International Journal of Economics, Business and Innovation Research
https://e-journal.citakonsultindo.or.id/index.php/IJEBIR
E-ISSN : 2964-0865
IJEBIR

Theoretical Synthesis Of Fraud Models (Fraud Triangle, Diamond, Pentagon, And Hexagon) In Developing A Predictive Framework For Organizational Fraud Prevention In The Digital Era

Berlianna Dewi Setiawan[1], Maria Yovita R. Pandin[2] ,Amiartuti Kusmaningtyas[3],

[1,2,3] Faculty of Economics and Business, Univeristas 17 Agustus 1945

Corresponding Author: berliannabaobei2002@gmail.com

Abstract

This study aims to synthesize the development of the Fraud Triangle, Fraud Diamond, Fraud Pentagon, and Fraud Hexagon models to develop a predictive framework for organizational sustainability in the digital era. The study uses a qualitative approach with a conceptual literature study design through the identification, comparison, and synthesis of literature on fraud theory and digital transformation. The results show that each model has complementary contributions in explaining the causes of fraud. This synthesis produces a Predictive Fraud Prevention Framework that integrates behavioral factors, governance, internal control, collusion, and digital technology as a basis for more proactive fraud prevention. This framework is intended to serve as a foundation for the development of empirical research and the implementation of risk-based anti-fraud systems in digital organizations.

Keywords: Fraud Theory, Fraud Hexagon, Fraud Prevention, Digital Governance, Predictive Framework

INTRODUCTION

Digital transformation has fundamentally changed organizational governance, business processes, and internal control systems across various sectors. The implementation of technologies such as artificial intelligence (AI), big data analytics, cloud

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

computing, blockchain, and the Internet of Things (IoT) can improve operational efficiency, speed decision-making, and organizational transparency. However, on the other hand, digitalization has also created new forms of fraud that are more complex, adaptive, and difficult to detect through conventional control mechanisms. These fraudulent practices are no longer limited to financial statement manipulation or asset brokerage, but have evolved to include digital data manipulation, algorithmic brokerage, identity theft, cyber fraud, and technology-based collusion (Association of Certified Fraud Examiners ACFE, 2024).

A 2024 report by the Association of Certified Fraud Examiners indicates that organizations worldwide lose approximately 5% of their total annual revenue to fraud, with median losses reaching over USD 145,000 per case. Furthermore, the increasing use of digital systems makes fraud risks increasingly difficult to identify as perpetrators exploit business process automation, remote access, artificial intelligence, and weaknesses in data governance. This phenomenon demonstrates that internal control systems, which have traditionally focused on post-event detection (detective control), are not fully capable of addressing the challenges of fraud in the digital age, necessitating a more predictive and preventative approach.

From this perspective, academic studies on the causes of fraud continue to evolve. The Fraud Triangle model, introduced by Cressey, explains that fraud occurs due to pressure, opportunity, and rationalization. This model was later developed into the Fraud Diamond by adding the dimension of ability as a factor enabling an individual to commit fraud (Wolfe & Hermanson, 2004). Furthermore, the Fraud Pentagon expanded this concept by adding the elements of competence and arrogance, while the Fraud Hexagon included the dimension of collusion as an adaptation to the increasing complexity of fraud practices in modern organizations (Vousinas, 2019). These developments demonstrate that fraud theory is dynamic and continually adapts to changes in the business environment and technological developments.

Empirical research in recent years has generally focused on testing each fraud model against specific cases, such as financial reporting conditions, corruption, or asset-related issues. For example, research (Sari & Nugroho, 2022) shows that the Fraud Hexagon model has a better ability to explain financial statement fraud than the Fraud Pentagon model. Research (Rahman & Anwar, 2023) found that collusion is a significant determinant of fraud in public sector organizations. On the other hand, (Pratama & Haryanto, 2021) stated that capability and opportunity remain dominant factors in various corporate fraud cases. These research results indicate that each model has advantages

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

in explaining fraud behavior, but they do not provide a complete conceptual integration regarding the evolutionary relationships between the models.

Based on the scientific literature, several research gaps remain. First, most studies use the Fraud Triangle, Diamond, Pentagon, or Hexagon models separately as the basis for empirical research, thus failing to produce a theoretical synthesis that comprehensively explains the evolution of the fraud concept. Second, the development of digital technology has changed the characteristics of fraud, yet most existing models are still built from an individual behavioral perspective without considering the interaction between humans, technology, digital governance, and cross-system collaboration. Third, previous research has primarily produced explanatory models that explain the causes of fraud after it has occurred, while the development of predictive frameworks to support fraud prevention in digital organizations remains relatively limited. Thus, there are still theoretical and practical gaps that need to be bridged through a more comprehensive conceptual synthesis.

This research offers novelty in the form of a theoretical synthesis of the development of fraud models, ranging from the Fraud Triangle, Fraud Diamond, Fraud Pentagon, to the Fraud Hexagon, to develop a predictive framework for preventing fraud in organizations in the digital era. Unlike previous research that examined these models partially, this study integrates the dimensions of pressure, opportunity, rationalization, capability, competence, arrogance, and collusion into a single conceptual framework.

LITERATURE REVIEW

Fraud Theory

Fraud Theory is a conceptual foundation that explains the factors that drive individuals and groups to commit fraud. This theory developed from studies of criminology, organizational behavior, and corporate governance, explaining that fraud results from the interaction between individual factors, the organizational environment, and weak internal control systems (Albrecht et al., 2019; Free, 2015). Over time, fraud theory has been continuously refined in response to changes in the business environment, globalization, and digital transformation, which have altered the risk characteristics of organizations (Vousinas, 2019; ACFE, 2024).

In the digital era, fraud is no longer limited to financial statement manipulation or asset brokerage, but has evolved into cyberfraud, digital data manipulation, artificial intelligence algorithms, digital identity theft, and technology-based collusion. Therefore, a contextual approach to fraud must be able to explain the relationship between individual

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

behavior, organizational governance, and developments in digital technology (Brennan & McGrath, 2022; ACFE, 2024).

The Fraud Triangle Theory

The Fraud Triangle was introduced by Donald R. Cressey (1953) as the first model to explain the causes of fraud. According to this theory, fraud arises from a combination of three main elements: pressure, opportunity, and rationalization. Pressure describes the financial and non-financial incentives experienced by the perpetrator, opportunity arises from weak internal controls, and rationalization is the moral justification used to legitimize the action (Cressey, 1953).

To date, the Fraud Triangle remains the most widely used theory in fraud research because it explains the basic behavior of individuals in certain situations. However, various studies have shown that this model is unable to explain the full complexity of modern fraud, particularly those involving technological capabilities, collaboration between perpetrators, and the characteristics of digital organizations (Dorminey et al., 2012; Said et al., 2023).

The Fraud Diamond Theory

To address the limitations of the Fraud Triangle, Wolfe and Hermanson (2004) expanded the Fraud Diamond by adding the Capability dimension. Capability explains that an individual can only commit fraud if they possess the ability, experience, intelligence, authority, or access to organizational systems.

The addition of the capability dimension provides the perspective that not all individuals under pressure and opportunity will commit fraud if they lack the ability to commit and conceal the act. Various studies have shown that capability is a significant predictor of financial statement fraud and occupational fraud in modern organizations (Wolfe & Hermanson, 2004; Sari & Nugroho, 2022).

Pentagon Fraud Theory

Crowe Horwath (2011) expanded the Fraud Diamond into the Fraud Pentagon by adding two new dimensions: Competence and Arrogance. Competence describes an individual's ability to exploit weaknesses in internal control systems, while arrogance indicates a superior character who feels immune to organizational rules.

The Fraud Pentagon is widely used in research on financial statement fraud because it is considered more capable of explaining top management behavior than the

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Fraud Triangle. Research shows that arrogance and competence significantly influence the occurrence of financial statement fraud in various industrial sectors (Marks, 2012; Tessa & Harto, 2016; Aprilia et al., 2023).

The Fraud Hexagon Theory

Recent developments have resulted in the Fraud Hexagon, introduced by Vousinas (2019). This model adds the Collusion dimension as a sixth factor, explaining that modern fraud is increasingly perpetrated through collaboration between individuals and organizations.

The collusion dimension is particularly relevant in the digital age because various forms of fraud today involve internal networks, vendors, consultants, and external parties working together to exploit system weaknesses. Recent research shows that collusion is a dominant factor in various fraud cases in both the public and private sectors (Vousinas, 2019; Rahman & Anwar, 2023; ACFE, 2024).

Digital Transformation and Fraud Prevention

Digital transformation is driving organizations to implement various technologies such as Artificial Intelligence (AI), Big Data Analytics, Blockchain, the Internet of Things (IoT), Cloud Computing, and Robotic Process Automation (RPA). These technologies improve organizational efficiency, enhance decision-making processes, and enable real-time business operations. However, at the same time, they also create opportunities for new, more sophisticated, and complex fraud patterns that are increasingly difficult to identify using conventional control systems.

Various studies show that fraud in the digital era is becoming more difficult to detect because perpetrators exploit automation systems, manipulate digital data, misuse algorithms, and take advantage of vulnerabilities in interconnected digital platforms. In addition, the rapid adoption of digital technologies often outpaces the development of internal control mechanisms and regulatory frameworks, creating new risks for organizations. Therefore, organizations must develop adaptive fraud prevention strategies by integrating advanced technologies, robust governance, and continuous monitoring systems to mitigate emerging digital fraud risks.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Economics, Business and Innovation Research
https://e-journal.citakonsultindo.or.id/index.php/IJEBIR
E-ISSN : 2964-0865
IJEBIR

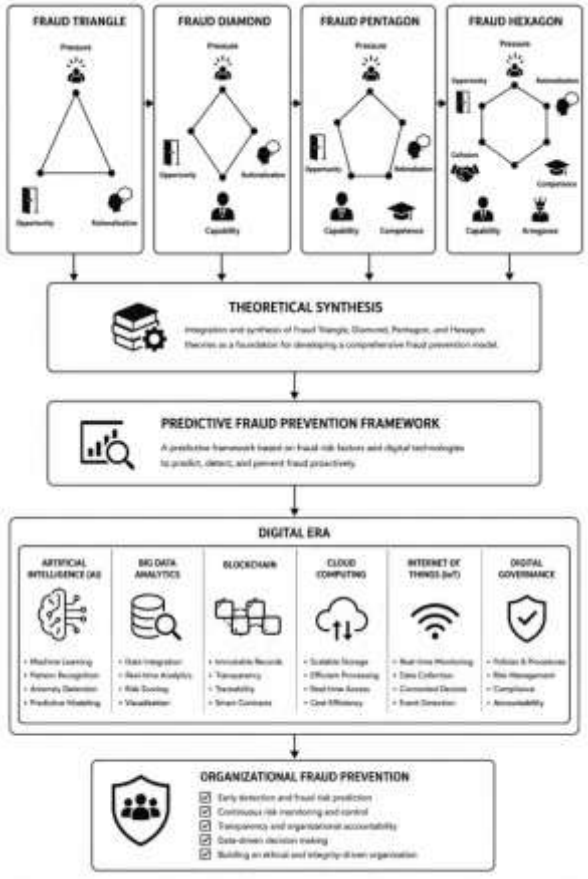


Figure 1. Theory Concept Diagram

METHODOLOGY

This research uses a qualitative approach with a conceptual literature study design. Data are sourced from academic literature, audit standards, fraud risk management guidelines, and professional reports discussing the Fraud Triangle, Fraud Diamond, Fraud Pentagon, Fraud Hexagon, and the development of fraud in the digital era. The analysis is conducted in three stages: identifying the core concepts of each model, comparing the contributions and limitations between models, and theoretical synthesis to formulate a predictive framework for organizational fraud prevention. Conceptual validity is maintained through source triangulation, consistency of theoretical argumentation, and the link between classic fraud concepts and the needs of digital governance. The research results are not intended to make statistical generalizations, but

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

rather offer conceptual propositions that can be further tested through empirical research, case studies, or the development of fraud risk measurement instruments.

DISCUSSION

The Evolution of Fraud Synthesis Models

The results of the synthesis indicate that fraud models have evolved from models focused on basic conditions to models more sensitive to actors, power, and networks. The Fraud Triangle describes the minimal conditions: an individual exerts pressure, perceives an opportunity, and develops moral justification. The Fraud Diamond adds that not all opportunities can be exploited without capability. The Pentagon Fraud model places competence and arrogance as crucial factors, particularly in frauds involving management or powerful actors. The Fraud Hexagon model expands the unit of analysis from individuals to networks through collusion.

This development is not commonly understood as a replacement for the old model, but rather as an expansion of the level of analysis. The Fraud Triangle remains relevant as a diagnostic basis. The Fraud Diamond analysis strengthens the perpetrator. The Pentagon Fraud model strengthens the analysis of organizational power and personality. The Fraud Hexagon model strengthens the analysis of network analysis. Arranged hierarchically, these models form a logic: motivation creates drive, opportunity opens access, rationalization lowers moral barriers, capability enables execution, arrogance encompasses achievement, and collusion increases scale while reducing the likelihood of detection.

In a predictive context, each element can be translated into a risk indicator. Pressure can be measured through pressure targets, debt burdens, dependency bonuses, and lifestyle changes. Opportunities can be observed through control weaknesses, excessive access, unfollowed exceptions, and dominant overrides. Rationalization can be seen through justification narratives, a permissive culture, the normalization of minor violations, and a cynical attitude towards compliance. Capability can be seen through a combination of authority, knowledge systems, data access, and a history of evading controls. Arrogance can be identified through leadership dominance, resistance to audits, conflicts with oversight committees, and oversight procedures. Collusion can occur through transaction relationship patterns, vendor overlap, repeat transactions, closed communications, and undisclosed personal relationships.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Economics, Business and Innovation Research
https://e-journal.citakonsultindo.or.id/index.php/IJEBIR
E-ISSN : 2964-0865
IJEBIR

Table 1. Comparative Synthesis of Fraud Models

Model	Main Elements	Unit of Analysis	Contribution	Limitations	Digital Era Adaption
Fraud Triangle	Pressure, opportunit, rationalization	Individuals in organizational structures	Provides a psychological and structural foundation for understanding the prerequisites for fraud.	Has not explained the ability to execute, power, and collusion.	Translated into target pressure indicators, system access, and digital justification narratives.
Fraud Diamond	Triangle + capability	Individuals who have the ability and access	Explains why only certain actors are able to exploit opportunities.	Capabilities can overlap with opportunities.	Mapping the risks of privileged access, system literacy, override rights, and concentration of technological knowledge.
Fraud Pentagon	Pressure, opportunity, rationalization, competence, arrogance	Power factors and management	Incorporating the role of ego, dominance, and superiority in fraud	Indicators of arrogance are often difficult to measure objectively.	Linking fraud to tone at the top, digital leadership, and resistance to systems audits.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Economics, Business and Innovation Research
https://e-journal.citakonsultindo.or.id/index.php/IJEBIR
E-ISSN : 2964-0865
IJEBIR

Model	Main Elements	Unit of Analysis	Contribution	Limitations	Digital Era Adaption
Fraud Hexagon	Stimulus, capability, opportunity, rationalization, ego, collusion	Network of internal and external factors	Explains complex fraud involving collective cooperation and concealment.	Requires strong relational data and network analysis.	Using graph analytics, vendor analytics, anomalous communications, and conflict of interest mapping.

Predictive Framework for Organizational Fraud Prevention

Based on this synthesis, this article proposes a Predictive Framework for Organizational Fraud Prevention in the Digital Age. This framework is built on the principle that fraud can be prevented more effectively if organizations are able to recognize pre-fraud conditions. Pre-fraud conditions are risk configurations where pressure, opportunity, rationalization, capability, arrogance, and collusion begin to converge, but do not necessarily result in an identifiable loss. In other words, the focus of prevention shifts from fraud event detection to the fraud risk ecology.

This predictive framework consists of six layers of analysis. The first layer is the behavioral layer, which examines behavioral indicators such as lifestyle changes, extreme work pressure, conflicts of interest, leave approvals, and resistance to oversight. The second layer is the governance layer, which assesses the quality of top-level tone, board independence, audit committee effectiveness, whistleblowing, and sanctions. The third layer is the control layer, which describes weaknesses in segregation of duties, authorization, reconciliation, access systems, and exception handling. The fourth layer is the digital footprint layer, which analyzes audit trails, access logs, master data changes, off-hours transactions, and override patterns. The fifth layer is the relational layer, which assesses the likelihood of collusion through relationships between employees, vendors, customers, and third parties. The sixth layer is the response layer, which measures the organization's speed in responding to red flags, conducting investigations, and improving controls.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Economics, Business and Innovation Research
https://e-journal.citakonsultindo.or.id/index.php/IJEBIR
E-ISSN : 2964-0865
IJEBIR

This model is integrative because it combines behavioral theory and digital data. The Fraud Triangle provides the basis for behavioral and structural drivers; the Fraud Diamond adds execution capacity; the Pentagon Fraud adds power and ego; and the Fraud Hexagon adds collusive networks. When all these elements are connected with operational data, organizations can build a more contextual fraud risk score. This score is calculated not only from anomalous transactions but also from the socio-organizational configuration that makes those anomalies significant.

Table 2. Predictive Framework Indicator Design for Fraud Prevention

Predictive Dimension	Theoretical Roots	Example Indicators	Preventive Response
Pressure/Stimulus	Fraud Triangle and Hexagon	Unrealistic targets, liquidity pressure, bonus dependency, pressure from superiors.	Target evaluation, ethics support, consultation channels, and incentive policy review.
Opportunity	Fraud Triangle	Excessive access, weak controls, late reconciliation, repeated overrides.	Segregation of duties, least privilege, layered approval, continuous control monitoring.
Rationalization	Fraud Triangle	Normalization of minor violations, “temporary” narrative, culture of turning a blind eye.	Ethics training, tone at the top communication, consistent discipline enforcement.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Economics, Business and Innovation Research
https://e-journal.citakonsultindo.or.id/index.php/IJEBIR
E-ISSN : 2964-0865
IJEBIR

Predictive Dimension	Theoretical Roots	Example Indicators	Preventive Response
Capability/Competence	Fraud Diamond and Pentagon	Key employees without rotation, concentrated system knowledge, cross-module access.	Job rotation, mandatory leave, dual control, periodic access review.
Arrogance/Ego	Fraud Pentagon and Hexagon	Resistance to audit, decision dominance, disregard for procedures.	Strengthening the board/audit committee, leadership evaluation, override restrictions.
Collusion	Fraud Hexagon	Unusual repeat vendors, circular transaction patterns, hidden personal relationships.	Vendor due diligence, conflict-of-interest declaration, graph analytics, whistleblowing.
Digital Traceability	Synthesis of the digital era	Anomalous access logs, master data changes, off-hours transactions.	Audit trail immutable, SIEM, exception dashboard, real-time alert.
Organizational Response	Fraud Risk Management	Red flags are not followed up, investigations are slow, sanctions are inconsistent.	Fraud response protocol, root-cause analysis, remediation tracking.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Economics, Business and Innovation Research
https://e-journal.citakonsultindo.or.id/index.php/IJEBIR
E-ISSN : 2964-0865
IJEBIR

The Role of Data Analytics in Fraud Prediction

Data analytics plays a crucial role in transforming fraud models from explanatory to predictive. Traditional approaches often identify red flags through manual inspections, whistleblower reports, or periodic audits. These approaches remain important, but they often arrive too late, as the fraud has already occurred and losses have already occurred. Data analytics enables organizations to continuously monitor transactions, access, data changes, and relationships between entities.

However, the use of data analytics must be guided by theory. Without theory, detection systems can generate numerous false positives because every anomaly is treated equally. By synthesizing fraud models, organizations can distinguish ordinary anomalies from those with a fraudulent context. For example, a change to vendor master data may be a normal administrative activity. However, if the change is made by an employee with excessive access, occurs outside of working hours, relates to a vendor with an unusual relationship, and occurs in conjunction with procurement target pressure, the risk of fraud increases significantly.

In this regard, predictive frameworks do not replace auditors, investigators, or risk managers, but rather enhance professional judgment. Machine learning can identify patterns, but ethical and organizational interpretations still require human input. Therefore, organizations need to develop explainable fraud analytics, namely an analytical system that not only generates a risk score but also explains the indicators that drive that score. This transparency is essential for the system to be trustworthy, auditable, and not create dependency on algorithms.

Implications for Governance and Internal Control

The fraud synthesis model has a direct impact on organizational governance. First, the board of commissioners, board of directors, audit committee, and risk management need to understand fraud as a risk stemming from a combination of human, system, and relationship factors. The focus of oversight should not be solely on formal compliance, but should also include incentive design, ethical culture, the effectiveness of reporting channels, and power patterns. If organizations rely solely on written procedures without assessing the behavior of key actors, fraud can still occur through override and collusion.

Second, internal controls need to be designed with the assumption that fraudsters can possess high capabilities. Statistical controls need to be complemented with adaptive controls. For example, system access should not be granted based on title but should be considered based on actual behavior. Layered approvals are insufficient if the approver

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

has a conflict of interest or collusion. Periodic reconciliations need to be complemented with dashboard exceptions to quickly identify critical anomalies.

Third, organizations need to treat data as a control asset. Audit trails, access logs, transaction metadata, and system change records must maintain their integrity. Without a reliable digital footprint, fraud detection is weakened and risk predictions inaccurate. Therefore, investments in data governance, cybersecurity, and IT audits are part of an anti-fraud strategy, not just a technology agenda.

Fourth, whistleblowing mechanisms remain relevant even when organizations are using data analytics. Much fraud information, particularly rationalization, informal pressure, intimidation, and collusion, is not always visible in transaction data. Human reporting can provide context not available in system logs. Therefore, an effective anti-fraud strategy must combine human-based and technology-based controls.

CONCLUSION AND RECOMMENDATIONS

This study concludes that fraud models have an evolutionary and complementary relationship. The Fraud Triangle provides a conceptual foundation for pressure, opportunity, and rationalization. The Fraud Diamond expands the model by adding capability as a prerequisite for execution. The Fraud Pentagon emphasizes the importance of competence and arrogance, particularly in the context of fraud involving powerful actors. The Fraud Hexagon enriches the analysis by incorporating collusion as a factor explaining complex and large-scale fraud.

In the digital era, the synthesis of these models becomes increasingly important because fraud occurs not only through manual irregularities but also through data manipulation, access abuse, transaction manipulation, opaque vendor relationships, and concealment of traces in information systems. Therefore, fraud prevention must shift from a reactive approach to a predictive one. The predictive framework proposed in this article combines behavioral indicators, governance, internal controls, digital footprints, collusive relationships, and organizational responses.

The main contribution of this article is to position fraud models as a basis for building operationalized prevention systems. Fraud models are not merely theoretical concepts but can be translated into risk indicators, analytical dashboards, control policies, and digital governance mechanisms. In this way, organizations can identify pre-fraud risk configurations earlier before fraud develops into material losses.

Recommendations for organizations include establishing a fraud risk management program that integrates fraud theory with data analytics. Organizations need to develop

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

a fraud risk assessment that assesses not only control weaknesses but also incentive pressures, leadership behavior, capability concentration, and potential collusion. System access rights need to be periodically evaluated, anomalous transactions need to be monitored in real time, and whistleblowing mechanisms must be maintained independently.

Recommendations for internal and external auditors include using fraud model synthesis as a risk assessment lens. Auditors need to assess whether emerging red flags are ordinary administrative anomalies or part of a broader fraud risk configuration. A data-driven audit approach should be combined with interviews, cultural observations, and governance analysis to provide a more contextualized risk assessment.

Future researchers can develop this article into an empirical model by examining the relationship between the dimensions of pressure, opportunity, rationalization, capability, arrogance, collusion, and digital traceability with fraud risk. Further research could also develop measurement instruments, case studies in digital organizations, or machine learning-based predictive models explained through theoretical fraud indicators.

REFERENCES

ACFE. (2026). *Occupational Fraud 2026: A Report to the Nations*. Association of Certified Fraud Examiners.

AICPA. (2002). *Statement on Auditing Standards No. 99: Consideration of Fraud in a Financial Statement Audit*. American Institute of Certified Public Accountants.

Albrecht, W. S., Howe, K. R., & Romney, M. B. (1984). *Deterring Fraud: The Internal Auditor's Perspective*. Institute of Internal Auditors Research Foundation.

Aprilia, N., Putri, D., & Hidayat, A. (2023). Pengaruh Fraud Pentagon terhadap financial statement fraud pada perusahaan publik. *Jurnal Akuntansi dan Keuangan*, 25(2), 145–160.

Association of Certified Fraud Examiners. (2024). *Occupational Fraud 2024: A Report to the Nations*. Association of Certified Fraud Examiners.

Brennan, N. M., & McGrath, M. (2022). Digital transformation, corporate governance, and fraud risk: A literature review. *Journal of Financial Crime*, 29(4), 1203–1221.

COSO, & ACFE. (2023). *Fraud Risk Management Guide* (2nd ed.). Committee of Sponsoring Organizations of the Treadway Commission & Association of Certified Fraud Examiners.

Cressey, D. R. (1953). *Other People's Money: A Study in the Social Psychology of Embezzlement*. Free Press.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Crowe Horwath. (2011). *Why the Fraud Triangle Is No Longer Enough*. Crowe Horwath LLP.

Dorminey, J., Fleming, A. S., Kranacher, M. J., & Riley, R. A. (2012). The evolution of fraud theory. *Issues in Accounting Education*, 27(2), 555–579.

Free, C. (2015). Looking through the fraud triangle: A review and call for new directions. *Meditari Accountancy Research*, 23(2), 175–196.

Kurshan, E., Shen, H., & Yu, H. (2021). Financial crime and fraud detection using graph computing: Application considerations and outlook. *arXiv*. https://arxiv.org/abs/2103.01854

Marks, J. (2012). *The Mind Behind the Fraudsters Crime: Key Behavioral and Environmental Elements*. Crowe Horwath LLP.

OECD. (2023). *OECD Digital Economy Outlook 2023*. Organisation for Economic Co-operation and Development.

PCAOB. (2024). *AS 2401: Consideration of Fraud in a Financial Statement Audit*. Public Company Accounting Oversight Board.

Pratama, A., & Haryanto, H. (2021). Pengaruh capability dan opportunity terhadap fraud korporasi. *Jurnal Akuntansi Multiparadigma*, 12(3), 421–437.

Rahman, A., & Anwar, S. (2023). Collusion as a determinant of fraud in public sector organizations. *Jurnal Akuntansi dan Auditing Indonesia*, 27(1), 45–58.

Said, J., Omar, N., & Yusuf, S. N. S. (2023). Fraud risk in the era of digital transformation: Challenges and opportunities. *Journal of Financial Crime*, 30(2), 389–406.

Sari, D., & Nugroho, R. (2022). Analisis Fraud Hexagon dalam mendeteksi financial statement fraud. *Jurnal Akuntansi Indonesia*, 11(2), 115–130.

Tessa, C., & Harto, P. (2016). Fraudulent financial reporting: Pengujian teori Fraud Pentagon pada perusahaan publik di Indonesia. *Diponegoro Journal of Accounting*, 5(2), 1–15.

Vousinas, G. L. (2019). Advancing theory of fraud: The S.C.O.R.E. model. *Journal of Financial Crime, 26*(1), 372–381. https://doi.org/10.1108/JFC-12-2017-0128

Wells, J. T. (2017). *Corporate Fraud Handbook: Prevention and Detection* (5th ed.). Wiley.

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

Zweers, B., Dey, D., & Bhaumik, D. (2025). The AI-Fraud Diamond: A novel lens for auditing algorithmic deception. *arXiv*. https://arxiv.org/abs/2508.13984

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.