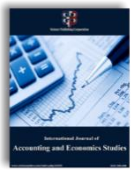
International Journal of Accounting and Economics Studies, 12 (8) (2025) 695-703

International Journal of Accounting and Economics Studies

Website: www.sciencepubco.com/index.php/IJAES
https://doi.org/10.14419/0a71t839
Research paper



Digital Transformation and Fraud Challenges: Cybersecurity Analysis in Indonesian State-Owned Enterprises Using The Heptagon Framework

Azalia Nadya Ayu Maharani, Imang Dapit Pamungkas *

Universitas Dian Nuswantoro
**Corresponding author E-mail: imangdapit.pamungkas@dsn.dinus.a.c.id*

Received: October 2, 2025, Accepted: November 28, 2025, Published: December 20, 2025

Abstract

Fraud and cyber-related threats represent critical challenges to the integrity of state-owned enterprises (SOEs), particularly during their ongoing digital transformation efforts aimed at improving transparency and operational efficiency. This study investigates how the Fraud Hep-tagon framework, digital forensic techniques, and risk management practices collectively contribute to mitigating fraudulent activities and enhancing the reliability of SOE information systems. A mixed-methods design was applied, integrating qualitative and quantitative ap-proaches. The qualitative strand involved semi-structured interviews with 25 participants, including IT managers, cybersecurity personnel, and internal auditors, to identify the underlying drivers of fraud in SOEs. Meanwhile, the quantitative strand examined the effectiveness of digital forensic practices in minimizing the likelihood of financial statement manipulation, drawing on secondary datasets. The qualitative findings highlight that systemic pressures, operational inefficiencies, and institutional vulnerabilities are dominant factors influencing fraudulent conduct. Conversely, technology-enabled controls and risk-based mechanisms significantly strengthen monitoring, detection, and accountability. The quantitative results further validate that digital forensic applications play a substantial role in fraud prevention. Collective-ly, the evidence suggests that fraud within SOEs is predominantly systemic rather than individual in nature, underscoring the necessity for integrated interventions across behavioral, technological, and governance dimensions. By combining the Fraud Heptagon perspective with digital forensic methodologies and structured risk management frameworks, organizations can establish more robust strategies to prevent and mitigate fraudulent practices, while simultaneously reinforcing the dependability of information systems. The insights derived from this research provide actionable recommendations for policymakers, corporate governance authorities, and financial professionals, while also laying the groundwork for comparative studies across sectors and organizational settings. Ultimately, this study advances the global dis-course on fraud prevention and cybersecurity in the context of digitally evolving enterprises.

Keywords: *Fraud Heptagon; Financial Statement Fraud; Digital Forensics; Risk Management; Cybersecurity.*

1. Introduction

The acceleration of the digital era has positioned the financial sector as one of the industries most vulnerable to increasingly sophisticated and complex cyber threats. Projections from Cybersecurity Ventures estimate that global economic losses due to cybercrime will escalate to USD 10.5 trillion in 2025, rising from USD 9.5 trillion in 2024. This surge reflects not only the expanding frequency of attacks but also their growing scale and severity across international markets. The rapid development of artificial intelligence (AI), machine learning, and quantum computing has further complicated detection and prevention mechanisms, enabling more advanced and elusive forms of cyberattacks. Traditional threats such as ransomware, malware, and phishing often driven by social engineering remain widespread. Recent statistics indicate that ransomware incidents increased by 81% between 2023 and 2024, while phishing attacks rose by 58.2% in 2023, with the financial sector emerging as a primary target. Moreover, the rise of deepfake technology has introduced new challenges; cases involving deepfakes have surged by over 550% since 2019 and are projected to exceed 8 million incidents by 2025, with such tools increasingly weaponized for large-scale fraud and digital disinformation. Compounding these risks, approximately 40% of current cyberattacks leverage AI, making them more adaptive and difficult to anticipate. Although AI-based defense systems are being deployed, adoption remains uneven only 37% of organizations have established security assessment frameworks prior to implementation, despite 66% acknowledging AI as a transformative factor in cybersecurity. Beyond direct threats, the sector also confronts systemic challenges, including vulnerabilities in digital supply chains, regulatory fragmentation across jurisdictions, and a persistent shortage of skilled cybersecurity professionals. These complexities necessitate urgent, coordinated interventions. In response, innovative approaches such as Zero Trust Architecture, micro-segmentation, real-time encryption, and automated Security Operations Centers (SOC) are increasingly recognized as pivotal strategies for enhancing resilience in 2025. However, the effectiveness of these measures will depend significantly on robust regulatory frameworks and the cultivation of an agile, highly skilled cybersecurity workforce capable of adapting to the rapidly evolving threat environment.

Copyright © Azalia Nadya Ayu Maharani, Imang Dapit Pamungkas. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Digital transformation has become a critical catalyst for improving organizational efficiency and strengthening competitive positioning in the modern business landscape. Within the sphere of State-Owned Enterprises (SOEs), digitalization provides significant potential to streamline processes, promote transparency, and support evidence-based strategic decision-making. Nevertheless, the transition toward digitally integrated operations also brings forth intricate risks, most notably in relation to cybersecurity vulnerabilities and the heightened possibility of financial statement manipulation. The occurrence of fraudulent reporting in digitally-driven environments not only compromises organizational integrity but also erodes investor confidence and diminishes public trust, posing severe implications for enterprises that occupy strategic positions within national economic structures.(Daraojimba et al., 2023; Westland, 2022). Conventional frameworks for fraud detection, though useful, are constrained in their explanatory capacity. Models such as the Fraud Triangle and Fraud Hexagon emphasize factors like pressure, opportunity, and rationalization but provide insufficient consideration of elements such as collusion, ignorance, and the growing influence of digital vulnerabilities in contemporary financial fraud. Furthermore, existing research on forensic technologies has primarily concentrated on the development of detection instruments, often neglecting the integration of behavioral dynamics and organizational risk dimensions. In addition, although internal audit functions, regulatory supervision, and auditor expertise remain fundamental pillars in fraud prevention, the expectation gap endures. Stakeholders frequently presume that auditors are able to guarantee the absolute absence of fraud in financial reporting, whereas in practice, auditors can only offer reasonable assurance regarding the reliability of financial statements (Amlayasa & Riasning, 2022; Arum et al., 2023; Lari Dashtbayaz et al., 2022). The limitations of fragmented approaches highlight the necessity for a comprehensive and multidimensional framework to effectively analyze and mitigate fraud risks.

This study seeks to address such gaps by employing the Fraud Heptagon framework, which advances traditional models through the inclusion of seven dimensions: pressure, opportunity, rationalization, capability, arrogance, ignorance, and gree. When combined with digital forensics and structured risk management practices, the framework enables a more holistic examination of both behavioral and technological drivers of financial statement fraud. Specifically, digital forensic instruments facilitate the early identification of anomalies, ensure the preservation of audit evidence, and strengthen investigative reliability, while risk management mechanisms enhance organizational resilience by embedding preventive measures that extend beyond the actions of individual auditors.

The primary novelty of this research lies in its integrative orientation, which bridges behavioral, technological, and managerial perspectives within the context of State-Owned Enterprises (SOEs). In contrast to prior studies that tend to isolate single aspects of fraud, this work develops a unified model capable of informing both policy and practice in entities characterized by high levels of public accountability and strategic economic significance. By investigating the interconnection among the Fraud Heptagon, digital forensic applications, and risk management systems, this study contributes practical insights to strengthen the integrity of financial reporting and enhance organizational defenses against fraud in digitally transformed environments.

2. Theoretical Framework and Hypotheses Development

2.1. Fraud heptagon

The Fraud Heptagon framework constitutes an advancement of preceding fraud conceptualizations, such as the Fraud Triangle, by broadening their scope and explanatory capacity (Cressey, 1953), Fraud Diamond (Wolfe & Hermanson, 2004), and Fraud Pentagon (Howarth, 2012). Vousinas, (2019). The Fraud Heptagon framework represents a further refinement of prior fraud models, such as the Fraud Triangle and Fraud Hexagon. While the Fraud Hexagon introduced collusion as a sixth dimension, the Heptagon extends this by incorporating a seventh factor, namely Ignorance. This addition reflects the institutional and managerial weaknesses that frequently facilitate fraudulent practices, particularly in state-owned enterprises (SOEs) navigating the challenges of digital transformation.

The model is applied through the S.C.C.O.R.E. framework, which delineates seven interrelated elements of fraud risk. Stimulus (Pressure) encompasses both internal and external demands such as organizational performance targets or digitalization initiatives that may generate fraudulent intent. Capability concerns the authority, expertise, and system access that empower individuals to commit fraud within digital infrastructures. Collusion involves cooperation between multiple actors to conceal fraudulent behavior, a phenomenon that becomes more pronounced with the prevalence of remote work and digitized workflows. Opportunity arises from deficiencies in internal controls, ineffective cybersecurity protocols, or governance loopholes. Rationalization represents the cognitive justifications used by perpetrators to normalize unethical conduct. Ego (Arrogance) underscores the role of overconfidence and dominance in disregarding institutional norms and controls. Finally, Ignorance emphasizes insufficient managerial capacity, weak oversight, and underdeveloped control systems that exacerbate vulnerability to fraud.

By synthesizing these dimensions, the Fraud Heptagon delivers a holistic lens for analyzing the behavioral, organizational, and systemic antecedents of fraudulent financial reporting particularly relevant for SOEs undergoing rapid digitalization. In the context of this study, the framework is employed to explore the role of digital forensic tools and risk management strategies in fraud detection and mitigation, effectively bridging theoretical risk constructs with practical mechanisms of prevention and control. The research adopts a mixed-methods design, integrating quantitative evidence from financial disclosures with qualitative insights obtained through interviews with auditors and risk management officers. This approach enables a more comprehensive understanding of how fraud risk dimensions intersect with cybersecurity weaknesses and governance practices.

Digital transformation itself can be understood as a strategic process through which organizations leverage advanced digital technologies to restructure operations, enhance stakeholder interactions, and generate new value propositions. Key technologies such as big data analytics, the Internet of Things (IoT), cloud computing, and artificial intelligence play a central role in this process. While these innovations enable organizations to collect, process, and analyze information more effectively, they simultaneously elevate the risk of cyber vulnerabilities and sophisticated cyberattacks.

Correspondingly, cybersecurity is a field dedicated to safeguarding information systems, networks, and digital assets against threats originating from cyberspace. It encompasses the protection of data integrity, system availability, and confidentiality from external infiltration or internal misuse. Research within this discipline emphasizes risk identification and mitigation, continuous monitoring of security threats, and the design of robust policies and protocols to strengthen resilience against cyber incidents.

2.2. Fraud heptagon and financial statement fraud in digitally transforming SOEs

The Fraud Heptagon framework conceptualizes fraud risk through seven interrelated determinants: pressure, opportunity, rationalization, capability, arrogance, collusion, ignorance. Compared to earlier theoretical models, this construct offers a more comprehensive analytical

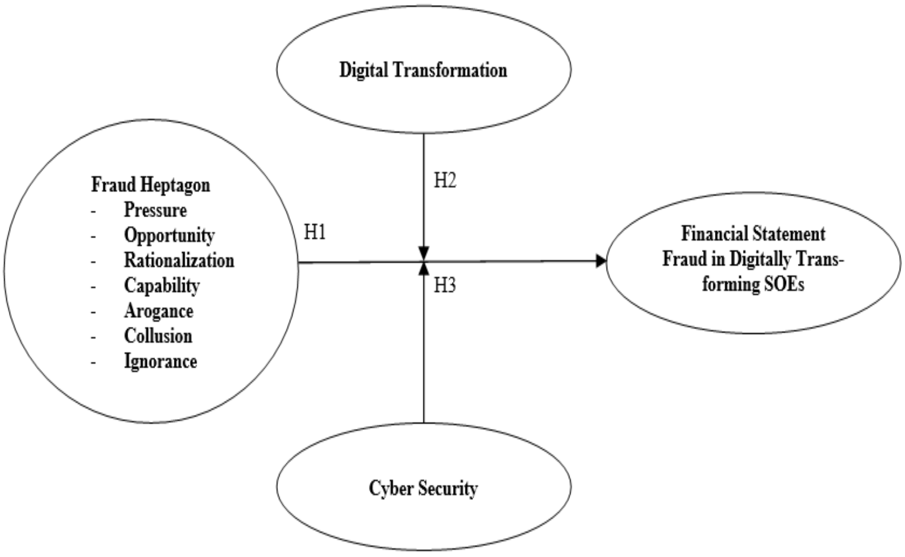
lens, as it integrates not only the behavioral aspects of individuals but also the organizational and institutional conditions that collectively foster fraudulent practices (Anisykurlillah et al., 2023; Sari, Maylia Pramono et al., 2020; Thamlim & Reskino, 2023; Wulandari & Maulana, 2022). Empirical findings demonstrate that fraudulent behavior is frequently motivated by external or internal pressures, whereas opportunity and collusion often stem from deficiencies in governance structures and inadequate internal controls. Furthermore, rationalization and arrogance provide cognitive and attitudinal justifications that normalize unethical conduct, while capability embodies the technical expertise and access to resources enabling perpetrators to conceal fraudulent activities effectively (Achmad et al., 2023; Lastanti et al., 2022; Thamlim & Reskino, 2023). Empirical findings demonstrate that fraudulent behavior is frequently motivated by external or internal pressures, whereas opportunity and collusion often stem from deficiencies in governance structures and inadequate internal controls. Furthermore, rationalization and arrogance provide cognitive and attitudinal justifications that normalize unethical conduct, while capability embodies the technical expertise and access to resources enabling perpetrators to conceal fraudulent activities effectively. In digitally transforming SOEs, the interaction among these seven dimensions becomes increasingly complex (Hafez et al., 2025), as digital technologies simultaneously create efficiency and fraud opportunities (Andalia et al., 2021; Bujaki et al., 2019; Chen et al., 2023). Viewing the Fraud Heptagon as a higher-order construct enables a more holistic evaluation of the multifaceted drivers of fraud, offering an integrated perspective within this analytical context.
H1: The Fraud Heptagon has a significant positive effect on financial statement fraud in digitally transforming SOEs.

2.3. Digital transformation as a moderator between fraud heptagon and financial statement fraud

Digital transformation can be defined as the strategic utilization of digital technologies aimed at strengthening organizational efficiency, supporting data-driven decision-making (Sarna et al., 2025), and optimizing the effectiveness of business processes (Abad-Segura et al., 2020; Alvarenga et al., 2020; Pizzi et al., 2021). In the context of State-Owned Enterprises (SOEs), digital transformation fundamentally reconfigures the architecture of financial information systems, influencing the way transactions are captured, processed, and supervised. From a theoretical standpoint, while the integration of digital technologies is expected to strengthen transparency and improve the accuracy of financial disclosures, it simultaneously generates systemic risks. These risks include the susceptibility of automated processes to manipulation and the increased exposure of digital infrastructures to unauthorized access, thereby reshaping the landscape of organizational fraud vulnerability (Buallay, 2019; Handayani et al., 2023; Roszkowska, 2021).
The integration of digital transformation initiatives with the Fraud Heptagon framework offers the potential to mitigate behavioral fraud antecedents such as pressure, and opportunity through strengthened monitoring mechanisms, automated control systems, and enhanced traceability of transactions. Nevertheless, the increasing sophistication of emerging technologies introduces governance and oversight complexities, suggesting that the effectiveness of such integration is highly contingent upon prudent design, phased implementation, and robust institutional capacity (Glembotskaya et al., 2020; Wahyudi et al., 2019).
H2: Digital transformation weakens the positive effect of the Fraud Heptagon on financial statement fraud in SOEs.

2.4. Cybersecurity as a moderator between fraud heptagon and financial statement fraud

Cybersecurity can be conceptualized as a comprehensive framework of governance mechanisms, organizational procedures, and technological controls aimed at safeguarding digital infrastructures from risks of unauthorized access, system manipulation, and operational disruption (Dutchak et al., 2021; Mangala & Soni, 2023; Todorović et al., 2020). Within state-owned enterprises undergoing digital transformation, insufficient cybersecurity measures exacerbate the risk of fraudulent activities by creating conditions that facilitate collusion, enable unauthorized data manipulation, and support the concealment of illicit practices (Nugroho & Diyanty, 2022; Pramana et al., 2019). Well-structured cybersecurity frameworks play a critical role in reducing fraud risks by safeguarding data integrity, strengthening audit trail reliability, and enabling real-time detection of anomalous activities. Empirical evidence further indicates that comprehensive cybersecurity controls limit the capacity of perpetrators to exploit technological or organizational vulnerabilities, thereby lowering both the probability and magnitude of financial statement fraud (Achmad et al., 2022; Akbar, 2017; Ibrani et al., 2019; Thamlim & Reskino, 2023). However, inadequate or fragmented adoption of cybersecurity controls may generate additional organizational complexity and operational costs, thereby undermining their overall effectiveness in mitigating fraud risks (Westland, 2022).
H3: Cybersecurity weakens the positive effect of the Fraud Heptagon on financial statement fraud in digitally transforming SOEs



3. Research Methodology

This research adopts a mixed-methods design, integrating quantitative and qualitative strategies to analyze the role of the Fraud Heptagon framework, digital transformation, and cybersecurity in mitigating financial statement fraud within Indonesia's State-Owned Enterprises (SOEs). The quantitative component draws on secondary data derived from corporate annual reports, audit findings, and relevant regulatory documents of the sampled SOEs, capturing observable measures of fraud risk and governance quality. The qualitative component utilizes semi-structured interviews with auditors, risk management personnel, and IT/cybersecurity experts to obtain nuanced insights into fraud determinants, institutional constraints, and the operationalization of technological safeguards. The integration of these two strands enhances methodological robustness and contextual validity, enabling a holistic assessment of how behavioral, technological, and organizational dimensions converge in addressing fraud vulnerabilities in digitally transforming SOEs.

3.1. Population and sample

The research population comprises all State-Owned Enterprises (SOEs) registered on the official government portal (bumn.go.id/portfolio/cluster) and listed on the Indonesia Stock Exchange (IDX) for the period 2020–2024. A purposive sampling technique was employed using the following criteria: (i) inclusion in the non-financial sector cluster, (ii) availability of complete annual reporting, and (iii) disclosure of information pertinent to fraud-related variables. Based on these parameters, 48 SOEs with a total of 89 firm-year observations were incorporated into the quantitative analysis. To complement these findings, qualitative data were obtained through semi-structured interviews with 25 key informants including auditors, risk management officers, and IT/cybersecurity professionals providing contextual perspectives on fraud mitigation mechanisms and practices of digital governance.

Table 1: Purposive Sampling Criteria

No	Description	Total
1	All SOEs listed on IDX and government portfolio during 2020–2024	68
2	Excluded: Banking SOEs and firms without complete data	(20)
3	Final SOEs sample with non-financial focus and partial-year availability	48
4	Total firm-year observations included in analysis	89

Source: Results of secondary data processing, 2025.

3.2. Data collection procedures

This study employs a mixed-methods design that integrates quantitative and qualitative evidence to provide a comprehensive understanding of financial statement fraud within Indonesia's State-Owned Enterprises (SOEs). The quantitative strand utilizes secondary data obtained from official SOE portals and annual financial reports, covering variables associated with the seven dimensions of the Fraud Heptagon, digital transformation initiatives, cybersecurity practices, and fraud indicators. A total of 89 firm-year observations met the eligibility criteria. To complement the quantitative data, semi-structured interviews were conducted with auditors, risk management officers, and IT/cybersecurity specialists from both SOEs and supervisory bodies. Participants were purposively selected based on their expertise in fraud detection, internal control, and digital governance. These qualitative insights enrich the interpretation of statistical findings and provide institutional context.

Quantitative data analysis was carried out using Partial Least Squares–Structural Equation Modeling (PLS-SEM) via WarpPLS 8.0, which is appropriate for analyzing complex models with relatively small to medium sample sizes. The measurement model was assessed through composite reliability, Average Variance Extracted (AVE), and the heterotrait–monotrait (HTMT) ratio. The structural model evaluated (i) the direct effects of Fraud Heptagon dimensions on financial statement fraud and (ii) the moderating effects of digital transformation and cybersecurity. Descriptive statistics (mean, standard deviation, minimum, maximum) were used to characterize data distribution.

Moderation analysis examined whether digital transformation and cybersecurity attenuate the influence of behavioral and organizational fraud antecedents on financial misreporting. Meanwhile, qualitative interview transcripts were analyzed using thematic coding to identify recurring patterns related to fraud risks, technological adoption, and cybersecurity challenges. Integrating both strands provides explanatory depth and practical relevance, allowing for a nuanced interpretation of how behavioral, organizational, and technological dynamics jointly shape financial statement fraud in digitally transforming SOEs.

3.3. Variable operational definition

Table 2 provides the operational definitions of all variables based on the Fraud Heptagon framework: Pressure, Opportunity, Rationalization, Capability, Arrogance, Collusion, and Ignorance. Measurements are fully aligned with prior literature while maintaining consistency with the theoretical model. This standardization ensures construct validity and supports the empirical testing of behavioral and structural antecedents of financial statement fraud in SOEs.

Table 2: Operational Definition of Variables

Variable Type	Variable	Measurement	Measurement Type	Source
Dependent Variable	Financial Statement Fraud (FSF)	Fraud Score Model (F-Score) including accrual quality and financial performance indicators: receivables, inventories, cash sales, earnings	Dummy (0/1)	Dechow et al., (2011)
Independent Variable	Pressure (PRS)	Leverage ratio = Total Liabilities / Total Assets	Index (0–1)	Handoko & Angelyca, (2023)
	Opportunity (OPT)	Independent board of commissioners ratio = Independent Commissioners / Total Commissioners	Index (0–1.35)	Mohamed Yusof, (2016)
	Rationalization (RTZ)	Related-party transaction ratio to total revenue	Dummy (0/1)	Ibrani et al., (2019)
	Capability (CP)	CEO education (1 = master's degree, 0 otherwise)	Dummy (0/1)	Widnyana & Widyawati, (2022)

	Arrogance (ARG)	Frequency of CEO photographs in annual reports	Score (3–12)	Pramesti & Kusumawati, (2023)
	Collusion (COL)	Ratio of politically connected commissioners	Dummy (0/1)	Nugroho & Diyanty, (2022)
	Ignorance (IG)	Material weaknesses in internal control disclosures	Continuous (0.7–35.5)	Author's adaptation
Moderating Variable	Digital Transformation (DT)	IT system adoption, process automation, and monitoring capabilities; proxied by disclosure of digital initiatives and fraud detection tools in annual/sustainability reports	Dummy (0/1)	Dosumu et al., (2024)
	Cybersecurity (CS)	Cybersecurity policies, controls, and monitoring systems; proxied by extent of IT security adoption and incident response reporting in corporate disclosures	Likert 1–5	Ejiofor, (2023)

Source: Results of secondary data processing, 2025.

3.4. Data collection and analysis procedures

This study adopts a mixed-methods strategy that integrates quantitative and qualitative strands to obtain a comprehensive understanding of financial statement fraud within Indonesia's State-Owned Enterprises (SOEs). The quantitative component utilized secondary data drawn from official SOE portals and annual financial reports, encompassing variables related to the seven dimensions of the Fraud Heptagon, digital transformation initiatives, cybersecurity practices, and fraud indicators. A total of 89 firm-year observations from the eligible SOEs were included in the analysis. To complement this dataset, semi-structured interviews were undertaken with auditors, risk management officers, and IT/cybersecurity professionals from SOEs and oversight institutions, with participants purposively selected for their expertise in fraud detection, governance, and digital systems. This triangulated approach enhanced the study's rigor, validity, and applied relevance. Quantitative analysis was conducted using Partial Least Squares–Structural Equation Modeling (PLS-SEM) via WarpPLS 8.0. PLS-SEM was deemed appropriate for evaluating complex relationships among latent constructs and is methodologically robust for small to medium sample sizes, consistent with the 89 firm-year dataset. The measurement model was validated for reliability and construct validity through composite reliability, average variance extracted (AVE), and the heterotrait-monotrait (HTMT) ratio. Subsequent structural model testing examined both the direct influence of the Fraud Heptagon on financial statement fraud and the moderating roles of digital transformation and cybersecurity. Descriptive statistics (mean, standard deviation, minimum, and maximum) were also applied to characterize data distribution and variability.

Moderation analysis explored whether digital transformation and cybersecurity attenuate the impact of Fraud Heptagon dimensions on fraudulent reporting. On the qualitative side, interview transcripts were thematically coded to identify emerging patterns, institutional challenges, and best practices related to fraud mitigation, technological adoption, and cybersecurity management. These qualitative insights contextualized the statistical results, illustrating the operational realities of fraud prevention in digitally transforming SOEs. By synthesizing quantitative modeling with qualitative evidence, this integrated design captures not only the empirical associations among constructs but also the behavioral, organizational, and technological dynamics that shape financial statement fraud, thereby offering a holistic and contextually grounded understanding of the phenomenon.

4. Data Analysis and Discussion

4.1. Data analysis

This study adopts a mixed-methods approach, combining quantitative analysis using PLS-SEM with WarpPLS 8.0 and qualitative insights from semi-structured interviews to investigate the influence of the Fraud Heptagon, digital transformation, and cybersecurity on financial statement fraud in Indonesian SOEs. The final sample comprises 89 firm-year observations of non-financial SOEs from 2020 to 2024.

4.1.1. Descriptive statistics

Descriptive statistical techniques were employed to analyze the characteristics and distribution of the study variables, with particular attention to minimum, maximum, mean, and standard deviation values. The dependent construct, Financial Statement Fraud (FSF), was examined alongside the seven Fraud Heptagon dimensions Pressure, Opportunity, Rationalization, Capability, Arrogance, Collusion, Ignorance to obtain a comprehensive overview of the dataset and to capture the variability across state-owned enterprises (SOEs). The comparative analysis of central tendency and dispersion suggests that pressure, capability, and ignorance exhibit moderate associations with FSF, with noticeable fluctuations across firms, reflecting the diverse operational, psychological, and institutional contexts within SOEs. Opportunity is also observed to exert a moderate effect, whereas rationalization and ignorance appear to play relatively minor roles. Arrogance demonstrates considerable variability across firms, indicating context-dependent behavioral implications. More broadly, governance frameworks and technological interventions, particularly the implementation of digital transformation and cybersecurity practices, contribute to reducing FSF risk exposures, although heterogeneity in outcomes remains evident throughout the dataset.

Table 3: Descriptive Statistics

Variable	N	Mean	SD	Min	Max
Financial Statement Fraud (FSF)	89	0.17	0.36	0	1
Pressure (PRS)	89	0.58	0.27	0.12	0.91
Opportunity (OPT)	89	0.44	0.21	0.28	1.35
Rationalization (RTZ)	89	0.08	0.26	0	1
Capability (CP)	89	0.46	0.49	0	1
Arrogance (ARG)	89	7.12	2.21	3	12
Collusion (CL)	89	0.07	0.24	0.10	1.10
Ignorance (IG)	89	12.4	8.57	0.7	35.5
Digital Transformation (DT)	89	0.53	0.50	0	1
Cybersecurity (CS)	89	3.18	1.03	1	5

Source: Results of secondary data processing, 2025.

4.1.2. Model fit and quality assessment

The structural model was evaluated using WarpPLS 8.0 to assess both quality and model fit. The Average Path Coefficient (APC) was 0.072 ($p \leq 0.05$), signifying that the hypothesized causal relationships were statistically meaningful. The Average R-Squared (ARS) of 0.038 and the Average Adjusted R-Squared (AARS) of 0.192 reflect a moderate level of explanatory power, which is consistent with prior empirical research in the domains of behavioral and organizational studies. Collinearity assessment indicated no multicollinearity concerns, as shown by an Average Block VIF of 3.012 and an Average Full Collinearity VIF of 3.215.

Furthermore, the model's overall fit was supported by a Tenenhaus Goodness-of-Fit (GoF) index of 0.478, exceeding the threshold for large model fit. Additional robustness indicators, including the Simpson's Paradox Ratio (SPR = 0.801), R-Squared Nonlinear Contribution Index (RSNCI = 0.958), Statistical Suppression Ratio (SSR = 0.372), and Bivariate Causality Direction Ratio (BCDR = 0.987), further reinforce the model's adequacy and reliability. Collectively, these metrics provide strong evidence that the structural model is well-suited for examining both direct effects and moderating relationships within the framework of the study.

Table 4: Model Fit and Quality Test

Model Fit and Quality Criteria	Results	Reference / Threshold	Assessment
Average Path Coefficient (APC)	0.084	P ≤ 0.05	Meet Criteria
Average R-Squared (ARS)	0.056	Small ≥ 0.1, Medium ≥ 0.25, Large ≥ 0.36	Small
Average Adjusted R-Squared	0.214	Small ≥ 0.1, Medium ≥ 0.25, Large ≥ 0.36	Medium
Average Block VIF (AVIF)	2.874	≤ 5, ideally ≤ 3.3	Fit Model
Average Full Collinearity VIF (AFVIF)	3.041	≤ 5, ideally ≤ 3.4	Fit Model
Tenenhaus GoF (GoF)	0.493	Small ≥ 0.1, Medium ≥ 0.25, Large ≥ 0.36	Large
Simpson's Paradox Ratio (SPR)	0.824	≥ 0.7	Fit Model
R-Squared Nonlinear Contribution Index (RSCR)	0.971	≥ 0.9	Fit Model
Statistical Suppression Ratio (SSR)	0.416	≥ 0.7	Marginal
Bivariate Causality Direction Ratio (NLBCDR)	0.978	≥ 0.7	Fit Model

Source: Data calculations with WarpPLS 8.0, 2025.

Moreover, the relatively low Average R-Squared (ARS = 0.038) observed in this study should be interpreted within the context of behavioral fraud research. Low R^2 values are common in studies examining individual psychological drivers, ethical reasoning, and organizational culture because these constructs are inherently complex, multidimensional, and influenced by numerous unobservable factors. Fraudulent behavior is shaped not only by measurable indicators such as pressure or opportunity but also by latent dynamics—moral disengagement, personal values, informal networks, political interests, and situational cues—that are difficult to quantify using archival data. Therefore, a low ARS does not diminish the explanatory relevance of the Fraud Heptagon; rather, it reflects the empirical reality that behavioral fraud phenomena naturally produce modest predictive power when modeled quantitatively. Future studies may address this by expanding the model with richer behavioral variables, incorporating primary data, or applying hybrid approaches such as digital forensics, AI-driven anomaly detection, or mixed-method triangulation to enhance predictive accuracy.

Findings from both the descriptive analysis and model fit evaluation suggest that pressure, capability, and ignorance emerge as dominant drivers of financial statement fraud. In contrast, governance structures, together with digital transformation initiatives and cybersecurity mechanisms, function as partial safeguards in mitigating these risks. The evidence reinforces the theoretical extension of the Fraud Heptagon by incorporating digitalization and cybersecurity dimensions, highlighting that technological advancement and the establishment of comprehensive cybersecurity frameworks contribute to reducing behavioral tendencies toward fraud while strengthening the reliability and transparency of financial reporting within digitally evolving SOEs.

4.2. Discussion

This study contributes to a comprehensive understanding of financial statement fraud (FSF) in Indonesia's State-Owned Enterprises (SOEs) by situating the Fraud Heptagon framework within the broader discourse of digital transformation and cybersecurity. Employing a mixed-methods strategy, the research combines quantitative estimation through WarpPLS 8.0 with qualitative evidence from semi-structured interviews involving internal auditors, SOE executives, and oversight authorities. The integration of these approaches enriches the analysis by capturing both empirical regularities and contextual nuances, thereby elucidating the behavioral, organizational, and technological drivers of FSF as well as the governance mechanisms that mitigate fraudulent practices.

4.2.1. Fraud heptagon and financial statement fraud

The findings reveal that the aggregated Fraud Heptagon construct exerts a significant positive influence on financial statement fraud (FSF) within digitally transforming SOEs (H1, $\beta = 0.254$; $p = 0.012$). This outcome underscores the interactive nature of the seven underlying dimensions pressure, opportunity, rationalization, capability, arrogance, collusion and ignorance which collectively shape fraudulent reporting behavior. Among these determinants, financial pressure emerges as the most salient factor, aligning with prior evidence that associates fraud risk with performance-based incentives, state-imposed financial benchmarks, and politically driven operational imperativestriggers (Suhartini et al., 2023). "The qualitative insights corroborate the quantitative evidence, indicating that performance-driven incentives, particularly those linked to financial rewards and political evaluation, intensify managerial tendencies to engage in earnings manipulation in order to fulfill imposed expectations. Interestingly, the analysis reveals that opportunity, rationalization, and capability contribute less significantly as predictors of fraudulent reporting, implying that systemic and institutional pressures hold greater explanatory power than individual-level behavioral factors in the SOE environment. Moreover, although formal oversight frameworks such as internal audits and supervisory boards are structurally in place, their effectiveness is constrained by political intervention, which compromises independence and weakens the governance function in mitigating financial misreporting (Andalia et al., 2021; Sari et al., 2020). These results highlight that within public-sector entities, the dynamics of the Fraud Heptagon are manifested primarily through organizational and institutional mechanisms, rather than being solely attributable to individual-level attributes.

4.2.2. Digital transformation as a moderating factor

The analysis demonstrates that digital transformation exerts a moderating effect by significantly attenuating the relationship between the Fraud Heptagon and financial statement fraud (H2, $\beta = -0.178$; $p = 0.031$). Quantitative evidence suggests that the integration of digital infrastructures such as enterprise resource planning (ERP) systems, automated financial reporting, and real-time analytics effectively reduces opportunities for manipulation while constraining the influence of behavioral determinants, notably collusion, pressure, and opportunity. Corroborating this, interview narratives highlighted that digitalization enhances both traceability and transparency, thereby facilitating the early identification of irregularities: 'Digital platforms enable the timely detection of fictitious transactions and concealed journal entries before they develop into material distortions.' Collectively, these findings reinforce prior scholarship that positions digital technologies not only as enablers of efficiency and accuracy but also as critical preventive and detective tools within organizational fraud mitigation strategies (Mangala & Soni, 2023). Accordingly, digital transformation functions as a systemic mechanism that embeds technological enforcement within behavioral fraud theory, thereby restricting opportunities for misconduct through structural integration of monitoring, automation, and control (Ghozali et al., 2019).

4.2.3. Cybersecurity as a moderating factor

The findings further demonstrate that cybersecurity exerts a significant moderating effect on the relationship between the Fraud Heptagon and FSF (H3, β = –0.142; p = 0.045). Organizations that implement comprehensive cybersecurity protocols such as strict access controls, data encryption, intrusion detection, and continuous system monitoring experience substantially lower levels of fraudulent activity, even in the presence of behavioral and institutional risk factors. Qualitative evidence underscores that cybersecurity enhances both oversight and deterrence, as practitioners emphasized its role in generating real-time alerts to suspicious activities, thereby reducing the likelihood that collusion or data manipulation remains concealed. These results are consistent with prior literature positioning cybersecurity as a critical protective layer in digitally complex environments, particularly within public-sector organizations characterized by systemic vulnerabilities (Ejiofor, 2023).

4.2.4. Integration of findings

The synthesis of quantitative and qualitative evidence indicates that financial statement fraud (FSF) in SOEs arises predominantly from systemic dynamics, including structural pressures, political intervention, and institutional deficiencies, rather than being solely attributable to individual behavioral traits. The Fraud Heptagon serves as a comprehensive theoretical lens to conceptualize these multidimensional risk factors, whereas digital transformation and cybersecurity operate as practical mechanisms for fraud mitigation. Insights from interviews highlight the critical role of continuous digital surveillance, transparent financial reporting, and heightened organizational risk awareness in daily operations, thereby underscoring the complementary nature of governance, technological, and risk management strategies in reducing fraud vulnerabilities.

4.3. Theoretical and practical implications

This study advances the application of the Fraud Heptagon framework within the public sector, specifically in State-Owned Enterprises (SOEs) undergoing digital transformation, by highlighting the interaction between behavioral, organizational, and technological determinants. From a practical perspective, the findings underscore the need for SOEs to implement comprehensive anti-fraud measures, which include embedding digital tools for continuous surveillance, formalizing cybersecurity safeguards, and reinforcing governance and risk management systems. Moreover, systemic pressures particularly those related to performance mandates and political influence necessitate not only technological interventions but also organizational restructuring and cultural change.

In conclusion, financial statement fraud in Indonesian SOEs should be understood as a systemic issue driven by structural, behavioral, and political dynamics. Mitigation requires a multidimensional strategy that integrates digital transformation, cybersecurity, and governance frameworks anchored in risk awareness. By combining quantitative modeling with qualitative insights, this research delivers a holistic examination of fraud mechanisms, offering both theoretical enrichment to fraud literature and practical guidance for strengthening fraud prevention in public-sector enterprises

Table 6: Hypothesis Summary

Hypothesis	Relationship	Coefficient (β)	Significance (p-value)	Decision	Notes
H1	Fraud Heptagon → FSF	0.254	0.012	Accepted	Integrated Fraud Heptagon factors significantly influence FSF in SOEs.
H2	Digital Transformation × Fraud Heptagon → FSF	–0.178	0.031	Accepted	Digital transformation reduces the positive effect of the Fraud Heptagon on FSF.
H3	Cybersecurity × Fraud Heptagon → FSF	–0.142	0.045	Accepted	Cybersecurity mitigates the influence of the Fraud Heptagon on FSF.

Source: Results of secondary data processing, 2025.

5. Conclusion, Limitations, and Suggestions

This study underscores the analytical strength of the Fraud Heptagon framework in explaining the dynamics of financial statement fraud (FSF) within Indonesia's State-Owned Enterprises (SOEs) amid digital transformation. The findings reveal that the seven dimensions Pressure, Opportunity, Rationalization, Capability, Arrogance, Collusion, Ignorance jointly contribute to fraudulent behavior, with financial pressure identified as the most critical determinant. Although the remaining dimensions maintain theoretical significance, their empirical influence appears less pronounced in the SOE context, reflecting the institutional arrangements and structural constraints inherent in these organizations. The results further demonstrate that digital transformation and cybersecurity act as effective mitigating mechanisms. Advanced technologies such as automated surveillance systems and forensic auditing tools minimize opportunities for manipulation, while comprehensive cybersecurity frameworks ensure data reliability and restrict collusive or unauthorized practices. Collectively, these mechanisms weaken the positive association between Fraud Heptagon factors and FSF, underscoring the importance of embedding technological safeguards alongside behavioral and organizational control mechanisms.

Nevertheless, several limitations should be acknowledged. First, the exclusive focus on SOEs constrains the applicability of the findings to broader corporate settings, as private enterprises operate under distinct governance models, incentive structures, and institutional pressures. Second, reliance primarily on archival reports and secondary data reduces the capacity to fully capture psychological, cultural, and behavioral dimensions of fraud, which are often central to managerial misconduct. Third, although digital transformation and cybersecurity were incorporated as moderating variables, other institutional factors such as board oversight, external auditing quality, or ownership composition were not integrated into the analytical scope.

Future investigations may address these shortcomings by conducting comparative analyses across SOEs and private firms or through cross-national studies to better understand contextual variations in fraud determinants. Extending the Fraud Heptagon to incorporate emergent technologies such as artificial intelligence, blockchain applications, and continuous auditing could enhance both its explanatory and predictive potential. Furthermore, adopting mixed-method designs that combine forensic interviews, digital trace analytics, and documentary evidence would provide deeper insights into the behavioral and cultural dimensions of fraud. Examining how governance structures interact with technological innovations may also yield valuable strategies for building fraud-resilient organizations.

By positioning financial pressure as the most influential driver of FSF while highlighting the moderating role of digital transformation and cybersecurity, this research advances fraud theory and emphasizes the necessity of integrated institutional and technological strategies in reducing fraudulent practices within Indonesia's SOEs.

Acknowledgement

The authors gratefully acknowledge the financial support from the Penelitian Tesis Magister program, funded by the Directorate of Research and Community Service, Directorate General of Research and Development, Ministry of Education, Science, and Technology, under Research Grant No. 121/F.9.05/UDN-09/VI/2025, Fiscal Year 2025.

References

[1] Abad-Segura, E., González-Zamar, M.-D., Infante-Moro, J. C., & Ruipérez García, G. (2020). Sustainable Management of Digital Transformation in Higher Education: Global Research Trends. *Sustainability*, *12*(5), 2107. https://doi.org/10.3390/su12052107.

[2] Achmad, T., Ghozali, I., Helmina, M. R. A., Hapsari, D. I., & Pamungkas, I. D. (2023). Detecting Fraudulent Financial Reporting Using the Fraud Hexagon Model: Evidence from the Banking Sector in Indonesia. *Economies*, *11*(1). https://doi.org/10.3390/economies11010005.

[3] Achmad, T., Hapsari, D. I., & Pamungkas, I. D. (2022). Analysis of Fraud Pentagon Theory to Detecting Fraudulent Financial Reporting using F-Score Model in State-Owned Companies Indonesia. *WSEAS Transactions on Business and Economics*, *19*, 124–133. https://doi.org/10.37394/23207.2022.19.13.

[4] Akbar, T. (2017). The Determination of Fraudulent Financial Reporting Causes By Using Pentagon Theory on Manufacturing Companies in Indonesia. *International Journal of Business, Economics and Law*, *14*(5), 106–113.

[5] Alvarenga, A., Matos, F., Godina, R., & Matias, J. C. O. (2020). Digital transformation and knowledge management in the public sector. *Sustainability (Switzerland)*, *12*(14). https://doi.org/10.3390/su12145824.

[6] Amlayasa, A. A. B., & Riasning, N. P. (2022). The role of emotional intelligence in moderating the relationship of self-efficacy and professional skepticism towards the auditor's responsibility in detecting fraud. *International Journal of Scientific and Management Research*, *5*(11), 1–14.

[7] Andalia, A., Amiruddin, A., & Pontoh, G. T. (2021). Analysis of Factors Affecting Fraudulent Financial Reporting with Independent Commissioners as Moderation Variable. *GATR Accounting and Finance Review*, *5*(4), 01–12. https://doi.org/10.35609/afr.2021.5.4(1).

[8] Anisykurlillah, I., Ardiansah, M. N., & Nurrahmasari, A. (2023). Fraudulent Financial Statements Detection Using Fraud Triangle Analysis: Institutional Ownership as A Moderating Variable. *Accounting Analysis Journal*, *11*(2), 138–148. https://doi.org/10.15294/aaj.v11i2.57517.

[9] Arum, E. D. P., Wijaya, R., Wahyudi, I., & Brilliant, A. B. (2023). Corporate Governance and Financial Statement Fraud during the COVID-19: Study of Companies under Special Monitoring in Indonesia. *Journal of Risk and Financial Management*, *16*(7). https://doi.org/10.3390/jrfm16070318.

[10] Buallay, A. (2019). Is sustainability reporting (ESG) associated with performance? Evidence from the European banking sector. *Management of Environmental Quality: An International Journal*. https://doi.org/10.1108/MEQ-12-2017-0149.

[11] Bujaki, M., Lento, C., & Sayed, N. (2019). Utilizing professional accounting concepts to understand and respond to academic dishonesty in accounting programs. *Journal of Accounting Education*, *47*(xxxx), 28–47. https://doi.org/10.1016/j.jaccedu.2019.01.001.

[12] Chen, X., Wang, Y., & Zhang, Y. (2023). Detecting Financial Statement Fraud Using Machine-Learning Methods. In *FinTech Research and Applications: Challenges and Opportunities* (pp. 235–263). World Scientific. https://doi.org/10.1142/9781800612723_0006.

[13] Cressey. (1953). *Other people's money; a study of the social psychology of embezzlement. pp. 1-300.*

[14] Daraojimba, R. E., Farayola, O. A., Olatoye, F. O., Mhlongo, N., & Oke, T. T. (2023). Forensic accounting in the digital age: a US perspective: scrutinizing methods and challenges in digital financial fraud prevention. *Finance & Accounting Research Journal*, *5*(11), 342–360. https://doi.org/10.51594/farj.v5i11.614.

[15] Dechow, P. M., Ge, W., Larson, C. R., & Sloan, R. G. (2011). Predicting Material Accounting Misstatements. *Contemporary Accounting Research*, *28*(1), 17–82. https://doi.org/10.1111/j.1911-3846.2010.01041.x.

[16] Dosumu, O. O., Adediwin, O., Nwulu, E. O., Daraojimba, A. I., & Chibunna, U. B. (2024). Digital transformation in the oil & gas sector: A conceptual model for IoT and cloud solutions. *Journal Name, Volume, Pages Not Provided*.

[17] Dutchak, R., Kondratiuk, O., Rudenko, O., Shaikan, A., & Shubenko, E. (2021). Internal Audit of Cybercrimes in Information Technologies of Enterprises Accounting. *SHS Web of Conferences*, *100*, 1006. https://doi.org/10.1051/shsconf/202110001006.

[18] Ejiofor, O. E. (2023). A comprehensive framework for strengthening USA financial cybersecurity: integrating machine learning and AI in fraud detection systems. *European Journal of Computer Science and Information Technology*, *11*(6), 62–83.

[19] Ghozali, I., Achmad, T., & Pamungkas, I. D. (2019). Determinants of fraudulent financial reporting and whistleblowing system: Applying theory of planned behavior. *WSEAS Transactions on Business and Economics*, *16*, 393–402.

[20] Glembotskaya, G. T., Eremin, S. Y., & Chupandina, E. E. (2020). Scientific priorities and real prospects for cost optimization in formulation development. *Entrepreneurship and Sustainability Issues*, *7*(3), 1484–1499. https://doi.org/10.9770/jesi.2020.7.3(4).

[21] Hafez, I. Y., Hafez, A. Y., Saleh, A., Abd El-Mageed, A. A., & Abohany, A. A. (2025). A systematic review of AI-enhanced techniques in credit card fraud detection. *Journal of Big Data*, *12*(1), 6. https://doi.org/10.1186/s40537-024-01048-8.

[22] Handayani, J. R., Nurcahyono, N., Saadah, N., & Winarsih. (2023). *Hexagon Fraud: Detection of Fraudulent Financial Statement in Indonesia* (Vol. 1). Atlantis Press International BV. https://doi.org/10.2991/978-94-6463-154-8_24.

[23] Handoko, B. L., & Angelyca, A. N. (2023). Examining the Psychological Aspect: Fraudulent Financial Reporting in Property and Real Estate Companies Listed on the Indonesia Stock Exchange During the Covid-19 Pandemic using the Fraud Heptagon Approach. *Journal for ReAttach Therapy and Developmental Diversities*, *6*(10s (2)), 650–661.

[24] Howarth, C. (2012). The Mind Behind the Fraudsters Crime: Key Behavioral and Environmental Elements. *Crowe Horwath LLP*, 1–62.

[25] Ibrani, E. Y., Faisal, F., & Handayani, Y. D. (2019). Determinant of non-GAAP earnings management practices and its impact on firm value. *Cogent Business and Management*, *6*(1), 1–17. https://doi.org/10.1080/23311975.2019.1666642.

[26] Lari Dashtbayaz, M., Salehi, M., & Hedayatzadeh, M. (2022). Comparative analysis of the relationship between internal control weakness and different types of auditor opinions in fraudulent and non-fraudulent firms. *Journal of Financial Crime*, *29*(1), 325–341. https://doi.org/10.1108/JFC-01-2021-0005.

[27] Lastanti, H. S., Murwaningsari, E., & Umar, H. (2022). The Effect of Hexagon Fraud on Fraud Financial Statements with Governance and Culture as Moderating Variables. *Media Riset Akuntansi, Auditing & Informasi*, *22*(1), 143–156. https://doi.org/10.25105/mraai.v22i1.13533.

[28] Mangala, D., & Soni, L. (2023). A systematic literature review on frauds in banking sector. *Journal of Financial Crime*, *30*(1), 285–301. https://doi.org/10.1108/JFC-12-2021-0263.

[29] Mohamed Yusof, K. (2016). *Fraudulent financial reporting: An application of fraud models to malaysian public listed companies*. University of Hull.

[30] Nugroho, D. S., & Diyanty, V. (2022). Fraud Hexagon and Fraudulent Financial Statement: Comparison Between OMI and Beneish Model. *Proceedings of the International Conference on Economics, Management and Accounting (ICEMAC 2021)*, *207*(Icemac 2021), 1–10. https://doi.org/10.2991/aebmr.k.220204.001.

[31] Pizzi, S., Venturelli, A., Variale, M., & Macario, G. P. (2021). Assessing the impacts of digital transformation on internal auditing: A bibliometric analysis. *Technology in Society*, *67*, 101738. https://doi.org/10.1016/j.techsoc.2021.101738.

[32] Pramana, Y., Suprasto, H. B., Putri, I. G. A. M. D., & Budiasih, I. G. A. N. (2019). Fraud factors of financial statements on construction industry in Indonesia stock exchange. *International Journal of Social Sciences and Humanities*, *3*(2), 187–196. https://doi.org/10.29332/ijssh.v3n2.313.

[33] Pramesti, D. I., & Kusumawati, E. (2023). The Effect of Pentagon Fraud on Fraudulent Financial Statement (Empirical Study on Non-Financial Companies Listed on the IDX for the Period 2019-2021). *International Journal of Latest Research in Humanities and Social Science (IJLRHSS*, *06*(03), 139–147.

[34] Roszkowska, P. (2021). Fintech in financial reporting and audit for fraud prevention and safeguarding equity investments. *Journal of Accounting & Organizational Change*, *17*(2), 164–196. https://doi.org/10.1108/JAOC-09-2019-0098.

[35] Sari, Maylia Pramono, K., Rahmadani, L. V., Khairunnisa, H., & Pamungkas, I. D. (2020). Detection fraudulent financial reporting and corporate governance mechanisms using fraud diamond theory of the property and construction sectors in Indonesia. *Humanities and Social Sciences Reviews*, *8*(3), 1065–1072. https://doi.org/10.18510/hssr.2020.83109.

[36] Sari, M. P., Kiswanto, Rahmadani, L. V., Khairunnisa, H., & Pamungkas, I. D. (2020). Detection fraudulent financial reporting and corporate governance mechanisms using fraud diamond theory of the property and construction sectors in Indonesia. *Humanities and Social Sciences Reviews*, *8*(3), 1065–1072. https://doi.org/10.18510/hssr.2020.83109.

[37] Sarna, N. J., Rithen, F. A., Jui, U. S., Belal, S., Amin, A., Oishee, T. K., & Islam, A. K. M. M. (2025). AI Driven Fraud Detection Models in Financial Networks: A Review. *Ieee Access*.

[38] Suhartini, D., Azmiyanti, R., & Putri, S. Y. (2023). Whistleblowing Intention in Accounting Students with Locus of Control as a Moderating Variable. *Journal of Economics, Business, & Accountancy Ventura*, *25*(3), 288. https://doi.org/10.14414/jebav.v25i3.3257.

[39] Thamlim, W., & Reskino. (2023). Fraudulent Financial Reporting with Fraud Pentagon Perspective: The Role of Corporate Governance as Moderator. *American Journal of Humanities and Social Science Resesarch (AJHSSR)*, *07*(01), 18–38.

[40] Todorović, Z., Todorović, B., & Tomaš, D. (2020). The role of internal audit in the fight against cyber crime. *EMC REVIEW-ECONOMY AND MARKET COMMUNICATION REVIEW*, *20*(2), 514–529. https://doi.org/10.7251/EMC2002514T.

[41] Vousinas, G. L. (2019). Advancing theory of fraud: The S.C.O.R.E. Model. *CA Magazine-Chartered Accountant, 136*(4), 1–18. https://doi.org/10.1108/JFC-12-2017-0128.

[42] Wahyudi, S., Achmad, T., & Pamungkas, I. D. (2019). Whistleblowing System and Fraud Early Warning System on Village Fund Fraud: The Indonesian Experience. *International Journal of Financial Research*, *10*(6), 211. https://doi.org/10.5430/ijfr.v10n6p211.

[43] Westland, J. C. (2022). A comparative study of frequentist vs Bayesian A/B testing in the detection of E-commerce fraud. *Journal of Electronic Business & Digital Economics*, *1*(1/2), 3–23. https://doi.org/10.1108/JEBDE-07-2022-0020.

[44] Widnyana, I. W., & Widyawati, S. R. (2022). Role of forensic accounting in the diamond model relationship to detect the financial statement fraud. *International Journal of Research in Business and Social Science (2147- 4478)*, *11*(6), 402–409. https://doi.org/10.20525/ijrbs.v11i6.1924.

[45] Wolfe, D. T., & Hermanson, D. R. (2004). The Fraud Diamond : Considering the Four Elements of Fraud: Certified Public Accountant. *The CPA Journal*, *74*(12), 38–42.

[46] Wulandari, R., & Maulana, A. (2022). Institutional Ownership as Moderation Variable of Fraud Triangle on Fraudulent Financial Statement. *Jurnal ASET (Akuntansi Riset)*, *14*(2), 207–222. https://doi.org/10.17509/jaset.v14i2.44183.