

Governance in the digital age: blockchain, artificial intelligence, and audit as integrated mechanisms against financial fraud in the financial services

Angel Ojeda, *Universidad Ana G. Méndez*, aojeda@uagm.edu
Juan Martínez, *Universidad Ana G Méndez*, martinezj9@uagm.edu
José Cruz, *Universidad Ana G. Méndez*, cruzjl@uagm.edu

Abstract

The increasing sophistication of financial fraud in digitalized organizational environments demands a reassessment of the mechanisms through which governance, technology, and oversight interact. This theoretical study proposes and examines five research propositions connecting blockchain technology, artificial intelligence (AI), machine learning (ML), internal control systems (ICS), audit, and fraud detection and prevention (FDP) within a unified conceptual model grounded in the Fraud Diamond Model. Rather than treating these variables in isolation, the study argues that their combined and sequentially dependent operation determines organizational anti-fraud capacity. The Internal Control Matrix (ICM) is analyzed as the documentary scaffold linking technological inputs to actionable governance. Audit is theorized as a moderating variable that amplifies ICS effectiveness rather than merely verifying its existence. Findings contribute to the governance and accounting information systems literature by extending the Fraud Diamond to the organizational level and providing a testable structural framework for future empirical research in the financial services sector.

Keywords: artificial intelligence, audit quality, blockchain, fraud detection and prevention, internal control systems

Theoretical Background and Fraud Framework

The Fraud Diamond as an Organizational Lens

Explaining financial fraud requires a theoretical model that accounts for the complexity of organizational conditions under which it emerges. The Fraud Diamond, developed as an extension of the classical Fraud Triangle, addresses this need by incorporating a fourth element, capability, alongside pressure, opportunity, and rationalization (Sánchez-García et al., 2022). Unlike its predecessor, the Diamond acknowledges that fraudulent intent is insufficient without the technical skill and positional access to execute it, a distinction of growing significance in digital financial environments where fraud increasingly requires sophisticated system knowledge (Mahdani, 2026; Ansari, 2025).

Pressure, the first element, encompasses financial incentives, demanding performance targets, or personal economic strain that create motivation for deceptive conduct (Dorminey et al., 2012). In competitive financial markets, performance pressure intensifies the risk of accounting manipulation or misrepresentation of financial information (Chen et al., 2025). Opportunity, the second element, is structurally enabled by weaknesses in supervision, segregation of duties, and organizational monitoring, precisely the dimensions addressed by internal control systems (Zhang et al., 2022). When controls are robust, opportunity contracts; when controls are deficient, it expands (Becerra Huamán et al., 2025).

Rationalization, the third element, refers to the cognitive and moral neutralization process through which perpetrators justify their conduct (Kaptein, 2022). Murphy and Dacin (2011) identify three psychological pathways supporting this process: absence of moral awareness, intuitive reasoning combined with post-hoc rationalization, and deliberate logical justification. Organizational cultures characterized by ambiguity, weak ethical leadership, or inconsistent policy enforcement amplify rationalization (Scott, 2021). Capability, the fourth element, has grown in importance as digital transformation has elevated the technical barriers to fraud execution: contemporary schemes require data manipulation expertise, access to privileged systems, and knowledge of control circumvention techniques (Sánchez-García et al., 2022; Mahdani, 2026).

The Fraud Diamond provides the organizing framework for this study's conceptual model. Each variable, financial fraud, internal control systems, blockchain, AI/ML, and audit, maps onto one or more Diamond elements, and the propositions derived in subsequent sections reflect how organizational and technological choices alter the probability that all four elements converge.

Financial Fraud: Definition, Manifestations, and Governance Implications

Financial fraud encompasses intentional behaviors that distort information or transactions to obtain undue benefits, and its analytical complexity increases with the volume and velocity of digital transactional data (Miao et al., 2024). It can manifest as transaction fraud, manipulation of individual payments or transfers, financial reporting fraud, deliberate misstatement of financial statements, or hybrid schemes combining both forms (Gkegkas et al., 2025). Beyond direct economic loss, fraud produces systemic consequences: investor confidence erodes, market value declines, regulatory scrutiny intensifies, and institutional legitimacy is weakened in ways that often exceed the immediate monetary impact (Becerra Huamán et al., 2025; Chen et al., 2025).

The governance implications of financial fraud extend well beyond the affected organization. Reliable financial reporting is a foundational pillar of capital market efficiency and macroeconomic stability (Chen et al., 2025; Zhang et al., 2022). When that reliability is compromised, whether through accounting manipulation, record alteration, or misrepresentation, the systemic trust sustaining financial activity weakens structurally (Becerra Huamán et al., 2025; Ansari, 2025). Contemporary literature consistently identifies deficiencies in internal control systems, insufficient monitoring, and the absence of formal risk assessment structures as the primary organizational conditions that enable fraud (Chen et al., 2025). The lack of integration between digital processes and control frameworks further amplifies vulnerability in high-velocity financial environments (Mahdani, 2026).

The dynamic and adaptive character of fraud demands that its analysis as a research variable incorporate both governance dimensions, control design, oversight quality, audit rigor, and technological dimensions, particularly the capacity of AI and data analytics to detect patterns that static controls and rule-based systems cannot (Miao et al., 2024; Gkegkas et al., 2025). This dual framing is central to the model developed in this study.

Literature Review

Internal Control Systems: Design, Effectiveness, and the Control Matrix

Internal control systems are conceptualized as integrated sets of policies, procedures, and mechanisms designed to ensure reliable operations, regulatory compliance, and effective risk management (Giannopoulos et al., 2025). The COSO Framework (2020) establishes five components as foundational to ICS effectiveness: control environment, risk assessment, control activities, information and

communication, and monitoring. Empirical evidence confirms that ICS effectiveness is associated with the quality of each of these components, and that well-structured systems protect organizational resources by reducing structural opportunities for improper conduct (Talla, 2025; Giannopoulos et al., 2025).

The Internal Control Matrix (ICM), described in the literature as a risk-control matrix, provides the documentary architecture through which ICS design is operationalized. The ICM maps each identified risk to its mitigating control, assigns ownership, and specifies the evidence expected from proper execution (Sáenz, 2021). From an audit perspective, this mapping functions as a planning instrument that aligns audit objectives with the risk profile of each process, improving work program consistency and enabling empirical measurement of control quality (Giannopoulos et al., 2025; Wirantika & Setyaningrum, 2025). Research demonstrates that when ICMs are limited to a subset of risks, typically labeled "key risks", the coverage of control testing is compromised, increasing residual vulnerability (Wirantika & Setyaningrum, 2025). Matrices connected to dynamic risk assessment and prioritization methodologies allow monitoring to concentrate on areas of greatest exposure rather than distributing attention uniformly (Sahin et al., 2025; Talla, 2025).

Blockchain Technology: Immutability, Traceability, and Control Enhancement

Blockchain technology is characterized by distributed ledgers governed by properties of immutability, consensus, and cryptographic traceability (Han et al., 2023). Its primary contribution to accounting and auditing environments is the structural impossibility of undetected retrospective alteration: once a transaction is recorded and validated by the distributed network, modifying it requires overcoming consensus mechanisms that are computationally prohibitive under most threat models (Kravchenko et al., 2023). This property directly addresses the opportunity element of the Fraud Diamond by rendering data manipulation structurally harder and audit trails inherently more tamper-evident (Ma et al., 2024).

In auditing contexts, blockchain-enabled near-real-time access to verified transaction records supports continuous auditing schemes that reduce the temporal gap between transaction occurrence and audit review (Devianto et al., 2025). Recent evidence on blockchain and internal audit functions discusses both the security and recording benefits and the implementation challenges, including data governance complexity, regulatory uncertainty, and organizational change management demands, that determine whether blockchain adoption translates into control effectiveness improvements (Gao et al., 2025; Zhang et al., 2025). Research on blockchain-based audit trails highlights their contribution to transparency and to the strengthening of fraud detection capacity within digital accounting systems, particularly when integrated with formal ICS frameworks rather than deployed as standalone technologies (Ma et al., 2024; Syahputra et al., 2026).

Artificial Intelligence and Machine Learning: Adaptive Detection and Governance Challenges

Artificial intelligence and machine learning address limitations of rule-based fraud detection by identifying anomalous patterns across high-dimensional, high-velocity financial datasets in ways that fixed-rule systems cannot (Miao et al., 2024). Deep learning architectures have been applied to fraud detection across transaction fraud, insurance fraud, and financial reporting fraud, demonstrating superior precision relative to legacy approaches (Chen, 2025). In auditing, simpler AI applications, automated data extraction, anomaly flagging, and analytical review, are now widely adopted, while more complex applications face ongoing challenges of interpretability, bias in training data, and professional liability when outputs drive consequential decisions (Kokina et al., 2025).

The explainability dimension of AI in fraud contexts has received growing attention, driven by regulatory demands for auditable decision-making. Explainable AI (XAI) frameworks seek to balance predictive accuracy with the transparency needed to sustain conclusions before regulators and courts (Hernandez-Aros et al., 2024). Federated learning approaches, which train models collaboratively across institutional

participants without centralizing data, address privacy concerns while preserving analytical power—a particularly relevant architecture for financial sector applications where data sovereignty constraints are substantial (Aljunaid et al., 2025). Critically, the literature consistently finds that AI and ML effectiveness is contingent on underlying data quality, formal control structures, and professional oversight: these technologies amplify governance rather than replace it (Hernandez-Aros et al., 2024; Satoto & Wibowo, 2026).

Audit: From Verification to Strategic Assurance

The role of audit in financial governance has evolved substantially from mechanical verification of account balances toward a strategic assurance function that evaluates the design and operating effectiveness of the entire internal control system (Becerra Huamán et al., 2025). Internal audit, conceived as a core ICS component, assesses whether controls are appropriately designed, whether they operate as designed, and whether they remain adequate given changes in the organizational risk profile (Chen et al., 2025). Modern auditing increasingly integrates data analytics and AI for risk-based evidence collection, expanding coverage, improving timeliness, and reducing reliance on sampling-based procedures susceptible to gaps (Becerra Huamán et al., 2025; Kokina et al., 2025).

Forensic auditing represents a specialized extension of this function, integrating accounting, legal, and technological knowledge to investigate irregularities, reconstruct complex financial events, and provide evidence for judicial or disciplinary proceedings (Ocampo, 2023; Becerra Huamán et al., 2025). Beyond its reactive role, forensic auditing fulfills a preventive function by identifying structural control weaknesses before they are exploited and by strengthening the organizational culture of ethics and accountability (Ansari, 2025; Mahdani, 2026). The attributes of independence, competence, objectivity, and professional skepticism are identified in the literature as the professional foundations that determine audit quality and, through quality, anti-fraud effectiveness (Oyedotun, 2025; Novatiani et al., 2024).

Fraud Detection and Prevention: Mechanisms, Limits, and the Technology Imperative

Fraud detection and prevention encompass the full range of preventive and corrective mechanisms through which organizations reduce the probability, duration, and impact of fraudulent incidents (Talla, 2025). Recent evidence demonstrates that effective internal controls are associated with significantly lower probability of fraudulent financial reporting, confirming the barrier function of control quality (Zaki & Adrianto, 2026). Advanced data analytics complement traditional audit procedures by identifying anomalous signals embedded in large datasets that manual review cannot surface (Gkegkas et al., 2025).

A critical limitation of rule-based detection systems, whether in controls or audit, is their static character: defrauders adapt their methods to known detection thresholds, rendering fixed rules progressively less effective over time (Miao et al., 2024). Adaptive, data-driven detection approaches that learn from behavioral patterns rather than predefined rules are increasingly positioned as necessary complements to structural controls. Blockchain reinforces prevention by making the transactional record more reliable and the evidence base for detection more complete (Syahputra et al., 2026). The operationalization of fraud detection and prevention as a research variable accordingly requires indicators spanning multiple dimensions: early detection capacity, preventive control effectiveness, incident frequency and severity, and the maturity of continuous monitoring practices (Gkegkas et al., 2025).

Conceptual Model and Research Propositions

The conceptual model integrates six constructs, Financial Fraud (FF), Internal Control System (ICS), Blockchain (BC), Artificial Intelligence and Machine Learning (AI/ML), Audit (AUD), and Fraud Detection and Prevention (FDP), within the explanatory structure of the Fraud Diamond. The model posits

that FF is an inverse function of ICS effectiveness; that BC and AI/ML each contribute positively to ICS quality; that ICS effectiveness drives FDP capacity; and that AUD moderates the strength of the ICS-to-FDP relationship. The Internal Control Matrix (ICM) operates as the governance scaffold linking technological inputs, blockchain-generated immutable records, AI-generated anomaly flags, to the formal control structures that organizational actors can interpret and act upon. Five research propositions capture these relationships and are presented in Table 1.

Table 1. Research Propositions and Supporting Literature

	Proposition	Supporting Literature
P1	Financial fraud is negatively associated with the effectiveness of the internal control system.	Kabuye et al. (2020); Zaki & Adrianto (2026); Miao et al. (2024)
P2	A more effective internal control system is positively associated with greater fraud detection and prevention capacity.	Talla (2025); Giannopoulos et al. (2025); COSO (2020)
P3	Blockchain technology is positively associated with the effectiveness of the internal control system.	Han et al. (2023); Ma et al. (2024); Gao et al. (2025)
P4	Artificial intelligence and machine learning are positively associated with the effectiveness of the internal control system.	Miao et al. (2024); Kokina et al. (2025); Hernandez-Aros et al. (2024)
P5	Audit positively moderates the relationship between internal control system effectiveness and fraud detection and prevention.	Becerra Huamán et al. (2025); Ansari (2025); Oyedotun (2025)

P1 and P2: The Internal Control - Fraud Nexus

P1 establishes the foundational logic of the model: financial fraud is inversely related to ICS effectiveness. Where controls are weak, the opportunity element of the Fraud Diamond expands, lowering the threshold for fraudulent action (Kabuye et al., 2020). Organizations with deficient risk assessment processes, insufficient segregation of duties, or undocumented control responsibilities exhibit systematically higher exposure to financial misrepresentation (Zaki & Adrianto, 2026). P2 completes the governance chain by establishing that ICS effectiveness translates into measurable fraud detection and prevention capacity: well-designed and consistently executed controls constrain the structural space within which fraud operates (Talla, 2025; Giannopoulos et al., 2025). Together, P1 and P2 position ICS as the central governance variable, both the primary target of technology-based enhancement and the primary driver of anti-fraud outcomes.

P3 and P4: Technology as Governance Amplifier

P3 and P4 situate blockchain and AI/ML as inputs to ICS effectiveness rather than independent anti-fraud mechanisms. Blockchain contributes through structural immutability: distributed ledger properties make the data environment resistant to manipulation, expanding the reliability of the information on which controls operate (Han et al., 2023; Ma et al., 2024). This directly reduces the opportunity element of the Fraud Diamond by hardening the record layer against retrospective alteration. AI and ML contribute through adaptive detection and enhanced monitoring: their capacity to process large transaction volumes and identify behavioral anomalies strengthens both the risk assessment and monitoring components of ICS in ways that static rule-based controls cannot match (Miao et al., 2024; Kokina et al., 2025).

A critical qualification applies to both propositions: neither technology generates anti-fraud value in isolation. Blockchain records require formal control structures to govern access, validate outputs, and trigger corrective action. AI-generated anomaly signals require professional judgment, governance frameworks, and quality controls to translate into decisions that withstand audit scrutiny (Hernandez-Aros et al., 2024; Aljunaid et al., 2025). Organizations that deploy these technologies without investing in the underlying ICS infrastructure and the ICM documentation that connects technological outputs to control responsibilities are unlikely to realize meaningful fraud prevention gains.

P5: Audit as Moderator of the ICS–FDP Relationship

P5 captures the most theoretically consequential relationship in the model. ICS effectiveness is not a fixed organizational property; it is contingent on the quality of the independent oversight that validates control design, tests operating effectiveness, and identifies gaps before they are exploited (Becerra Huamán et al., 2025; Oyedotun, 2025). A rigorous, independent, and risk-based audit function transforms formal controls into operational deterrents by closing implementation gaps, the space between how controls are designed and how they are executed, reducing rationalization through increased accountability, and signaling to all organizational actors that oversight is real and consequential (Ansari, 2025; Novatiani et al., 2024).

This moderation operates through two Fraud Diamond elements simultaneously. Audit reduces opportunity by validating that controls operate as designed. Audit reduces rationalization by making the consequences of control evasion credible and visible. The moderating effect is expected to be strongest in organizations where audit is technologically enabled, deploying data analytics and AI for risk-based planning and continuous monitoring, and weakest where audit remains a periodic, sampling-based compliance exercise without independence from operational management (Kokina et al., 2025; Becerra Huamán et al., 2025).

Discussion

Theoretical Contributions

This study makes three principal theoretical contributions. First, it extends the Fraud Diamond from an individual-level behavioral model to an organizational-level governance framework. By mapping each study variable onto Diamond elements, FF onto pressure and capability; ICS onto opportunity; AUD onto opportunity and rationalization; BC and AI/ML onto opportunity and capability, the model demonstrates that the Diamond's explanatory architecture scales to organizational analysis without requiring modification of its core logic. This extension broadens the Diamond's applicability to governance and accounting information systems research and provides a theoretically coherent basis for testing organizational anti-fraud interventions.

Second, the explicit theorization of the ICM as a governance scaffold distinguishes this study from prior work that treats internal controls generically. The ICM operationalizes the interface between technological inputs and organizational control action: blockchain-generated tamper-evident records and AI-generated anomaly signals produce anti-fraud value only when formal risk-control documentation provides the structural capacity to interpret and act on these outputs. Without ICM infrastructure, technology deployment generates outputs that organizations lack the governance architecture to use. This argument provides a precise mechanism through which technology adoption translates, or fails to translate, into ICS effectiveness improvements.

Third, the moderation architecture of P5 advances the theoretical treatment of audit beyond its conventional role as a fraud detection mechanism. By theorizing audit as a variable that amplifies the strength of the ICS-to-FDP relationship rather than acting directly on fraud, the study positions audit quality as a contingency condition that determines whether control investments produce their expected anti-fraud returns. This

framing has direct implications for research design in governance and assurance studies: audit quality should be modeled as a moderator rather than a mediator or independent predictor in structural analyses of fraud outcomes.

Practical Implications

For financial institutions and their governance structures, the model's central implication is that anti-fraud investment requires coherence across three interdependent layers: formal ICS design documented through comprehensive ICMs, technological enhancement through blockchain and AI/ML integrated within those control frameworks, and audit oversight of sufficient quality, independence, competence, and technological capability, to validate execution and close gaps. Optimizing any single layer without investing in the others is unlikely to produce proportionate anti-fraud returns. Organizations that deploy AI without robust ICMs, or that maintain extensive control documentation without independent audit validation, leave structural vulnerabilities that the Fraud Diamond's remaining elements can exploit.

For regulators and standard-setters in the financial services sector, the model suggests that compliance frameworks should evaluate organizations not only on whether formal controls exist but on the quality of the oversight validating their operational effectiveness. Regulatory examination protocols that emphasize documentation of controls over testing of their execution will consistently underestimate actual fraud exposure. Requirements for audit functions that combine risk-based planning, continuous monitoring capability, and genuine independence from operational management are more likely to produce institutions with the governance infrastructure that the model identifies as necessary for effective fraud prevention.

Limitations and Future Research

This study is theoretical in scope, and its propositions await empirical validation. The most immediate research priority is a quantitative test of the structural model using data from financial services professionals with direct knowledge of ICS design, audit practices, and technology adoption within their organizations. Geographic scope is a second limitation of the initial model. The study's contextual grounding in the financial services sector of Puerto Rico reflects a specific regulatory environment, organizational culture, and technological adoption trajectory that may not generalize to other jurisdictions. Comparative studies across Caribbean and Latin American financial systems would test whether the structural relationships identified here are context-specific or broadly applicable across comparable emerging-economy financial sectors. Such comparisons would also allow researchers to examine how regulatory stringency, supervisory capacity, and technology infrastructure interact with the model's variables in determining fraud outcomes.

A third limitation involves measurement fidelity. Self-reported perceptual data, the most practically accessible source for constructs such as audit quality and ICS effectiveness, introduces common method bias that affects coefficient estimates. Future designs should complement survey instruments with objective organizational data: audit findings and remediation rates, technology adoption metrics, fraud incident records, and regulatory examination results. Longitudinal designs tracking the same organizations as technology adoption matures and audit practices evolve would allow researchers to disentangle the temporal dynamics of the ICS-technology-audit relationship that cross-sectional designs cannot capture.

Conclusion

This study developed a theoretically grounded conceptual model examining how blockchain, artificial intelligence and machine learning, internal control systems, and audit interact to shape financial fraud detection and prevention in digitalized financial environments. Grounded in the Fraud Diamond Model and drawing on recent literature spanning governance, accounting information systems, and emerging technology adoption, the model advances five research propositions that collectively articulate a view of fraud not as a discrete event but as a structurally enabled outcome, one that is made more or less probable by deliberate organizational choices about control design, technology integration, and audit quality.

The central argument is both straightforward and consequential: effective financial fraud prevention requires the coherent and simultaneous operation of formal internal controls documented through the ICM, technologically enhanced monitoring through blockchain and AI/ML embedded within those controls, and independent audit oversight of sufficient depth and rigor to make those controls real in practice rather than nominal on paper. When these elements operate in coordination, and when audit amplifies rather than merely verifies control effectiveness, the organizational conditions that enable fraud contract across all four Fraud Diamond dimensions.

The theoretical contributions of this study, the empirical agenda it defines, and the practical implications it identifies for governance practitioners and regulators collectively invite the field to treat financial fraud prevention not as a compliance obligation but as an organizational capability built deliberately at the intersection of technology, governance design, and professional oversight quality. That capability, the evidence suggests, is neither automatic nor guaranteed by technology adoption alone, it must be constructed, maintained, and continuously validated.

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.
- 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. (2025). Deep learning in financial fraud detection: Innovations, challenges, and applications. *Data Science and Management*.
- Devianto, H., Mediaty, M., & Junus, A. (2025). A new era of audit by blockchain technology: Continuous auditing. In Proceedings of ICAME 2024 (pp. 849–874). *Atlantis Press*.

- Dorminey, J., Fleming, A. S., Kranacher, M. J., & Riley, R. A., Jr. (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.
- Han, H., Shiwakoti, R. K., Jarvis, R., Mordi, C., & Botchie, D. (2023). Accounting and auditing with blockchain technology and artificial intelligence: A literature review. *International Journal of Accounting Information Systems*, 48, 100598.
- Hernandez Aros, L., Bustamante Molano, L. X., Gutierrez-Portela, F., Moreno Hernandez, J. J., & Rodriguez 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.
- Kabuye, F., Nkundabanyanga, S. K., Opiso, J., & Nakabuye, Z. (2020). Internal audit activities, governance mechanisms and fraud management practices. *Managerial Auditing Journal*, 35(2), 289–306.
- Kaptein, M. (2022). The moral entrepreneur: A new component of ethical leadership. *Journal of Business Ethics*, 176(4), 781–791.
- 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. *Financial and Credit Activity Problems of Theory and Practice*, 1(48), 166–179.
- 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.
- Miao, Z. (2024). Financial fraud detection and prevention: Automated approach based on deep learning. *Journal of Organizational and End User Computing*, 36(1), 1–27.
- 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.

- 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.
- Sahin, F., & Menekse, A. (2025). Internal control risk assessment using interval valued spherical fuzzy CRITIC EDAS. *Scientific Reports*, 15(1), 21505.
- 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.
- Sánchez García, J., Martínez Ramos, M., & Mendoza López, J. (2022). Fraud Diamond Model in contemporary organizational contexts. *Journal of Accounting Research*, 15(2), 45–67.
- 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.
- Scott, B. F. (2021). Red teaming financial crime risks in the banking sector. *Journal of Financial Crime*, 28(1), 98–111.
- Syahputra, M., 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).
- 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.
- 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).
- Zaki, M. J., & Adrianto, Z. (2026). The impact of internal control on fraudulent financial reporting of state-owned enterprises. *International Journal of Management and Business Economics*.
- Zhang, Y., Ma, Z., & Meng, J. (2025). Auditing in the blockchain: a literature review. *Frontiers in Blockchain*, 8, 1549729.
- Zhang, Z., Wang, L., & Liu, Y. (2022). Globalization, digital transformation, and financial fraud: An integrated analysis. *Journal of Financial Regulation*, 8(1), 112–134.