p-ISSN: 2774-518X ←ISSN→ e-ISSN: 2775-2828
JURNAL AKUNTANSI DAN BISNIS INDONESIA
JABISI
Vol. 7, No. 2, Oktober 2026, pp. 205-221
DOI: https://doi.org/10.55122/jabisi.v7i2.2380

REGULATORY ARCHITECTURE, INSTITUTIONAL GOVERNANCE AND TECHNOLOGICAL ADOPTION IN FINANCIAL FRAUD PREVENTION: A SYSTEMATIC LITERATURE REVIEW WITH IMPLICATIONS FOR EMERGING ECONOMICS

AUTHOR

[1)]Ardiani Ika Sulistyawati, [2)]Aria Hendrawan, [3)]Aprih Santoso, [4)]Aristo Kevin Ardyaneira Pratama

ABSTRACT

Financial fraud and money laundering severely destabilize sustainable financial ecosystems, disproportionately harming emerging economies through weak supervisory capacity, as revealed by a systematic review of 192 studies spanning 1993 to 2026. While technologies like AI and RegTech improve detection accuracy, they simultaneously create a compliance divide between advanced and developing nations, whereas fragmented cross-border oversight continually fuels unmanageable regulatory arbitrage. Ultimately, the evidence demonstrates that internal control maturity, ethical governance, and forensic auditing are the most reliable deterrents against fraud, prompting the study to advocate for a risk-to-resilience framework rooted in harmonized enforcement and targeted capacity building.

Keyword

Financial Fraud, Money Laundering, Internal Control, Regulatory Compliance, Forensic Auditing, Regtech, Emerging Economies

AFFILIATION

Study Program: [1,2,3)]Accounting
Name of Institution: [1,2,3)]Universitas Semarang, [4)]University of Regensburg
Institution Address: [1,2,3)]Semarang, Central Java, Indonesia, [4)]Regensburg, Germany

CORRESPONDENCE

Author: Ardiani Ika Sulistyawati
Email: ardiani@usm.ac.id

LICENSE

This work is licensed under a Creative Commons Attribution 4.0 Internasional License.

I. INTRODUCTION

Financial fraud and money laundering are no longer peripheral operational nuisances; they are systemic threats that erode public trust, distort capital allocation, and weaken the institutional foundations of economic development (Chatain et al., 2009; "Money laundering: impact…", 2024). Estimates place global fraud losses at more than USD 5 trillion annually, a figure that dwarfs the development finance flows directed to the economies most exposed to illicit financial activity (Arunasalam, 2023). Because financial integrity underpins investment confidence, tax capacity, and financial inclusion, the effectiveness of fraud prevention is directly implicated in the sustainable development agenda, particularly in emerging and developing jurisdictions where supervisory capacity is thinnest (Onyekaonwu, 2025; Sultan et al., 2025; Vaithilingam & Nair, 2007).

The regulatory field has evolved from rule-based reporting obligations toward risk-based architectures anchored in the recommendations of the Financial Action Task Force (FATF) and their regional transpositions (Alexander, 2001; Hopton, 2016). However, the proliferation of directives has not resolved a basic question: under what institutional conditions do such frameworks actually reduce fraud? Some studies report that well-designed internal control systems materially lower fraud incidence (Enofe et al., 2017; Malahim et al., 2023; Nyakarimi et al., 2019); others find that prescriptive obligations impose disproportionate compliance costs without curbing sophisticated, technology-enabled crime (Iheonunekwu, 2024; Killick & Parody, 2007; Unger & van Waarden, 2009). A parallel disagreement surrounds technology. Machine learning and RegTech demonstrably improve real-time anomaly detection and reduce false positives (Akinsanya et al., 2025; Amoako et al., 2025; Jo et al., 2025), but critics point to algorithmic opacity, data-protection conflicts, and an infrastructure gap that leaves emerging economies unable to realize those gains (Chitimira & Ncube, 2021; Chukwu, 2025; Ononiwu et al., 2025).

These unresolved tensions matter because criminal actors optimize across jurisdictions. Where enforcement is fragmented and risk-based approaches are applied inconsistently, the resulting asymmetries become exploitable (Alnuaimi & Dahlan, 2025; Kirschenbaum & Véron, 2018; Kuzior et al., 2025). Existing reviews tend to isolate one pillar regulation, internal control, or technology and to draw on a narrow geographic base, which limits their usefulness for policymakers designing integrated responses in resource-constrained settings. This review, therefore, treats fraud prevention as the joint product of three interacting pillars: external regulatory architecture, the internal governance processes of financial institutions, and technological capability (Adeosun, 2025; Raoui & Leila, 2023; Wahyu & Nasution, 2025; Zmarialy & Harikumar, 2025). The framing is grounded in the fraud triangle and its hexagon extension, which locate fraud in the interaction of pressure, opportunity, rationalization, capability, arrogance, and collusion, and in risk-based regulatory theory, which treats supervision as the allocation of scarce enforcement attention to the highest-risk exposures (Dalla Pellegrina & Masciandaro, 2009; Pamungkas et al., 2025; Rehman & Hashim, 2020; Salihu, 2025).

Accordingly, the study asks: (i) how effective are regional regulatory frameworks in mitigating financial fraud and money laundering; (ii) what role do internal control systems and forensic auditing play in detecting sophisticated financial crime; (iii) how does digital transformation reshape prevention and compliance strategies; (iv) which cross-border supervisory mechanisms constitute best practice; and (v) how do corporate governance structures condition financial reporting integrity and fraud deterrence? The paper contributes in three ways. First, it synthesizes a large and geographically diverse body of evidence spanning 1993 to 2026 into a single comparative account. Second, it distinguishes empirically supported determinants of fraud outcomes from those that are

merely widely asserted, notably by separating internal control maturity from rule density. Third, it derives a policy agenda oriented toward emerging economies, where the gap between formal adoption of international standards and their effective enforcement is widest. The remainder of the paper is organized as follows. Section 2 develops the conceptual framework; Section 3 sets out the review methodology; Section 4 reports the results; Section 5 discusses convergences, divergences, and implications; Section 6 presents limitations and a future research agenda; and Section 7 concludes.

II. LITERATURE REVIEW

2.1 Regulatory Architecture and The Risk-Based Turn

The international anti-money laundering (AML) regime is a soft-law order in which FATF recommendations acquire binding force through national transposition and peer evaluation (Alexander, 2001; Hopton, 2016). Its central design question is the trade-off between rule-based and risk-based supervision. Rule-based regimes offer legal certainty and ease of enforcement but generate defensive over-reporting, the so-called crying-wolf problem, in which the volume of suspicious transaction reports degrades the informational value of each (Dalla Pellegrina & Masciandaro, 2009; Unger & van Waarden, 2009). Risk-based regimes concentrate resources on material exposures but presuppose supervisory sophistication and institutional integrity that many jurisdictions lack (Killick & Parody, 2007; Sultan et al., 2025). This conditionality is central to the present review: the same regulatory instrument can be effective or merely costly depending on the institutional environment in which it is implemented.

2.2 Internal Governance as The Operative Control Layer

Regulation acts on fraud only through the internal processes of financial institutions. The COSO framework control environment, risk assessment, control activities, information and communication, and monitoring remains the dominant reference model in the reviewed literature (Alisen, 2025; Masabanda & Vélez, 2025). Its explanatory power is strongest when paired with governance mechanisms that shape the control environment itself: board independence, audit committee effectiveness, whistleblowing channels, and ethical tone at the top (Mohd-Sanusi et al., 2015; Pamungkas et al., 2025; Shonhadji & Irwandi, 2024). Forensic auditing sits alongside these as a specialized investigative capability focused on intentional deception rather than unintentional misstatement (Dalwadi, 2023; Idrus et al., 2024; Jacob & Funmi, 2024).

2.3 Technology as an Enabler and a Source of New Exposure

Digital transformation is doubly implicated. It provides analytical capabilities for supervised and unsupervised learning, network analytics, and blockchain forensics, enabling real-time monitoring at scale (Agorbia-Atta, 2024; Amoako et al., 2025; Chitimira et al., 2024). It simultaneously creates new attack surfaces through instant payments, virtual assets, and cross-border digital channels that outpace the legal categories designed for intermediated banking (Covolo, 2020; Faccia et al., 2020; Neto, 2025). The reviewed literature converges on the view that technological adoption is a necessary but insufficient condition, effective only where governance, data quality, and staff capability are already adequate (Essien et al., 2025; Hossain, 2025).

Figure 1 summarises the framework: regulatory architecture sets the external constraint, internal governance operationalizes it, technology modulates the detection frontier, and cross-border cooperation determines whether gains in one jurisdiction survive contact with others.

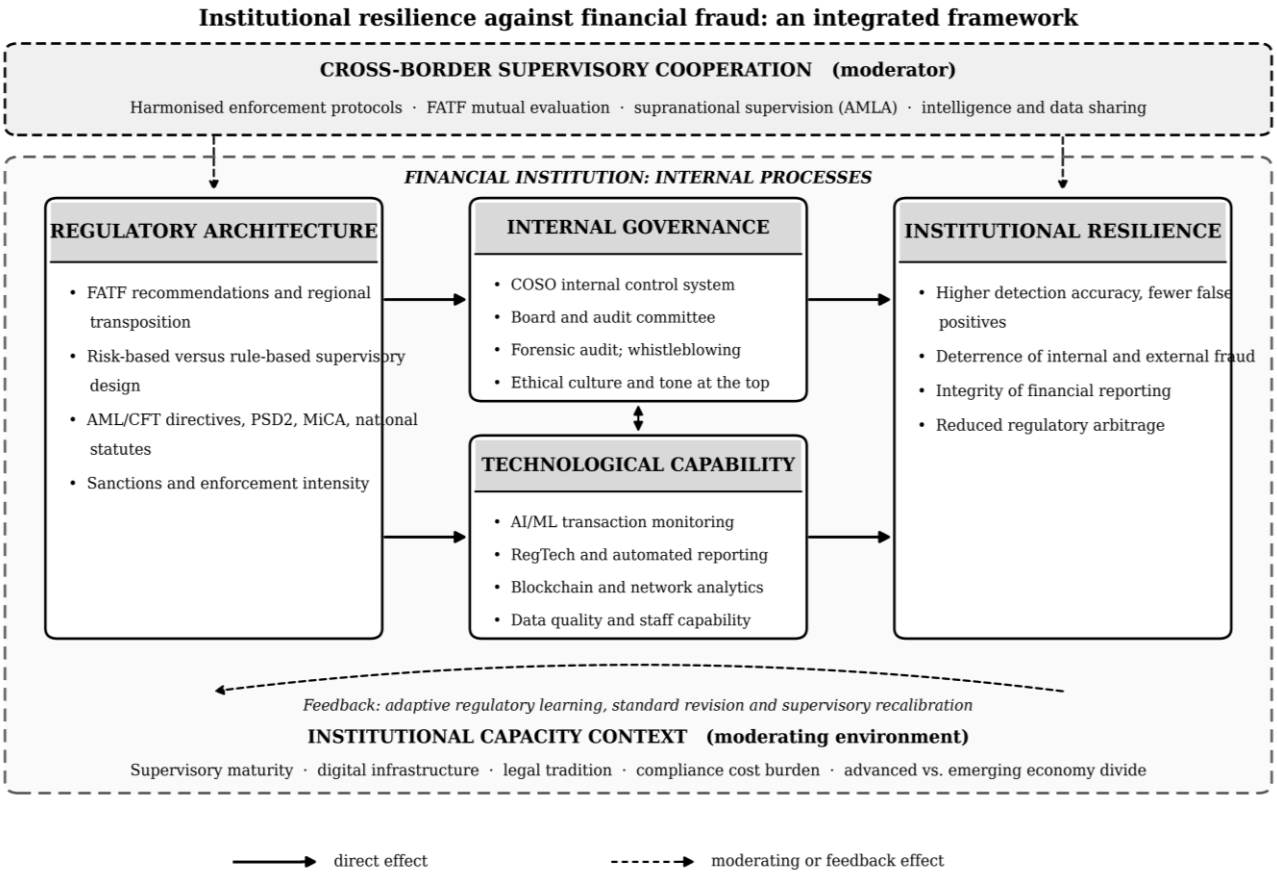


Figure 1. Conceptual framework linking regulatory architecture, internal governance, technological capability, and cross-border cooperation to institutional resilience against financial fraud.

III. RESEARCH METHOD

3.1 Review Design

The study follows the PRISMA 2020 reporting guideline (Page et al., 2021) and the three-stage protocol for management and finance reviews of planning, conducting, and reporting (Tranfield et al., 2003). A systematic rather than narrative design was chosen because the research question concerns the accumulation and consistency of evidence across heterogeneous jurisdictions, which requires transparent and reproducible selection criteria.

3.2 Search Strategy and Query Expansion

The primary research question, regulatory and legal frameworks for financial fraud prevention in specific regions or countries, and the role of financial institutions and their internal processes, was expanded into five targeted search statements to balance comprehensiveness against precision. The expanded statements addressed, respectively: regional frameworks and cross-border supervisory cooperation together with bank internal control, governance and forensic auditing; AML/CFT regulatory governance in the European Union, FATF-style regional bodies and Asia-Pacific; regional AML/CFT implementation, including MENAFATF, EAG, and the EU Anti-Money Laundering Authority (AMLA); and regulatory harmonization covering fintech sandboxes and crypto asset regulation such as MiCA and FATF cross-border guidance. Searches covered peer-reviewed journal articles, book chapters, working papers, and supervisory reports indexed in a multidisciplinary database of scholarly records, without language restriction, up to the search date.

3.3 Eligibility Criteria

Records were included where they (i) addressed financial fraud, money laundering, or terrorist financing prevention; (ii) examined regulatory frameworks, institutional internal processes, or

technological controls; (iii) concerned financial institutions or their supervisors; and (iv) reported empirical evidence, systematic legal analysis, or documented case study material. Records were excluded where they addressed fraud outside the financial sector, offered opinion without analytical or evidentiary support, or duplicated an included record.

3.4 Screening, Citation Chaining, and Appraisal

The expanded queries returned 257 candidate records. Backward citation chaining through the reference lists of core studies identified foundational work not surfaced by the keyword search, and forward chaining identified subsequent studies building on those results, adding 90 records. Of the resulting pool of 347 candidates, 345 were judged relevant to the research question, and 192 were classified as highly relevant based on topical fit, methodological transparency, and jurisdictional specificity; these 192 constitute the synthesis corpus. Screening and relevance classification were conducted independently by two reviewers, with disagreements resolved by discussion and, were unresolved, by a third reviewer.

3.5 Data Extraction and Synthesis

Each included study was coded along five analytical dimensions derived from the conceptual framework: regulatory compliance posture, fraud detection accuracy, internal control maturity, cross-border cooperation, and technological adoption level. Given the heterogeneity of designs, outcome measures, and jurisdictions, a meta-analysis was not appropriate; a narrative synthesis combining thematic, chronological, and comparative analyses was used instead. Themes were derived inductively from the coded extracts and retained where they appeared in a substantial share of the corpus.

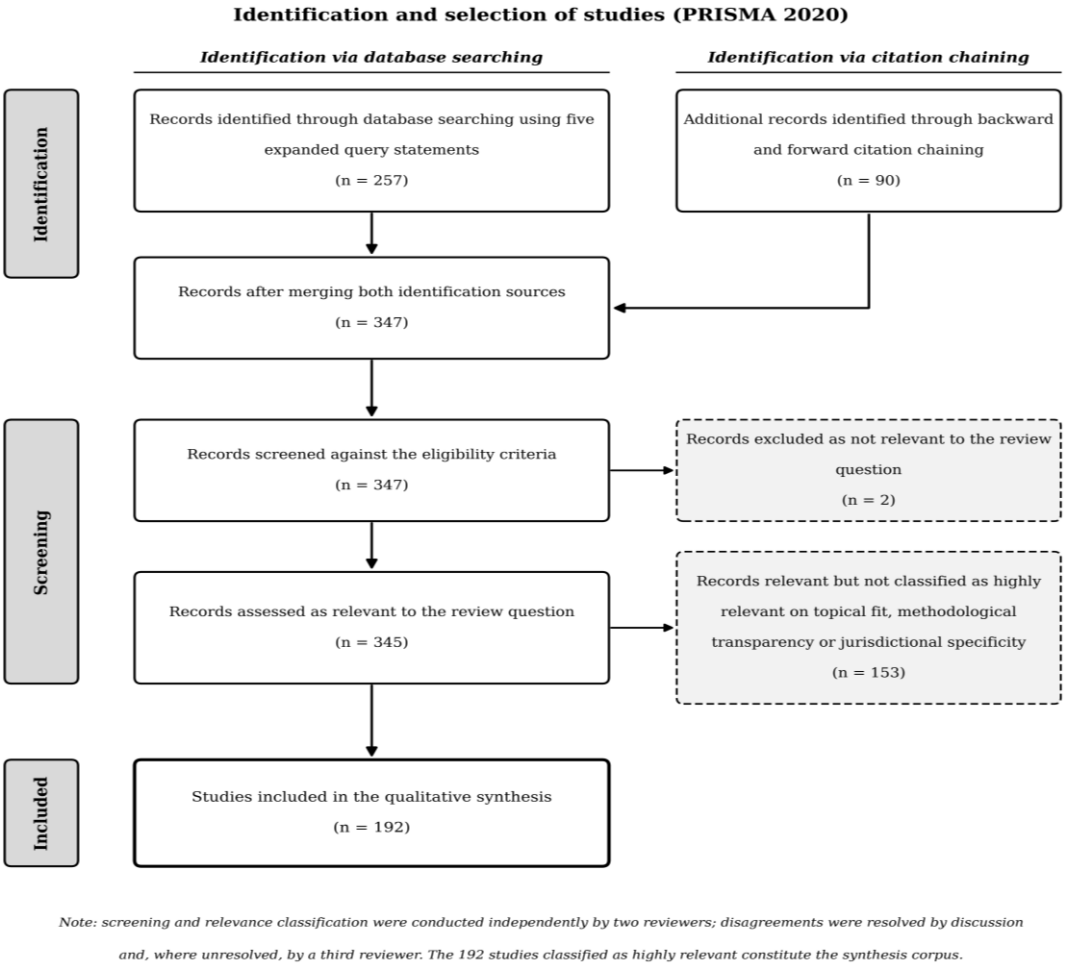


Figure 2. PRISMA 2020 flow diagram of identification, screening, and inclusion (257 records identified through database searching; 90 additional records identified through citation chaining; 347 records screened; 345 assessed as relevant; 192 included in the synthesis).

IV. RESULT AND DISCUSSION

4.1 Research Result

4.1.1 Descriptive Characteristics of The Corpus

The corpus spans a broad set of jurisdictions, including the United States, the European Union, the United Kingdom, Nigeria, India, Indonesia, Malaysia, Pakistan, Tanzania, South Africa, Kenya, Angola, Iran, the United Arab Emirates, Mexico, and the member states of the Eurasian Economic Union. Designs range from systematic reviews and quantitative surveys analyzed using structural equation modeling to doctrinal legal analysis and single-institution case studies. Table 1 summarises the distribution of evidence across the five coded dimensions.

Table 1. Distribution of evidence across the five coded analytical dimensions (n = 192).

Dimension	Studies	Principal findings and qualifications
Regulatory compliance	192	Compliance is treated as foundational for financial integrity across the corpus. Fifteen studies indicate that customer due diligence and know-your-customer requirements serve only as a baseline, with enhanced due diligence and risk-based calibration required for effectiveness (Ononiwu et al., 2025; Sarfaraz et al., 2025; Sultan et al., 2025). Ten studies identify fragmented frameworks and inconsistent enforcement as the binding constraint on realized compliance (Alnuaimi & Dahlan, 2025; Kirschenbaum & Véron, 2018; Kuzior et al., 2025).
Fraud detection accuracy	192	Integration of artificial intelligence and machine learning improves precision while reducing false positives (Akinsanya et al., 2025; Amoako et al., 2025; Jo et al., 2025). Twelve studies find forensic accounting and specialized audit units necessary to uncover schemes that conventional audits miss (Dalwadi, 2023; Idrus et al., 2024; Jacob & Funmi, 2024). Eight studies report that detection performance is undermined by inadequate staff training and weak organizational support (Pinho, 2015; Sarfaraz et al., 2025; Younus, 2021).
Internal control maturity	192	The COSO framework is the dominant reference model (Alisen, 2025; Masabanda & Vélez, 2025). Fourteen studies argue controls must be dynamic and adaptive rather than static and rule-bound (Hossain, 2025; Zmarialy & Harikumar, 2025). Nine studies find that ethical organizational culture matters as much as technical control design for durable deterrence (Olaoye et al., 2023; Shonhadji & Irwandi, 2024).
Cross-border cooperation	192	International cooperation and information sharing are considered indispensable in combating transnational crime (Cotoc et al., 2021; Olalekan, 2025). Eleven studies foreground FATF's role in setting standards and aligning jurisdictions (Alkaabi et al., 2010; Hopton, 2016; Manning et al., 2021). Seven studies identify data protection law and privacy obligations as recurring obstacles to exchange (Abdullahi et al., 2025; Ishii, 2025).
Technological adoption	192	Blockchain analytics, artificial intelligence, and data analytics are considered essential to modernizing prevention (Agorbia-Atta, 2024; Chitimira et al., 2024). Thirteen studies warn that adoption requires governance and ethical safeguards to contain algorithmic bias (Chukwu, 2025; Essien et al., 2025). Six studies note resource differentials that constrain adoption in developing economies (Chitimira & Ncube, 2021; Ononiwu et al., 2025; Onyekaonwu, 2025).

4.1.2 Thematic Synthesis

Six themes were derived inductively from the coded corpus (Table 2). The distribution indicates that regulatory compliance and internal governance dominate the field, while digital transformation, though the fastest-growing theme, remains comparatively under-researched.

Table 2. Themes derived from the synthesis corpus.

Theme	Frequency	Description
Regulatory compliance and international standards	148/192	FATF recommendations and their regional transpositions establish a baseline for institutional integrity, but effectiveness is constrained by inconsistent local enforcement and by compliance costs that fall disproportionately on smaller institutions (Alkaabi et al., 2010; Hopton, 2016; Iheonunekwu, 2024; Killick & Parody, 2007).
Internal control systems and governance	132/192	Internal controls, predominantly modeled on COSO, are identified as the primary operational defense. Their maturity, supported by an ethical culture and independent audit committees, conditions both the deterrence of fraud and the reliability of reporting (Kharbach & Zaam, 2025; Masabanda & Vélez, 2025; Pamungkas et al., 2025; Shonhadji & Irwandi, 2024).
Technological innovation in detection	125/192	Artificial intelligence, machine learning, and analytics improve real-time monitoring and reduce false positives, while raising unresolved questions about algorithmic accountability and a persistent capability divide (Amoako et al., 2025; Chitimira & Ncube, 2021; Chukwu, 2025; Jo et al., 2025).
Cross-border supervisory cooperation	98/192	Transnational crime requires harmonized enforcement and information sharing. Bilateral instruments are widely regarded as insufficient, prompting proposals for supranational supervisory authorities, such as AMLA (Asenov, 2025; Buttigieg, 2025; Cotoc et al., 2021; Kaiser, 2024).
Forensic accounting and investigative auditing	72/192	Forensic capability targets intentional deception and complex schemes that conventional audits may miss; its integration into internal governance improves detection and accountability (Dalwadi, 2023; Idrus et al., 2024; Jacob & Funmi, 2024; Wahyu & Nasution, 2025).
Digital transformation and emerging risks	48/192	Fintech, cryptoassets, and instant payment rails introduce vulnerabilities that existing categories address imperfectly, prompting calls for regulatory sandboxes and updated legal frameworks (Covolo, 2020; Faccia et al., 2020; Neto, 2025; Roide, 2022).

4.1.3 Chronological Development of The Field

The literature displays four discernible phases (Table 3), moving from procedural internal audit concerns to an integrated, technology-mediated conception of institutional resilience.

Table 3. Chronological development of research on financial fraud prevention.

Period	Research Direction	Characteristics
1993–2002	Foundational controls	Focus on internal audit functions, the responsibility of senior management for fraud prevention, and the initial articulation of international AML standards (Alexander, 2001; Bowe & Jobome, 2001).
2005–2012	Regulatory formalisation	Examination of the shift from rule-based to risk-based supervision, transposition of FATF recommendations, and the role of know-your-customer policy in banking (Arnone & Padoan, 2008; Dalla Pellegrina & Masciandaro, 2009; Killick & Parody, 2007; Vaithilingam & Nair, 2007).
2013–2019	Institutional integration	Assessment of internal control effectiveness, the influence of corporate governance on deterrence, and the design of cross-border supervisory architectures (Adetiloye et al., 2016; Mohd-Sanusi et al., 2015; Salehi & Molla Imeny, 2019; van den Broek, 2014).
2020–2026	Digital transformation	Emphasis on artificial-intelligence-driven detection, fintech and cryptoasset exposure, supranational supervision, and adaptive technology-integrated regulation (Amoako et al., 2025; Buttigieg, 2025; Covolo, 2020; Hossain, 2025).

4.1.4 Convergence and Divergence Across Studies

Convergence is strongest where the claim is structural and weakest where it is instrumental. Studies agree that internal controls, regulatory compliance, and technological capability are the constitutive pillars of prevention and that financial institutions act as primary gatekeepers. They diverge on the comparative merits of prescriptive versus adaptive regulation and on how far organizational culture substitutes for or complements formal control (Table 4).

Table 4. Points of agreement and divergence in the reviewed literature.

Criterion	Agreement	Divergence	Plausible explanation
Effectiveness of internal controls	Robust internal controls with forensic auditing are essential to detection (Jacob & Funmi, 2024; Kharbach & Zaam, 2025; Wahyu & Nasution, 2025)	Controls alone are insufficient absent ethical culture or wider organizational reform (Adetiloye et al., 2016; Olaoye et al., 2023)	Differences in organizational maturity and in whether whistleblowing is integrated with formal audit (Prayoga & Sukristanta, 2025; Shonhadji & Irwandi, 2024)
Rule-based versus risk-based regulation	The risk-based turn reduces over-reporting and improves allocative efficiency (Cociug & Andrusceac, 2020; Dalla Pellegrina & Masciandaro, 2009)	Some jurisdictions retain rule-based systems for deterrence and legal certainty (Unger & van Waarden, 2009)	Divergent legal traditions, notably adversarial legalism versus cooperative informalism (Unger & van Waarden, 2009)
Technology and prevention	Machine learning materially improves real-time monitoring accuracy (Agorbia-Atta, 2024; Akinsanya et al., 2025; Amoako et al., 2025; Chukwu, 2025)	Adoption is constrained by privacy law, algorithmic bias, and poor interoperability (Akinsanya et al., 2025; Essien et al., 2025)	Uneven infrastructure maturity and jurisdiction-specific constraints such as data-protection regimes (Abdullahi et al., 2025; Essien et al., 2025)
Cross-border cooperation	International cooperation and information sharing are indispensable (Cotoc et al., 2021; Iheonunekwu, 2024; Olalekan, 2025)	Fragmented oversight and non-standardized enforcement persist as barriers (Kirschenbaum & Véron, 2018; Nga et al., 2025)	Geopolitical factors, uneven institutional development, and the absence of a harmonized supervisor (Alnuaimi & Dahlan, 2025; Kuzior et al., 2025)

4.1.5 Critical Appraisal of The Evidence Base

The corpus is methodologically uneven. A substantial subset employs structural equation modeling or path analysis to test the relationship between control constructs and fraud outcomes, thereby permitting inference about mediating mechanisms (Kharbach & Zaam, 2025; Nyakarimi et al., 2019; Wahyu & Nasution, 2025). A larger subset, however, relies on cross-sectional perception surveys administered to bank employees, an instrument susceptible to social desirability bias and unlikely to track actual fraud incidence (Arunasalam, 2023; Biswakarma & Bhusal, 2023; Sarfaraz et al., 2025; Younus, 2021). The confidentiality of loss data constrains data quality, so perceived effectiveness often substitutes for realized outcomes (Musa, 2025; Pinho, 2015). Consistency is high for the internal-control finding and low for the effect of specific regulatory interventions, with results reversing across resource-constrained and well-resourced settings (Iheonunekwu, 2024; Killick & Parody, 2007; Unger & van Waarden, 2009).

4.2 Discussion

4.2.1 Theoretical Implications

The evidence substantiates the opportunity component of the fraud triangle theory: regulatory weakness, procedural lapses, and digital deficits are shown to create the conditions that criminal actors exploit, rather than merely correlate with fraud (Sudi & Mwendapole, 2025). The extension of the fraud hexagon is supported by findings that capability, arrogance, and collusion operate alongside pressure and rationalization, implying that governance models restricted to segregation of duties address only part of the causal structure (Pamungkas et al., 2025; Salihu, 2025). The review also qualifies risk-based regulatory theory. Its efficiency claim holds where supervisory capacity and institutional integrity are already high, and weakens where they are not; in low-capacity settings, discretion may be captured or simply unexercised, so that the risk-based approach delivers neither the deterrence of rules nor the efficiency of targeting (Dalla Pellegrina & Masciandaro, 2009; Sultan et al., 2025; Unger & van Waarden, 2009). This conditionality is a boundary condition that the theory does not currently specify. Finally, the literature supports reframing compliance from a static obligation to a dynamic capability. The risk-to-resilience formulation treats compliance investment as an organizational absorptive capacity that accelerates adaptation to novel laundering techniques, thereby aligning fraud prevention with the resilience literature in sustainable finance (Hossain, 2025; Zmarialy & Harikumar, 2025).

4.2.2 Practical and Policy Implications

For financial institutions, the priority is to move beyond tick-box compliance by positioning internal audit as a strategic function rather than an administrative one and by integrating forensic capabilities into the second and third lines of defense (Idrus et al., 2024; Killick & Parody, 2007; Prayoga & Sukristanta, 2025). Investment in staff capability is not optional: detection technology underperforms where analysts cannot interpret its output (Pinho, 2015; Sarfaraz et al., 2025). For supervisors and policymakers, three actions follow from the evidence. First, harmonize enforcement protocols and fraud taxonomies to ensure cross-jurisdictional data are comparable, a precondition for meaningful intelligence sharing (Moes & Ruesing, 2024). Second, invest in supervisory technological capacity in emerging economies, since the compliance divide is a systemic vulnerability rather than a domestic one; the weakest node determines the network's exposure (Kuzior et al., 2025; Onyekaonwu, 2025). Third, design regulation to be adaptive, permitting sandboxes and staged authorization for new business models while requiring algorithmic accountability and explainability from those deploying automated decision systems (Chukwu, 2025; Roide, 2022).

4.2.3 Implications for Sustainable Development

The findings bear directly on the development agenda. Illicit financial flows divert domestic resources that would otherwise finance public goods, and the reputational consequences of weak AML performance raise the cost of external capital for the economies least able to bear it (Manning et al., 2021; Vaithilingam & Nair, 2007). Conversely, over-calibrated compliance requirements can

produce financial exclusion by making low-value customers uneconomic to serve, and by driving de-risking in correspondent banking relationships (Killick & Parody, 2007; Sultan et al., 2025). Effective fraud prevention in emerging economies, therefore, requires calibration that protects integrity without foreclosing inclusion, a trade-off the current literature acknowledges but has not resolved empirically.

4.2.4 Limitations and Future Research

4.2.4.1 Limitations of The Reviewed Literature and of This Review

Four limitations constrain the reviewed evidence (Table 5). In addition, this review has its own limitations. Relevance classification involved judgment despite dual screening; grey literature and supervisory documents not indexed in the source database may have been missed; and the absence of formal quality weighting means that findings from methodologically weaker studies enter the narrative synthesis alongside stronger ones.

Table 5. Limitations of the reviewed literature.

Limitation	Description	Illustrative studies
Geographic concentration	Much of the empirical work is anchored in a small set of national contexts, notably Nigeria, India, and Indonesia, which limits generalisability across regulatory cultures.	(Adeosun, 2025; Adetiloye et al., 2016; Ahmed et al., 2023; Dalwadi, 2023; Enofe et al., 2017; Musa, 2025; Panggabean et al., 2025; Prayoga & Sukristanta, 2025; Shonhadji & Irwandi, 2024; Suhardi & Bernanthos, 2024)
Data confidentiality and access	Sensitivity of loss data forces reliance on small samples and qualitative interviews, reducing statistical power and precluding reliable prevalence estimates.	(Arunasalam, 2023; Pinho, 2015; Sarfaraz et al., 2025; Younus, 2021)
Methodological fragmentation	Fraud is operationalized using non-comparable metrics and frameworks, which impede cross-study synthesis and knowledge accumulation.	(Arnone & Padoan, 2008; Braun et al., 2016; Hanifah, 2024)
Regulatory lag behind technology	Legal frameworks trail innovation in cryptoassets and automated decision-making, so compliance strategies validated against current rules may not address live operational risk.	(Alnuaimi & Dahlan, 2025; Covolo, 2020; Panggabean et al., 2025; Sudi & Mwendapole, 2025; Wankhade, 2026)

4.2.4.2 Future Research Agenda

Table 6 sets out a prioritized agenda. High-priority items address the evidentiary deficits that most constrain policy inference; medium- and low-priority items address scope extensions.

Table 6. Prioritized future research agenda.

Gap	Proposed direction	Justification	Priority
Longitudinal fraud impact	Multi-year panel tracking realized fraud losses across banks in emerging markets, rather than perceived effectiveness.	Validates whether preventive investment produces measurable loss reduction (Musa, 2025; Pinho, 2015)	High

Compliance divide	Comparative cost-benefit analysis of low-technology versus high-technology compliance solutions in resource-constrained supervisors	Determines whether capability transfer or simplification is the more efficient route to harmonization (Chitimira & Ncube, 2021; Onyekaonwu, 2025)	High
Algorithmic accountability	Development and field-testing of an audit framework for AI-based compliance models covering transparency, fairness, and explainability	Automated decision-making is becoming central to AML without a corresponding assurance regime (Chukwu, 2025; Essien et al., 2025; Jo et al., 2025)	High
Cross-border data privacy	Evaluation of privacy-preserving techniques, including federated learning, for compliant cross-jurisdictional exchange	Resolves the standing conflict between data-protection obligations and information sharing (Abdullahi et al., 2025; Ishii, 2025; Olalekan, 2025)	High
Compliance cost incidence	Empirical estimation of the differential burden of rule-based versus risk-based regimes on small financial institutions	Excessive fixed compliance cost risks exclusion and market concentration (Iheonunekwu, 2024; Killick & Parody, 2007; Unger & van Waarden, 2009)	Medium
Control culture	Mixed-methods measurement of the association between specific ethical leadership behaviors and control effectiveness	Culture is widely asserted to matter but rarely operationalized (Enofe et al., 2017; Olaoye et al., 2023)	Medium
Forensic integration	Assessment of whether mandating forensic certification for internal audit staff advances early detection.	Formalizes the bridge between compliance and active investigation (Dalwadi, 2023; Idrus et al., 2024; Jacob & Funmi, 2024)	Medium
Informal financial channels	Qualitative study of integrating informal value transfer providers into national AML/CFT frameworks	Exclusion of informal channels leaves a structural gap in coverage (Alkaabi et al., 2010; Sultan et al., 2025)	Medium
Whistleblowing efficacy	Analysis of anonymous third-party-managed reporting platforms and their effect on internal reporting rates	Whistleblowing surfaces fraud that automated monitoring cannot detect (Pamungkas et al., 2025; Shonhadji & Irwandi, 2024)	Low
Taxonomic harmonisation	Proposal and testing of a standardized global fraud taxonomy for supervisory data exchange	Comparability is a precondition for cross-border intelligence sharing (Moes & Ruesing, 2024; Nga et al., 2025)	Low

IV. CONCLUSION

This review synthesized 192 studies to examine how regulatory architecture, institutional governance, and technological adoption jointly determine financial fraud prevention outcomes. Three conclusions follow. First, the field has shifted decisively from static rule compliance to risk-based governance. Still, the efficiency gains of that shift are contingent on supervisory and organizational capacity that many jurisdictions do not yet possess. Second, internal control maturity, integrated with forensic auditing and an ethical governance culture, is the most consistently supported determinant of deterrence; the density of external rules is not. Third, technological capability is transforming detection while simultaneously widening a compliance divide, and fragmented cross-border supervision allows the arbitrage that divide creates to persist.

The principal implication is that fraud prevention should be treated as a systemic, multilayered institutional capability rather than an administrative obligation. Financial institutions should position internal audit and forensic functions as strategic enablers; supervisors should prioritize harmonized enforcement protocols, comparable fraud taxonomies, and adaptive frameworks that accommodate innovation while requiring algorithmic accountability. For emerging economies in particular, technological capacity-building is a precondition for participating in, rather than being exploited by, the global integrity regime. Two questions remain open. The optimal balance between privacy-preserving technology and comprehensive financial surveillance is unresolved, as is the long-run sustainability of risk-based supervision in low-capacity jurisdictions. Progress on both requires longitudinal evidence of realized fraud losses and standardized taxonomies that enable cross-jurisdictional comparison. Until such evidence exists, claims about the effectiveness of any particular regulatory design should be advanced with corresponding caution.

REFERENCE

Abdullahi, M. B., Jiya, M., & Shehu, I. S. (2025). Strengthening digital sovereignty in the fight against money laundering and terrorism financing. IGI Global. https://doi.org/10.4018/979-8-3693-9137-2.ch008

Adeosun, O. A. (2025). Combating financial fraud through forensic audit and corporate governance. https://doi.org/10.5281/zenodo.14710782

Adetiloye, K. A., Olokoyo, F. O., & Taiwo, J. (2016). Fraud prevention and internal control in the Nigerian banking system. *International Journal of Economics and Financial Issues, 6*(3), 1172–1179.

Agorbia-Atta, C. (2024). Setting new benchmarks to combat financial crimes and ensure the safety and security of America's digital financial landscape. *International Journal of Science and Research Archive, 13*(1), 1291–1298. https://doi.org/10.30574/ijsra.2024.13.1.1738

Ahmed, I., Abubakar, N., Garba, H. A., & Hamzah, M. A. (2023). Effect of detection and control of financial fraud on performance of Nigerian deposit money banks – a conceptual review. *Journal of Global Social Sciences, 4*(13), 47–61. https://doi.org/10.58934/jgss.v4i13.133

Akinsanya, O. B., Gokah, B. E., & Adom, S. G. (2025). Cloud-based risk controls for financial fraud prevention in US digital banking. *EPRA International Journal of Economics, Business and Management*. https://doi.org/10.36713/epra25488

Alexander, K. (2001). The international anti-money-laundering regime: the role of the Financial Action Task Force. *Journal of Money Laundering Control, 4*(3), 231–248. https://doi.org/10.1108/EB027276

Alisen, J. P. (2025). Implementation of internal control systems for fraud prevention and detection in the Rural Bank of Batangas. https://doi.org/10.26480/mbmj.01.2025.20.32

Alkaabi, A., Mohay, G. M., McCullagh, A., & Chantler, N. (2010). Money laundering and FATF compliance by the international community. In the *Lecture Notes of the Institute for Computer Sciences*. Springer. https://doi.org/10.1007/978-3-642-15479-9_8

Alnuaimi, T. A. S. A. T., & Dahlan, N. H. (2025). Financial cybercrime in the United Arab Emirates: an analytical assessment of legal and regulatory frameworks. *Lex Localis, 23*(S6), 3740–3755. https://doi.org/10.52152/qfsb5z28

Amoako, D., Boboye, C. O., Boateng, V., & Laryea, J. E. (2025). Artificial intelligence and machine learning for fraud detection in the US banking industry: regulatory frameworks, implementation, and challenges. *EPRA International Journal of Economics, Business and Management*, 57–69. https://doi.org/10.36713/epra23647

Arnal, J. (2025). Two sides of the same coin: fraud prevention and accountability in retail payments. *Journal of Financial Regulation*. https://doi.org/10.1093/jfr/fjaf007

Arnone, M., & Padoan, P. C. (2008). Anti-money laundering by international institutions: a preliminary assessment. *European Journal of Law and Economics, 26*(3), 361–386. https://doi.org/10.1007/S10657-008-9069-3

Arunasalam, K. (2023). Anti-fraud measures and corporate policies to combat financial fraud in Malaysian financial institutions. *E3S Web of Conferences, 389*, 09028. https://doi.org/10.1051/e3sconf/202338909028

Asenov, E. (2025). On the need to establish a European Union authority for combating money laundering and terrorist financing (AMLA). https://doi.org/10.56065/accountcont/2025.107

Bartolozzi, D., Gara, M., Marchetti, D. J., & Masciandaro, D. (2019). Designing the anti-money laundering supervisor: theory, institutions and empirics. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.3501650

Bergström, M. (2024). The EU's fight against money laundering and terrorist financing in a digital and fragmented world. Springer. https://doi.org/10.1007/978-3-031-54200-8_8

Biswakarma, G., & Bhusal, P. (2023). Banks' level factors affecting the effective implementation of anti-money laundering practices in Nepalese banks. *South Asian Journal of Finance, 3*(1). https://doi.org/10.4038/sajf.v3i1.53

Bowe, M., & Jobome, G. (2001). Regulating securities fraud: evidence from unauthorized trading cases. *Journal of Financial Regulation and Compliance, 9*(2), 151–160. https://doi.org/10.1108/EB025070

Braun, J., Kasper, M., Majdanska, A., & Somare, M. (2016). Drivers of suspicious transaction reporting levels: evidence from a legal and economic perspective—*Journal of Tax Administration, 2*(1).

Buttigieg, C. P. (2025). The EU anti-money-laundering authority: a strategic roadmap. *Journal of Financial Compliance, 8*(4), 339. https://doi.org/10.69554/jrfu9377

Chatain, P., McDowell, J., Mousset, C., Schott, P. A., & van der Does de Willebois, E. (2009). *Preventing Money Laundering and Terrorist Financing: A Practical Guide for Bank Supervisors.* World Bank Publications.

Chitimira, H., & Ncube, M. (2021). Towards ingenious technology and the robust enforcement of financial markets laws to curb money laundering in Zimbabwe. *Potchefstroom Electronic Law Journal, 24*(1), 1–47. https://doi.org/10.17159/1727-3781/2021/V24I0A10729

Chitimira, H., Torerai, E., & Jana, L. (2024). Leveraging artificial intelligence to combat money laundering and related crimes in the banking sector in South Africa. *Potchefstroom Electronic Law Journal, 27*. https://doi.org/10.17159/1727-3781/2024/v27i0a18024

Christensen, L. D. (2025). Financial fraud and the PSD2. Oxford University Press. https://doi.org/10.1093/9780198949084.003.0006

Chukwu, B. N. (2025). Fintech innovation and digital security: AI applications for fraud mitigation and regulatory compliance in US financial markets. *International Journal of Science and Research Archive, 17*(1), 1031–1041. https://doi.org/10.30574/ijsra.2025.17.1.2916

Cociug, V., & Andrusceac, T. (2020). Risk-based approach in the European Union legislation to prevent money laundering and financing of terrorism. *Economy and Sociology*(1), 43–52.

Cotoc, C., Nitu, M., Scheau, M. C., & Cozma, A. (2021). Efficiency of money laundering countermeasures: case studies from European Union member states. *Risks, 9*(6), 120. https://doi.org/10.3390/RISKS9060120

Covolo, V. (2020). The EU response to criminal misuse of cryptocurrencies: the young, already outdated 5th anti-money laundering directive. *European Journal of Crime, Criminal Law and Criminal Justice, 28*(3), 217–251. https://doi.org/10.1163/15718174-BJA10003

Dalla Pellegrina, L., & Masciandaro, D. (2009). The risk-based approach in the new European anti-money laundering legislation: a law-and-economics view. *Review of Law and Economics, 5*(2), 931–952. https://doi.org/10.2202/1555-5879.1422

Dalwadi, P. (2023). Uncovering financial fraud: the role of forensic accounting in preventing and detecting fraud in India. *International Journal of Management, Public Policy and Research, 2*(2), 1–5. https://doi.org/10.55829/ijmpr.v2i2.145

Djordjevic, A., Jevtic, B., & Dedjanski, S. (2024). Interactions between regulations, law, new technologies, and organizational policies in financial fraud detection: a case study of Serbia. *Pravo - teorija i praksa, 41*(4), 48–68. https://doi.org/10.5937/ptp2404048d

Enofe, A., Abilogun, T., & Omoolorun, A. J. (2017). Bank fraud and preventive measures in Nigeria: an empirical review. *International Journal of Academic Research in Business and Social Sciences, 7*(7), 40–51. https://doi.org/10.6007/IJARBSS/V7-I7/3076

Essien, I. A., Ajayi, J. O., Erigha, E. D., Obuse, E., & Ayanbode, N. (2025). AI-driven governance systems for proactive regulatory compliance and fraud risk management in financial service environments. https://doi.org/10.5281/zenodo.17157706

Faccia, A., Mosteanu, N. R., Cavaliere, L. P. L., & Mataruna-Dos-Santos, L. J. (2020). Electronic money laundering, the dark side of fintech: an overview of the most recent cases. In *Proceedings of the 2020 12th International Conference on Information Management and Engineering*. https://doi.org/10.1145/3430279.3430284

Fauzi, F., Szulczyk, K. R., & Basyith, A. (2018). Moving in the right direction to fight financial crime: prevention and detection. *Journal of Financial Crime, 25*(2), 362–368. https://doi.org/10.1108/JFC-06-2017-0060

Hanifah, H. S. (2024). Global insights into financial statement fraud detection and prevention. *Summa, 2*(1), 1–15. https://doi.org/10.61978/summa.v2i1.972

Hopton, D. (2016). Financial Action Task Force (FATF). In *Money Laundering: A Concise Guide for All Business*es. Routledge. https://doi.org/10.4324/9781315596006-4

Hossain, M. A. (2025). Data-driven compliance frameworks for anti-money laundering (AML) and tax risk management in financial institutions. https://doi.org/10.63125/2n5pd137

Idrus, M., Adriana, N., Rustam, A., Sulistyowati, N. W., & Rewa, K. A. (2024). The impact of forensic accounting on financial fraud prevention: a comparative analysis across countries. *The Journal of Academic Science, 1*(8), 1074–1084. https://doi.org/10.59613/m6jrt421

Iheonunekwu, P. (2024). The trifecta against financial crime: a collaborative analysis of the roles of banks, consulting firms, and governments. *World Journal of Advanced Research and Reviews*. https://doi.org/10.30574/wjarr.2024.23.3.2739

Ishii, Y. (2025). Financial institutions. Oxford University Press. https://doi.org/10.1093/9780198957089.003.0014

Jacob, E. O., & Funmi, P. A. (2024). Effect of forensic accounting practices on financial accountability and transparency in Nigeria's deposit money banks. *Journal of Economics, Finance and Management Studies, 7*(7). https://doi.org/10.47191/jefms/v7-i7-24

Jo, H., Bui, H., & Moreland, D. (2025). Role of AI in fraud detection: Are financial institutions using the most effective systems?. *Journal of Finance Issues, 23*(2), 1–31. https://doi.org/10.58886/jfi.v23i2.10086

Kaiser, R. (2024). Compliance requirements in the future EU anti-money laundering and counter-terrorism financing framework. *Journal of Financial Compliance*. https://doi.org/10.69554/lptq3527

Kharbach, M., & Zaam, H. (2025). The contribution of internal audits to the detection and prevention of financial fraud in listed companies: an empirical study. *Multidisciplinary Reviews, 9*(2), 2026051. https://doi.org/10.31893/multirev.2026051

Killick, M., & Parody, D. (2007). Implementing AML/CFT measures that address risks, not tick boxes. *Journal of Financial Regulation and Compliance, 15*(2), 210–216. https://doi.org/10.1108/13581980710744093

Kirschenbaum, J., & Véron, N. (2018). A better European Union architecture to fight money laundering. Bruegel Policy Contribution.

Kuzior, A., Vasylieva, T., Smutka, L., & Ammar, O. (2025). Toward tailored AML/CFT strategies: clustering countries by FATF compliance and effectiveness. *Journal of International Studies, 18*(2), 229–254. https://doi.org/10.14254/2071-8330.2025/18-2/13

Lo Schiavo, G. (2021). The Single Supervisory Mechanism (SSM) and the EU anti-money laundering framework: governance, rules, challenges, and opportunities. *Journal of Banking Regulation*, 1–15. https://doi.org/10.1057/S41261-021-00166-0

Malahim, S., Alrawashdeh, S. T. A., Saraireh, S., & Salameh, R. S. (2023). The relevance of the internal control system on money laundering in Jordanian Islamic and commercial banks. *International Journal of Professional Business Review, 8*(6), e02363. https://doi.org/10.26668/businessreview/2023.v8i6.2363

Manning, M., Wong, G. T. W., & Jevtovic, N. (2021). Investigating the relationships between FATF recommendation compliance, regulatory affiliations, and the Basel anti-money laundering index. *Security Journal, 34*(3), 566–588. https://doi.org/10.1057/S41284-020-00249-Z

Masabanda, M. C. Y., & Vélez, D. A. A. (2025). Modelos de control interno para la prevención del lavado de activos: una revisión sistemática de literatura en cooperativas financieras de América Latina. https://doi.org/10.65415/rcs.v3i4.22

Moes, A., & Ruesing, M. (2024). A pan-European fraud taxonomy: do you speak fraud? *Journal of Financial Compliance*. https://doi.org/10.69554/xofk3234

Mohd-Sanusi, Z., Rameli, M. N. F., Omar, N., & Ozawa, M. (2015). Governance mechanisms in the Malaysian banking sector: mitigating fraud. *Asian Journal of Criminology, 10*(3), 231–249. https://doi.org/10.1007/S11417-015-9211-4

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *PLoS Medicine, 6*(7), e1000097. https://doi.org/10.1371/journal.pmed.1000097

Money laundering: impact on financial institutions and international law – a systematic literature review. (2024). *Pakistan Journal of Criminology*. https://doi.org/10.62271/pjc.16.4.823.835

Musa, A. I. (2025). Securing the Nigerian banking industry: approaches to fraud prevention. https://doi.org/10.5281/zenodo.17417535

Neto, P. R. (2025). Fintechs, bancos digitales y criptoactivos al servicio del delito: la necesidad de regulación y cooperación internacional para combatir el lavado de activos. *ESCPOGRA PNP, 5*(1), 54–62. https://doi.org/10.59956/escpograpnpv5n1.4

Nga, N. T. T., Samphy, Shawin, & Mai (2025). Combating illicit finance in digital payment services: the role of data analytics and technology in preventing payment fraud and scams. https://doi.org/10.1142/s2811004825300054

Nyakarimi, S. N., Kariuki, S. N., & Kariuki, P. W. (2019). Moderating effect of government regulations on internal control system and fraud prevention: a case of the banking sector in Kenya. *The Journal of Social Sciences Research, 5*(12), 1900–1907. https://doi.org/10.32861/JSSR.512.1900.1907

Olalekan, O. A. (2025). Cryptocurrency and cross-border financial crime: strengthening global regulatory frameworks through international cooperation and information sharing networks. https://doi.org/10.5281/zenodo.15257256

Olaoye, K. S., Remi-Aworemi, I., Adeyemi, J. R., & Adebayo, O. N. (2023). Internal control systems as catalysts for preventing fraud in Nigerian financial institutions. https://doi.org/10.5281/zenodo.8406419

Ononiwu, M. I., Onwuzulike, O. C., & Shitu, K. (2025). Comparative analysis of customer due diligence and compliance: balancing efficiency with regulatory requirements in the banking sectors of the United States and Nigeria. https://doi.org/10.5281/zenodo.14928500

Onyekaonwu, C. B. (2025). Designing resilient anti-fraud architectures for digital financial services in sub-Saharan Africa. *International Journal of Innovative Science and Research Technology*. https://doi.org/10.38124/ijisrt/25oct1026

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., & Mulrow, C. D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ, 372*, n71. https://doi.org/10.1136/bmj.n71

Pamungkas, I. D., Oktafiyani, M., Swatyayana, P. A., Kurniawati, R., Putri, A. A., & Alfared, M. A. A. (2025). Can corporate governance structures reduce fraudulent financial reporting in the banking sector? Insights from the fraud hexagon framework. https://doi.org/10.20944/preprints202511.0241.v1

Panggabean, M. L., Panjaitan, H., & Widiarty, W. S. (2025). An integrated legal framework for digital investment fraud prevention in Indonesia. *Journal of Sustainable Development and Regulatory Issues, 3*(3), 540–567. https://doi.org/10.53955/jsderi.v3i3.154

Pinho, C. (2015). Implementation of internal control systems to combat money laundering and financing of terrorism: an applied exploratory study to the Angolan financial sector. *International Journal of Business and Social Research, 5*(7), 38–50. https://doi.org/10.18533/IJBSR.V5I7.811

Prayoga, C. J., & Sukristanta (2025). Institutionalizing internal auditing in Indonesian startups: regulatory alignment and fraud-prevention strategies. *Summa, 3*(1), 41–52. https://doi.org/10.61978/summa.v3i1.876

Raoui, A., & Leila, E. G. (2023). Gouvernance financière des banques et lutte contre la criminalité financière à l'ère du digital. https://doi.org/10.5281/zenodo.8195402

Rehman, A., & Hashim, F. (2020). Impact of fraud preventive measures on good corporate governance. *Journal of Corporate Governance Research, 4*(1). https://doi.org/10.5296/JCGR.V4I1.17490

Roide, N. A. (2022). Fintech and anti-money laundering regulation: implementing an international regulatory hierarchy premised on financial innovation. *Texas A&M Law Review, 9*(2). https://doi.org/10.37419/lr.v9.i2.5

Roy, N. C., & Prabhakaran, S. (2023). Insider employee-led cyber fraud (IECF) in Indian banks: from identification to sustainable mitigation planning. *Behavior and Information Technology*, 1–31. https://doi.org/10.1080/0144929x.2023.2191748

Salehi, M., & Molla Imeny, V. (2019). Anti-money laundering developments in Iran: Do Iranian banks have an integrated framework for money-laundering deterrence? *Qualitative Research in Financial Markets, 11*(4), 387–410. https://doi.org/10.1108/QRFM-05-2018-0063

Salihu, A. S. (2025). Re-examining the fraud hexagon through corruption deterrence by regulatory undertakings and corporate disclosures in Nigerian financial institutions. *Journal of Financial Crime*. https://doi.org/10.1108/jfc-08-2024-0262

Sarfaraz, M., Humna, H., Iqbal, Z., Younis, R., Nadeem, N., & Naveed, Z. (2025). Evaluating compliance-based crime prevention in Lahore's banks: a criminological study of KYC and AML tools against digital financial offenses. https://doi.org/10.63056/acad.004.04.0912

Shonhadji, N., & Irwandi, S. A. (2024). Fraud prevention in the Indonesian banking sector using an anti-fraud strategy. *Banks and Bank Systems, 19*(1). https://doi.org/10.21511/bbs.19(1).2024.02

Sudi, S. J., & Mwendapole, M. J. (2025). Impact of regulatory weaknesses on bill of lading fraud in Tanzanian financial institutions: evidence from CRDB Bank. *Social Science and Humanities Journal, 9*(08), 8875–8886. https://doi.org/10.18535/sshj.v9i08.1947

Suhardi, S., & Bernanthos, B. (2024). Reconstruction of the role of the financial services authority in overcoming fraud in the business sector in Indonesia. *Digital Bisnis, 3*(1), 32–38. https://doi.org/10.30640/digital.v3i1.2164

Sultan, N., Hussain, D., Mohamed, N. A., Latif, H. M., & Passas, N. (2025). Jurisdictional challenges in implementing customer due diligence in financial institutions in developing countries. *Qualitative Research in Financial Markets*. https://doi.org/10.1108/qrfm-09-2024-0282

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management, 14*(3), 207–222. https://doi.org/10.1111/1467-8551.00375

Unger, B., & van Waarden, F. (2009). Attempts to dodge drowning in data: rule- and risk-based anti-money laundering policies compared. *Review of Law and Economics*, 399–425.

Utama, A. N. B., & Purwoko, B. (2024). Corporate governance and financial transparency: a legal perspective on reducing fraud in global financial markets. *International Journal of Business, Law, and Education, 5*(2), 2838–2848. https://doi.org/10.56442/ijble.v5i2.946

Vaithilingam, S., & Nair, M. (2007). Factors affecting money laundering: lessons for developing countries. *Journal of Money Laundering Control, 10*(3), 352–366. https://doi.org/10.1108/13685200710763506

van den Broek, M. (2014). Designing supervision under the preventive anti-money laundering policy in the European Union. *Utrecht Law Review, 10*(5), 151–167. https://doi.org/10.18352/ULR.306

Wahyu, A. B., & Nasution, M. I. (2025). Systematic literature review: the influence of forensic audit and anti-fraud programs on money laundering crimes with regulatory compliance as a moderating variable. *Formosa Journal of Science and Technology, 4*(9), 2653–2662. https://doi.org/10.55927/fjst.v4i9.225

Wankhade, A. (2026). Banking frauds in India: a road map for effective regulation and prevention. *International Journal for Multidisciplinary Research, 8*(1). https://doi.org/10.36948/ijfmr.2026.v08i01.67038

Younus, M. (2021). The rising trend of fraud and forgery in Pakistan's banking industry and the precautions taken against them. *Qualitative Research in Financial Markets, 13*(2), 215–225. https://doi.org/10.1108/QRFM-03-2019-0037

Zmarialy, Y., & Harikumar, P. N. (2025). From risk to resilience: strengthening AML frameworks in banks amid emerging laundering techniques. *i-manager's Journal on Economics and Commerce, 5*(3), 26. https://doi.org/10.26634/jecom.5.3.22282