

Emirati Journal of Business, Economics and Social Studies
Vol 5 Issue 2 (2026)
Pages 345 - 355
Available at
www.emiratesscholar.com

Beyond the Fraud Triangle: Developing a Technology-Enabled Theory of Fraud in the Digital Accounting Era.

Dikko Bello
Department of Accounting, Alqalam University, Katsina, Nigeria

ARTICLE INFO

KEYWORDS
Technology-Enabled Fraud Framework (TEFF); Socio-Technical Systems; Affordance Theory; Algorithmic Governance; Forensic Accounting; Accounting Information Systems.

HOW TO CITE
Bello, D. (2026). Beyond the Fraud Triangle: Developing a Technology-Enabled Theory of Fraud in the Digital Accounting Era. Emirati Journal of Business, Economics and Social Studies, 5(2), 345-355.
https://doi.org/10.54878/rdx9qz46

ABSTRACT

Accounting environments increasingly rely on cloud systems, automated processes, distributed technologies, and artificial intelligence. Although established fraud models provide useful explanations of human behavior, they give limited attention to the role of technology in contemporary accounting systems. This study addresses this limitation by developing the Technology-Enabled Fraud Framework (TEFF), which incorporates technological conditions into the explanation of how financial misconduct can arise and be concealed. The study draws on Socio-Technical Systems Theory, socio-materiality, and Affordance Theory to develop a four-dimensional framework from the forensic accounting and Accounting Information Systems literature. The framework comprises four constructs: Digital Pressure, Technological Opportunity, Digital Rationalization, and Technological Capability. Each construct captures a different way in which digital systems may influence fraud-related behavior. Four propositions are developed to explain the proposed relationships among these dimensions and technology-enabled financial misconduct. The framework extends fraud theory by considering these conditions alongside human behavior and has implications for internal control and continuous auditing. The study offers a socio-technical perspective in which technology is considered an important component of contemporary fraud processes.

Double-blind peer review by independent reviewers.
Received: 24 Jul 2026, Accepted: 29 Oct 2026, Published: 12 Nov 2026
*Corresponding author: dikkobello69@gmail.com
Copyright: © 2026 by the author. Licensee Emirates Scholar Center for Research & Studies, UAE.
Open access under the Creative Commons Attribution (CC BY) license
https://creativecommons.org/licenses/by/4.0

1. Introduction

Financial fraud continues to pose significant challenges for corporate governance, capital markets, and the reliability of financial reporting. Over several decades, accounting research has examined the factors associated with fraudulent financial conduct, developing seminal conceptual frameworks grounded predominantly in behavioral psychology and organizational control theory. The foundational Fraud Triangle Theory (Cressey, 1953) attributed fraudulent behavior to the convergence of three lconstructs: pressure, opportunity, and rationalization. Subsequent theoretical extensions, notably the Fraud Diamond (Wolfe & Hermanson, 2004) and the Fraud Pentagon (Marks, 2012), enriched these explanations by introducing individual capability, arrogance, and competence.

These models remain useful, but their explanations were developed largely around human behavior and controls. They were conceived within human-centric, manual, or early computerized enterprise environments. In those situations operational agency resided exclusively in interpersonal relationships. In these classical frameworks, the focus of agency is exclusively human. Technology, when acknowledged, is treated either as an external tool used to execute an act or as a passive computational mechanism designed for ex-post internal control and anomaly detection.

However, the accounting environment has changed substantially with the adoption of cloud-based systems, automation. The widespread integration of cloud-native enterprise resource planning (ERP) tools, autonomous smart contracts, robotic process automation (RPA), machine learning decision engines, and application programming interfaces (APIs) has isolated transaction processing and financial reporting from direct, visible human intervention (Appelbaum et al., 2017; Moffitt et al., 2018; Wang & Cuthbertson, 2015). Accounting data is no longer merely recorded by human hands. It is now integrated and reconciled through multi-layered pipelines.

Table 1: Theoretical Structural transformation

Classical Anthropocentric Paradigm	Contemporary Socio-Technical Paradigm
• Human-to-Human transactional agency • Technology as a passive recording tool • Opportunity = Weak internal controls • Pressure = Interpersonal/Managerial • Rationalization = Social justifications	• Human-to-Algorithm & API-driven execution • Technology as an active non-human actant • Opportunity = Architectural vulnerability • Pressure = Algorithmic surveillance & KPIs • Rationalization = Virtual abstraction

Source: Author

These changes raise an important limitation for existing fraud theories. This is because they were conceptualized under the assumption that financial transactions are governed and executed through direct human-to-human agency. Consequently, they cannot adequately explain misconduct that emerges at the boundary between human intent and systemic algorithmic potential. While classical theories explain why individuals desire to commit fraud, they offer limited insight into how digital environments enable such. Greater attention to technological conditions is therefore needed if fraud theory is to explain misconduct enterprise systems.

Several changes illustrate this limitation. Real-time dashboards can place employees under continuous performance monitoring, while software vulnerabilities, access-control weaknesses, and fragmented system designs can create opportunities that are not captured by traditional segregation-of-duties controls. Digital interfaces may also create greater distance between an individual and the consequences of a transaction. In addition, access to technical knowledge may become more important than formal position when digital systems are manipulated. By continuing to relegate technology to the background, current fraud literature struggles to explain how algorithmic environments enable fraudulent behavior.

To bridge this theoretical gap, this article develops the Technology-Enabled Fraud Framework (TEFF). Grounded in Socio-Technical Systems (STS) Theory and Affordance Theory, TEFF views fraud as a socio-technical phenomenon arising from the interaction between human behavior and digital systems. The framework comprises four dimensions. Digital Pressure refers to stress associated with continuous monitoring and automated performance targets. Technological Opportunity captures vulnerabilities arising from system

schemes and limited transparency. Digital Rationalization concerns the ways in which digital abstraction affects moral justification. Technological Capability refers to the technical knowledge required to exploit digital systems.

This study contributes to the literature in three ways:

1. Extension of the theoretical perspective: It considers the interaction between human actors and technological systems. It demonstrates that high-tech systems possess non-human agency that enables illicit acts. Thus, it places greater emphasis on the interaction between human decisions and technical conditions.
2. Construct Operationalization: It defines four distinct dimensions—Digital Pressure, Technological Opportunity, Digital Rationalization, and Technological Capability—providing clear sub-dimensions suitable for empirical validation.
3. Implications for governance and internal control: It derives theoretical propositions that guide future empirical inquiry and provide a basis for considering how internal controls may need to adapt to increasingly automated accounting systems.

2. Theoretical Foundations & Evolution of Fraud Models.

2.1 Systematic Evolution and Constraints of Classical Models.

Fraud research has traditionally examined financial misconduct from psychological and organizational perspectives, with particular attention to the behavior of individual perpetrators. Cressey's (1953) foundational Fraud Triangle established that occupational fraud emerges from the convergence of financial pressure, perceived opportunity, and cognitive rationalization. Wolfe and Hermanson (2004) subsequently extended the model by introducing the Fraud Diamond, positing that individual's authority is a mandatory prerequisite for exploiting control weaknesses. Subsequent theoretical extensions, such as the Fraud Pentagon (Marks, 2012) and the S.C.O.R.E. model (Vousinas, 2019), further enriched this discourse by integrating behavioral variables like arrogance and competence.

Although these frameworks remain influential, they give limited attention to the role of hi-tech expertise in fraud processes. They hypothesize this environment as a passive medium through which human agency operates. In these models, technology is relegated to a dualistic role. Seen either as an external tool utilized to execute a crime or as a static internal control mechanism designed to detect anomalies (Munoko et al., 2020). This limitation becomes more relevant in contemporary Accounting Information Systems (AIS), where autonomous algorithms, robotic process automation (RPA), and interconnected APIs increasingly mediate financial execution with minimal direct human intervention (Ahmi, 2026).

Table 2: Comparative Evolution of Fraud Theoretical Paradigms.

Fraud framework	Core dimensions	Locus of agency	Role of technology	Key boundary inadequacy
Fraud Triangle(Cressey, 1953)	Pressure; opportunity; rationalization	Individual human actor	Passive recording and control medium	Primarily assumes human-to-human control interactions and provides limited explanation of fraud enabled by autonomous digital processes.
Fraud Diamond(Wolfe & Hermanson, 2004)	Pressure; opportunity; rationalization; capability	Individual actor, particularly through position, access, and capability	Passive tool used by individuals with authority or access	Conceptualizes capability primarily as an individual characteristic and gives limited attention to technological

				fluency and system-level capabilities.
Fraud Pentagon(Marks, 2012)	Pressure; opportunity; rationalization; competence; arrogance	Individual personality and organizational position	Passive operating environment	Emphasizes individual psychological and positional characteristics while giving insufficient attention to architectural affordances, system opacity, and digitally mediated fraud.
S.C.O.R.E. Model(Vousinas, 2019)	Stimulus; capability; opportunity; rationalization; ego	Individual and organizational actors	External contextual condition	Treats technology largely as part of the external environment.
Technological–Enabler Fraud Framework (TEFF)(Present study)	Digital pressure; technological opportunity; digital rationalization; technological capability	Socio-technical nexus involving human and non-human actors	Active non-human actors and structural condition	Specifically formulated to address fraud risks arising from cloud systems, APIs, algorithmic processes, automated controls, and digitally enabled AIS environments.

Note. AIS = accounting information systems. TEFF = Technological–Enabler Fraud Framework. The table synthesizes the conceptual evolution of fraud theories from predominantly individual-centred explanations toward a socio-technical perspective that incorporates technological agency.

Source: Author's synthesis based on Cressey (1953), Wolfe and Hermanson (2004), Marks (2012), and Vousinas (2019).

This limitation is relevant where accounting processes depend on distributed systems and automated controls. In such settings, weaknesses may arise from the interaction of system tools, access arrangements, data flows, and human decisions. TEFF therefore considers technological affordances alongside traditional control weaknesses when explaining fraud opportunities.

To resolve the explanatory constraints imposed by this anthropocentric view, fraud research requires an ontological modification. It need to consider technical infrastructure not as an external actor, but as an active participant. This theoretical pivot is provided by Socio-Technical Systems (STS) Theory and Actor-Network Theory (ANT), which establish the epistemological foundation for analyzing human-machine interaction in accounting.

2.2 Epistemological Foundations of Socio-Technical Systems (STS).

To address this limitation, this study anchors the Technology-Enabled Fraud Framework (TEFF) in the epistemologies of Socio-Technical Systems (STS) Theory and Actor-Network Theory (ANT). By showing how social dynamics and technical subsystems continuously shape outcomes (Bostrom & Heinen, 1977), STS provides a macro-level framework to examine digital accounting.

Furthermore, ANT (Latour, 2005) provides a basis for examining how human and non-human elements participate in processes. It posits that non-human things like ERP are effective agents that influence administrative reality. Digital accounting tools can influence how transactions are processed and how opportunities for misconduct arise (Orlikowski & Scott, 2008).

2.3 Affordance Theory and the Materiality of Digital Accounting.

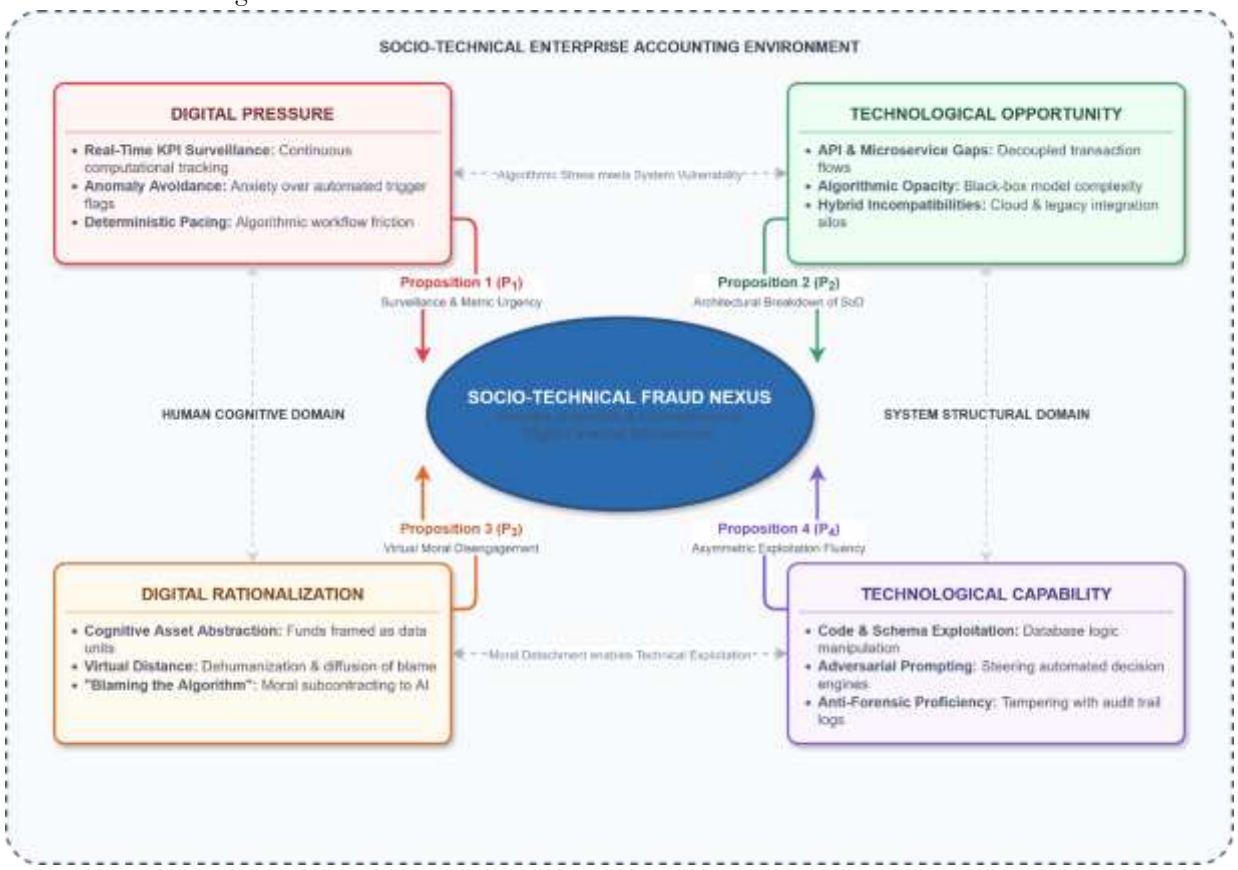
This study uses Affordance Theory in order to explain how digital architectures enable fraud. Introduced by Gibson in (1979), the theory was later extended to information systems research (Leonardi, 2011; Majchrzak & Markus, 2012). It was used to describe opportunities that emerge when users interact with technological tools.

In organizations, affordances exist because of the interaction between human agency and technological capabilities (Leonardi, 2011; Markus & Silver, 2008). In Accounting Information Systems, this contact dictates whether system architectures restrict or enable material financial misstatements. For instance, algorithmic ambiguity (Simeunović et al., 2023) masks misstatements inside data pipelines, while cloud-native microservices introduce access points that bypass traditional separation of duties (SoD) controls. Through a sociomaterial lens (Leonardi, 2012), the TEFF framework treats digital systems as active participants that shape fraudulent practices. The following section outlines TEFF's four core dimensions and models how they operate within accounting environments.

3. The Technology-Enabled Fraud Framework (TEFF).

TEFF uses socio-technical and affordance lenses to frame fraud as a direct outcome of human-system interactions. Instead of treating IT as docile background factor, TEFF models fraud across four distinct dimensions: Digital Pressure, Technological Opportunity, Digital Rationalization, and Technological Capability.

Figure 1. Technology-Enabled Fraud Framework (TEFF)



3.1 Workplace Monitoring and Performance Demands.

The TEFF extend the works of Appelbaum et al., (2024) and (Glan, 2026) in which they saw pressure arising from persistent monitoring and output quotas. Whereas classical fraud models attribute pressure to personal bankruptcy (Cressey, 1953) or executive demands (Dechow et al., 1996) ERP platforms and computerized performance management systems generate continuous demand which creates sources of behavioral pressure:

Real-Time KPI Surveillance Intensity: Continuous automatic evaluation enforces execution pace benchmarks and efficiency indices with strictness thereby creating pressure to maintain compliance.

Systemic Evasion of Oversight: Because algorithmic monitoring systems flag unusual transactions for audit review, such monitoring may create pressure to maintain reported inputs within specified parameters.

System-Enforced Behavior: Persistent tracking mechanisms create psychological conflict by transferring pressure from supervisory relationships to systemic compliance.

3.2 Technical Risks and Hidden System Logic.

According to Wolfe & Hermanson, (2004); Beasley, (1996), opportunity arises from weak internal controls and in some cases lack of duties segregation. TEFF extends the idea of opportunity to include weaknesses associated with enterprise software. Distributed cloud systems and interconnected applications can make audit trails more

difficult to monitor (Bandara et al., 2021; CISA, 2026). The folowing dimensions explains this opportunity:

In distributed cloud environments, technological opportunity manifests across three primary architectural vulnerabilities. First, event-driven communication between isolated ERP modules and external payment gateways creates unmonitored transfer channels that bypass standard oversight (Bandara et al., 2021; Brazel & Dang, 2008; Cybersecurity and Infrastructure Security Agency [CISA], 2026). Second, automated accounting increasingly relies on pattern-recognition algorithms that conceal underlying transaction pathways, generating an information asymmetry that minimizes reporting discrepancies from audit review (Munoko et al., 2020; Simeunović et al., 2023; Wamba et al., 2024). Finally, when databases interface with modern cloud or AI analytical layers, the resulting integration boundaries often lack traditional control mechanisms, leaving structural deficits that facilitate undetected financial alterations (Brazel & Dang, 2008).

3.3 Mechanisms of Digital Disengagement.

In traditional fraud models, rationalization refers to the explanations individuals use to justify misconduct to maintain a positive moral self-concept (Bandura, 1999; Dorminey et al., 2012). In technology-mediated settings, interfaces can create psychological distance between the user and the consequences of an action. (Leonardi, 2012; Moore et al., 2012):

While classical fraud theory views rationalization as an internal cognitive strategy used to preserve moral self-regard during misconduct (Bandura, 1999; Dorminey et al., 2012), technological mediation actively alters how individuals perceive their actions (Leonardi, 2012; Moore et al., 2012). In digital environments, this moral disengagement operates through three interrelated dynamics. First, interacting with numerical ledger entries rather than physical currency diminishes the psychological visibility of the real-world stakeholders and corporate assets affected by the manipulation. Second, because automated decision-making workflows lack direct physical interactions, individual culpability becomes diluted across distributed software layers (Bandura, 2002; Detert et al., 2008). Finally, perpetrators engage in moral subcontracting by blaming illicit transactions on algorithmic hallucinations or software errors, effectively transferring personal responsibility onto the technology itself (Alshurafat, 2023; Bandura, 2002; Detert et al., 2008; Mökander, 2023).

3.4 Technical Sophistication and System Evasion.

Wolfe and Hermanson (2004) regarded capability as an individual's power and skills. Within technology-mediated accounting system, access may become important complements to authority. This suggests an individual's competence to exploit technological affordances and evade forensic discovery (Dornheim & Zarnekow, 2025; Al-Sayyed, 2024).

Table 3.

TEFF Operational Constructs, Sub-Dimensions, and Empirical Indicators

Construct	Core conceptual definition	Key sub-dimensions	Observable empirical indicators
Digital Pressure	Structural stress arising from real-time computational monitoring, automated performance evaluation, and digitally enforced workflow targets.	• Real-time KPI surveillance• Automated anomaly monitoring• Deterministic workflow pacing	• Frequency and intensity of automated performance alerts• Evidence of automated KPI thresholds linked to performance evaluation• Rigid system-enforced workflow deadlines or pacing requirements
Technological Opportunity	Action possibilities created by weaknesses in digital architectures, interfaces, system integration, and limited transparency of automated processes.	• API and microservice vulnerabilities• Algorithmic opacity• Hybrid integration incompatibilities	• Existence of unmonitored or weakly controlled API endpoints• Limited explainability or transparency of automated decision processes• Documented integration gaps, synchronization failures, or control

			inconsistencies across distributed systems
Digital Rationalization	Cognitive mechanisms through which interface abstraction, virtual distance, and technological mediation facilitate the justification or normalization of inappropriate digital actions.	• Digital asset abstraction• Virtual distance and diffusion of responsibility• Algorithmic attribution of responsibility	• Treatment of financial or organizational resources as abstract digital records• Reduced visibility of affected parties within digitally mediated transactions• Attribution of inappropriate outcomes to system errors, algorithms, or automated processes
Technological Capability	Socio-technical competence required to exploit digital systems, direct system logic, and reduce the visibility of unauthorized digital activity.	• Code and database exploitation• Model directing• Digital trace evasion	• Ability to develop or modify scripts and database queries• Ability to steer automated models or algorithmic outputs• Ability to modify, conceal, or circumvent digital logs and audit trails

Note. TEFF = Technological–Enabler Fraud Framework. The indicators are proposed observable manifestations of the four TEFF constructs and should be refined and empirically validated through the subsequent measurement-development and construct-validation procedures.

Within accounting structures, technological capability requires technical proficiencies to execute and hide illicit activity, using knowledge of database diagrams and machine learning limitations to plan data misrepresentations. Individuals can manipulate prompt logic or feed biased inputs into automated decision models, driving reporting outcomes toward benchmarks without triggering automated irregularity warnings. Once alterations are executed, anti-forensic techniques prevent investigators from reconstructing the audit trail (Ahmi, 2026; Al-Sayyed, 2024; Amani & Fadlalla, 2017; Dornheim & Zarnekow, 2025).

In order to modify the framework into a testable empirical model, the relationships among these four dimensions must be operationalized. The next section establishes propositions that detail how these socio-technical interactions drive technology-enabled financial misstatements.

While defining the four TEFF dimensions provides a necessary theoretical classification, positioning the framework for empirical investigation requires specifying the mechanisms through which these socio-technical conditions produce fraudulent outcomes. The following section develops theoretical propositions showing these interactions.

4. Formal Theoretical Propositions

To make the framework open to empirical testing, the study develops propositions concerning the relationships between its four dimensions and the likelihood of technology-enabled financial misstatement.

4.1 Digital Pressure and System-Generated Performance Monitoring.

Corporate governance research traditionally views performance pressure as an interpersonal phenomenon driven by executive mandates (Dechow et al., 1996). In contrast, automated accounting environments generate continuous pressure through algorithmic monitoring and real-time dashboards (Appelbaum et al., 2024). Under pervasive tracking, employees prioritize short-term metric compliance over reporting accuracy, maneuvering inputs to suppress system-flagged anomalies

Proposition 1: Organizations with higher reliance on real-time automated KPI tracking experience elevated Digital Pressure, increasing the likelihood of input misuse to prevent irregularity exposure.

4.2 Systemic Complexity and Potential.

According to Wolfe and Hermanson, (2004), classical theory bases fraud opportunity in governance failures and managerial disregard. However, CISA (2026) contended that distributed cloud infrastructures introduced technical opportunities via interface gaps and

data pipeline vulnerabilities. Therefore, as microservices and black-box valuation models replace centralized systems, traditional segregation-of-duties (SoD) controls become autonomous (Brazel & Dang, 2008). Knowledge asymmetries between IT administrators and financial controllers further prevent normal audits from catching these structural integration flaws.

Proposition 2: Higher architectural intricacy and API independence expand technological opportunity by creating integration gaps that bypass conventional segregation-of-duties controls.

4.3 Digital Rationalization via Sociomaterial Abstraction.

Whereas traditional fraudsters rationalize misconduct through personal excuses (Cressey, 1953; Bandura, 1999), digital interfaces separate actors from the physical consequences of their entries (Leonardi, 2012; Moore et al., 2012).

Proposition 3: Sophisticated interface belief and virtual distance raise digital rationalization by helping detach users from the material impact of fraudulent entries and facilitate the moral attribution of misconduct to automated systems.

4.4 Technological Requirements for Execution.

The Fraud Diamond links capability to executive rank and interpersonal persuasion (Wolfe & Hermanson, 2004). In digital workflows, however, system access and software fluency supersede organizational hierarchy as the primary drivers of financial alteration (Dornheim & Zarnekow, 2025; Amani & Fadlalla, 2017).

Proposition 4: Advanced technological capability increases an operator's capacity to execute and conceal accounting misstatements, moving the direction of fraud execution to specialized technical access.

4.5 Systemic Interaction & Socio-Technical Convergence

While each dimension independently influences fraud dynamics, TEFF proposes that fraud risk may be greater when human behavioural factors coincide with weaknesses or affordances in digital systems.

Table 4.

Proposition	Focus	Proposed mechanism
P1	Digital Pressure	Real-time monitoring may increase pressure associated with performance irregularities.
P2	Technological Opportunity	Architectural complexity and limited system transparency may build control or monitoring gaps.
P3	Digital Rationalization	Interface abstraction and virtual distance may increase psychological distance from misconduct.
P4	Technological Capability	Technical expertise and system access may increase the ability to execute and conceal forgery.

Propositions 1–4 suggest that orthodox controls may be insufficient when fraud risks arise from interactions between human behavior and technological conditions. Subsequently, converting TEFF into institutional practice requires an improvement of internal control mechanisms and forensic investigative protocols.

5. Discussion, Governance Implications & Methodological Agenda

5.1 Modernizing Internal Control Through Zero-Trust Architecture (ZTAA)

Established internal control models like COSO, assume human-to-human complicity and rely on physical safeguards and segregation of duties (Albrecht et al., 2018; Beasley, 1996; Brazel & Dang, 2008; Li et al., 2018). Addressing socio-technical fraud requires bringing about controls to lessen pressure, eliminate opportunities, reduce rationalization, and restrict technical misuse. Mitigating technological opportunity requires adopting ZTAA as proposed by (Dornheim & Zarnekow, 2025).

5.2 Forensic Accounting Practice and Continuous Auditing.

In this era of digital auditing, forensic accountants should not rely on traditional investigations only, they must integrate continuous automated ledger analysis with field investigation (Ahmi, 2026; Qatawneh, 2025). There is also

risk that people justify unethical actions because they feel disconnected from the consequences of their actions. In such cases accounting software should include features that force users to verify transactions and remind them that their decisions affect real people (Leonardi, 2012; Moore et al., 2012). However, TEFF still needs to be tested in organizations to prove that it actually works.

5.3 Empirical Research Agenda.

Going forward, theses framework can be used to assess the validity and empirical usefulness of TEFF.

Empirical studies should develop and validate psychometric survey scales measuring Digital Pressure, Technological Opportunity, Digital Rationalization and Technological Capability.

Surveying corporate accountants, internal auditors, and IT professionals using structural equation modeling to test Propositions 1–4 and quantify the structural pathways leading to reporting fraud.

Multi-case qualitative investigations into actual corporate fraud incidents can document how perpetrators interact with technical interfaces and exploit architecture to execute misstatements.

6. Conclusion

By incorporating fraud research with Socio-Technical and Affordance theories, TEFF offers a tool for accounting environments. The framework treats technology as an active structural force which gives foundation for future empirical research and internal control design.

References

Abdo-Salloum, A. M., & Chehade, S. (2026). The role of artificial intelligence in transforming accounting and auditing practices: A systematic review. SAGE Open, 16(1), 1–13.

Ahmi, A. (2026). AI-driven auditing: Trends, themes, and research trajectories. International Journal of Accounting & Information Management, 34(2), 210–235.

Al-Sayyed, R. (2024). Machine learning and data mining architectures in financial fraud detection: A review. Computers & Security, 139, 103720.

Alshurafat, H. (2023). Factors affecting accounting students' misuse of ChatGPT: An application of the fraud triangle theory. Journal of Financial Reporting and Accounting, 22(2), 274–292.

Amani, F. A., & Fadlalla, A. M. (2017). Data mining applications in accounting: A review of the literature and organizing framework. International Journal of Accounting Information Systems, 24, 32–58.

Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big Data and analytics in the modern audit engagement: Research needs. Auditing: A Journal of Practice & Theory, 36(4), 1–27.

Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2024). Sociotechnical considerations in the adoption of continuous audit analytics. Journal of Emerging Technologies in Accounting, 21(1), 45–62.

Albrecht, W. S., Albrecht, C. O., Albrecht, C. C., & Zimbelman, M. F. (2018). Fraud Examination (6th ed.). Cengage Learning.

Al Natour, M. R., et al. (2026). Fraud detection: Do psychological traits, auditor ethics and professional skepticism make any difference? International Journal of Organizational Analysis, 34(1), 45–68.

Beasley, M. S. (1996). An empirical analysis of the relation between the board of director composition and financial statement fraud. The Accounting Review, 71(4), 443–465.

Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective. Part I: The causes. MIS Quarterly, 1(3), 17–32.

Bandara, E., Shetty, S., Mukkamala, R., & Liang, X. (2021). Data governance in decentralized systems: A blockchain perspective. IEEE Transactions on Network and Service Management, 18(4), 3980–3994.

Bandura, A. (1999). Moral disengagement in the perpetration of inhumanities. Personality and Social Psychology Review, 3(3), 193–209.

Bandura, A. (2002). Selective moral disengagement in the exercise of moral agency. Journal of Moral Education, 31(2), 101–119.

Brazel, J. F., & Dang, L. (2008). The effect of ERP system implementations on available internal control and financial statement audit fees. Journal of Information Systems, 22(2), 1–21.

Cho, S., Vasarhelyi, M. A., Sun, T., & Zhang, C. (2020). IT initiatives in accounting: A review of research in the Journal of Information Systems. Journal of Information Systems, 34(1), 1–25.

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

Cybersecurity and Infrastructure Security Agency (CISA). (2026). Known Exploited Vulnerabilities and Enterprise Access Controls Catalog. U.S. Department of Homeland Security.

Dechow, P. M., Sloan, R. G., & Sweeney, A. P. (1996). Causes and consequences of earnings manipulation: An analysis of the firms subject to enforcement actions by the SEC. Contemporary Accounting Research, 13(1), 1–36.

Dellaportas, S. (2013). Conversations with inmate accountants: Motivation, opportunity and the fraud triangle. Accounting Forum, 37(1), 29–39.

Dornheim, S., & Zarnekow, R. (2025). Cybersecurity management: An empirical analysis of dynamic capabilities framework for enhancing cybersecurity intelligence. Information & Computer Security, 33(4), 473–495.

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.

Detert, J. R., Treviño, L. K., & Sweitzer, V. L. (2008). Moral disengagement in ethical decision making: A study of antecedents and outcomes. Journal of Applied Psychology, 93(2), 374–391.

Gibson, J. J. (1979). The Ecological Approach to Visual Perception. Houghton Mifflin

Gepp, A., Linnenluecke, M. K., O'Neill, T. J., & Smith, T. (2018). Big data techniques in auditing research and practice: Current trends and future opportunities. Journal of Accounting Literature, 40, 102–115.

Glan, V. (2026). Fraud triangle revisited: How pressure, opportunity, and rationalization have evolved. Journal of Financial Crime, 33(3), 512–528.

Kassem, R., & Higson, A. (2012). The new fraud triangle model. Journal of Emerging Trends in Economics and Management Sciences, 3(3), 191–195.

Latour, B. (2005). Reassembling the Social: An Introduction to Actor-Network-Theory. Oxford University Press.

Leonardi, P. M. (2011). When flexible routines meet flexible technologies: Affordance, constraint, and the imbrication of human and material agencies. MIS Quarterly, 35(1), 147–167.

Leonardi, P. M. (2012). Materiality, sociomateriality, and infrastructure: What difference do the talk and the tools make? In Materiality and Organizing: Social Interaction in a Technological World (pp. 25–48). Oxford University Press.

Leonardi, P. M. (2013). Theoretical foundations for the study of sociomateriality. Information and Organization, 23(2), 59–76.

Li, H., Dai, J., Gershberg, T., & Vasarhelyi, M. A. (2018). Understanding usage and value of audit analytics for internal auditors: An organizational approach. International Journal of Accounting Information Systems, 28, 59–76.

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

Majchrzak, A., & Markus, M. L. (2012). Technology affordances and constraints in management information systems (MIS). Encyclopedia of Management Theory, 832–836.

Markus, M. L., & Silver, M. S. (2008). A foundation for the study of IT effects: A new look at DeSanctis and Poole's concepts of structural features and spirit. Journal of the Association for Information Systems, 9(10), 609–632.

Moffitt, K. C., Rozario, A. M., & Vasarhelyi, M. A. (2018). Robotic Process Automation for auditing. Journal of Emerging Technologies in Accounting, 15(1), 1–10.

Munoko, I., Brown-Liburd, H. L., & Vasarhelyi, M. A. (2020). The ethical implications of using artificial intelligence in auditing. Journal of Business Ethics, 167(2), 209–234.

Mökander, J. (2023). Auditing of AI systems: A governance framework for assessing algorithmic risk. Minds and Machines, 33(2), 241–268.

Moore, C., Detert, J. R., Treviño, L. K., Baker, V. L., & Mayer, D. M. (2012). Why employees do bad things: Moral disengagement and unethical organizational behavior. Personnel Psychology, 65(1), 1–48.

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

Orlikowski, W. J. (2007). Sociomaterial practices: Exploring technology at work. Organization Studies, 28(9), 1435–1448.

Orlikowski, W. J., & Scott, S. V. (2008). Sociomateriality: Challenging the separation of technology, work and organization. Academy of Management Annals, 2(1), 433–474.

Qatawneh, A. M. (2025). The role of artificial intelligence in auditing and fraud detection in accounting information systems: Moderating role of

natural language processing. International Journal of Organizational Analysis, 33(6), 1391–1409.

Schuchter, A., & Levi, M. (2016). The fraud triangle revisited. Security Journal, 29(2), 107–121.

Simeunović, N., Kamissoko, F. B., & Djurić, Z. (2023). Algorithmic opacity and systemic vulnerabilities in cloud-native enterprise systems. Computers in Human Behavior, 142, 107645.

Tieu, T. T. H. (2026). Integrating the fraud triangle with machine learning for financial misstatement detection: Evidence from an emerging market. Cogent Business & Management, 13(1), 2614367.

Vasarhelyi, M. A., Kogan, A., & Tuttle, B. M. (2015). Big Data in accounting: An overview. Accounting Horizons, 29(2), 381–396.

Vousinas, G. L. (2019). Advancing theory of fraud: The S.C.O.R.E. model. Journal of Financial Crime, 26(1), 145–159.

Wang, T., & Cuthbertson, R. (2015). The eight value triggers of enterprise resource planning (ERP) systems. Information & Management, 52(4), 434–445.

Wamba, S. F., Queiroz, M. M., & Trinchera, L. (2024). Dynamics of artificial intelligence adoption in accounting: A multi-theoretical lens. International Journal of Information Management, 74, 102711.