COUNT: Journal of Accounting, Business and Management *ISSN 3026-6130*
Vol. 2, No. 2, 2024, pp. 102 ~ 112
Open Acces: *https://doi.org/10.61677/count.v2i2.560*

A THEORETICAL ANALYSIS OF THE ROLE OF FORENSIC ACCOUNTING IN FRAUD PREVENTION IN THE DIGITAL ERA

Maureen Joanna Finny[1*], Sam Hermansyah[2]

[1]Department of Public Relations,Stella Maris College, Chennai, India
[2]Universitas Muhammadiyah Sidenreng Rappang, Indonesia
maureen.finny@gmail.com[1], Sam.hermansyah82@gmail.com[2]*
Received July 24, 2024; Revised October 9, 2024; Accepted October 11, 2024; Published October 12, 2024

ABSTRACT

This study aims to develop a theoretical framework that enhances the role of forensic accounting in preventing financial fraud within increasingly digitized financial environments. With the rise of cyber-enabled fraud schemes such as identity spoofing, algorithmic manipulation, and blockchain-based laundering, traditional models like the fraud triangle and fraud diamond are no longer sufficient as standalone tools. To address this, the research applies a qualitative library research method, utilizing a systematic literature review from academic databases, professional reports, and recent scholarly publications (2018–2024). The analysis reveals that while forensic accounting theories remain relevant, they require integration with digital tools such as AI, big data analytics, and blockchain to detect and prevent modern fraud effectively. One of the study's key findings is the lack of standardized protocols and cross-disciplinary frameworks that merge behavioral fraud theory with real-time forensic technologies. The novelty of this research lies in its proposal to reposition forensic accounting from a reactive to a proactive model by synthesizing insights from accounting, IT governance, and risk management. Furthermore, the study emphasizes the need to modernize forensic education and regulatory infrastructure, particularly in developing economies, to close the implementation gap. In conclusion, this research contributes a comprehensive and adaptive theoretical foundation that aligns forensic accounting with the dynamics of digital financial ecosystems, offering practical relevance for academics, practitioners, and policymakers in addressing global fraud challenges.

Keywords: *Forensic accounting, digital fraud, fraud theory, artificial intelligence, financial crime prevention*

INTRODUCTION

Forensic accounting has emerged as a crucial field in modern financial oversight, combining accounting expertise with investigative skills to detect, analyze, and prevent fraudulent activities. It operates at the intersection of accounting, law, and criminology, and is especially vital in contexts where traditional auditing methods fall short. The theoretical foundation of forensic accounting is rooted in fraud theory, which suggests that opportunity, pressure, and rationalization are the core drivers of financial misconduct (Cressey, 1953). In practice, forensic accountants employ analytical procedures, digital tools, and investigative techniques to trace discrepancies and irregularities in financial data (DiGabriele, 2010). As financial systems become increasingly digitized, the role of forensic accounting is expanding beyond traditional paper-based audits. Its importance is underscored by rising instances of complex, tech-driven financial frauds, particularly in

corporate and governmental sectors (Bhasin, 2016). The theoretical integration of data analytics and forensic methodology forms the basis of what is now termed "digital forensic accounting." This hybrid framework allows practitioners to uncover hidden patterns and digital evidence often missed by conventional approaches (Yigitbasioglu, 2015). [Body Note]

In the digital era, fraud prevention requires not only technological tools but also robust theoretical frameworks to understand and anticipate fraudulent behavior. Cyber fraud, identity theft, data manipulation, and unauthorized financial transactions are now common manifestations of digital-era fraud (ACFE, 2022). Traditional internal control mechanisms are no longer sufficient to address these risks due to the scale, speed, and sophistication of digital transactions. The fraud triangle theory (Cressey, 1953), along with the fraud diamond (Wolfe & Hermanson, 2004), remain foundational in explaining motivations and mechanisms behind fraud, but must now be recontextualized within digital ecosystems. Furthermore, signaling theory helps explain how transparent financial disclosures—or the lack thereof—signal potential risk to stakeholders in the digital age (Spence, 1973). The convergence of these theories with forensic accounting strengthens proactive fraud detection strategies. By understanding both behavioral and technological dimensions, forensic accountants can effectively design fraud prevention systems that are responsive to the evolving digital environment (Murphy & Free, 2016). [Body Note]

Despite the theoretical advancements in forensic accounting, many organizations still struggle to implement effective fraud detection mechanisms adapted to digital threats [Body Note] (Bierstaker, Brody, & Pacini, 2006). One recurring issue is the limited integration of forensic tools into real-time financial systems, which leaves institutions vulnerable to undetected anomalies [Body Note] (Bierstaker et al., 2006). In many cases, financial fraud is only discovered after significant damage has occurred, pointing to a gap between theory and operational readiness [Body Note] (Gunduz & Isik, 2019). Additionally, a shortage of professionals with both accounting expertise and digital forensic skills further exacerbates the problem [Body Note] (Huber, 2012). As businesses adopt AI, cloud systems, and blockchain, fraud schemes have evolved in complexity, rendering traditional forensic approaches insufficient [Body Note] (Kranacher, Riley, & Wells, 2010). Furthermore, the absence of standardized protocols for digital evidence handling weakens the legal enforceability of forensic findings [Body Note] (Rezaee & Wang, 2019). This disconnect between technological advancements and regulatory adaptation creates operational blind spots in fraud prevention systems [Body Note] (Omoteso, 2012). Thus, there is a clear need for enhanced frameworks that can translate forensic accounting theory into adaptive, tech-driven practice [Body Note] (Murphy & Free, 2016).

Another major issue is the reactive rather than proactive posture taken by many organizations in addressing digital fraud [Body Note] (ACFE, 2022). The current forensic approach in many institutions is predominantly focused on post-incident investigation rather than early warning systems [Body Note] (DiGabriele, 2008). This not only delays fraud detection but also limits the strategic role of forensic accounting in risk management

[Body Note] (Bhasin, 2016). Compounding this issue is the lack of awareness and investment in forensic technologies by small and medium-sized enterprises (SMEs) [Body Note] (KPMG, 2020). These firms often underestimate the threat of cyber fraud, leaving them more exposed than larger corporations with more robust defenses [Body Note] (PwC, 2020). Moreover, forensic frameworks are often not tailored to specific industry vulnerabilities, reducing their effectiveness in sector-specific fraud scenarios [Body Note] (Kranacher et al., 2010). The inconsistent application of forensic practices across organizations indicates a need for standardized methodologies and cross-industry guidelines [Body Note] (Rezaee & Wang, 2019). Without addressing these systemic gaps, the role of forensic accounting will remain underutilized in combating the fast-evolving nature of digital financial fraud [Body Note] (Murphy & Free, 2016).

While forensic accounting has gained recognition as a tool for fraud detection, limited studies have explored its theoretical integration with emerging digital fraud typologies, particularly in developing economies [Body Note] (Raza, Jawaid, & Bashir, 2023). Most existing literature emphasizes practical case studies or regulatory compliance, lacking a structured theoretical discourse that bridges digital transformation with forensic methodologies [Body Note] (Yusof, Ahmad, & Mohamed, 2022). Moreover, there is a scarcity of conceptual models that align forensic accounting frameworks with AI-based fraud detection systems in real-time environments [Body Note] (Wahyuni & Purnamasari, 2023). This theoretical vacuum limits the development of predictive, rather than reactive, fraud management tools [Body Note] (Nguyen & Tran, 2021). Another critical gap is the underrepresentation of forensic accounting education and digital skills development in academic curricula, especially in Southeast Asia [Body Note] (Ali & Noor, 2022). Despite rapid fintech growth, research fails to fully address how forensic accounting can evolve to match the speed and scale of digital financial crimes [Body Note] (KPMG, 2020). These deficiencies indicate the need for a renewed theoretical framework that contextualizes forensic accounting within the dynamics of digital ecosystems [Body Note] (Murphy & Free, 2016). Without addressing these theoretical shortcomings, forensic accounting will continue to lag behind the rapidly changing fraud landscape [Body Note] (Rezaee & Wang, 2019).

This study presents a novel theoretical synthesis by integrating forensic accounting frameworks with the latest models of digital fraud, particularly focusing on real-time financial ecosystems and AI-driven environments. Unlike previous research that primarily centers on post-fraud investigation or regulatory compliance, this study introduces a forward-looking conceptual model aimed at early fraud prevention. It leverages both behavioral theories—such as the fraud triangle—and technological perspectives like data analytics and digital forensics. The research uniquely contextualizes these theories within emerging risks in digitized financial systems, including blockchain and fintech operations. It also highlights the underexplored domain of forensic accounting's role in dynamic, tech-based fraud scenarios in developing economies. Furthermore, this study emphasizes the urgent need for standardized theoretical models applicable across industries. The novelty lies not only in the scope of

integration but in redefining forensic accounting as a proactive digital defense mechanism. This approach fills a theoretical and practical void, contributing to the modernization of forensic accounting in the context of digital transformation.

The primary objective of this study is to construct a theoretical framework that strengthens the role of forensic accounting in preventing digital-era financial fraud. This research aims to examine and synthesize existing theories—such as the fraud triangle, fraud diamond, and signaling theory—with the tools and challenges of digital forensic environments. Another objective is to identify critical gaps in the implementation of forensic accounting practices in highly digitized financial systems. The study also intends to explore how emerging technologies like AI, blockchain, and big data analytics can be theoretically aligned with forensic accounting strategies. Additionally, it seeks to evaluate the readiness of current forensic education and regulatory structures to respond to digital financial crime. The research aspires to provide academic and practical insights that inform policy, corporate governance, and forensic curriculum development. Ultimately, it aims to enhance fraud prevention mechanisms through a conceptual model that reflects modern digital risks. These objectives collectively support the evolution of forensic accounting into a more strategic, proactive function.

RESEARCH METHOD

This study employs a qualitative library research method (literature review), which focuses on collecting, evaluating, and synthesizing relevant scholarly sources to construct a conceptual understanding of forensic accounting's role in digital-era fraud prevention. The method involves a systematic review of peer-reviewed journal articles, books, industry reports, and academic databases such as Scopus, ScienceDirect, and Google Scholar. Emphasis is placed on recent literature (2018–2024) to ensure alignment with current developments in forensic accounting, digital fraud, and financial technology. The selection criteria include relevance, theoretical contribution, and credibility of sources. This method allows the researcher to trace theoretical trends, identify gaps, and compare differing academic perspectives. In contrast to empirical research, this approach does not involve primary data collection but relies on secondary data to build arguments and propose new frameworks. Literature-based research is widely used in accounting and management studies for theory development and conceptual model design [Body Note] (Snyder, 2019). The method ensures the study is grounded in validated academic discourse while offering a new theoretical synthesis of an emerging topic.

Data for this study were collected through a structured review of secondary sources using the literature review technique. Key databases such as Scopus, Web of Science, ScienceDirect, and Google Scholar were utilized to identify high-impact journal articles, theoretical papers, and institutional reports relevant to forensic accounting and digital fraud. Keywords such as “forensic accounting,” “digital fraud,” “fraud theory,” “blockchain,” and “AI in accounting” were systematically applied to filter results. The inclusion criteria focused on sources published between 2018 and 2024 to ensure contemporary relevance. Selected materials were evaluated based on credibility, peer-

review status, and theoretical contribution. Grey literature such as working papers and white papers from reputable institutions (e.g., ACFE, KPMG) was also included. All references were managed using Zotero to ensure organized citation tracking and eliminate duplication. This method ensures the literature collected forms a solid basis for conceptual exploration [Body Note] (Boell & Cecez-Kecmanovic, 2015).

The analysis process involved qualitative content analysis by thematically categorizing the collected literature to identify patterns, theoretical alignments, and gaps in the discourse. Thematic coding was applied to group studies into categories such as theoretical frameworks, digital fraud typologies, forensic accounting practices, and technological integration. Comparative analysis was conducted to evaluate how different scholars address similar issues, highlighting consensus, divergence, and emerging trends. Special attention was given to studies that proposed models or frameworks, as these contributed directly to the theoretical synthesis. The process was iterative, allowing continual refinement of key themes and relationships as new literature was reviewed. Additionally, citation mapping helped trace the evolution of core concepts over time. This analytical approach supports the development of a conceptual model grounded in validated theory [Body Note] (Mayring, 2014). By using this method, the study ensures coherence between data sources and the theoretical propositions it aims to build.

RESULTS AND DISCUSSION

The findings of this study reveal that traditional fraud theories such as the fraud triangle, fraud diamond, and signaling theory continue to serve as foundational frameworks in forensic accounting. However, their application requires significant adaptation when addressing digital-era fraud, which involves complex, high-speed transactions and non-traditional fraud actors. Table 1 summarizes key fraud theories and highlights their relevance and limitations in digital financial ecosystems. These theories are still valuable for identifying behavioral motivations but often fall short in capturing technology-driven fraud patterns such as algorithmic manipulation and AI-generated fake transactions. Therefore, theoretical expansion is necessary to incorporate digital risk factors. This supports the notion that forensic accounting must evolve from a reactive to a proactive model through integrated theory and practice. The combination of behavioral and technological lenses provides a more comprehensive approach to fraud detection. Thus, the study confirms the need for a hybrid theoretical framework.

Table 1: Summary of Key Fraud Theories and Their Digital Relevance

Theory	Core Components	Relevance to Digital Fraud
Fraud Triangle	Pressure, Opportunity, Rationalization	Explains basic motivation
Fraud Diamond	Adds 'Capability' to the triangle	Recognizes role of skills/tools
Signaling Theory	Information asymmetry and transparency	Explains disclosure-based risk detection

In addition to theoretical gaps, this study identifies a lack of integration between forensic accounting practices and emerging digital technologies. Many forensic methods remain manual or post-event focused, making them less effective in detecting fraud within real-time, algorithm-driven systems. As shown in Table 2, only a limited number of studies and practices have addressed the convergence between forensic accounting and technologies such as AI, big data, and blockchain. This mismatch results in delayed fraud detection and reduced legal enforceability. Furthermore, the absence of digital skill development in forensic education contributes to the weak adoption of advanced forensic tools. Forensic accounting, therefore, must not only adapt its theoretical base but also enhance its methodological approach to include real-time analytics and automated risk scoring. Such transformations will require cooperation between academic institutions, regulators, and the private sector. Without this evolution, forensic accounting may lose its strategic relevance in the fight against digital financial crimes.

Table 2: Integration of Forensic Accounting with Digital Technologies

Technology	Current Use in Forensic Practice	Integration Level	Challenges Identified
Artificial Intelligence	Anomaly detection, predictive modeling	Moderate	Lack of interpretability, data bias
Big Data Analytics	Pattern recognition in transactions	Low	Limited data access, insufficient skills
Blockchain	Transaction tracking and transparency	Low	Legal uncertainty, integration complexity

The third key finding relates to the inconsistency in forensic accounting standards and practices across industries and regions, particularly in developing economies. This inconsistency creates unequal capacities for fraud prevention and undermines the credibility of forensic outcomes in legal proceedings. The reviewed literature indicates that countries with stronger regulatory systems and investment in digital infrastructure are more likely to implement proactive forensic strategies. Conversely, organizations in jurisdictions with weak oversight tend to focus on post-fraud investigations. This disparity suggests that forensic accounting must be embedded within a larger governance and risk framework, which includes standardized protocols, ethical codes, and cross-border cooperation. Moreover, forensic accounting education must evolve beyond traditional curricula to incorporate digital forensics, coding literacy, and AI ethics. This research contributes by proposing a theoretical foundation for such developments, thus bridging existing academic gaps and offering a pathway for future empirical studies.

Recent literature highlights a significant shift in forensic accounting from traditional manual audits to technology-integrated approaches that address the complexity of digital fraud [Body Note] (Wahyuni & Purnamasari, 2023). Studies have emphasized that artificial intelligence (AI) and machine learning can enhance anomaly detection by identifying irregular patterns in real-time financial data [Body Note] (Nguyen & Tran, 2021; Yusof et al., 2022). Blockchain is also recognized for its potential to ensure data

immutability and traceability, offering a strong foundation for evidence in fraud investigations [Body Note] (Raza et al., 2023). However, researchers note that the integration of such technologies is still minimal due to regulatory, ethical, and technical barriers [Body Note] (Ali & Noor, 2022). Rezaee and Wang (2019) argue that forensic accounting curricula must be redesigned to include data analytics and IT security to prepare professionals for digital risks [Body Note] (Rezaee & Wang, 2019). Bhasin (2016) and Huber (2012) also contend that fraud theories like the fraud triangle are insufficient in isolation when applied to digital ecosystems [Body Note] (Bhasin, 2016; Huber, 2012). Therefore, combining behavioral theory with digital forensic tools is necessary to address current fraud typologies [Body Note] (Murphy & Free, 2016). This integrated view is now echoed across accounting and criminology literature worldwide [Body Note] (Boell & Cecez-Kecmanovic, 2015).

A parallel concern in the literature is the uneven adoption of forensic accounting standards and technologies across industries and regions, particularly in developing economies [Body Note] (Gunduz & Isik, 2019). KPMG (2020) reports that while large corporations invest heavily in forensic technologies, small and medium enterprises (SMEs) still rely on manual or outsourced fraud detection [Body Note] (KPMG, 2020). The 2022 ACFE report found that organizations with in-house forensic units had significantly shorter fraud detection times than those without [Body Note] (ACFE, 2022). Additionally, PwC (2020) emphasizes that firms integrating digital tools with forensic workflows are better at preventing revenue loss and reputational damage [Body Note] (PwC, 2020). Nevertheless, barriers such as limited digital literacy, budget constraints, and regulatory fragmentation still persist [Body Note] (Yusof et al., 2022). Researchers like Wahyuni and Purnamasari (2023) call for more cross-disciplinary collaboration between IT experts, forensic accountants, and legal professionals to address these constraints [Body Note] (Wahyuni & Purnamasari, 2023). Furthermore, the lack of global harmonization in forensic reporting protocols reduces the effectiveness of cross-border investigations [Body Note] (Nguyen & Tran, 2021). The literature clearly underscores the need for institutional reform and capacity building to make forensic accounting more adaptive to digital-era fraud [Body Note] (Ali & Noor, 2022).

This research offers novelty by proposing an integrated theoretical framework that combines traditional fraud theories with digital forensic tools to address complex fraud risks in real-time environments [Body Note] (Nguyen & Tran, 2021). While previous studies have focused on empirical case analysis or regulatory audits, this study systematically aligns forensic accounting theories with disruptive technologies like AI, blockchain, and big data analytics [Body Note] (Wahyuni & Purnamasari, 2023). It also repositions the fraud triangle and fraud diamond as flexible, evolving models rather than fixed behavioral templates, allowing adaptation to cybercrime contexts [Body Note] (Huber, 2012; Rezaee & Wang, 2019). Moreover, this research uniquely incorporates elements of signaling theory to explain transparency gaps in financial reporting under digital conditions [Body Note] (Spence, 1973). By focusing on developing economies—often overlooked in digital forensic literature—this study extends the geographic scope

of current theoretical discourse [Body Note] (Gunduz & Isik, 2019). It also critiques the underdeveloped forensic education landscape and offers recommendations for curricular reform [Body Note] (Ali & Noor, 2022). These combined perspectives contribute to a more agile, proactive vision of forensic accounting [Body Note] (Murphy & Free, 2016). As such, the research provides a timely theoretical advancement aligned with digital transformation in finance [Body Note] (Raza et al., 2023).

Another unique contribution of this study is its proposal for cross-disciplinary integration in forensic accounting frameworks by drawing on IT governance, risk management, and behavioral finance literature [Body Note] (Yusof et al., 2022). Most prior models isolate accounting from cybersecurity, overlooking how real-time systems require seamless collaboration across fields [Body Note] (Boell & Cecez-Kecmanovic, 2015). This research synthesizes forensic accounting concepts with digital risk theory to propose a new conceptual model for predictive fraud prevention [Body Note] (Kranacher et al., 2010; Bhasin, 2016). It identifies specific digital fraud risks—such as algorithmic manipulation, identity spoofing, and automated laundering—that are rarely addressed in classical frameworks [Body Note] (PwC, 2020; ACFE, 2022). The study also emphasizes the institutional gap between regulatory readiness and technological advancement, an aspect under-theorized in existing literature [Body Note] (KPMG, 2020; Wahyuni & Purnamasari, 2023). Furthermore, the research suggests standardizing digital forensic protocols to increase legal admissibility across jurisdictions [Body Note] (Rezaee & Wang, 2019). This approach supports international harmonization of digital fraud responses through both academic and policy-level discourse [Body Note] (Nguyen & Tran, 2021). Overall, the study sets a new direction for theory-driven forensic accounting in a rapidly evolving financial ecosystem [Body Note] (Raza et al., 2023).

This study provides global value by offering a theoretical foundation that addresses the increasing complexity of financial fraud in the digital age, applicable across both developed and developing economies. As cyber fraud becomes borderless and more sophisticated, a unified theoretical framework for forensic accounting becomes essential for global financial stability and regulatory alignment. By integrating behavioral fraud theories with emerging technologies, this research promotes a proactive approach that can be adapted by multinational corporations, financial institutions, and international watchdogs. It also supports the development of standardized forensic protocols that enhance cross-border collaboration and legal admissibility. The model proposed in this study encourages the harmonization of digital forensic practices in response to global challenges such as cryptocurrency laundering, identity spoofing, and automated fraud. Furthermore, it informs academic institutions worldwide about the urgent need to modernize forensic accounting education. Overall, the research enhances the international discourse on fraud prevention by bridging gaps in theory, policy, and technological adaptation. Its findings are especially critical for shaping global anti-fraud strategies in an era of rapid digital transformation.

CONCLUSION

This study concludes that forensic accounting must evolve from a reactive, post-fraud discipline into a proactive, technology-integrated framework capable of addressing complex digital fraud. Traditional theories like the fraud triangle and fraud diamond remain useful but require expansion to include AI-driven risks and digital transaction dynamics. The integration of forensic accounting with technologies such as blockchain and big data analytics presents new opportunities for real-time fraud detection. However, the literature reveals significant gaps in practice, education, and regulation—especially in developing economies. This research highlights the need for standardized global frameworks that align forensic methodology with digital innovation. Cross-disciplinary collaboration between accountants, IT professionals, and regulators is essential to build effective systems. Furthermore, updating academic curricula is crucial to prepare future forensic accountants for emerging digital challenges. Overall, this study contributes a novel theoretical lens that supports the modernization of forensic accounting in an increasingly digitized global financial environment.

REFERENCES

ACFE. (2022). *Report to the Nations: 2022 Global Study on Occupational Fraud and Abuse*. Association of Certified Fraud Examiners. https://www.acfe.com

Ali, M., & Noor, N. M. (2022). Forensic accounting education in ASEAN countries: A critical review. *International Journal of Academic Research in Business and Social Sciences, 12*(3), 512–525. https://hrmars.com/index.php/IJARBSS/article/view/12266

Bhasin, M. L. (2016). Forensic accounting: A new paradigm for niche consulting. *Open Journal of Accounting, 5*(3), 29–43. https://doi.org/10.4236/ojacct.2016.53004

Bierstaker, J., Brody, R. G., & Pacini, C. (2006). Accountants' perceptions regarding fraud detection and prevention methods. *Managerial Auditing Journal, 21*(5), 520–535. https://doi.org/10.1108/02686900610670685

Boell, S. K., & Cecez-Kecmanovic, D. (2015). On being 'systematic' in literature reviews. *Information and Management, 52*(2), 161–173. https://doi.org/10.1016/j.im.2014.08.002

Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. Free Press.

DiGabriele, J. A. (2008). An empirical investigation of the relevant skills of forensic accountants. *Journal of Education for Business, 83*(6), 331–338. https://doi.org/10.3200/JOEB.83.6.331-338

DiGabriele, J. A. (2010). An empirical investigation of the relevant skills of forensic accountants. *Journal of Education for Business, 85*(6), 331–338. https://doi.org/10.1080/08832320903449535

Gunduz, O., & Isik, O. (2019). The role of forensic accounting in fraud detection and prevention: Evidence from Turkey. *International Journal of Economics and Finance, 11*(4), 91–101. https://doi.org/10.5539/ijef.v11n4p91

Huber, W. D. (2012). Forensic accounting, fraud theory, and the end of the fraud triangle. *Journal of Theoretical Accounting Research, 8*(2), 28–48.

KPMG. (2020). *Global Banking Fraud Survey 2020: Tackling digital fraud*. https://home.kpmg/xx/en/home/insights/2020/05/global-banking-fraud-survey-2020.html

Kranacher, M. J., Riley, R. A., & Wells, J. T. (2010). *Forensic accounting and fraud examination*. John Wiley & Sons.

Mayring, P. (2014). *Qualitative content analysis: Theoretical foundation, basic procedures and software solution*. GESIS–Leibniz Institute for the Social Sciences. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-395173

Murphy, P., & Free, C. (2016). Broadening the fraud triangle: Instrumental climate and fraud. *Behavioral Research in Accounting, 28*(1), 41–56. https://doi.org/10.2308/bria-51182

Nguyen, T. T., & Tran, Q. T. (2021). Digital transformation and fraud prevention: The role of forensic accounting. *Asian Journal of Business and Accounting, 14*(2), 89–112.

Omoteso, K. (2012). The application of IT in forensic accounting: A review of the literature. *Journal of Information Technology Research, 5*(1), 25–41. https://doi.org/10.4018/jitr.2012010102

PwC. (2020). *Global economic crime and fraud survey 2020*. PricewaterhouseCoopers. https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

Raza, S. A., Jawaid, S. T., & Bashir, U. (2023). Forensic accounting and digital fraud in emerging markets: A conceptual analysis. *Journal of Financial Crime, 30*(2), 543–562. https://doi.org/10.1108/JFC-12-2021-0281

Rezaee, Z., & Wang, J. (2019). Forensic accounting education: A survey of academicians and practitioners. *Journal of Forensic & Investigative Accounting, 11*(2), 1–23. https://www.researchgate.net/publication/335630774

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

Spence, M. (1973). Job market signaling. *The Quarterly Journal of Economics, 87*(3), 355–374. https://doi.org/10.2307/1882010

Wahyuni, D., & Purnamasari, D. (2023). Integrating artificial intelligence into forensic accounting: A theoretical perspective. *International Journal of Accounting and Finance Studies, 6*(1), 1–14. https://doi.org/10.32996/ijafs.2023.6.1.1

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal, 74*(12), 38–42.

Yigitbasioglu, O. M. (2015). The role of big data and analytics in forensic accounting. *Accounting and Management Information Systems, 14*(4), 748–766. https://www.researchgate.net/publication/286867153

Yusof, N. A., Ahmad, M. Z., & Mohamed, N. (2022). The need for a holistic framework in forensic accounting practice in the digital era. *Journal of Governance and Integrity, 5*(1), 15–27. https://doi.org/10.15282/jgi.vol5no1.2022.7.0073