Journal of Business Crime

e-ISSN: 3090-4412

Vol 01(2) 2025 p. 82-93

Corresponding author:
Vania Elifia Putri Sofianto
Email : vaniaelif06@gmail.com

Received 16 September 2025;
Accepted 30 September 2025;
Published 30 September 2025.

Conflict of interest statement:
Author(s) reported no conflict of interest

DOI: http://doi.org/10.70764/gdpu-jbc.2025.1(2)-08

FORENSIC ACCOUNTING IN THE DIGITAL ERA: DETECTING AND PREVENTING FINANCIAL CRIME IN HIGH-GROWTH START-UPS

Vania Elifia Putri Sofianto[1]

[1]Universitas Islam Nahdlatul Ulama Jepara, Indonesia

ABSTRACT

Objective: This study aims to evaluate the role and effectiveness of modern forensic accounting technology—particularly that based on artificial intelligence (AI) and data analytics—in detecting and preventing financial crime (fraud) in rapidly growing digital start-up companies.

Research Design & Methods: This study uses a descriptive qualitative approach and case studies. The analysis technique is conducted through content analysis to identify patterns of internal control weaknesses and the use of forensic tools in financial reporting systems.

Findings: The results of the study show that fraud in start-ups is largely triggered by weak internal control systems, the lack of separation between personal and company funds, and the non-involvement of digital audit technology. Transaction anomaly patterns such as undocumented fund transfers, GMV manipulation, and project documentation engineering were found to be key indicators of fraud. Conversely, the implementation of digital forensic tools such as IDEA, FTK Imager, Tableau TD3, and machine learning algorithms has proven effective in detecting anomalies early on and strengthening oversight systems.

Implications and Recommendations: This research's implications include the urgent need for start-ups to integrate digital audits into their financial systems from the outset. Regulators need to formulate more adaptive digital oversight policies, while investors and venture capitalists are advised to make forensic audits part of their due diligence process before funding.

Contribution & Value Added: This study provides theoretical and practical contributions to developing technology-based forensic accounting for the digital start-up sector. This research expands the literature on preventing financial crime in the digital age.

Keywords: Forensic Accounting, Start-Up, Digital Fraud, Internal Control.

JEL codes: M41, K42, G32
Article type: research paper

INTRODUCTION

The surge in investment in start-ups in Asia has shown a significant trend in recent years. In 2021, the region recorded a record funding of US$25.7 billion, more than double the total from the previous year. The acceleration of digitalization drove this sharp increase due to the COVID-19 pandemic and growing global investor interest in the region's digital market potential (Rogozhin, 2022). The main driver of this trend is the rapid development of Southeast Asia's digital economy,

marked by the emergence of many technology companies valued at more than one billion US dollars (unicorns), particularly in the e-commerce, financial technology (fintech), and logistics sectors (Beschorner, 2021).

Indonesia, in particular, has played a major role in this growth. The surge in the number of digital start-ups in the country has been driven by rapid growth in internet users, government initiatives such as the 1000 Digital Start-ups Movement, and increasingly open access to funding from venture capitalists. Indonesian start-ups have also become major contributors to the overall digital ecosystem in Southeast Asia (Judijanto, 2024). Meanwhile, increased involvement from venture capital and private equity has strengthened the funding structure in the region, positioning Southeast Asia as a new hub for digital economic growth at the global level (Liu, 2024).

However, behind this growth lies a significant phenomenon of financial fraud. As a result of rapid digital economic growth and rampant investment in start-ups in Southeast Asia, serious challenges have emerged about financial integrity and operational transparency. Several major global scandals serve as important lessons relevant to this context. One such case is the Wirecard scandal in Germany. This digital payment company came under international scrutiny in 2020 after revealing that €1.9 billion in funds listed in its financial statements had never existed. The scandal was caused by weak internal oversight systems, financial statement manipulation, and the failure of external audits to detect the fraud early on (Jo et al., 2021; Teichmann et al., 2024). This incident highlights the dangers of asymmetric technology, where fintech companies' digital innovations are developing much faster than regulators' ability to conduct adequate supervision (Zeranski and Sancak, 2020).

The Theranos case in the United States is another example of governance and oversight failures in the tech start-up world. The company claimed it could perform various blood tests using just a single drop of blood, but it eventually came to light that its technology did not work. The company's founder, Elizabeth Holmes, and her team were found to have falsified test results and misled investors and regulators, resulting in losses exceeding 700 million US dollars and a prison sentence for Holmes (Griffin, 2022; Williams, 2022). This case shows how personal branding and technological hype can mask a product's flaws.

Meanwhile, in Southeast Asia, although there have been no cases on the scale of Wirecard or Theranos, several startups have also been embroiled in financial scandals, particularly those related to valuation manipulation and misleading financial reporting. The phenomena of overvaluation, lack of transparency, and dependence on short-term investments from venture capital are the main risk factors that can trigger fraud in the regional startup ecosystem (Liu, 2024). In Indonesia, weaknesses in the supervisory system and the absence of specific regulations governing digital start-ups create loopholes that open up the potential for fraud or business failure (Judijanto, 2024). Thus, despite the rapid growth of the digital ecosystem, the risk of fraud and financial crime in the startup world has become a crucial issue that requires greater attention from regulators, auditors, and other stakeholders.

The phenomenon of fraud in the digital startup ecosystem is inseparable from weak internal controls and extreme pressure from investors. Companies with poor internal controls are more susceptible to financial manipulation, especially when entities fail to establish effective oversight systems at the organizational level (Donelson et al., 2017; Tsai and Huang, 2021). When CEOs or startup founders have excessive self-confidence, this often leads to neglect of control systems that should serve as a foundation for transparency and accountability (Lee, 2015). Meanwhile, pressure from investors demanding rapid growth and aggressive financial targets has also encouraged management to engage in accounting manipulation to maintain funding flows, especially in the early stages of a company's growth (Saud et al., 2021). The combination of weak control systems and financial pressure makes the startup sector increasingly vulnerable to systemic fraud, especially in Southeast Asia.

Based on the background and phenomena described above, the research question in this study focuses on how modern forensic accounting technology can help detect and prevent financial crimes in the digital start-up environment. This question is important given the increasing number of fraud cases due to weak internal controls, investor pressure, and regulatory limitations in the digital start-up sector. Therefore, the purpose of this study is to evaluate the effectiveness of a digital technology-based forensic accounting approach in detecting early indications of fraud, as well as to develop a framework of recommendations that can be used as a guide for preventing financial crime in start-up companies, particularly in the context of the digital economy in Southeast Asia.

LITERATURE REVIEW

Forensic Accounting and Development

The term forensic accounting comes from the word forensic, which, according to Merriam Webster's Collegiate Dictionary in Tuanakotta (2010) has two meanings, namely (1) intended, used, or appropriate for court or judicial proceedings and public discussion and debate, (2) related or connected to the application of scientific knowledge or legal issues. Crumbley, quoted in Tuanakotta (2010), explains simply that forensic accounting is accounting that is accurate and appropriate for legal purposes. This can be interpreted as accounting that can withstand court proceedings or review processes based on legal or administrative aspects.

A major challenge for forensic accountants in computer forensics is the constant evolution of technology. With rapid technological advances, forensic experts must keep up with new digital devices, storage systems, and software applications. Forensic accountants face difficulties understanding the details of new technologies such as cloud computing, blockchain, artificial intelligence, and Internet of Things (IoT) devices (Kumar et al., 2021). Maintaining up-to-date knowledge and developing expertise in this field is essential for effectively analyzing and interpreting digital evidence in the context of financial fraud investigations (Dixon, 2005).

Using encryption and anonymization techniques like TOR and crypto transactions is a big challenge in computer forensics because it makes it hard to access data and track down the people involved. Forensic accountants must keep developing innovative ways to uncover financial fraud cases even as privacy and digital anonymity get stronger (Hou et al., 2020). Technological developments such as cloud computing and artificial intelligence (AI) have brought new challenges to forensic accounting practices. Cloud-based data storage and processing complicate the investigation process, particularly regarding legal access, evidence integrity, and cross-platform service analysis. Forensic accountants must have specialized skills and adequate tools to navigate complex digital environments (Yaqoob et al., 2019). Meanwhile, AI and machine learning (ML) offer the potential to automate data analysis and anomaly detection. Still, their use must be accompanied by human oversight to avoid bias and maintain the accuracy of investigation results (Iqbal and Abed Alharbi, 2019).

Financial Crime in Start-ups

According to the Association of Certified Fraud Examiners (ACFE 2013), fraud in the context of auditing is divided into three main categories known as "fraud groups". First, financial statement fraud is a form of fraud committed by management by manipulating information in financial statements to mislead users of those statements. These practices can take the form of financial fraud, such as overstating or understating cash, assets, income, and expenses to present a better financial condition than reality, for example, to obtain bank credit or avoid taxes. Additionally, there is non-financial fraud, such as forging internal or external documents. Second, there is the misuse of assets (misappropriation of assets), which includes fraud involving cash, inventory, other assets, and unauthorized expenditures or payments. Third, corruption, which is divided into several forms, namely: conflicts of interest that occur when individuals within a company have hidden interests in transactions; bribery, which is the giving of something of value to influence the policies or decisions of public officials; illegal gratuities, which are rewards for decisions that have already been made; and extortion, in which company employees demand payments from outside parties, as

opposed to bribery. These three forms of fraud are the main focus in efforts to detect and prevent fraud in forensic audits (Arianto et al., 2023).

Fraud is one of the risks that must be faced by various government agencies and private companies, including technology-based start-ups (Dinata and Nurbaiti, 2022). In 2019, McCormack, CFE reported that Theranos, a US-based unicorn startup in the medical device industry, had committed fraud using fake patents. Holmes, Theranos' CEO, had been using Theranos as her personal savings account. This was one of the forms of fraud committed by Holmes. In 2020, as reported by Wall Street, the Las Vegas-based startup NS8 was also found to have manipulated its financial reports by acknowledging fictitious revenue of 10 billion, another form of fraud. Meanwhile, in Indonesia, various startups have been reported as victims of fraud, including Tokopedia, which revealed that its employees were involved in fraudulent activities by exploiting a discount program intended for partner stores, which constitutes a violation (Kompas, 2018). Gleason et al. (2022) indicate that start-ups are breeding grounds for fraudulent behavior. This phenomenon arises from close collaboration between founders and investors, either implicitly or explicitly through agreements or, in certain cases, by following investor requests, which can encourage aggressive behavior in business (Dinata and Nurbaiti, 2022).

Fraud can be defined as a form of cheating that involves elements of deviation and deliberate unlawful acts (Arianto et al., 2023). However, before discussing forensic accounting further, it is important to understand the origins of fraud theory. The theory of fraud was first introduced by Cressey in 1972. However, as fraud practices evolved, the Fraud Pentagon theory emerged, an extension of the Fraud Triangle theory proposed by Cressey in 1972 and the Fraud Diamond theory proposed by Wolfe and Hermanson in 2004. In the Fraud Pentagon theory, there are several key elements, including: (1) Opportunity, (2) Pressure, (3) Rationalization, (4) Competence, and (5) Arrogance (Marks, 2012).

The control environment consists of an integrated internal control system, internal audit function, risk management, and compliance function, as well as environmental and social (E&S) risk management, subsidiary governance, and related components of external audit control involving the board of directors, management, and other personnel of a company (International Finance Corporation, 2023). This provides reasonable assurance regarding achieving objectives related to operations, reporting, and compliance, covering both the company and its subsidiaries. Reporting must comply with globally recognized disclosure standards (such as the upcoming IFRS Sustainability Disclosure Standards set by the International Sustainability Standards Board, the European Sustainability Reporting Standards, and the Global Reporting Initiative), and should reflect the company's sustainability disclosure resilience regarding internal control, governance, and risk management, internal audit, and compliance. The Institute of Internal Auditors' definition of control environment states that the control environment is "the foundation upon which an effective internal control system is built and operates within an organization that seeks to (1) achieve its strategic objectives, (2) provide reliable financial reporting to internal and external stakeholders, (3) operate its business efficiently and effectively, (4) comply with all applicable laws and regulations, and (5) protect its assets." There are five principles of internal control (Clarke, 2020).

1. Control Environment: This refers to the standards, structures, and processes that form the foundation for implementing internal control within an organization.
2. Risk Assessment： This is a systematic process used to identify (regularly), evaluate, and manage risks that could hinder the achievement of organizational objectives.
3. Control Activities： These are actions taken under management guidance, by organizational policies and procedures, aimed at reducing risks to the achievement of organizational objectives
4. Information and Communication： this involves disseminating information necessary to carry out control activities and explaining internal control responsibilities to internal and external personnel of the organization.
5. Monitoring Activities： These consist of ongoing assessment of the implementation and functioning of the internal audit's five (5) components.

METHODS

This study uses a descriptive qualitative method with a case study approach to describe the dynamics of fraud practices and the role of forensic accountants in the technology-based start-up ecosystem. Data was obtained through document analysis of company financial reports, external audit reports, and investigation documents from relevant regulators. For data processing, content analysis techniques were used to explore key themes related to internal control weaknesses, financial manipulation practices, and the use of forensic audit technology in detecting deviations. This approach enables researchers to build a contextual understanding of fraud patterns and evaluate the effectiveness of forensic accountants in preventing and addressing digital financial crimes.

RESULT AND DISCUSSION

Financial crimes in start-ups often stem from fundamental weaknesses in cash transaction monitoring systems and the lack of digital audit technology. Recent studies indicate that many startups, including those affiliated with public companies in Indonesia, lack adequate cash control mechanisms. The absence of functional separation in cash management, coupled with an organizational culture that tolerates deviations, enables corrupt practices to develop systematically within the organization (Dinata and Nurbaiti, 2022). Additionally, some start-ups use Gross Merchandise Value (GMV) as a key indicator of financial performance, even though GMV does not represent actual cash flow. In this case, GMV figures are manipulated to attract funding from investors, while there is no real-time cash verification system, making cash flow monitoring very weak (Prayuda et al., 2022).

Furthermore, the absence of technology-based audit tools exacerbates the situation. Digital audits such as data analytics-based systems, machine learning, and real-time automated transaction monitoring have proven capable of detecting patterns of manipulation and transaction anomalies that are difficult to find with manual approaches. Unfortunately, many start-ups caught up in fraud rely on conventional monitoring methods that are opaque and prone to manipulation. Studies in India and Indonesia have found that these companies have not integrated modern audit systems, such as ERP systems connected to cash audits, resulting in weak internal controls that are not adaptive to fraud risks (Dhamija and Nayyar, 2024; Mujati and Laily, 2024). Without reforming the financial oversight system and adopting digital audit technology, start-ups will remain vulnerable to various forms of financial fraud.

Comparison of Financial Statement Structure and Internal Control

A study of PT. G revealed that the company's financial reporting structure and internal control system were very weak, creating a significant opportunity for fraud (Dinata and Nurbaiti, 2022). The financial statements prepared by PT. G don't show what's going on with the business and are far from the transparency and accountability that a company managing public funds, especially from investors, should have. A fundamental weakness is the lack of clear separation between personal and company funds, which allows public investment funds to be easily transferred to the personal accounts of CEOs and capital owners without official documentation. This practice occurs routinely and is not formally recorded in the company's books. Moreover, such actions do not go through the appropriate legal process, such as approval by the General Meeting of Shareholders (GMS), as mandated by Article 71 of the Limited Liability Companies Act No. 40 of 2007, which requires that the distribution of profits or company funds must be based on a mutual agreement among shareholders.

Furthermore, in terms of internal control, PT. G shows very serious weaknesses. There is no multi-layered authorization system for each cash transaction, which should be a basic procedure in corporate financial management. In addition, the company does not utilize digital audit tools, such as cloud-based accounting software or data analytics, to verify cash flow and revenue in real time. The lack of an Enterprise Resource Planning (ERP) system also results in insufficient integration between financial reports, operational reporting, and project management. Instead, transaction

oversight is conducted manually and heavily relies on direct instructions from the CEO, without any objective validation mechanisms. Some employees admitted to receiving direct orders to transfer funds to specific accounts without access to documentation or official reasons for the transactions.

This situation indicates that internal controls at PT. G are permissive, poorly documented, and rely on personal trust rather than standardized systems and procedures. This creates ample opportunity for abuse of authority by management and makes fraud a systemic practice in the company's operations. In the long term, this weakness not only jeopardizes the company's sustainability but also undermines public trust in the startup-based investment ecosystem.

Identify anomaly patterns in transaction data

Field observations and interviews with informants revealed various patterns of transaction anomalies that strongly indicate fraud in the operations of PT. G. These patterns appear systematically and show that financial manipulation did not occur incidentally, but rather was part of a practice that had become ingrained in the company's management structure. The most striking anomaly is the regular transfer of funds to the personal accounts of the CEO and shareholders. This information was provided by Zainab, a finance staff member, who stated that every month, there is a large flow of funds from the company's account to personal accounts without any justification or valid documentation. This not only violates the principle of accountability, but also indicates the conversion of public funds into personal assets, which is a serious form of fraud.

The second anomaly was the discrepancy between the campaign promises and project results. The fundraising campaign run by PT. G often promised investors a profit share of up to 30%, with project values ranging from Rp700 million to Rp1 billion. However, the results fell far short of expectations: investors only received 7% of the profits or even suffered losses. Information from Soraya, a call center staff member, reveals that most projects are not implemented because the funds have already been depleted before being disbursed to partners. This indicates that campaign funds are being used in a manner inconsistent with their original purpose, highlighting the lack of transparency and weak reporting systems regarding fund usage.

Furthermore, there was also manipulation of project documentation, where photos of successful projects were reused to report on other projects that had failed. This action constitutes a form of non-financial information falsification that is highly misleading to investors, as visual information is used as a tool to maintain the image of project success. This shows that fraud is not only committed through financial records, but also through engineered visual communication strategies. The next pattern is the existence of internal gratification in the form of cash and luxurious facilities, such as expensive meals or the provision of silence compensation money. Based on information from Teguh and Andre, the CEO provided these facilities to employees with the aim of maintaining loyalty and silencing questions regarding irregularities in the use of funds. This created an informal control system that was not based on professional procedures, but rather on personal relationships and compliance based on short-term gains. This practice is dangerous because it creates false loyalty that perpetuates fraud.

Finally, it was also found that there was no synchronization between the financial reports and operational realization in the field. Project partners in the field complained about limited funds that severely hampered operations, such as the purchase of seeds, lighting equipment, and other technical needs. Meanwhile, internal financial reports portray the project as successful. This discrepancy indicates that company reports are not based on operational realities but are instead compiled to meet investor or stakeholder expectations without valid data as a foundation. Overall, these anomalous transaction patterns are not only early indicators of fraud, but also reveal weaknesses in internal control systems and poor management integrity, which allow manipulative practices to occur repeatedly and spread throughout the company's ecosystem. Detecting and preventing such patterns is essential in building sound and sustainable financial governance for start-ups.

The effectiveness of digital audit tools in early fraud detection

1. Improved Efficiency and Accuracy of Fraud Detection

Digital audit tools have been shown to significantly improve efficiency in detecting errors and fraud, especially in complex financial environments such as start-ups. These tools enable data tracing processes to be faster and more accurate than traditional methods that rely on manual sampling. In addition to speeding up the process, digital auditing tools also strengthen the professional skepticism of auditors, which is crucial in ensuring the objectivity and independence of assessments. This is particularly helpful in detecting transaction anomalies earlier. Another positive effect is the increased transparency of financial reports and investor confidence, especially if the implementation of these tools is accompanied by adequate regulatory frameworks and auditor training (Al Otaibi and Mohamed, 2024).

2. Digital Forensics: Case Study on the Use of Tools

In the context of digital forensics, technology-based audits have been used to deepen investigations into suspicious financial activities. Case studies involving the use of Table au TD3 and FTK Imager show that these tools are highly effective for accessing and analyzing metadata, tracking computer user activity, and identifying deviant transaction patterns in digital environments. These capabilities are crucial in addressing fraud cases that are not only cash-based but also involve non-cash assets and manipulation of internal digital documentation. As a result, digital forensic tools enable the audit process to be not only administrative but also investigative (Simeunovic et al., 2016).

3. Continuous Auditing: Effective but Dependent on System Design

Continuous auditing is an approach that enables real-time and continuous monitoring of transactions. Although this approach is theoretically very effective in expanding the scope of supervision, its effectiveness is highly dependent on the design of the reporting system used. A weak but fast notification system can actually be exploited by fraudsters to evade detection. Conversely, a robust continuous audit system with rapid feedback has proven effective in deterring fraudsters from committing fraud in the first place. Therefore, the success of continuous auditing lies in the quality of the technology and system integration (Gonzalez and Hoffman, 2018).

4. Digital Red Flag-Based Fraud Detection

Digital audit tools also provide the ability to build an early warning system integrated with red flag indicators. These indicators include early signs that point to potential fraud, such as sudden changes in transaction volume, financial ratio deviations, or unusual cash transactions. With this system, auditors can be proactive in detecting patterns of fraud, rather than merely reactive after an incident has occurred. The integration of red flags into digital audit systems makes the monitoring process more strategic and data-driven (Widyastuti and Ratnawati, 2023).

5. Data Analytics & Machine Learning: High Accuracy and Speed

The use of data analytics supported by machine learning technology such as random forest algorithms has been proven to significantly improve fraud detection accuracy, even reaching 93%. Case studies in digital banking transaction audits show that this system can process thousands of transactions per second, detect high-risk transactions based on historical patterns, and reduce audit time from weeks to just a few hours. This efficiency and speed make data analytics and AI essential pillars in responsive and adaptive digital financial surveillance systems (Kamdjoug et al., 2024).

Forensic accountants' role in tech-based start-ups

The absence of technology-based audit systems such as Enterprise Resource Planning (ERP), data analytics, or continuous auditing systems meant that financial oversight at PT. G was heavily reliant on individual authority, in this case, the CEO, without any objective and automated control mechanisms. When forensic accountants are actively involved in the monitoring and investigation process at PT. G, a number of technologies can be used to uncover and prevent fraudulent practices.

Technologies such as Tableau TD3 and FTK Imager, which are commonly used in digital forensics, can be utilized to access transaction metadata, track the computer activities of executives, and identify the manipulation of project documents or harvest photos used to cover up fictitious projects.

Additionally, the use of machine learning systems with algorithms such as random forest can assist forensic accountants in automatically analyzing thousands of transactions, detecting suspicious transaction patterns, and providing early warnings of unusual activities. Integrated red flag analytics systems within digital audit software can also flag financial ratio deviations, suspicious transaction volumes, and unusual cash usage. Beyond the role of forensic accountants as analysts and investigators, the implementation of digital audit technology is an absolute requirement for building a modern, transparent, and reliable financial oversight system. The absence of such technology has allowed fraud to develop systematically, whereas digital audit technology can serve as the primary tool for forensic accountants in creating a clean and accountable financial ecosystem for start-ups.

Table 1. Roles of Digital Forensic Tools in Fraud Detection

Additional Roles	Explanation	Technologies	Special Functions
Big Data analysis for fraud patterns	Forensic tools such as IDEA can trace millions of transactions and identify unusual patterns in income and expenditure, including round-tripping (Wells et al., 2007).	IDEA (Interactive Data Extraction and Analysis)	Detection of fictional income, duplication, and transactions between affiliates.
AI-based income manipulation detection	AI algorithms such as decision trees, random forests, and neural networks detect false revenue entries based on seasonal anomalies and transaction behavior (Mehta et al., 2022).	AI-based audit systems (e.g., MindBridge AI)	Identifying deviations in revenue trends from normal historical patterns.
Mapping of transactions between affiliated companies	Forensic software can visualize the relationships between entities in a startup group to detect circular transactions (Adelakun et al., 2024).	Network analytics tools, IDEA, ACL Analytics	Uncovering the potential for manipulation between companies with the same owners.
Forensics system, ERP, and cloud accounting	Forensic tools can extract user activity logs in cloud accounting systems (such as Xero, QuickBooks) and trace audit trail records (Simeunovic et al., 2016).	EnCase Forensic, FTK Imager, Tableau TD3	User audit, journal input history, and data deletion/modification log.
Continuous auditing-based automation	Automatic audit systems integrated with live transaction data can provide early warnings of risky activities (Mandala, 2024).	Power BI + RPA tools, real-time alert systems	Automatic monitoring without waiting for periodic audit cycles.

Forensic accountants play a strategic role in the technology-based start-up ecosystem, not only in detecting but also in preventing and comprehensively handling digital financial crimes. First, they are responsible for conducting in-depth fraud detection and investigation, including uncovering investor fund misuse, valuation manipulation, and financial statement fraud. This task requires an evidence-based approach and systematic forensic investigation (Nunn et al., 2011). Second, given that start-ups generally use cloud-based financial systems and digital transactions, forensic accountants are also required to master digital technology-based auditing. They utilize tools such as data analytics, cyber auditing, and anomaly detection algorithms to efficiently and in real-time trace patterns of irregular transactions (Basu, 2014).

Additionally, in situations of conflict or when fraud enters the legal realm, forensic accountants provide litigation support in the form of documentation, forensic financial analysis results, and even expert testimony that can be used as evidence in court (Boakye-Sarkodie, 2023).

More than just technical skills, they also rely on investigative soft skills such as communication skills, in-depth interviewing, and psychological understanding to uncover the motives and rationalizations of fraud perpetrators, especially in complex and rapidly changing digital organizations (Italia, 2012). Finally, forensic accountants play an important role in preventing fraud through the establishment of strong governance, including the development of internal control systems, organizational codes of ethics, and the development of risk-based early detection mechanisms. With this comprehensive role, they are key to maintaining the sustainability and integrity of start-ups in the digital age (Subash, 2015).

Strengthening internal control systems with a data analytics-based approach is a highly effective strategic measure for detecting and preventing fraud early on. Organizations that adopt technologies such as data mining, machine learning, and digital auditing are better able to monitor transactions in real time and identify suspicious patterns than manual systems, which tend to be reactive and slow to detect issues (Al Otaibi and Mohamed, 2024). Digital audits enable the automatic processing of thousands of transactions without human capacity limitations, thereby significantly increasing efficiency and accuracy in fraud detection (Al Otaibi and Mohamed, 2024). Additionally, algorithms such as random forest and unsupervised learning are capable of identifying anomalies even when there are no previously documented fraud patterns, making them highly relevant in addressing new and evolving fraud schemes (Adelakun et al., 2024).

The integration of artificial intelligence (AI) in forensic accounting has also been proven to strengthen the effectiveness of financial oversight, particularly in digital-based start-up environments. AI-based systems are capable of providing early warnings to management when transaction irregularities occur, enabling preventive measures to be taken immediately before fraud spreads (Mehta et al., 2022). Other research also shows that the use of big data and AI enables faster and more accurate detection of red flags in the context of high-frequency, high-risk digital retail transactions (Mandala, 2024).

CONCLUSION

This study concludes that fraud in technology-based start-up ecosystems, as reflected in the case of PT. G, stems from fundamental weaknesses in internal control systems, a lack of transparency in financial reporting, and minimal adoption of digital audit technology. Practices such as the commingling of personal and company funds, project data manipulation, and unauthorized fund transfers without proper documentation highlight the lax oversight and high reliance on individual authority, particularly the CEO. These conditions enable fraud to grow systematically and persist repeatedly without structural barriers. Additionally, various patterns of transaction anomalies identified, such as the use of fake GMV, visual manipulation, and internal gratification, could not be detected early because the company still relies on manual audit approaches that are unresponsive to the dynamics of digital transactions.

This finding also confirms that forensic accountants play a central role in detecting and handling digital financial crimes. Not only do they function as financial statement auditors, forensic accountants also act as investigators who utilize digital tools such as Tableau TD3, FTK Imager, and machine learning-based data analytics systems to automatically analyze thousands of transactions and identify hidden patterns of fraud. Approaches such as continuous auditing, red flag system-based monitoring, and ERP forensics integration enable real-time transaction tracking and strengthen internal oversight systems comprehensively. With their technical and investigative expertise, forensic accountants also play a role in restructuring internal controls, providing governance recommendations, and supporting litigation when fraud enters the legal domain.

The implications of this research are highly relevant to industry practices and future start-up governance policies. First, start-ups operating in the digital sector must make audit and forensic technology an integral part of their oversight systems from the outset of business growth. The use of big data, AI-based audit tools, and automated notification systems is no longer an optional extra, but a strategic necessity for maintaining financial integrity and building investor confidence. Second, regulators and policymakers need to formulate governance guidelines that encourage the

use of digital-based monitoring technologies and expand the role of forensic accountants in the startup industry. Third, education and training in forensic accounting should be focused on mastering technology and understanding the digital context, so that auditors are prepared to address fraud challenges in the era of financial transformation.

REFERENCES

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

Al Otaibi, D. F. K. , & Mohamed, E. (2024). The Role of Digital Auditing in Enhancing the Efficiency of Detecting Error and Financial Fraud. *Arab Journal for Literature and Humanities Studies., 8*(32), 633–658. https://doi.org/10.21608/ajahs.2024.365890

Arianto, B., Dinata, R. O., Ridhawati, R., Indarto, S. L., Syahrir, D. K., Rukmana, A. Y., Faisol, I. A., Yusran, M., & Andaningsih, I. R. (2023). Akuntansi forensik (M. . Diana Purnama Sari (ed.); 1st ed.). *GETPRESS INDONESIA*. https://perpustakaan.borobudur.ac.id/repository/0ad619e3044f10bf1187300e40795fb5.pdf

Association of Certified Fraud Examiners. (2013). Fraud Examiner Manual. *Austin:ACFE*.

Basu, S. (2014). Forensic Accounting in the Cyber World: A New Challenge for Accountants. *The Management Accountant, 49*(9), 18–21.

Beschorner, N. (2021). The digital economy in Southeast Asia: Emerging policy priorities and opportunities for regional collaboration. *In New Dimensions of Connectivity in the Asia-Pacific* (pp. 121–156). ANU Press. https://doi.org/10.22459/NDCAP.2021.04

Boakye-Sarkodie, R. (2023). Forensic Accounting: The Intersection of Law and Accounting. Asian *Journal of Business and Management, 11*(1). https://doi.org/10.24203/h6gz9r42

Clarke, I. (2020). Establishing an Effective Internal Control Environment. https://linfordco.com/. https://linfordco.com/blog/internal-control-environment/

Dhamija, S., & Nayyar, R. (2024). Corporate governance mishap in a startup: a case of GoMechanic. *Emerald Emerging Markets Case Studies, 14*(1), 1–25. https://doi.org/10.1108/EEMCS-05-2023-0179

Dinata, R. O., & Nurbaiti, A. (2022). Start-Up and Fraud Shenanigans: Case Study on Start-Ups Affiliated with Public Companies. *Asia Pacific Fraud Journal, 7*(1), 1. https://doi.org/10.21532/apfjournal.v7i1.247

Dixon, P. D. (2005). An overview of computer forensics. *IEEE Potentials, 24*(5), 7–10. https://doi.org/10.1109/MP.2005.1594001

Donelson, D. C., Ege, M. S., & McInnis, J. M. (2017). Internal Control Weaknesses and Financial Reporting Fraud. *Auditing: A Journal of Practice & Theory, 36*(3), 45–69. https://doi.org/10.2308/ajpt-51608

Gleason, K., Kannan, Y. H., & Rauch, C. (2022). Fraud in startups: what stakeholders need to know. *Journal of Financial Crime, 29*(4), 1191–1221. https://doi.org/10.1108/JFC-12-2021-0264

Gonzalez, G. C., & Hoffman, V. B. (2018). Continuous Auditing′ s Effectiveness as a Fraud Deterrent. *AUDITING: A Journal of Practice & Theory, 37*(2), 225–247. https://doi.org/10.2308/ajpt-51828

Griffin, O. H. (2022). Promises, Deceit and White-Collar Criminality Within the Theranos Scandal. *Journal of White Collar and Corporate Crime, 3*(2), 109–121. https://doi.org/10.1177/2631309X20953832

Hou, J., Li, Y., Yu, J., & Shi, W. (2020). A Survey on Digital Forensics in Internet of Things. *IEEE Internet of Things Journal, 7*(1), 1–15. https://doi.org/10.1109/JIOT.2019.2940713

International Finance Corporation. (2023). Control Environment.

www.ifcbeyondthebalancesheet.org. https://www.ifcbeyondthebalancesheet.org/about-the-toolkit/governance/control-environment

Iqbal, S., & Abed Alharbi, S. (2019). Advancing Automation in Digital Forensic Investigations Using Machine Learning Forensics. In Digital Forensic Science. *Intech Open*. https://doi.org/10.5772/intechopen.90233

Italia, M. (2012). The Multi-Disciplined Skills Required of Forensic Accountants. *Journal of Modern Accounting and Auditing, 8*(3), 365–373.

Jo, H., Hsu, A., Llanos-Popolizio, R., & Vergara-Vega, J. (2021). Corporate Governance and Financial Fraud of Wirecard. *European Journal of Business and Management Research, 6*(2), 96–106. https://doi.org/10.24018/ejbmr.2021.6.2.708

Judijanto, L. (2024). Perkembangan Startup Digital di Indonesia: Sebuah Tinjauan. *Indo-Fintech Intellectuals: Journal of Economics and Business, 4*(5), 2011–2032. https://doi.org/10.54373/ifijeb.v4i5.1875

Kamdjoug, J. R. K., Sando, H. D., Kala, J. R., Teutio, A. O. N., Tiwari, S., & Wamba, S. F. (2024). Data analytics-based auditing: a case study of fraud detection in the banking context. *Annuals of Operations Research, 340*(2–3), 1161–1188. https://doi.org/10.1007/s10479-024-06129-8

Kompas. (2018). Tokopedia Dikabarkan Pecat Puluhan Karyawan Terkait Kecurangan Flash Sale. *https://tekno.kompas.com/*. https://tekno.kompas.com/read/2018/08/27/13324797/tokopedia-dikabarkan-pecat-puluhan-karyawan-terkait-kecurangan-flash-sale

Kumar, G., Saha, R., Lal, C., & Conti, M. (2021). Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications. *Future Generation Computer Systems*, 120, 13–25. https://doi.org/10.1016/j.future.2021.02.016

Lee, J. E. (2015). CEO Overconfidence and The Effectiveness of Internal Control Over Financial Reporting. *Journal of Applied Business Research (JABR), 32*(1), 81. https://doi.org/10.19030/jabr.v32i1.9525

Liu, C. (2024). The Financing Ecosystem of Startups in Southeast Asia: A Review of the Role and Challenges of Venture Capital and Private Equity. *Journal of World Economy, 3*(4), 15–26. https://doi.org/10.56397/JWE.2024.12.03

Mandala, V. (2024). Leveraging Big Data and AI/ML for Fraud Detection in Retail Transactions. *Educational Administration: Theory and Practice*. https://doi.org/10.53555/kuey.v30i10.8103

Marks, J. (2012). The mind behind the fraudsters crime: Key behavioral and environmental elements. *Crowe Howarth LLP (Presentation)*.

Mehta, K., Mittal, P., Gupta, P. K., & Tandon, J. K. (2022). Analyzing the Impact of Forensic Accounting in the Detection of Financial Fraud: The Mediating Role of Artificial Intelligence (pp. 585–592). https://doi.org/10.1007/978-981-16-2597-8_50

Mujati, S. Y., & Laily, W. (2024). Pengaruh Elemen Fraud Pentagon terhadap Deteksi Kecurangan Laporan Keuangan. *JAD: Jurnal Riset Akuntansi & Keuangan Dewantara, 6*(2), 61–71. https://doi.org/10.26533/jad.v6i2.1189

Nunn, L., McGuire, B. L., Whitcomb, C., & Jost, E. (2011). Forensic Accountants: Financial Investigators. *Journal of Business & Economics Research (JBER), 4*(2). https://doi.org/10.19030/jber.v4i2.2631

Prayuda, J. R., Zakiyuddin, Z., & Firmansyah, A. (2022). Skema Ponzi: Indikasi Kecurangan Pada Valuasi Startup Menggunakan Gross Merchandise Value. *Jurnal Ilmiah Manajemen Kesatuan, 10*(1), 35–50. https://doi.org/10.37641/jimkes.v10i1.1184

Rogozhin, A. A. (2022). Startup′s Boom in Southeast Asia in 2021. *Southeast Asia: Actual Problems of Development, 3*(56), 11–17. https://doi.org/10.31696/2072-8271-2022-3-3-56-011-017

Saud, I. M., Diyar, L., & Hakim, A. T. (2021). The Influence of Internal Control, Financial Pressure, and Compensation Compatibility on the Tendency of Accounting Fraud. https://doi.org/10.2991/aer.k.210121.015

Simeunovic, N., Grubor, G., & Ristic, N. (2016). Forensic accounting in the fraud auditing case. *The European Journal of Applied Economics, 13*(2), 45–56. https://doi.org/10.5937/ejae13-10509

Subash. (2015). Forensic accounting and Corporate Governance. *International Journal of Multidisciplinary Management Studies, 5*(11), 49–54. https://www.indianjournals.com/ijor.aspx?target=ijor:xijmms&volume=5&issue=11&article=004

Teichmann, F. M. J., Boticiu, S. R., & Sergi, B. S. (2024). Wirecard scandal. A commentary on the biggest accounting fraud in Germany's post-war history. *Journal of Financial Crime, 31*(5), 1166–1173. https://doi.org/10.1108/JFC-12-2022-0301

Tsai, Y.-C., & Huang, H.-W. (2021). Internal control material weakness opinions and the market's reaction to securities fraud litigation announcements. *Finance Research Letters, 41*, 101833. https://doi.org/10.1016/j.frl.2020.101833

Tuanakotta, T. M. (2010). Akuntansi Forensik & Audit Investigatif (edisi 2). *Salemba Empat*.

Wells, J. T., Riley, R. A., & Kranacher, M.-J. (2007). Forensic Accounting and Fraud Examination.

Widyastuti, R. A., & Ratnawati, T. (2023). Studi Literatur: Mengungkap Fraud – Red Flag, Fraud Evidence, dan Audit Digital. *Jurnal Riset Akuntansi, 2*(1), 198–209. https://doi.org/10.54066/jura-itb.v2i1.1356

Williams, M. (2022). Elizabeth Holmes and Theranos: A play on more than just ethical failures. *Business Information Review, 39*(1), 23–31. https://doi.org/10.1177/02663821221088899

Yaqoob, I., Hashem, I. A. T., Ahmed, A., Kazmi, S. M. A., & Hong, C. S. (2019). Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. *Future Generation Computer Systems*, 92, 265–275. https://doi.org/10.1016/j.future.2018.09.058

Zeranski, S., & Sancak, E. (2020). Does the "Wirecard AG" Case Address FinTech Crises? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3666939