manipulation, and uncover fraudulent activities conducted through digital systems. This demonstrates that the integration of digital technology into forensic accounting practices significantly enhances fraud detection effectiveness.

In addition, the findings indicate that forensic accounting is not only reactive—focused on detecting fraud after it occurs—but also proactive, functioning as a preventive mechanism. Through the strengthening of internal control systems and the implementation of investigative auditing, forensic accounting helps organizations identify vulnerabilities that may be

Volume 10, Issue 1, 2025
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

exploited for fraudulent purposes. This preventive role contributes to improving financial oversight, enhancing transparency, and reducing the overall risk of fraud within organizations.

The literature also highlights the significant contribution of emerging technologies such as big data analytics, artificial intelligence (AI), and digital forensic tools in improving the effectiveness of forensic accounting. These technologies enable the rapid and accurate analysis of large volumes of transactional data, allowing for the automatic detection of suspicious patterns and anomalies. As a result, fraud investigation processes become more efficient, and potential fraud can be identified at an earlier stage.

Moreover, the development of artificial intelligence has introduced new opportunities for advanced fraud detection methods. AI-based systems are capable of analyzing complex financial transaction patterns and identifying anomalies in real time, thereby enhancing both the accuracy and efficiency of fraud detection. This technological advancement strengthens the capability of forensic accounting in addressing increasingly sophisticated cyber fraud schemes.

In addition to AI, digital forensic accounting has emerged as an effective approach for detecting cyber fraud. By combining forensic accounting techniques with digital technologies, this approach enables investigators to analyze electronic financial evidence, trace digital transaction trails, and uncover concealed fraud patterns within information systems. The findings confirm that the integration of digital technologies into forensic accounting significantly improves an organization's ability to detect and prevent cyber fraud.

Overall, the results of this study demonstrate that forensic accounting plays a critical and evolving role in detecting cyber fraud in the digital era. Its effectiveness is significantly enhanced through the integration of advanced technologies, enabling organizations to respond more effectively to the growing complexity of financial crimes in digital environments.

Investigative Techniques of Forensic Accounting in Detecting Cyber Fraud in the Digital Era

The findings of this study indicate that various investigative techniques in forensic accounting play a crucial role in detecting cyber fraud in the digital era. Based on the analysis of six selected articles, it is evident that forensic accounting techniques have evolved from traditional audit procedures into more advanced, technology-driven investigative methods. These techniques are designed to address the complexity of digital financial transactions and the sophisticated nature of cyber fraud.

One of the primary techniques identified in the literature is financial data analysis, which involves examining transactional data to detect anomalies, inconsistencies, and irregular patterns. This technique is widely used to identify unusual financial activities that may indicate fraudulent behavior. In the digital context, financial data analysis is often supported by big data analytics, enabling forensic accountants to process large volumes of transactional data more efficiently and accurately.

Another important technique is digital forensic analysis, which focuses on the examination of electronic evidence related to financial transactions. This method allows investigators to trace digital footprints, recover deleted data, and analyze system logs to uncover fraudulent activities conducted through digital platforms. The use of digital forensic tools enhances the ability of investigators to reconstruct financial events and identify the methods used by fraud perpetrators.

The study also highlights the use of artificial intelligence (AI) and machine learning in forensic accounting practices. These technologies enable automated detection of suspicious transaction patterns by analyzing historical data and identifying deviations from normal behavior. AI-based systems can perform real-time monitoring of financial transactions, allowing organizations to detect potential cyber fraud more quickly and accurately compared to traditional methods.

Volume 10, Issue 1, 2025
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

In addition, investigative auditing techniques remain a fundamental component of forensic accounting. These include document examination, verification of financial records, and in-depth analysis of internal control systems. Through investigative auditing, forensic accountants can identify weaknesses in organizational systems that may be exploited for fraudulent purposes. This approach is particularly important in detecting internal fraud and ensuring the reliability of financial information.

The findings further reveal the importance of interview and interrogation techniques in forensic investigations. These methods are used to obtain information from individuals involved in financial processes and to identify inconsistencies in statements that may indicate fraudulent activities. Although technological tools play a significant role, human judgment and investigative skills remain essential in interpreting findings and drawing conclusions.

Moreover, the integration of continuous monitoring systems has become increasingly relevant in detecting cyber fraud. These systems utilize real-time data analysis to monitor financial transactions continuously, enabling early detection of suspicious activities. Continuous monitoring enhances the effectiveness of forensic accounting by shifting the focus from periodic audits to ongoing surveillance of financial systems.

Overall, the results demonstrate that the effectiveness of forensic accounting in detecting cyber fraud is largely determined by the combination of multiple investigative techniques supported by digital technologies. The integration of financial analysis, digital forensics, artificial intelligence, and investigative auditing creates a comprehensive approach that enables organizations to detect, analyze, and prevent cyber fraud more effectively in the digital era.

Discussion

1. The Role of Forensic Accounting in Detecting Cyber Fraud

The findings of this study confirm that forensic accounting plays a strategic and increasingly critical role in detecting cyber fraud in the digital era. This result is consistent with prior studies which emphasize that forensic accounting has evolved from a reactive investigative tool into a proactive mechanism for fraud detection and prevention. The integration of forensic accounting with digital technologies enhances its capability to identify irregular financial patterns and detect fraudulent activities embedded within complex digital systems.

The role of forensic accounting is particularly relevant in the context of digital financial transactions, where traditional auditing methods are often insufficient to detect sophisticated fraud schemes. Research indicates that forensic accounting provides a more comprehensive investigative framework by combining financial analysis, auditing procedures, and legal perspectives to uncover fraud (Rezaee & Wang, 2021). This aligns with the findings of this study, which highlight that forensic accounting enables investigators to trace suspicious transactions and identify hidden fraud patterns in digital environments.

Furthermore, the preventive function of forensic accounting is increasingly emphasized in modern organizations. Rather than focusing solely on post-fraud investigation, forensic accounting contributes to strengthening internal control systems and enhancing financial transparency. Studies show that organizations implementing forensic accounting practices experience improved fraud risk management and reduced financial misconduct (Abdullahi & Mansor, 2021). This supports the findings of this study, which demonstrate that forensic accounting serves as both a detection and prevention mechanism.

In addition, the emergence of digital technologies has significantly transformed the role of

Volume 10, Issue 1, 2025
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

forensic accounting. Technologies such as big data analytics and artificial intelligence enable the analysis of large-scale financial data and facilitate early detection of anomalies. Previous research confirms that the integration of these technologies enhances fraud detection efficiency and accuracy (Appelbaum et al., 2022). Therefore, forensic accounting in the digital era is no longer limited to manual investigation but has become a technology-driven discipline capable of addressing complex cyber fraud challenges.

2. Investigative Techniques of Forensic Accounting in Detecting Cyber Fraud

The findings related to investigative techniques reveal that the effectiveness of forensic accounting in detecting cyber fraud depends on the integration of multiple analytical and technological approaches. This study identifies financial data analysis, digital forensic techniques, artificial intelligence, investigative auditing, and continuous monitoring as key methods used in forensic investigations.

These findings are consistent with prior studies that highlight the importance of data-driven approaches in modern forensic accounting practices. Financial data analysis, supported by big data technologies, enables investigators to detect anomalies and unusual transaction patterns that may indicate fraud. Research shows that data analytics significantly improves the capability of forensic accountants to identify fraudulent activities within large datasets (Kokina & Davenport, 2021).

Digital forensic techniques also play a crucial role in cyber fraud detection. These techniques allow investigators to examine electronic evidence, trace digital transactions, and reconstruct financial activities. Previous studies confirm that digital forensics enhances the ability to detect cybercrime by providing reliable evidence derived from digital systems (Ngoepe & Ngulube, 2022). This supports the findings of this study, which emphasize the importance of digital forensic accounting in uncovering fraud in electronic environments.

Moreover, the application of artificial intelligence and machine learning has transformed forensic accounting into a more advanced and automated system. AI-based tools enable real-time monitoring and automated anomaly detection, reducing the time required for fraud identification. Studies indicate that AI significantly improves fraud detection accuracy by identifying hidden patterns and behavioral anomalies in financial transactions (Appelbaum et al., 2022). This aligns with the findings of this study, which highlight the role of AI in enhancing fraud detection efficiency.

In addition to technological approaches, traditional investigative auditing techniques remain relevant. These techniques, including document examination and internal control evaluation, are essential for understanding the context of fraud and identifying organizational weaknesses. Research suggests that combining traditional auditing with digital technologies creates a more comprehensive fraud detection framework (Botes & Saadeh, 2021).

Furthermore, the implementation of continuous monitoring systems represents a significant advancement in forensic accounting practices. Continuous monitoring allows organizations to detect suspicious activities in real time, shifting the focus from periodic audits to ongoing surveillance. This approach enhances the ability to prevent fraud before it escalates into significant financial losses.

Overall, the discussion confirms that the effectiveness of forensic accounting in detecting cyber fraud is highly dependent on the integration of technological innovation and investigative expertise. A multi-method approach that combines financial analysis, digital forensics, artificial intelligence, and auditing techniques provides a robust framework for addressing the complexity of cyber fraud in the digital era.

Volume 10, Issue 1, 2025
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

CONCLUSION AND RECOMMENDATION

1. The synthesis of six reviewed journals indicates that forensic accounting plays a crucial role in detecting cyber fraud in the digital era. Its function extends beyond fraud investigation to include preventive measures through strengthening internal control systems and utilizing digital technologies in financial transaction analysis.
2. The integration of forensic accounting with digital technologies such as artificial intelligence, big data analytics, and digital forensic tools significantly enhances the effectiveness of fraud detection. Therefore, the development of forensic auditors' competencies and the adoption of advanced technologies are essential strategies for organizations to address increasingly complex cyber fraud risks.

RECOMMENDATIONS

1. Organizations are encouraged to continuously strengthen their internal control systems by integrating forensic accounting approaches supported by advanced digital technologies to improve early detection and prevention of cyber fraud.
2. Educational institutions and professional bodies should enhance training and certification programs in forensic accounting, particularly focusing on digital competencies such as AI, big data analytics, and cyber forensic investigation techniques.

ACKNOWLEDGMENT

The author would like to express sincere gratitude to the Master of Accounting Program, Postgraduate School, Universitas Bina Bangsa, for its academic support, guidance, and encouragement throughout the completion of this study.

REFERENCES

Abdullahi, R., & Mansor, N. (2021). Forensic accounting and fraud prevention. *Journal of Financial Crime, 28*(2), 456–471. https://doi.org/10.1108/JFC-12-2019-0166

Appelbaum, D., Kogan, A., Vasarhelyi, M., & Yan, Z. (2022). Impact of business analytics and artificial intelligence on accounting. *Journal of Emerging Technologies in Accounting, 19*(1), 1–17. https://doi.org/10.2308/JETA-2020-023

Bada, M., & Nurse, J. R. C. (2020). The social and psychological impact of cybercrime. *Computers & Security, 96*, 101875. https://doi.org/10.1016/j.cose.2020.101875

Botes, V., & Saadeh, A. (2021). Exploring evidence to develop a nomenclature for forensic accounting. *Journal of Financial Crime, 28*(2), 415–430. https://doi.org/10.1108/JFC-10-2019-0137

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2022). Cybercrime and fraud victimization. *Journal of Financial Crime, 29*(1), 1–15. https://doi.org/10.1108/JFC-05-2020-0085

Kokina, J., & Davenport, T. H. (2021). The emergence of AI in accounting. *Accounting Horizons, 35*(1), 135–152. https://doi.org/10.2308/HORIZONS-19-010

Kranacher, M.-J., Riley, R. A., & Wells, J. T. (2020). *Forensic accounting and fraud examination*. Wiley. https://doi.org/10.1002/9781119372394

Levi, M., Doig, A., Gundur, R. V., & Wall, D. S. (2021). Cyber fraud and financial crime. *Crime, Law and Social Change, 75*(1), 1–20. https://doi.org/10.1007/s10611-020-09916-5

Ngoepe, M., & Ngulube, P. (2022). Digital forensics and fraud detection. *Records Management Journal, 32*(2), 123–140. https://doi.org/10.1108/RMJ-09-2020-0044

Ngoepe, M., & Ngulube, P. (2022). Digital forensics and fraud detection. *Records Management Journal, 32*(2), 123–140. https://doi.org/10.1108/RMJ-09-2020-0044

Volume 10, Issue 1, 2025
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

Nuryanto, U. W., & Basrowi. (2024). Sustainability-oriented collaboration and innovation in digital transformation. *Social Sciences & Humanities Open, 10*, 101100. https://doi.org/10.1016/j.ssaho.2024.101100

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, n71. https://doi.org/10.1136/bmj.n71

Putri, R. L., Hersugondo, H., Asnawi, R., Hanif, Z., Normal, I. N., Suprapto, S., Sinaini, L., Saputra, M. H., Krismawati, A., Yasing, A., & Basrowi, B. (2025). Strategic synergy: Artificial intelligence, organizational databases, and profitability enhancement with risk management as the mediator. *International Journal of Data and Network Science, 9*, 1051–1066. https://www.growingscience.com/ijds/Vol9/ijdns_2024_184.pdf

Rezaee, Z., & Wang, J. (2021). Relevance of forensic accounting in fraud detection. *Managerial Auditing Journal, 36*(3), 317–334. https://doi.org/10.1108/MAJ-07-2019-2359

Rezaee, Z., & Wang, J. (2021). Relevance of forensic accounting. *Managerial Auditing Journal, 36*(3), 317–334. https://doi.org/10.1108/MAJ-07-2019-2359

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Sukidin, S., Hudha, C., & Basrowi, B. (2025). Shaping democracy in Indonesia: The influence of multicultural attitudes and social media activity on participation in public discourse and attitudes toward democracy. *Social Sciences & Humanities Open, 11*, 101440. https://doi.org/10.1016/j.ssaho.2025.101440

Suseno, B. D. (2022). Industrial revolution 4.0 as a strategic issue of higher education. *International Journal of Scientific Research and Management, 10*(2), 3045–3051. https://doi.org/10.18535/ijsrm/v10i2.em05

Suseno, B. D. (2023). Adaptive governance and sustainability strategy in educational institutions. *International Journal of Professional Business Review, 8*(6), 1–12. https://doi.org/10.26668/businessreview/2023.v8i6.1542

Suseno, B. D., & Yusuf, M. (2024). Digital transformation and governance adaptability in strengthening organizational sustainability. *International Journal of Professional Business Review, 9*(2), 1–15. https://doi.org/10.26668/businessreview/2024.v9i2.2150

Vousinas, G. L. (2019). Advancing theory of fraud: Fraud Diamond. *Journal of Financial Crime, 26*(1), 372–381. https://doi.org/10.1108/JFC-11-2017-0118