

DOI: https://doi.org/10.48009/3_iis_2026_139

Emerging technologies, internal control systems, and audit as mechanisms for financial fraud detection and prevention in the financial services sector

Oscar Santiago, *Universidad Ana G. Méndez*, osantiago52@email.uagm.edu

Angel Ojeda, *Universidad Ana G. Méndez*, aojeda@uagm.edu

Edda Martínez, *Universidad Ana G. Méndez*, martineze3@uagm.edu

María Meléndez, *Universidad Ana G. Méndez*, melendezm4@uagm.edu

José Sánchez, *Universidad Ana G. Méndez*, jsanchez@uagm.edu

Carlos Rosa, *Universidad Ana G. Méndez*, crosa31@uagm.edu

Abstract

Financial fraud poses a critical and multidimensional threat to the sustainability, governance, and reputational integrity of organizations in the financial services sector. This article is developed as a conceptual paper grounded in a narrative review of recent literature on financial fraud, internal control systems, emerging technologies, and audit. Drawing primarily on studies published between 2021 and 2026, it synthesizes current evidence on how the integration of emerging technologies, specifically artificial intelligence (AI), machine learning (ML), and blockchain, relates to the effectiveness of internal control systems, and on how audit functions may moderate the relationship between internal control effectiveness and financial fraud detection and prevention. The paper is grounded in the Fraud Diamond Model, which provides a theoretical framework for understanding the convergence of pressure, opportunity, rationalization, and capability as determinants of fraudulent behavior, and uses that framework as the theoretical microfoundation for an integrative conceptual model. The central contribution of the paper is this conceptual model itself, together with six theoretical propositions (P1-P6) that articulate testable relationships among financial fraud, internal control system effectiveness, blockchain, AI/ML, and audit, including audit's proposed moderating role. The propositions are offered as a structured foundation for future empirical research rather than as findings that have already been tested; the paper does not report primary data collection, statistical analysis, or empirical results.

Keywords: financial fraud, internal control systems, blockchain, artificial intelligence, machine learning, auditing, fraud prevention

Introduction

This article is developed as a conceptual paper, grounded in a narrative review of recent literature, rather than as an empirical study. Its objective is to synthesize current evidence on financial fraud, internal control systems, emerging technologies, and audit, and to organize that evidence into an integrative conceptual model supported by a set of theoretical propositions (P1-P6), presented in full in the Conceptual Framework and Propositions section below. The paper does not report data collection, statistical analysis, or empirical findings; the propositions are offered as a structured basis for future empirical testing.

Financial Fraud as a Systemic Challenge

Financial fraud constitutes one of the most critical risks to the sustainability, stability, and governance of contemporary organizations, particularly in the financial sector, where the integrity of information is fundamental to market functioning (Becerra-Huamán et al., 2025). Recent literature indicates that this phenomenon has evolved significantly in complexity due to the digitalization of financial processes and the intensive use of emerging technologies in organizational environments (Mahdani & Soufyan, 2026). Similarly, the globalization of markets and digital interconnectedness have expanded opportunities for more sophisticated transnational fraudulent schemes (Becerra-Huamán et al., 2025). This growing complexity hinders early detection and amplifies the adverse effects on the operational and financial stability of institutions (Ansari et al., 2025).

Beyond direct economic losses, financial fraud generates systemic consequences that undermine the trust of investors, regulators, and the general public (Chen et al., 2025). Recent research demonstrates that financial scandals can trigger cascading effects that deteriorate corporate reputation and significantly reduce the market value of the entities involved (Becerra-Huamán et al., 2025). The reputational damage resulting from fraudulent events often exceeds the immediate monetary impact, affecting organizations' ability to attract capital and maintain stable strategic relationships (Mahdani & Soufyan, 2026). Consequently, fraud not only compromises financial results but weakens institutional legitimacy within the economic ecosystem (Chen et al., 2025).

Furthermore, financial fraud compromises the integrity of financial statements and the quality of information used for strategic decision-making (Ansari et al., 2025). Accounting manipulation and the intentional alteration of records distort the accurate representation of organizations' economic situation, affecting market transparency (Gkegkas et al., 2025). Recent studies highlight that the reliability of financial reports constitutes an essential pillar for the efficient functioning of capital markets and macroeconomic stability (Chen et al., 2025). When this reliability is compromised, a structural weakening occurs in the systemic trust that sustains financial activity (Becerra-Huamán et al., 2025).

Empirical evidence consistently indicates that financial fraud is facilitated by deficiencies in internal control systems, insufficient monitoring, and weaknesses in organizational supervisory mechanisms (H. Chen et al., 2025). The literature also notes that the absence of formal risk assessment structures and control matrices aligned with frameworks such as the Internal Control Matrix increases organizational vulnerability to fraudulent events (Chen et al., 2025). Additionally, the lack of integration between emerging technologies and internal controls limits detection and prevention capabilities in highly dynamic digital environments (Mahdani & Soufyan, 2026). These conditions, combined with economic pressures and opportunities derived from digital transformation, create a fertile environment for the commission of fraudulent acts in the financial sector (Ansari et al., 2025).

Accordingly, financial fraud must not be understood merely as an accounting or administrative problem, but as a multidimensional phenomenon affecting corporate governance, economic stability, and public trust (Becerra-Huamán et al., 2025). Addressing it requires comprehensive strategies that include strengthening internal control systems, adopting technologies such as blockchain and artificial intelligence, and developing an audit function capable of supervising and enhancing the effectiveness of these controls (Mahdani & Soufyan, 2026). From this perspective, the analysis of the relationships among financial fraud, internal control systems, emerging technologies, and audit becomes a central axis for understanding the mechanisms that explain fraud detection and prevention in the financial sector (Chen et al., 2025).

Audit as a Strategic Assurance Function

Auditing has evolved from a traditional accounting verification mechanism into a strategic assurance function that directly contributes to governance and organizational sustainability in complex and digitalized environments (Becerra-Huamán et al., 2025). This assurance role is consistent with agency-theoretic explanations of auditing, which frame the function as a mechanism that reduces information asymmetries and aligns the incentives of managers and owners (Watts & Zimmerman, 1983). In the literature, internal audit is conceived as an essential component of the internal control system, whose purpose is to evaluate the effectiveness of controls and strengthen confidence in financial information (Chen et al., 2025). This evolution responds to structural transformations in financial markets, characterized by greater digitalization, interconnectivity, and exposure to technological risks (Mahdani & Soufyan, 2026).

Financial fraud has experienced growing sophistication, driven by the adoption of digital technologies that enable more complex and difficult-to-detect schemes using traditional methods (Ansari et al., 2025). Recent research argues that the use of automated tools, social engineering, and digital data manipulation has increased the vulnerability of financial systems (Miao, 2024). In this context, the audit function faces the challenge of adapting to an environment where emerging risks evolve rapidly and require advanced analytical capabilities (Becerra-Huamán et al., 2025).

Modern auditing has incorporated data analytics, artificial intelligence, and continuous auditing approaches to improve coverage and timeliness of control reviews (Mahdani & Soufyan, 2026). Recent empirical studies indicate that the integration of advanced analytics tools enables the identification of anomalous patterns in large volumes of financial transactions, strengthening monitoring and risk assessment (Ansari et al., 2025). In the financial sector, auditing acquires particular relevance due to high exposure to fraud risks, cyberattacks, and sensitive information manipulation (Kokina et al., 2025). Furthermore, the adoption of emerging technologies in auditing is associated with greater precision in detecting irregularities and reduced risk of human error (Chen et al., 2025).

From both theoretical and empirical perspectives, auditing is positioned as a factor that amplifies the impact of internal controls on fraud detection and prevention, especially when it adopts a risk-based approach supported by technology (Chen et al., 2025). This moderating function is particularly relevant in highly regulated financial environments, where the effectiveness of the internal control system depends largely on the quality and depth of independent oversight (Ansari et al., 2025). Consequently, recent evidence supports the analysis of auditing as a mechanism that strengthens the relationship between internal control systems and fraud detection and prevention, underpinning Proposition 6 of the conceptual framework proposed in this article (Mahdani & Soufyan, 2026).

Forensic Auditing and Financial Statement Integrity

In the contemporary context of the financial sector, financial audits play an essential role in strengthening the transparency and reliability of accounting information (Becerra-Huamán et al., 2025). Recent literature argues that financial auditing not only verifies the reasonableness of financial statements but also contributes to reducing information asymmetries and strengthening corporate governance (Chen et al., 2025). In environments characterized by increasing digitalization and transactional complexity, the audit function has transformed into a strategic mechanism for mitigating risks associated with financial fraud (Mahdani & Soufyan, 2026).

According to Ocampo (2023), forensic auditing constitutes a specialized discipline that integrates the foundations of traditional auditing with investigation and forensic analysis techniques, primarily oriented toward the identification, verification, and documentation of fraudulent activities. Within this framework, forensic auditing has acquired particular relevance as a specialized tool for investigating irregularities and

providing evidence in judicial or disciplinary proceedings (Becerra-Huamán et al., 2025). Recent studies highlight that forensic auditing integrates accounting, legal, and technological knowledge to analyze suspicious patterns and reconstruct complex financial events (Ansari et al., 2025). Empirical research also indicates that its application enables the identification of structural weaknesses in internal control systems and the strengthening of preventive mechanisms (Chen et al., 2025). In the public and financial sectors, forensic auditing has proven effective in detecting corruption, embezzlement, and accounting manipulation (Mahdani & Soufyan, 2026).

Contemporary literature also highlights that corruption and financial fraud maintain a close relationship, particularly in environments with supervisory and control weaknesses (Talla et al., 2025). In this sense, forensic auditing does not fulfill only a reactive function but also plays a preventive role by identifying emerging risks and recommending structural improvements (Ansari et al., 2025). Recent research underscores that the investigative capacity of auditing strengthens the organizational culture oriented toward ethics and transparency (Mahdani & Soufyan, 2026).

Literature Review

Fraud Diamond Theory

The Fraud Diamond Model constitutes a contemporary extension of the Fraud Triangle (Cressey, 1953) by incorporating the element of capability, thereby broadening the explanation of fraudulent behavior in complex organizational contexts (Wolfe & Hermanson, 2004). Additionally, Murphy and Dacin (2011) deepen the rationalization component of fraud by identifying three psychological pathways through which individuals justify the act: lack of awareness, intuition combined with rationalization, and logical reasoning. These pathways explain how individuals neutralize the moral discomfort associated with fraud, fostering dissonance-reduction mechanisms such as minimizing the harm caused. Recent research in the financial sector confirms that these four elements continue to be determinants in the majority of contemporary corporate fraud schemes (Becerra-Huamán et al., 2025).

The first component, pressure, refers to financial incentives, demanding organizational goals, or personal economic difficulties that motivate an individual to commit fraud (Dorminey et al., 2012). Recent empirical studies indicate that in highly competitive financial environments, performance pressure can intensify, increasing the risk of accounting manipulation or distortion of financial information (Chen et al., 2025). Higher levels of organizational pressure may increase the incidence of fraudulent behavior when controls are insufficient (Mahdani & Soufyan, 2026); this relationship between internal control effectiveness and the incidence of financial fraud is formalized later in this article as Proposition 1 of the conceptual framework.

The second component, opportunity, is considered the element most directly related to internal control systems, as it arises when there are weaknesses in supervision, segregation of duties, or organizational monitoring (Giannopoulos et al., 2025). Recent literature demonstrates that opportunity decreases significantly when organizations implement effective and updated internal control systems (Chen et al., 2025). The effectiveness of the internal control system acts precisely as the mechanism that reduces opportunity, a relationship formalized later in this article as Proposition 2, linking internal control system effectiveness to fraud detection and prevention capacity (Becerra-Huamán et al., 2025).

The third component, rationalization, refers to the cognitive process through which the perpetrator justifies fraudulent conduct as acceptable or necessary (Kaptein, 2011). Contemporary research evidences that weak organizational cultures, normative ambiguity, and deficient ethical leadership increase the probability of

fraud rationalization (Scott, 2021). Rationalization is mitigated when clear policies, active audits, and a solid ethical culture exist, elements that indirectly strengthen the internal control system within the conceptual model (Chen et al., 2025).

The fourth component, capability, distinguishes the Fraud Diamond from previous models by recognizing that not all individuals with pressure, opportunity, and rationalization possess the technical skills or necessary access to execute fraud (Wolfe & Hermanson, 2004). In digitalized environments, capability is closely related to technological knowledge and privileged access to information systems (Mahdani & Soufyan, 2026). Recent literature indicates that digital transformation has increased the weight of capability within the model, as current frauds require advanced technical skills to manipulate data or compromise systems (Ansari et al., 2025).

In relation to the conceptual framework developed in this article, the incorporation of artificial intelligence and blockchain acts as a mechanism that reduces both the opportunity and the effective capability of the perpetrator by increasing traceability, automation, and continuous monitoring (Chen et al., 2025). Recent empirical studies suggest that emerging technologies strengthen the monitoring component of the internal control system, decreasing the probability that the four elements of the Fraud Diamond converge (Becerra-Huamán et al., 2025). These technology-related relationships are formalized later in this article as Propositions 3 and 4, linking blockchain and artificial intelligence/machine learning, respectively, to internal control system effectiveness.

Furthermore, auditing directly influences the reduction of opportunity and rationalization by increasing independent supervision and reinforcing the perception of consequences for improper conduct (Mahdani & Soufyan, 2026). Recent research in financial governance indicates that robust audits amplify the impact of the internal control system on fraud prevention, limiting the convergence of the Diamond's elements (Chen et al., 2025). Audit's dual role, both as a direct contributor to fraud detection and prevention and as a moderator of the relationship between internal control effectiveness and fraud outcomes, is developed later in this article as Propositions 5 and 6, respectively. It should be emphasized that P1 through P6, introduced in full in the Conceptual Framework and Propositions section below, denote relationships among the organizational-level constructs of the proposed model; they are not labels for the four elements of the Fraud Diamond discussed in this subsection, which instead function as the theoretical microfoundations from which those constructs and their proposed relationships are derived.

Internal Control Matrix

The Internal Control Matrix (ICM), also described as a risk-control matrix, organizes, by process, key risks, the controls that mitigate them, the control owner, and the expected evidence, facilitating clear traceability between risk and control response (Sáenz, 2021). In contemporary reviews of internal control, it is emphasized that structurally documenting controls and procedures improves the evaluation of design and operational effectiveness, and a matrix contributes to this systematization (Giannopoulos et al., 2025).

Recent studies on internal control over financial reporting show that when the risk-control matrix is limited only to 'key risks,' it may deviate from the ideal standard and affect the coverage of control testing, reinforcing the need for complete and well-defined matrices (Wirantika & Setyaningrum, 2025). The utility of the matrix is enhanced when connected to risk assessment and prioritization methodologies, allowing tests and monitoring to be focused on areas of greatest exposure (Sahin & Menekse, 2025).

From an internal audit perspective, the matrix functions as a 'map' to align audit objectives, process risks, and existing controls, elevating the consistency of the work program (Sáenz, 2021). Empirical evidence on internal controls in organizations indicates that documentary clarity and the assignment of control

responsibilities favor an environment where supervision and compliance become more verifiable (Giannopoulos et al., 2025). Recent research also connects internal control and fraud prevention, suggesting that well-designed matrices support preventive controls and reduce fraud opportunities by making control gaps visible (Talla et al., 2025). Methodologically, the matrix facilitates the operationalization of variables (e.g., quality of internal control) because it allows converting control descriptions into observable indicators for measurement or evaluation (Wirantika & Setyaningrum, 2025).

Financial Fraud

Financial fraud encompasses intentional behaviors that distort information or transactions to obtain undue benefits, and its complexity increases with digitalization and the volume of transactional data (Miao, 2024). Recent literature describes that fraud can manifest as transaction fraud, financial reporting fraud, or hybrid schemes, which demands differentiated analysis and control approaches (Gkegkas et al., 2025). Contemporary empirical studies continue to use theoretical frameworks, such as 'hexagon/pentagon' approaches, to explain conditions that increase the probability of fraud, especially when control and supervisory weaknesses exist (Bermeo-Giraldo et al., 2021).

Recent systematic reviews indicate that traditional auditing methods may be insufficient against sophisticated fraud patterns 'hidden' in large volumes of data, elevating the risk of non-detection (Gkegkas et al., 2025). Recent research also shows associations between internal control effectiveness and a lower probability of fraudulent financial reporting, supporting the role of control as a barrier against fraud opportunities (Novatiani et al., 2024).

Evidence on internal controls and auditing suggests that competencies, independence, and quality of the audit function relate to better controls and to the prevention of fraud in financial statements (Novatiani et al., 2024). In synthesis, the literature from 2021–2026 converges on the notion that financial fraud is a dynamic and adaptive phenomenon, so its analysis as a variable must incorporate both organizational factors of control and governance, as well as technological factors in analytics and artificial intelligence (Miao, 2024).

Blockchain Technology

Blockchain is characterized by distributed ledgers with properties of immutability, consensus, and traceability, which can improve transparency and trust in accounting and auditing environments (Han et al., 2023). Recent literature explains that blockchain's main contribution to accounting is to strengthen data integrity and enable more robust audit trails, reducing the possibility of subsequent alterations (Kravchenko et al., 2023). Reviews of adoption in auditing show that blockchain can support 'blockchain + audit' models, although operational, regulatory, and standardization risks and challenges persist (Han et al., 2023). In technology-based auditing, it is argued that near-real-time access to verified records can favor continuous auditing schemes and more timely monitoring (Devianto et al., 2025).

Recent evidence on blockchain and the internal audit function also discusses benefits (e.g., security/recording) and implementation challenges, including data governance and change management (Gao, 2025). In terms of internal control, recent research links digital technologies (including blockchain) with potential improvements in control effectiveness by decreasing manipulation and elevating verifiability, especially when integrated with organizational processes (Ma & Li, 2024). Conceptual studies on blockchain-based audit trails highlight their contribution to transparency and the strengthening of fraud detection within digital accounting systems (Maryani et al., 2026).

Artificial Intelligence and Machine Learning

Artificial intelligence and machine learning are used to detect anomalies and complex patterns in financial data, surpassing rule-based approaches when data is massive and high-dimensional (Miao, 2024). Recent systematic reviews show that deep learning has been widely applied to financial fraud across multiple domains (cards, insurance, reports), consolidating a body of evidence from 2019–2024 with strong methodological growth (Chen et al., 2025). In auditing, field studies report that simple AI tools (extraction, automation, analytics) are widely used, while complex AI faces challenges of applicability, bias, and robustness (Kokina et al., 2025).

Recent literature underscores that AI adoption in auditing must manage risks of excessive auditor dependence, privacy concerns, and the need for clear professional guidelines (Kokina et al., 2025). In fraud detection, there is a growing emphasis on explainable AI models (XAI) to sustain decisions before regulators and users, balancing predictive accuracy and transparency (Hernandez Aros et al., 2024). Recent research proposes approaches combining applicability and privacy (Federated Learning + XAI) for financial fraud detection with usable interpretability for analysts (Aljunaid et al., 2025).

From internal auditing, recent studies describe AI use cases for real-time big data analysis oriented toward detection and prevention, although they highlight data governance and competency challenges (Satoto & Wibowo, 2026). AI and machine learning have the capacity to improve early detection, reduce false positives/negatives, and enable continuous monitoring, but their effectiveness depends on data quality, controls, and professional oversight (Hernandez Aros et al., 2024).

Internal Control Systems

Internal control systems are conceptualized as an integrated set of policies, procedures, and mechanisms to ensure reliable operations, compliance, and risk management (Giannopoulos et al., 2025). Recent evidence shows that the effectiveness of the internal control system is associated with the quality of components such as controls/procedures, internal audit, risk management, and compliance (Giannopoulos et al., 2025). Recent literature in the public sector highlights that a well-structured internal control system protects resources and increases transparency by reducing opportunities for improper conduct (Talla et al., 2025).

Recent studies highlight that the use of risk-control matrices improves the traceability and documentation of financial controls (Wirantika & Setyaningrum, 2025). Empirical research shows that organizations implementing structured matrices exhibit greater clarity in responsibilities and control monitoring (Sáenz, 2021). The literature also highlights that periodic updating of the risk-control matrix improves preventive capacity against new fraud schemes (Talla et al., 2025).

Audit

Auditing is positioned in recent literature as an assurance mechanism that contributes to reducing information asymmetries and strengthening confidence in reports, especially in contexts of fraud risk (Becerra-Huamán et al., 2025). The contemporary research highlights that modern auditing increasingly integrates data analytics and artificial intelligence for risk assessment and evidence collection, with implications for efficiency and scope (Becerra-Huamán et al., 2025). Field studies on AI adoption in auditing warn of practical challenges, applicability, bias, privacy, that affect how auditors can rely on and document conclusions based on intelligent tools (Kokina et al., 2025).

Recent literature on internal auditing and fraud identifies attributes such as independence, competence, objectivity, and professional skepticism as critical for detecting and mitigating fraud (Oyedotun et al., 2025). In technological environments, reviews of blockchain in auditing show that new sources of evidence (immutable records) can transform procedures but also introduce risks and require new capabilities (Han et

al., 2023). Consequently, auditing as a variable can be approached by measuring perceived quality, use of technology analytics, competencies, and risk-based planning practices, consistent with recent findings in the field (Kokina et al., 2025).

Fraud Detection and Prevention

Fraud detection and prevention are understood as a set of mechanisms (preventive and corrective) that reduce the opportunity and duration of fraud, impacting expected losses (Talla et al., 2025). Recent evidence indicates that effective internal controls are associated with a lower probability of fraud in financial reporting, reinforcing prevention from governance and processes (Novatiani et al., 2024). Recent systematic reviews on data analytics applied to financial statement fraud argue that advanced techniques complement traditional audits by identifying hidden signals in large datasets (Gkegkas et al., 2025).

Recent research on financial fraud highlights that rule-based methods lose effectiveness when defrauders adapt patterns, making data-driven adaptive detection necessary (Miao, 2024). In digital environments, it is argued that blockchain can strengthen prevention by elevating the integrity and traceability of transactions, improving the availability of evidence for detection (Maryani et al., 2026). Accordingly, this variable can be operationalized with indicators such as early detection capacity, preventive effectiveness, reduction of incidents, and maturity of continuous monitoring, aligned with recent evidence in control, auditing, and analytics (Gkegkas et al., 2025). Taken together, the constructs reviewed in this section, financial fraud, the Internal Control Matrix, internal control systems, blockchain, artificial intelligence and machine learning, audit, and fraud detection and prevention, provide the building blocks for the integrative conceptual model and propositions developed in the following section.

Conceptual Framework and Propositions

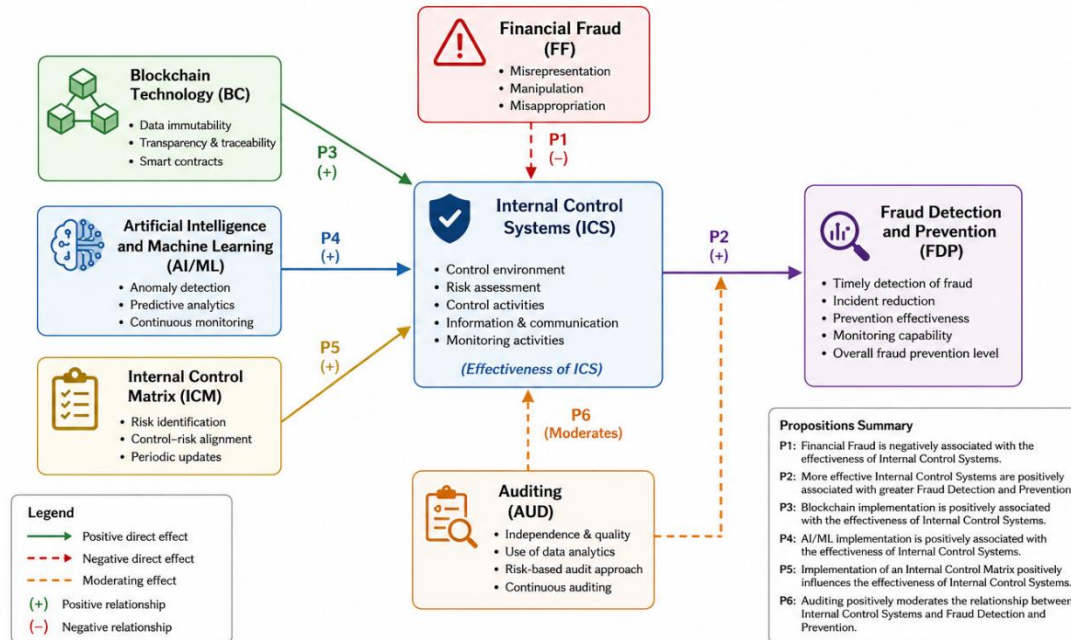
The preceding review situates financial fraud, internal control systems, blockchain, artificial intelligence and machine learning, audit, and fraud detection and prevention within a common theoretical space. Building on the Fraud Diamond Model microfoundations discussed above, together with the Internal Control Matrix as a supporting governance structure, this section develops an integrative conceptual model and states, in full, the six theoretical propositions (P1-P6) that follow from it. The model is depicted in Figure 1. Consistent with the conceptual, literature-based nature of this paper, the propositions are stated as relationships among the model's organizational-level constructs, financial fraud, internal control system effectiveness, blockchain, artificial intelligence/machine learning, and audit, rather than as the four elements (pressure, opportunity, rationalization, capability) of the Fraud Diamond itself. Those four elements, discussed in the Literature Review, function as the psychological and behavioral microfoundations from which the model's constructs and propositions are derived; they are not, themselves, numbered as P1 through P6.

The Conceptual Model

As shown in Figure 1, the model positions internal control system effectiveness as the central organizational mechanism through which financial fraud is reduced. Blockchain and artificial intelligence/machine learning are modeled as antecedents that strengthen internal control system effectiveness, reflecting their capacity to increase traceability, automation, and continuous monitoring. Internal control system effectiveness, in turn, is modeled as a direct antecedent of fraud detection and prevention capacity. Audit enters the model in two distinct ways: as a direct antecedent of fraud detection and prevention capacity, and as a moderator that strengthens the path linking internal control system effectiveness to fraud detection and prevention. The Internal Control Matrix is positioned as a supporting documentary structure that underlies the effective functioning of the internal control system construct, rather than as a separate causal path.

Conceptual Model: Emerging Technologies, Internal Control Systems, and Auditing in Financial Fraud Detection and Prevention

The model illustrates the proposed relationships among key constructs. Propositions (P1–P6) represent the expected directions of relationships based on the literature.



Note: The model is based on the integration of the Fraud Diamond Theory, Internal Control frameworks (e.g., COSO), and the literature on emerging technologies and auditing.

Figure 1. Proposed conceptual model linking emerging technologies, internal control systems, and audit to financial fraud detection and prevention.

Propositions P1-P6

Building on this model and the literature reviewed above, six propositions are advanced as a structured basis for future empirical research:

P1. Internal control system effectiveness is negatively related to the incidence of financial fraud; organizations with more effective internal control systems are expected to experience a lower incidence of financial fraud (Giannopoulos et al., 2025; Novatiani et al., 2024).

P2. Internal control system effectiveness is positively related to fraud detection and prevention capacity (Becerra-Huamán et al., 2025; Talla et al., 2025).

P3. The integration of blockchain technology into organizational processes is positively related to internal control system effectiveness (Han et al., 2023; Ma & Li, 2024).

P4. The integration of artificial intelligence and machine learning into organizational processes is positively related to internal control system effectiveness (Miao, 2024; Hernandez Aros et al., 2024; Kokina et al., 2025).

P5. Audit quality is positively related to fraud detection and prevention capacity (Oyedotun et al., 2025; Novatiani et al., 2024).

P6. Audit moderates the relationship between internal control system effectiveness and fraud detection and prevention capacity, such that this relationship is stronger when audit quality, independence, and use of technology-enabled analytics are higher (Ansari et al., 2025; Chen et al., 2025).

Proposition 6: The Moderating Role of Audit

Proposition 6 occupies a distinctive position in the model because it does not propose a direct relationship between two constructs, but rather specifies a condition under which an existing relationship, the path from internal control system effectiveness to fraud detection and prevention capacity established in Proposition 2, becomes stronger or weaker. Four mechanisms, drawn from the literature reviewed above, explain why audit is expected to play this moderating role.

First, risk-based audit planning directs audit attention and testing toward the areas of highest fraud exposure, so that the same underlying set of controls is scrutinized more effectively where it matters most (Sáenz, 2021; Sahin & Menekse, 2025). Second, auditor independence increases the credibility of control evaluations and reduces the likelihood that control weaknesses are overlooked or understated, which strengthens the practical, as opposed to merely formal, effectiveness of controls (Oyedotun et al., 2025). Third, the use of data analytics and, increasingly, artificial intelligence within the audit function extends the volume and granularity of transactions that can be examined, allowing audit to detect control breakdowns that would otherwise remain invisible until a fraud has already occurred (Kokina et al., 2025; Aljunaid et al., 2025). Fourth, continuous or near-continuous monitoring, increasingly supported by blockchain-based audit trails, shortens the interval between a control failure and its detection, converting internal controls from a periodically tested safeguard into a more consistently enforced one (Devianto et al., 2025; Maryani et al., 2026).

Taken together, these four mechanisms imply that internal control system effectiveness is not a fixed organizational property with a constant effect on fraud outcomes; rather, its practical impact is contingent on the quality of the audit function that supervises it. This is what Proposition 6 formalizes, and it is why the proposition is treated in this paper as a moderating rather than a direct effect: the same level of internal control system effectiveness is expected to translate into materially different fraud detection and prevention outcomes depending on whether audit is risk-based, independent, technologically enabled, and continuous, or the converse. Proposition 6 therefore completes the logic of the conceptual model: without it, the model would treat audit as simply one more antecedent of fraud detection and prevention among several, rather than as the governance mechanism that determines how fully the organization's investment in controls, blockchain, and AI/ML is actually converted into reduced fraud.

Conclusion

This paper developed an integrative conceptual framework examining how emerging technologies, internal control systems, and audit relate to the detection and prevention of financial fraud in the financial services sector, grounding its theoretical architecture in the Fraud Diamond Model. The six propositions that constitute the conceptual model collectively articulate a view of fraud not as an isolated event but as a structurally enabled outcome, one whose likelihood can be reduced through deliberate, technology-informed organizational design. Consistent with the conceptual, literature-based nature of this paper, the propositions are offered as a structured basis for future empirical research; they have not been tested statistically in this paper, and no claim of empirical validation is made.

The model begins with Proposition 1, which positions financial fraud as inversely related to internal control effectiveness. This relationship is foundational: where controls are weak, opportunity expands, and the

Fraud Diamond's convergence becomes more likely (Giannopoulos et al., 2025; Novatiani et al., 2024). Proposition 2 then holds that stronger internal control systems are associated with measurably greater fraud detection and prevention capacity, consistent with the COSO Framework's premise that control quality shapes organizational resilience against irregular conduct (Talla et al., 2025; Giannopoulos et al., 2025).

Propositions 3 and 4 situate the framework at the intersection of governance and digital transformation. Blockchain's immutability and distributed consensus properties are proposed to strengthen internal control system effectiveness by rendering retrospective manipulation structurally harder and audit trails more tamper-evident (Han et al., 2023; Ma & Li, 2024). Artificial intelligence and machine learning, through anomaly detection, predictive risk modeling, and continuous monitoring, are proposed to strengthen internal control system effectiveness by addressing both the opportunity and capability elements of the Fraud Diamond that are most sensitive to technological countermeasures (Miao, 2024; Hernandez Aros et al., 2024). Critically, the literature reviewed suggests that neither technology is likely to be effective in isolation: their anti-fraud value is expected to be realized only when they are integrated within formal control frameworks and governed by professionals who understand both their capabilities and their limitations (Kokina et al., 2025; Aljunaid et al., 2025).

Propositions 5 and 6 capture what may be the most consequential relationships in the model: the direct contribution of audit quality to fraud detection and prevention capacity, and the moderating effect of audit on the path from internal control effectiveness to fraud outcomes. A rigorous, independent, and risk-based audit function is proposed not merely to verify that controls exist, but to amplify their deterrent and detective power by closing implementation gaps, reducing rationalization through accountability, and signaling to organizational members that oversight is real and consequential (Becerra-Huamán et al., 2025; Oyedotun et al., 2025; Ansari et al., 2025). This moderation argument reflects a broader theoretical point developed in the Conceptual Framework and Propositions section: the effectiveness of internal controls is treated in this model not as a fixed organizational property, but as a contingent one, shaped by the quality of the oversight that supervises those controls.

The Internal Control Matrix (ICM) plays a structural role across several of these proposed relationships, providing the documentary architecture through which risks are mapped to controls, responsibilities are assigned, and evidence of execution is made verifiable (Sáenz, 2021; Wirantika & Setyaningrum, 2025). Its inclusion in the model reinforces the argument that technology-enabled fraud prevention is expected to require an underlying governance scaffold: without formal risk-control documentation, AI and blockchain tools may produce outputs that organizations lack the structural capacity to act upon.

From a theoretical standpoint, this paper contributes to the literature by organizing the Fraud Diamond's four elements, pressure, opportunity, rationalization, and capability, into a set of testable propositions expressed at the organizational level, aligned with constructs (financial fraud, internal control system effectiveness, blockchain, AI/ML, audit, and fraud detection and prevention) that can, in principle, be operationalized through structured instruments consistent with validated frameworks. This conceptual extension aims to enrich the Diamond's explanatory reach beyond its original individual-level application and to position it as a candidate framework for future governance research in digital environments.

For practitioners, the framework carries tentative implications, to be treated as propositions for practice rather than as established findings. Financial institutions should consider treating AI and blockchain not as substitutes for sound governance but as amplifiers of it, investing in their technical deployment together with the internal control infrastructure that gives that deployment meaning. Audit functions that combine risk-based planning, advanced analytics, professional independence, and continuous monitoring are, according to the framework developed here, better positioned to convert control investments into measurable anti-fraud outcomes. Regulators and standard-setters may wish to consider evaluating

organizations not only on whether formal controls exist, but on the quality of the oversight that validates their execution; empirical work is needed to test whether this distinction holds in practice.

As a conceptual paper, this study is subject to limitations inherent to the narrative literature review method. The propositions advanced here have not been subjected to empirical testing within this paper, and their validity, direction, and magnitude remain to be assessed with organizational data. The narrative review approach, while allowing integration across a broad and fast-moving literature, is not a systematic review and does not guarantee exhaustive coverage of all relevant studies. The reliance on recently published sources (2021-2026), while capturing the current state of a rapidly evolving field, means that the framework should be revisited as the literature on AI, blockchain, and audit continues to develop.

These limitations point toward a productive empirical research agenda. Future studies should operationalize the model's constructs and test Propositions 1 through 6 using organizational data, ideally combining objective records (e.g., audited financial statements, regulatory filings, documented fraud incidents) with perceptual measures to reduce common method variance. Cross-sectional designs would offer an initial test of the proposed relationships, while longitudinal studies tracking organizations as they deepen their AI and blockchain implementations would allow researchers to distinguish adoption effects from contextual confounds. Comparative studies across Caribbean, Latin American, and other financial systems would help establish whether the relationships proposed here are broadly applicable or contingent on jurisdiction-specific regulatory and institutional conditions.

Ultimately, this paper advances a conceptual argument to be tested empirically: effective fraud prevention in digitalized financial environments is expected to require the coordinated operation of well-designed controls, technologically enhanced monitoring, and independent oversight of sufficient quality to make those controls effective in practice. Whether these elements function together as proposed, and whether audit amplifies rather than merely verifies, are empirical questions that this framework is intended to make tractable for future research.

References

- Aljunaid, S. K., Almheiri, S. J., Dawood, H., & Khan, M. A. (2025). Secure and transparent banking: Explainable AI-driven federated learning model for financial fraud detection. *Journal of Risk and Financial Management*, 18(4), 179.
- Ansari, A., Valipour, H., & Salehi, H. (2025). The Impact of Artificial Intelligence Algorithms on Financial Fraud Detection and Prevention: The Moderating Role of Internal Control Systems. *International Journal of Finance & Managerial Accounting*, 12(47), 93-110.
- Becerra Huamán, C., De la Cruz-Montoya, D., Gutierrez-Cuadros, J., Pilco Labajos, S., & Lopez-Almeida, M. (2025). Financial auditing as an effective tool for fraud detection: a systematic review. *Journal of Risk and Financial Management*, 18(9), 523.
- Bermeo-Giraldo, M. C., Grajales-Gaviria, D., Valencia-Arias, A., & Palacios-Moya, L. (2021). Evolución de la producción científica sobre el fraude contable en las organizaciones: análisis bibliométrico. *Estudios Gerenciales*, 37(160), 492-505.
- Chen, H., Wang, S., Yang, D., & Zhou, N. (2025). COSO-Based Internal Control and Comprehensive Enterprise Risk Management: Institutional Background and Research Evidence from China. *Encyclopedia*, 5(3), 106.

- Chen, Y., Zhao, C., Xu, Y., Nie, C., & Zhang, Y. (2025). Deep learning in financial fraud detection: Innovations, challenges, and applications. *Data Science and Management*.
- Cressey, D. R. (1953). Other people's money; a study of the social psychology of embezzlement.
- Dorminey, J., Fleming, A. S., Kranacher, M. J., & Riley Jr, R. A. (2012). The evolution of fraud theory. *Issues in accounting education*, 27(2), 555-579.
- Gao, L. (2025). Enterprise internal audit data encryption based on blockchain technology. *PloS one*, 20(1), e0315759.
- Giannopoulos, V., Lymperopoulos, A., Kariofyllas, S., & Kariofyllas, C. (2025). Determinants of Internal Control System Effectiveness: Evidence from Greek Listed Companies. *Risks*, 13(11), 219.
- Gkegkas, M., Kydros, D., & Pazarskis, M. (2025). Using data analytics in financial statement fraud detection and prevention: A systematic review of methods, challenges, and future directions. *Journal of Risk and Financial Management*, 18(11), 598.
- Hernandez Aros, L., Bustamante Molano, L. X., Gutierrez-Portela, F., Moreno Hernandez, J. J., & Rodríguez Barrero, M. S. (2024). Financial fraud detection through the application of machine learning techniques: a literature review. *Humanities and Social Sciences Communications*, 11(1), 1-22.
- Kaptein, M. (2011). Understanding unethical behavior by unraveling ethical culture. *Human relations*, 64(6), 843-869.
- Kokina, J., Blanchette, S., Davenport, T. H., & Pachamanova, D. (2025). Challenges and opportunities for artificial intelligence in auditing: Evidence from the field. *International Journal of Accounting Information Systems*, 56, 100734.
- Kravchenko, O. V., Nebaba, N. O., & Aiyedogbon, J. O. (2023). Blockchain technologies in accounting: bibliometric analysis.
- Ma, W., & Li, W. (2024). Blockchain technology and internal control effectiveness. *Finance Research Letters*, 64, 105442.
- Mahdani, R., & Soufyan, D. A. (2026). Blockchain and Artificial Intelligence in Combating Financial Corruption: A Systematic Literature Review. *Journal of Central Banking Law and Institutions*, 5(1), 125-152.
- Maryani, N., Muchlish, M., Mulyadi, R., & Solehah, N. (2026). Blockchain-Based Audit Trails: Improving Transparency and Fraud Detection in Digital Accounting Systems. *International Journal of Advanced Computer Science & Applications*, 17(1).
- Miao, Z. (2024). Financial Fraud Detection and Prevention: Automated Approach Based on Deep Learning. *Journal of Organizational and End User Computing (JOEUC)*, 36(1), 1-27. <https://doi.org/10.4018/JOEUC.354411>

- Murphy, P. R., & Dacin, M. T. (2011). *Psychological pathways to fraud: Understanding and preventing fraud in organizations*. *Journal of Business Ethics*, 101(4), 601–618. <https://doi.org/10.1007/s10551-011-0741-0>
- Novatiani, R. A., Kusumah, R. W. R., Yadiati, W., Abdul Halim Rachmat, R., & Arifian Rachman, A. (2024). Internal auditor competence and internal control: Improving internal audit quality to prevent fraudulent financial statements. *Cogent Business & Management*, 11(1), 2409339.
- Ocampo, C. A. B. (2023). Detectando el fraude con inteligencia artificial: Una perspectiva avanzada en auditoría forense. *Revista la Junta*, 6(2), 13-40.
- Oyedotun, S. A., Oise, G. P., Akilo, B. E., Nwabuokei, O. C., Ejenarhome, P. O., Fole, M., & Onwuzo, C. J. (2025). The role of internal audit in fraud detection and prevention: A multi-contextual review and research agenda. *Journal of Science Research and Reviews*, 2(2), 76-85.
- Sáenz, L. (2021). La matriz de gestión y control de riesgos: Herramienta efectiva en la auditoría interna para las empresas comerciales de la ciudad de Panamá. *Revista FAECO sapiens*, 4(2), 15-42.
- Sahin, F., & Menekse, A. (2025). Internal control risk assessment using interval valued spherical fuzzy CRITIC EDAS. *Scientific Reports*, 15(1), 21505.
- Satoto, E. B., & Wibowo, Y. G. (2026). Implementation of Artificial Intelligence in Fraud Detection and Prevention Through a Systematic Literature Review and Its Implications for the Financial Sector. *Ilomata International Journal of Management*, 7(1), 460–483. <https://doi.org/10.61194/ijjm.v7i1.1919>
- Talla, A., Sapulette, S. G., & Limba, F. B. (2025). The relationship between public sector internal controls and fraud prevention. *International Journal of Economic Literature*, 2(12), 2150-2170.
- Watts, R. L., & Zimmerman, J. L. (1983). Agency problems, auditing, and the theory of the firm. *Journal of Law and Economics*, 26(3), 613–633.
- Wirantika, N. L. P. A. P., & Setyaningrum, D. (2025). Analysis of Internal Control over Financial Reporting on Inventory Accounts: A Case Study at Institution X. *E-Jurnal Akuntansi*, 35(7).
- Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, 74(12), 38–42.