Vol. 11, No. 2, 2026, pp. 232-245
DOI: https://doi.org/10.29210/30036993000

Contents lists available at Journal ELORA

JRTI (Jurnal Riset Tindakan Indonesia)
ISSN: 2502-079X (Print) ISSN: 2503-1619 (Electronic)

Journal homepage: https://jrti.eloracenter.org/jrti



Internal control systems, risk management, and fraud prevention in indonesian regional financial management

Salomi Jacomina Hehanussa
Universitas Kristen Indonesia Maluku, Indonesia

Article Info

Article history:

Received Aug 18th, 2026
Revised Sep 25th, 2026
Accepted Oct 07th, 2026

Keyword:

Fraud prevention,
Internal control,
Local government finance,
Public-sector risk management,
Regional financial management

ABSTRACT

This study examines how internal control systems and risk management are linked to fraud prevention in Indonesian regional financial management through a qualitative integrative literature review rather than causal estimation. The revised corpus comprises 42 sources: 16 regulations, professional standards, or official reports and 26 scholarly works. Sources were purposively selected from official repositories, publisher pages, DOI records, and academic indexes using four criteria: direct relevance to the focal constructs, traceable bibliographic identity, methodological or normative authority, and contribution to mechanism explanation. Unverifiable metadata, duplicate materials, popular opinion, and statistical claims without an original source were excluded. Source-type-specific appraisal assessed provenance and scope for official materials and design transparency, construct relevance, and stated limitations for scholarly studies. A pre-specified codebook guided extraction and deductive-inductive coding, followed by cross-source triangulation, pattern matching, negative-case analysis, and explanation building. Official statistics are used only as contextual signals and are not treated as comparable fraud outcomes: Indonesia's 2024 National Integrity Index was 71.53 and remained in the vulnerable category; the Audit Board reported 491 unmodified, 53 qualified, and one disclaimer opinion for 545 local government financial statements for fiscal year 2024; and the ACFE global benchmark reported that 43% of occupational fraud cases were initially detected through tips. The synthesis indicates that internal controls restrict opportunity and improve traceability, while risk management strengthens anticipatory identification and prioritisation of fraud scenarios. These mechanisms are most credible when risk sensing is translated into controls that are actually executed, tested, and improved. The study develops the Regional Financial Risk-Control and Antifraud Integration Model (MIPRA-KD), consisting of risk sensing, risk-calibrated control response, behavioural integrity, digital traceability, and an assurance-learning loop. It provides a diagnostic typology, testable propositions, and measurable implementation indicators while explicitly limiting inference to qualitative, mechanism-based conclusions.

© 2026The Authors.
This is an open access article under the CC BY-NC-SA license
(https://creativecommons.org/licenses/by-nc-sa/4.0)

Corresponding Author:

Salomi Jacomina Hehanussa,
Universitas Kristen Indonesia Maluku,
Email: amyhehanussa@gmail.com

Introduction

Fiscal decentralization expands the authority of local governments in planning, budgeting, spending, administering, and accounting for public resources. The breadth of the transaction chain also increases points of discretion, information asymmetry, conflicts of interest, and opportunities for collusion. Fraud in this context is not limited to misrepresenting financial statements. It can take the form of fabricated procurement, package

breaking, affiliated vendors, fictitious business trips, revenue manipulation, unauthorized grant distribution, double payment, loss of assets, or misuse of system access. Therefore, fraud prevention must follow the entire APBD cycle, not just document checks at the end of the year.

Indonesia's regulatory framework has placed internal control as a management responsibility. Government Regulation Number 60 of 2008 establishes a Government Internal Control System (SPIP) through the control environment, risk assessment, control activities, information and communication, and monitoring. Government Regulation Number 12 of 2019 and Minister of Home Affairs Regulation Number 77 of 2020 regulate the process of regional financial management which must be the object of control from planning to reporting (Republik Indonesia, 2008, 2019; Kementerian Dalam Negeri RI, 2020). BPKP Regulation Number 5 of 2021 then directs the assessment of the maturity of integrated SPIP, while Presidential Regulation Number 39 of 2023 strengthens the national development risk management architecture (BPKP, 2021; Presiden Republik Indonesia, 2023).

However, the existence of regulations, risk documents, and audit opinions have not automatically proven that fraud has been prevented. The results of the 2024 Integrity Assessment Survey on 94 ministries/institutions, 37 provincial governments, 508 district/city governments, and two state-owned enterprises produced a National Integrity Index of 71.53—up 0.56 points, but still in the vulnerable category (KPK, 2025). BPK audited 545 LKPD in 2024 and gave 491 Reasonable Opinions Without Exception (WTP), 53 Reasonable With Exception (WDP), and one No Opinion (TMP)) (BPK RI, 2025a). The two statistics measure different objects. SPI is an indicator of perception/experience of integrity, while the audit opinion concludes the fairness of the presentation based on the examination criteria. Thus, the WTP opinion should not be interpreted as a fraud-free certificate.

The gap between formal compliance and substantive effectiveness is also seen in the literature. Data from a panel of 508 local governments for the period 2010–2018 showed that weaknesses in internal control were positively associated with corruption, especially weaknesses in budget, revenue, and expenditure administration (Muhtar et al., 2023). A survey of local government internal oversight apparatus found that the risk management dimension was significantly related to fraud prevention and detection (Tarjo et al., 2022). Other research confirmed the role of internal audit in strengthening control and prevention (Nadirsyah et al., 2024), but the dynamic ability of local government internal auditors still faces motivation and capacity constraints (Sumiyana et al., 2025). The evidence suggests that system design, control implementation, actor behavior, and quality assurance should be read as a single configuration.

Previous studies have commonly examined internal control, internal audit, or risk management as separate predictors of fraud-related outcomes. These studies establish important associations, but they leave an operational gap: they do not fully explain how risk registers are translated into transaction-level controls, how control exceptions are fed back into risk assessment, or why apparently complete documentation can coexist with fraud exposure. The present study therefore focuses on mechanisms and boundary conditions rather than estimating a new causal coefficient. It addresses three research questions: (1) through what mechanisms are internal control systems and risk management linked to fraud prevention in Indonesian regional financial management; (2) which organizational and behavioural conditions strengthen or weaken those mechanisms; and (3) what integrative model can connect risk sensing, control execution, assurance, and learning across the APBD cycle?

Accordingly, this study aims to examine and integrate the evidence on internal control and risk-management mechanisms associated with fraud prevention, identify the conditions under which those mechanisms are strengthened or weakened, and develop an auditable integrative framework for Indonesian provincial, regency, and municipal financial management. The contribution is theoretical, methodological, and practical. Theoretically, the study distinguishes risk-sensing capacity from control-execution reliability and treats their fit as an analytical problem. Methodologically, it triangulates peer-reviewed studies, authoritative standards, and official contextual statistics while preserving the measurement boundaries of each source. Practically, it develops MIPRA-KD, a four-condition diagnostic typology, an APBD-cycle risk-control matrix, and implementation indicators that can be operationalised in subsequent case studies or quantitative tests. Because the design is qualitative, terms such as relationship, linkage, and mechanism are used instead of causal effect estimates.

Theoretical Foundations and Development of Analytical Frameworks

Fraud as an Organizational Process

Fraud is a deliberate act to obtain unauthorized benefits through fraud, concealment, abuse of authority, or breach of trust. The fraud triangle explains that pressure, opportunity, and rationalization form the basic conditions for fraud to occur (Cressey, 1953). The fraud diamond adds to the perpetrator's ability to take advantage of opportunities (Wolfe & Hermanson, 2004), while the SCORE model expands attention to stimulus, capability, opportunity, rationalisation, and ego (Vousinas, 2019). A review of the evolution of theory

emphasizes that individual motives are not enough to explain fraud without reading the organizational processes and control environment (Dorminey et al., 2012; Free, 2015).

In regional finance, "opportunity" is shaped by process architectures: concentration of access, weak third-party verification, easily overridden controls, disconnected data, or delayed monitoring. "Capability" can be knowledge of application loopholes, the ability to build collusion, or positions that can pressure subordinates. Therefore, prevention strategies that only contain ethical socialization are inadequate; controls must reduce opportunities, increase the probability of detection, clarify consequences, and make traces of transactions difficult to remove.

Studies of financial reporting show that weak controls are related to fraud, but existing controls can also fail when management overrides or when the assurance process is too compliance-oriented (Hogan et al., 2008; Donelson et al., 2017). In the context of corruption, audit is also in a network of social, political, and institutional relations; it is not a neutral mechanism that is automatically effective (Neu et al., 2013; Jeppesen, 2019). Therefore, prevention design needs to include conflicts of interest, APIP independence, political pressure, and reporting safe spaces.

Internal Control System

COSO defines internal control as a process that is influenced by board, management, and personnel to provide adequate confidence in operations, reporting, and compliance objectives (COSO, 2013). SPIP adapts the logic of the five components to the government sector. The control environment shapes the tone at the top, accountability structure, competence, and discipline enforcement. Risk assessment identifies events that hinder objectives. Control activities translate risk into authorization, separation of functions, verification, reconciliation, asset security, and technology control. Information–communication ensures that evidence reaches decision-makers, while monitoring assesses whether components are actually functioning.

The effectiveness of internal audits is important because this function provides assurance and insight into improvement. A synthesis of literature shows that the effectiveness of internal audits is influenced by independence, competence, management support, quality of work, and relationships with the audited parties (Lenz & Hahn, 2015). However, internal auditors can shift from watchdogs to helpers or protectors of management when relational closeness erodes objectivity (Roussy, 2013). The Three Lines Model places activity managers as the first line, risk/compliance functions as the second line, and independent internal audits as the third line, but coordination should not obscure individual accountability (IIA, 2020).

Risk Management and Fraud Risk Management

Risk management is not just filling in a register, but a series of contextualization, identification, analysis, evaluation, treatment, monitoring, and risk communication (ISO, 2018). COSO ERM relates risk to governance, strategy, goal setting, performance, review, and information and reporting (COSO, 2017). The Fraud Risk Management Guide operationalizes it through antifraud policy governance, fraud risk assessment, preventive and detective control activities, investigation/corrective action processes, and overall program evaluation (COSO & ACFE, 2023).

ERM research shows that implementation is shaped by leadership support, risk function, governance quality, and organizational context (Beasley et al., 2005; Arena et al., 2010). The contingency perspective reminds us that there is no uniform configuration for the entire organization; risk systems must be adapted to complexity, technology, and environment (Woods, 2009; Mikes & Kaplan, 2015). Criticism of risk ritualization is also relevant: abundant documentation can produce the illusion of control when the risk being assessed is a risk that is easily recorded, rather than a scheme that is actually possible (Power, 2009).

In local governments, integration is needed because SPIP and risk management have slices but are not identical. Risk management starts from the objectives and threat scenarios; internal controls ensure that responses are implemented on transactions and processes. Spira and Page (2003) refer to this shift as the reinvention of internal control through risk management. The OECD's public integrity framework and INTOSAI's corruption prevention audit guidelines add to the need for coordination, a culture of integrity, participation, enforcement, and institutional learning (OECD, 2020; INTOSAI, 2019).

Table 1. Operational Definition of Main Constructs

Construct	Operational meaning	Antifraud mechanism	Qualitative indicators
Risk sensing	Ability to recognize fraud schemes, actors, process points, triggers, and risk changes before losses occur.	Reduce blind spots and prioritize resources.	Specific scenarios; red flag data; risk owners; periodic updates.

Construct	Operational meaning	Antifraud mechanism	Qualitative indicators
Control execution reliability	Consistency of control is done by the right parties, at the right time, with traceable evidence.	Reduces the chance and increases the probability of detection.	Proof of authorization; reconciliation; segregation of access; exception log; effectiveness test.
Behavioral integrity	Leadership ethics, competence, conflict of interest management, and whistleblower safety.	Suppressing rationalization, collusion, and override.	Declaration of conflict; follow-up of reports; consistent sanctions; speak-up surveys.
Assurance–learning	Independent testing and feedback from findings, near misses, complaints, and investigations.	Prevent recurrence and update risks/controls.	Risk-based audits; root cause analysis; verified follow-ups; control changes.
Fraud prevention	Decreased opportunity, increased deterrence, and cessation of deviations before losses accrue.	The result of a system configuration, not a single activity.	Red flag resolved; response time; recurrence of findings; loss/near-loss validated.

Sources: COSO (2013, 2017), ISO (2018), COSO & ACFE (2023), and IIA (2020).

Method

This research uses a qualitative integrative literature review design to synthesise theory, regulation, professional standards, institutional statistics, and empirical evidence that cannot be meaningfully pooled into a single effect estimate. Following methodological guidance on literature reviews as a research method (Snyder, 2019; Paul & Criado, 2020), the review is designed to build a transparent mechanism-based explanation rather than to calculate causal effects. The unit of synthesis is therefore an evidence statement linked to a clearly identified source, construct, context, and inference boundary.

The corpus was assembled purposively and in layers. Layer 1 contains Indonesian regulations directly governing SPIP, regional financial management, maturity assessment, and development risk management. Layer 2 contains authoritative standards or guidance issued by COSO, ISO, IIA, OECD, INTOSAI, and ACFE. Layer 3 contains peer-reviewed scholarly work on fraud theory, internal control, enterprise/fraud risk management, internal audit, corruption, and Indonesian local government. Layer 4 contains contextual statistics from KPK and BPK. The revised corpus contains 42 sources that are all used in the argument: 16 regulations, standards, or official reports and 26 scholarly works. No fixed lower publication-year limit was imposed because seminal fraud, internal-control, and risk-management sources were retained; more recent empirical evidence was prioritised where available.

Source identification used official agency repositories, publisher pages, DOI records, and academic indexes with combinations of Indonesian and English terms covering internal control/SPIP, enterprise risk management/fraud risk management, fraud prevention, corruption, internal audit/APIP, regional or local government, public finance, procurement, and Indonesia. Inclusion required (1) direct relevance to at least one focal construct, (2) verifiable bibliographic identity or official provenance, (3) sufficient methodological transparency for scholarly studies or normative authority for regulations/standards, and (4) a clear contribution to the mechanism analysis. Duplicate items, popular opinion, unverifiable metadata, and statistical claims without an identifiable original source were excluded. A single generic appraisal checklist such as MMAT or JBI was not imposed on the entire corpus because the evidence base combines statutes, standards, official statistical reports, conceptual papers, and heterogeneous empirical designs. Instead, source-type-specific appraisal was applied: official materials were assessed for issuing authority, version, scope, and definition; scholarly studies were assessed for peer-review status, design transparency, construct relevance, analytical method, and stated limitations.

Analysis proceeded through four linked stages. First, evidence was extracted into a matrix containing source type, context, design or data basis, main finding or normative requirement, relevance to the research questions, and limitations. Second, a pre-specified deductive codebook used the five COSO/SPIP components and the risk-management process, while inductive coding captured execution gaps, management override, political pressure, digital traceability, whistleblowing, and learning loops. Third, cross-source pattern matching compared whether regulatory expectations, empirical findings, and official context signals converged, diverged, or produced negative cases. Fourth, explanation building connected the sequence risk sensing → risk-calibrated control response → execution → assurance → learning and used that chain to derive the MIPRA-KD model,

diagnostic typology, propositions, and implementation indicators. Official statistics were never arithmetically combined with study estimates; they were used only as contextual signals with explicit interpretation limits.

The review is an integrative rather than exhaustive systematic review. It therefore does not report a PRISMA record count that was not generated during the original targeted search process. Procedural trustworthiness is instead supported by a source-to-claim audit trail, a documented codebook, source-type-specific appraisal, triangulation across different evidence types, explicit negative-case reasoning, and separation of fact from author inference. Coding was not independently duplicated by two documented coders; accordingly, no Cohen's kappa or other inter-coder coefficient is claimed. This limitation is reported transparently rather than replaced with an unsupported reliability statistic, and future replication should use independent double coding if a formal reliability coefficient is required.

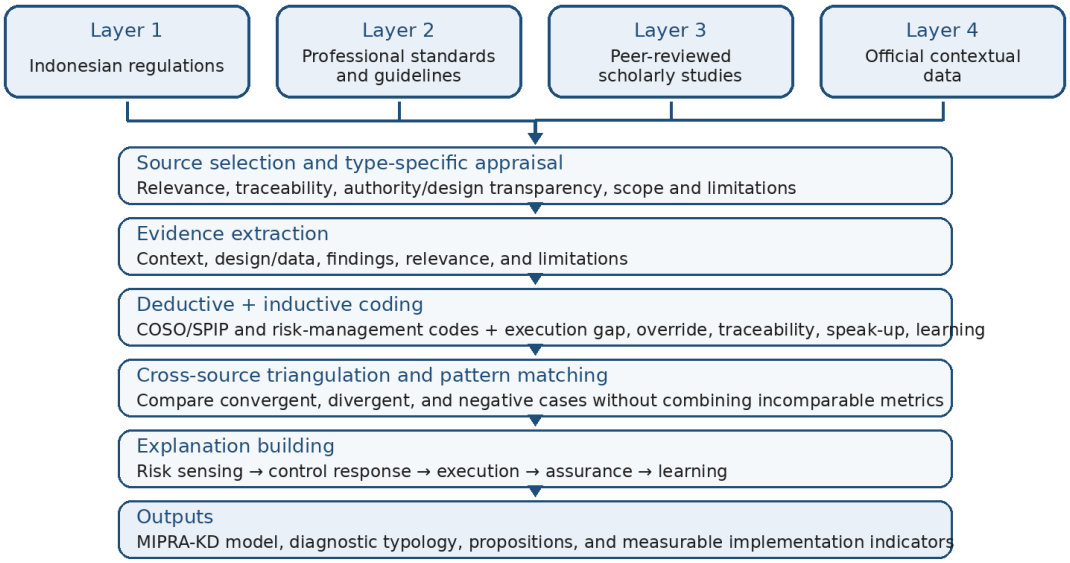

Figure 1. Integrative literature review workflow

Source: Author synthesis based on the documented review protocol.

Table 2. Integrative Literature Review and Source Auditability Protocol

Stages	Audit question	Output	Bias-control rule
Source selection	Is the source directly relevant, traceable, and appropriate for its role?	42-source corpus used in the manuscript.	Exclude duplicates, unverifiable metadata, popular opinion, and unsupported statistics.
Quality appraisal	Does the source meet criteria appropriate to its source type?	Type-specific appraisal record.	Official: authority/version/scope; scholarly: peer review, design transparency, construct relevance, method, limitations.
Extraction	What are the context, design/data basis, evidence statement, relevance, and limits?	Evidence matrix with source-to-claim traceability.	Separate source facts, source interpretation, and author inference.
Coding	Which control/risk mechanisms and boundary conditions are present?	Deductive and inductive codebook.	Apply predefined definitions; compare codes across more than one evidence type.
Synthesis	Where do sources converge, diverge, or reveal negative cases?	Pattern-matched explanations, propositions, and MIPRA-KD.	Do not combine incomparable metrics; retain contradictory/negative cases.
Reporting	Is each claim proportionate to the design and source scope?	Mechanism-based conclusions, not causal coefficients.	Explicit inference limits; no fabricated data, effect sizes, or reliability coefficients.

Table 3. Example coding and construct-mapping matrix

Source	Source type	Extracted evidence / requirement	Code and MIPRA-KD link	Inference boundary
Muhtar et al. (2023)	Panel study	Internal-control weaknesses are positively associated with corruption; budget, revenue, and expenditure weaknesses are salient.	Control execution reliability; risk-calibrated control response	Association based on secondary proxies; not a direct fraud-incidence estimate.
Tarjo et al. (2022)	Cross-sectional survey	ERM/COSO dimensions are related to fraud prevention and detection among local-government supervisory officers.	Risk sensing; risk-calibrated response	Perceptual, cross-sectional evidence; causal direction is not established.
Nadirsyah et al. (2024)	Public-sector empirical study	Internal audit supports internal control and fraud prevention.	Assurance-learning loop	Depends on audit independence and capacity; not evidence that audit alone prevents fraud.
KPK (2025)	Official survey statistic	National Integrity Index 71.53 and classified as vulnerable.	Behavioural integrity / governance context	Integrity perception/experience indicator; not fraud prevalence.
BPK RI (2025a)	Official audit statistic	491 WTP, 53 WDP, and 1 TMP across 545 LKPD for FY2024.	Assurance context; execution diagnostics	Audit opinion addresses fair presentation; it is not a fraud-free certificate.
ACFE (2024)	Global case benchmark	Tips detected 43% of studied occupational fraud cases; absence/override of controls are frequently reported factors.	Speak-up; control execution; override	Global case sample; not projected to Indonesian local-government rates.

Results and Discussions

Contextual Evidence and Analytical Integration

The synthesis uses a triangulation and pattern-matching strategy rather than numerical aggregation. Each evidence stream has a distinct analytical role: regulations and standards define expected control/risk architecture; peer-reviewed studies provide empirical or conceptual evidence about mechanisms and boundary conditions; KPK and BPK statistics provide Indonesian governance and assurance context; and ACFE data provide a global fraud-detection benchmark. Convergence is inferred only when different source types point to the same mechanism, while divergence is retained as a negative or boundary case. Construct validity is addressed by mapping every contextual indicator to a specific MIPRA-KD component and by stating what the indicator cannot establish.

No effect sizes or confidence intervals are calculated from Table 3 because the underlying datasets have different units of analysis, populations, purposes, and measurement models, and the manuscript does not reanalyse their microdata. Likewise, measurement uncertainty is not numerically propagated across sources because no cross-dataset arithmetic is performed. Instead, uncertainty is handled through explicit scope statements and inference boundaries for each source. This prevents integrity scores, audit opinions, audit findings, and global case statistics from being transformed into a synthetic fraud rate that the evidence cannot support. Table 4 presents the contextual indicators used in this triangulation and keeps their units of analysis separate. The indicators are not treated as substitute measures of a single latent fraud construct. Instead, each is interpreted only within its source-defined scope and is subsequently mapped to the part of the analytical framework for which it provides contextual evidence.

Table 4. Validated Context Data Matrix

Source	Scope	Validated data	Interpretation limits	Ref.
KPK—SPI 2024	94 ministries/agencies; 37 provinces; 508 regencies/cities; 2 state-owned enterprises	National Integrity Index 71.53; up 0.56 points from the previous year; still in the vulnerable category.	Integrity indicators based on surveys; not the prevalence or number of fraud incidents.	KPK (2025)
BPK—IHPS I 2025	545 local-government financial statements (FY2024)	491 WTP; 53 WDP; 1 TMP. WTP proportion: province 82%; district 89.6%; city 96%.	The opinion concludes the fairness of the report; WTP does not prove the absence of fraud.	BPK RI (2025a)
BPK—IHPS II 2024	511 audit reports: 16 financial, 227 performance, 268 specific-purpose; 329 related to local governments/region-owned enterprises	The reported national financial impact was IDR 43.43 trillion; IDR 1.00 trillion was paid/followed up during the audit.	The value covers the scope of the national audit, not just the local government and is not a fraud estimate.	BPK RI (2025b)
ACFE—RTTN 2024	1,921 occupational-fraud cases in 138 countries/territories	Median loss of US$145,000; total >US$3.1 billion; tips 43%; internal audit 14%; management review 13%; external audit 3%.	The global benchmark is based on the case studied; it should not be projected into Indonesian figures.	ACFE (2024)
ACFE—control factors	Cases in RTTN 2024	Absence of internal control 32%; override of existing control 19% as the main factor.	Category of causes based on ACFE cases; shows the relevance of control, not the effect size of the local government.	ACFE (2024)

Table 5. Construct linkage and inference boundaries for contextual indicators

Context indicator	Primary construct link	Analytical use	Prohibited inference
KPK SPI 2024	Behavioural integrity / governance environment	Signals perceived/experienced integrity vulnerability that may condition control execution.	Not a count or prevalence rate of fraud.
BPK IHPS I 2025 audit opinions	Assurance and reporting context	Shows the reporting-assurance environment in which antifraud controls operate.	WTP does not establish absence of fraud or effective antifraud controls.
BPK IHPS II 2024 findings	Control execution / assurance-learning	Signals control, compliance, and follow-up issues requiring diagnostic attention.	National financial impact is not a local-government fraud estimate.
ACFE RTTN 2024 detection channels	Speak-up / monitoring / assurance	Supports the importance of reporting channels and monitoring as detection mechanisms.	Global case percentages are not Indonesian regional-government effect sizes.
ACFE control factors	Control execution / management override	Illustrates why formal controls must be executed and protected from override.	Case categories do not quantify the causal effect of SPIP maturity.

Two implications emerge. First, the vulnerability of integrity scores coexists with a high proportion of WTPs. This is not a contradiction, but rather a consequence of different constructs. Audit opinions provide adequate confidence in the fairness of reports based on audit materiality and evidence, while integrity surveys capture experiences/perceptions of governance vulnerabilities. Second, the dominance of tips as a global detection channel confirms the importance of safe and responsive whistleblowing, but its design must be adapted to the laws, structures, and cultures of regional organizations.

Research Synthesis Matrix

Table 6. Research Synthesis Matrix

Studies	Design/context	Relevant findings	Position in synthesis & limits
Tarjo et al. (2022)	Survey of 151 local government supervisory officers	ERM/COSO dimensions were reported as significantly associated with fraud prevention and detection.	Supports risk sensing and response; cross-sectional perception limits causality.
Muhtar et al. (2023)	508 local governments, 2010–2018; 4,530 observations	Weaknesses in internal control are positively associated with corruption; weaknesses in budget/revenue/expenditure administration stand out.	Panel evidence is strong; proxies of findings and corruption remain dependent on secondary data.
Nadirsyah et al. (2024)	Indonesian public sector; internal control and audit model	Internal audit is reported as supporting stronger internal control and fraud-prevention capacity.	Supports the assurance layer; reported relationships depend on independence and capacity.
Tarjo et al. (2024)	151 Indonesian local-government respondents	Fraud risk management was negatively associated with asset misuse; ethical leadership, religiosity, and local wisdom strengthened the reported relationship.	Shows that formal controls operate within a behavioural-integrity context.
Sumiyana et al. (2025)	Internal auditor of the Indonesian local government; dynamic capability study	Low motivation can constrain the development of dynamic capabilities among Indonesian local-government internal auditors.	Identifies an execution gap in assurance and highlights organizational context.
Safkaur et al. (2025)	111 respondents; SEM-PLS of the Indonesian local government	FRM, organizational culture, and political pressure moderate the governance–financial performance relationship.	Political pressure becomes a boundary condition; focus on performance outcomes, not fraud incidents.
Zahra et al. (2021)	E-purchasing of Indonesian local governments	Procurement fraud prevention requires competence, control, and electronic process design.	Digitization helps traceability but does not eliminate collusion/override.
Donelson et al. (2017)	Company; archival	Internal-control weaknesses are associated with financial-reporting fraud.	Supports the opportunity mechanism; transfer to local-government settings requires caution.
Lenz & Hahn (2015)	Synthesis of internal audit effectiveness studies	Independence, competence, support, and quality of work determine effectiveness.	Explain why the existence of APIP alone is not enough.
Roussy (2013)	Qualitative study of the role of internal auditors	Auditors can act as watchdogs, helpers, or management protectors.	Highlights role-capture risk and the need for safeguards that preserve independence.
Woods (2009)	Birmingham City Council; contingency studies	The risk-control system is shaped by organizational and environmental context.	Supports contingent designs that vary with regional capacity and complexity.
Arena et al. (2010)	Study of ERM organizational dynamics	ERM is shaped by interactions among actors, artefacts, and organizational practices.	Rejects treatment of the risk register as a stand-alone system.
Power (2009)	Critical analysis of risk management	Risk-management ritualisation can shift attention toward risks that are easier to manage symbolically.	Conceptual basis for the compliance-illusion diagnosis.
Jeppesen (2019)	Review of the role of audit against corruption	Audit contributions depend on mandate, capacity, and connection with prevention and enforcement.	Supports the assurance-learning loop and coordination.
Neu et al. (2013)	Analysis of corruption networks	Accounting/auditing practices operate within a network of power and relationships.	Explains why transaction controls can fail in the face of collusion.

Internal Control Mechanisms Linked to Fraud Prevention

The literature links internal controls to fraud prevention through three principal mechanisms. The first path is opportunity restriction. The separation of functions between initiators, verifiers, signatory officials, consignees, and payers reduces a single person's ability to complete fictitious transactions. Tiered authorizations, account/vendor verification, bank reconciliation, stock taking, and access rights restrictions magnify the efforts required to commit fraud and leave evidence. The second path is deterrence: perpetrators take into account the probability of detection and consequences when exception logs are monitored, real employer reviews, and consistent sanctions. The third path is information: controls generate data about irregularities that can lead to audits, investigations, or process improvements.

The five components of SPIP must work as a system. A control environment without verification activities generates only a statement of value; a control activity without information results in a checklist that is not associated with the pattern; monitoring without corrective action results in repetitive findings. Muhtar et al.'s (2023) findings on the weaknesses of budget, receipt, and expenditure administration reinforce the importance of control points in the transactional process. However, Donelson et al. (2017) and Hogan et al. (2008) caution that control design does not close all opportunities, especially when there is collusion and override.

Therefore, the measure of quality should not stop at the existence of SOPs. Execution reliability requires proof of time, execution, exceptions, exception resolution, and retesting. For example, "reconciliation is done monthly" is not enough; the quality is determined whether the discrepancy is resolved, who reviews, how long the discrepancy is alive, and whether high-risk accounts are examined more deeply. The same logic applies to e-procurement: digitization increases traceability, but affiliated vendors, directed specifications, or shared accounts can still generate fraud if identity controls and analytics are weak (Zahra et al., 2021).

Risk-Management Mechanisms Linked to Fraud Prevention

Risk management provides a prospective orientation. Local governments start from the goal—for example, obtaining goods of the right quality and price—then build a fraud scenario, identify perpetrators/parties who may collude, map red flags, assess inherent risks, and choose a response. Thus, control is not chosen because of habit, but because it is suitable for the scheme. The risk of package breaking, for example, requires value/time/user pattern analysis, not just checking the completeness of each package's documents.

Fraud risk assessment is different from generic risk registers. Statements such as "ineffective procurement risk" are too broad and do not indicate a mode, trigger, or control. Actionable statements call a scheme: "officials and vendors collude to break down similar needs to be below the limits of a certain method"; red flags can be the same vendor, narrow time intervals, near-threshold values, or similar accounts/addresses. The risk owner must then have the authority and deadline to respond.

Indonesian evidence is consistent with this pathway. Tarjo et al. (2022) report a relationship between the risk-management dimension and fraud prevention/detection, while Tarjo et al. (2024) report that fraud-risk management is negatively associated with asset misuse and that the relationship varies with ethical leadership, religiosity, and local wisdom. Safkaur et al. (2025) identify political and organizational-cultural pressure as an important boundary condition. Taken together, these findings are consistent with a contingency view: similar risk-management structures can be associated with different outcomes because behaviour, power, and implementation capacity differ across settings.

The weakness is formalization. The risk register can be filled out after the activity, using redacted uniforms between agencies, or not updated when the process changes. In these conditions, risk becomes an artifact of compliance (Power, 2009), not a decision input. Prevention only occurs when the results of the risk assessment change the allocation of audits, access design, transaction approvals, analytical parameters, APIP audit plans, or decisions to deny/stop activities.

Complementarity in the Regional Financial Cycle

Table 7. Complementarity in the Regional Financial Cycle

Stages	Priority fraud schemes	Risk sensing	Response control	Assurance/ learning
Planning & budgeting	Deposit program; target/volume manipulated; conflict of interest	Intervention scenarios; conflict disclosure; ceiling change analysis; rationality review	Traces of proposals–changes; different proposers/approvers; documented reasons	APIP assesses changes in risk and concentration of benefits
Revenue	Under-assessment; invalid write-off/receivables; unpaid receipts	Payroll segmentation; tariff anomalies; cash risk and master data access	Source–bank–ledger reconciliation; change log audit; third-party confirmation	Potential-realization gap analytics and user override
Procurement	Specification directed; bid rigging; package breakdown; affiliate vendor	Schema/vendor mapping; network red flags; pre-tender–contract stage risk	Segregation; Beneficial Ownership Verification; e-catalog/log; Admission Inspection	Thematic audits are pattern-based, not just random samples

Stages	Priority fraud schemes	Risk sensing	Response control	Assurance/ learning
Shopping & Payment	Fictitious/double bills; mark-ups; fictitious business trips	Duplication scenarios; Mapping of risky accounts/offices/vendors	Three-way match; account validation; duplicate check; proof of location/results	Exception ageing and recovery validated
Grants/social assistance	Unqualified/fictitious recipients; political intervention; deviant use	Eligibility risks and affiliate relationships; Recipient scoring	Identity verification; recipient publication; proof of distribution/use; complaint channel	Risk-based field tests and complaint follow-up
Assets	Removal; personal utilization; grade/status not updated	Map of vulnerable assets and status changes	Labels/geotags; stock taking; mutation approvals; reconciliation with balance sheets	Analysis of idle/missing assets and root cause
Reporting	Journal manipulation; concealment; management override	End-of-term manual journal risk and suspense account	Limited journal access; independent review; continuous monitoring	Journal testing, late adjustment, and recurring findings

The matrix shows that risk management determines "what can happen and where", while internal controls determine "who did what, when, and what evidence remains". APIP then tests whether the two logics are coherent. When the risk register mentions an affiliated vendor but the control only checks the completeness of the documents, there is a control mismatch. When the controls are correct but never implemented or exceptions are not resolved, there is an execution gap. These two diagnoses are more useful than simply stating a high/low maturity value.

Novelty: Integrated Model of Risk Control and Regional Financial Antifraud (MIPRA-KD)

The conceptual novelty of this research is MIPRA-KD. This model does not combine SPIP and risk management administratively, but rather connects preventive mechanisms in a traceable order. The starting point is the service/financial goals of the region; the end point is not the number of documents, but the reduction of fraud exposure, faster response, and reduced recurrence of weaknesses. The model consists of five layers that give each other feedback.

Table 8. MIPRA-KD Architecture

MIPRA-KD layer	Mechanism	Minimum artifacts/evidence	Prevented failures
Risk sensing	Specific fraud scenarios; red flags; process changes; risk owners	Process-level fraud-risk register; map of discretion/collusion points	Blind spots and unidentified inherent risks
Calibrated control response	Preventive, detective, corrective controls are selected according to the scheme	Risk–control matrix; control owner; frequency; evidence	Generic controls or controls that do not address the identified scheme
Behavioral integrity	Ethical leadership; competence; conflict of interest; speak-up	Declaration/recusal; scenario-based training; whistleblower protection	Collusion, rationalisation, override, and silence
Digital traceability	Identity, access segregation, immutable logs, data integration, analytics	Exception dashboard; vendor/entity matching; log review	Shared accounts, data silos, trackless changes
Assurance–learning loop	Risk-based audits; root-cause; follow-up; near-miss learning	Responsive audit plan; verification of improvements; risk/control updates	Recurring findings and ceremonial follow-up

From the model, two diagnostic axes are derived: the quality of risk sensing and the reliability of the control execution. High quality means that the scenario is specific, dynamic, data-driven, and connected to the risk owner. High execution means that control is precisely designed, done consistently, leaves evidence, exceptions

are resolved, and its effectiveness is tested. The intersection of the two axes results in four conditions that explain why organizations with the same document can have different vulnerabilities.

Table 9. Matrix Diagnostics MIPRA-KD

Risk sensing	Control execution	Type	Diagnosis	Intervention priorities
Low	Low	Exposed–reactive	Illegible risk and weak control; the organization responds after the case/finding.	Build priority scenarios and minimum viable controls.
Low	High	Compliance illusion	Routine controls are executed, but not directed at changing schemas; checklists can be complete but blind spots are large.	Redesign fraud-risk assessment; test control-risk fit.
High	Low	Analytical but unenforced	Risk is understood, but the response is not implemented, not supported by capacity, or is overridden.	Clarify owners, resources, escalations, and consequences.
High	High	Adaptive prevention	Risk signals are translated into control, monitored, and updated through learning.	Maintain continuous monitoring and independent challenge.

MIPRA-KD expands the literature in four ways. First, the model separates risk reading capacity from control execution capacity, while some studies treat both as aggregate constructs. Second, the model adds control–risk fit and execution fidelity as intermediate mechanisms. Third, the model places behavioral integrity and political pressure as boundary conditions, in line with Tarjo et al. (2024) and Safkaur et al. (2025). Fourth, the model closes the cycle with an assurance–learning loop; findings, complaints, investigations, and near misses should update the risk register and control design, not stop at administrative completion.

Research Proposition

Because research is qualitative-conceptual, the right output is a testable proposition, not a hypothesis that is claimed to have been proven. The following six propositions maintain the chain of MIPRA-KD mechanisms: P1. Higher internal-control execution reliability is expected to be associated with stronger fraud prevention when control activities reduce opportunities and increase detection at high-risk process points; P2. Higher-quality fraud-risk sensing is expected to be associated with stronger fraud prevention when risk assessments specify schemes, red flags, risk owners, and responses that change operational decisions; P3. Risk-control fit is proposed as an explanatory link between risk management and fraud prevention; risk sensing without a corresponding control response should not produce substantive protection; P4. Control-execution reliability is proposed as an explanatory link between SPIP design and fraud prevention; documented controls that are not executed may produce a compliance illusion rather than substantive protection; P5. Ethical leadership, APIP competence, whistleblower protection, and conflict-of-interest management are expected to strengthen the risk-control configuration, whereas political pressure, collusion, and management override are expected to weaken it; and P6. Stronger assurance-learning loops are expected to be associated with lower recurrence when findings and near misses lead to root-cause analysis, control correction, follow-up verification, and risk-profile updates.

Policy Implications and Implementation Agenda

For regional heads and regional secretaries, the main implication is to change the success indicator from the number of documents to the quality of decisions and execution. The tone at the top needs to be seen in the decision to reject conflicts of interest, protect whistleblowers, provide control resources, and crack down on overrides. For regional apparatus, risk registers should be prepared per fraud process and scheme, not copying generic risks. For risk management units/inspectorates, evaluation needs to test the relationship between objectives–risk–control–evidence–results.

APIP must maintain a combination of assurance and advisory. Advisory can help design the risk-control matrix, but assurance of the effectiveness of control must be done objectively. The role capture risk described by Roussy (2013) requires direct access to the supervisory leadership/committee, controlled rotation of assignments, conflict disclosure, and quality assurance. The capability gap found by Sumiyana et al. (2025) directs investment in data analytics, investigation, business processes, information technology, and communication of findings.

Digital transformation must be judged from traceability, not just a form migration to an application. Access rights need to be role-based and least privilege principles; shared accounts are deleted; changes to master data/vendors require approval and logs; procurement, payment, population, tax, and asset data can be matched

legally and proportionally. Red flags should not be automatically considered fraud. They are signals for triage, verification, and documentation of decisions, so that analytics do not turn into accusations without due process.

Table 10. MIPRA-KD implementation roadmap and indicators

Horizon	Priority actions	Minimum output	Indicators that are not easy to manipulate
0–3 months	Choose 3–5 risky processes; form a cross-functional team; define scenarios and risk appetite/tolerance.	Process maps; schema catalogs; owners; control baseline	Scenario coverage; percentage of risk with owner and response
3–6 months	Build a risk–control matrix; close a shared account; set exception workflows; strengthen WBS.	Preventive/detective controls; SLA response; secure channels	Control-design gap; triage time; proportion of reports handled according to SLAs
3–6 months	Integrate data; build a red-flag dashboard; conduct thematic audits; perform root-cause analysis of recurring findings.	Exception dashboard; audit trail; corrective action plan	Exception ageing; recurring findings; verified follow-up
12–24 months	Validate operating performance; expand across the APBD cycle; use peer benchmarking; update continuously.	Operating-effectiveness testing; MIPRA-KD maturity model	Control failure rate; recurrence; validated near-loss/loss; remediation cycle time

Interpretation Limits of Advanced Research Agenda

This article has five limitations. First, the purposive integrative review does not guarantee that every relevant publication was captured. Second, primary studies use different proxies, samples, designs, and periods, so their reported relationships should not be interpreted as directly comparable effect sizes. Third, official KPK, BPK, and ACFE indicators have different units of analysis and are used only as contextual signals, not as a synthetic fraud measure. Fourth, coding was not independently duplicated by two documented coders, so no inter-coder reliability coefficient is reported; reproducibility instead relies on the disclosed codebook, source-to-claim audit trail, construct mapping, and negative-case logic. Fifth, MIPRA-KD is a conceptual synthesis and has not yet been validated as a measurement instrument across provinces, regencies, and cities. These limitations constrain statistical generalisation but do not prevent the model from serving as a transparent framework for subsequent empirical testing.

The next research can develop the MIPRA-KD instrument through Delphi with BPKP, BPK, KPK, APIP, financial managers, and academics; conduct multiple-case studies in provinces, districts, and cities; then test the model using longitudinal data. The outcome variables should not only be self-reported fraud prevention, but also triangulation of exception resolution, repeated findings, follow-up time, WBS quality, validated loss/near-loss, and control design changes. Quasi-experiment can be used when red flag or segregation-of-access dashboards are implemented gradually, while maintaining ethics, confidentiality, and non-stigmatization.

Conclusions

This integrative review concludes that internal control systems and risk management are linked to fraud prevention through distinct but interdependent mechanisms. Internal controls restrict opportunities, increase traceability, and generate evidence through segregation of duties, authorisation, reconciliation, access controls, exception monitoring, and follow-up. Risk management contributes an anticipatory function by specifying fraud scenarios, identifying red flags and risk owners, and directing control resources toward the most material process points. The synthesis therefore supports a configuration view: risk sensing without an appropriate response leaves exposure untreated, while formally designed controls that are not executed create a compliance illusion. MIPRA-KD organises this configuration into five layers—risk sensing, risk-calibrated control response, behavioural integrity, digital traceability, and the assurance-learning loop—and distinguishes four diagnostic conditions based on the quality of risk sensing and control execution. The model should not be interpreted as a causal estimate. Instead, it provides propositions and operational indicators for future testing. Two immediately measurable indicators are: (1) fraud-scenario coverage, defined as the proportion of designated high-risk APBD processes with a documented scheme, red flags, a named risk owner, and an approved response; and (2) control-execution reliability, defined as the proportion of scheduled key controls completed on time with traceable evidence and documented closure of exceptions. Additional indicators can include median exception-resolution time and recurrence of previously corrected findings. For practice, regional governments should evaluate whether risk assessments alter control design and whether controls operate reliably, rather than relying on the

volume of SOPs, risk registers, or audit-opinion status. APIP can use the model to focus assurance on control-risk mismatches, unresolved exceptions, override, and recurring findings. The conclusions remain bounded by the purposive review design, heterogeneity of the evidence base, non-comparability of contextual statistics, and absence of independent double coding. Future research should validate the MIPRA-KD indicators through Delphi review, multiple-case studies, and quantitative testing using comparable regional-government data before stronger causal or generalisability claims are made.

References

Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of enterprise risk management. Accounting, Organizations and Society, 35(7), 659–675. https://doi.org/10.1016/j.aos.2010.07.003

Association of Certified Fraud Examiners. (2024). Occupational fraud 2024: A report to the nations. ACFE. https://www.acfe.com/fraud-resources/report-to-the-nations

Badan Pemeriksa Keuangan Republik Indonesia. (2025a). Ikhtisar Hasil Pemeriksaan Semester I Tahun 2025. BPK RI. https://www.bpk.go.id/ihps

Badan Pemeriksa Keuangan Republik Indonesia. (2025b). BPK sampaikan LHP atas LKPP Tahun 2024 dan IHPS II Tahun 2024 kepada DPD RI. https://www.bpk.go.id/news/bpk-sampaikan-lhp-atas-lkpp-tahun-2024-dan-ihps-ii-tahun-2024-kepada-dpd-ri

Badan Pengawasan Keuangan dan Pembangunan. (2021). Peraturan BPKP Nomor 5 Tahun 2021 tentang Penilaian Maturitas Penyelenggaraan Sistem Pengendalian Intern Pemerintah Terintegrasi pada Kementerian/Lembaga/Pemerintah Daerah. BPKP.

Beasley, M. S., Clune, R., & Hermanson, D. R. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. Journal of Accounting and Public Policy, 24(6), 521–531. https://doi.org/10.1016/j.jaccpubpol.2005.10.001

Committee of Sponsoring Organizations of the Treadway Commission, & Association of Certified Fraud Examiners. (2023). Fraud risk management guide (2nd ed.). COSO/ACFE.

Committee of Sponsoring Organizations of the Treadway Commission. (2013). Internal control—Integrated framework. COSO.

Committee of Sponsoring Organizations of the Treadway Commission. (2017). Enterprise risk management—Integrating with strategy and performance. COSO.

Cressey, D. R. (1953). Other people's money: A study in the social psychology of embezzlement. Free Press.

Donelson, D. C., Ege, M. S., & McInnis, J. M. (2017). Internal control weaknesses and financial reporting fraud. Auditing: A Journal of Practice & Theory, 36(3), 45–69. https://doi.org/10.2308/ajpt-51608

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. https://doi.org/10.2308/iace-50131

Free, C. (2015). Looking through the fraud triangle: A review and call for new directions. Meditari Accountancy Research, 23(2), 175–196. https://doi.org/10.1108/MEDAR-02-2015-0009

Hogan, C. E., Rezaee, Z., Riley, R. A., Jr., & Velury, U. K. (2008). Financial statement fraud: Insights from the academic literature. Auditing: A Journal of Practice & Theory, 27(2), 231–252. https://doi.org/10.2308/aud.2008.27.2.231

Institute of Internal Auditors. (2020). The IIA's three lines model: An update of the three lines of defense. IIA.

International Organization for Standardization. (2018). ISO 31000:2018 risk management—Guidelines. ISO.

International Organization of Supreme Audit Institutions. (2019). GUID 5270: Guideline for the audit of corruption prevention. INTOSAI.

Jeppesen, K. K. (2019). The role of auditing in the fight against corruption. The British Accounting Review, 51(5), 100798. https://doi.org/10.1016/j.bar.2018.06.001

Kementerian Dalam Negeri Republik Indonesia. (2020). Peraturan Menteri Dalam Negeri Nomor 77 Tahun 2020 tentang Pedoman Teknis Pengelolaan Keuangan Daerah.

Komisi Pemberantasan Korupsi. (2025). KPK rilis hasil SPI 2024: Skor indeks meningkat, namun masih di kategori rentan. https://kpk.go.id/id/ruang-informasi/berita/kpk-rilis-hasil-spi-2024-skor-indeks-meningkat-namun-masih-di-kategori-rentan

Lenz, R., & Hahn, U. (2015). A synthesis of empirical internal audit effectiveness literature pointing to new research opportunities. Managerial Auditing Journal, 30(1), 5–33. https://doi.org/10.1108/MAJ-08-2014-1072

Mikes, A., & Kaplan, R. S. (2015). When one size doesn't fit all: Evolving directions in the research and practice of enterprise risk management. Journal of Applied Corporate Finance, 27(1), 37–40. https://doi.org/10.1111/jacf.12102

Muhtar, M., Winarna, J., & Sutaryo, S. (2023). Internal control weakness and corruption: Empirical evidence from Indonesian local governments. International Journal of Professional Business Review, 8(6), e01278. https://doi.org/10.26668/businessreview/2023.v8i6.1278

Nadirsyah, N., Indriani, M., & Mulyany, R. (2024). Enhancing fraud prevention and internal control: The key role of internal audit in public sector governance. Cogent Business & Management, 11(1), 2382389. https://doi.org/10.1080/23311975.2024.2382389

Neu, D., Everett, J., Rahaman, A. S., & Martinez, D. (2013). Accounting and networks of corruption. Accounting, Organizations and Society, 38(6–7), 505–524. https://doi.org/10.1016/j.aos.2012.01.003

Organisation for Economic Co-operation and Development. (2020). OECD public integrity handbook. OECD Publishing. https://doi.org/10.1787/ac8ed8e8-en

Paul, J., & Criado, A. R. (2020). The art of writing literature review: What do we know and what do we need to know? International Business Review, 29(4), 101717. https://doi.org/10.1016/j.ibusrev.2020.101717

Power, M. (2009). The risk management of nothing. Accounting, Organizations and Society, 34(6–7), 849–855. https://doi.org/10.1016/j.aos.2009.06.001

Presiden Republik Indonesia. (2023). Peraturan Presiden Nomor 39 Tahun 2023 tentang Manajemen Risiko Pembangunan Nasional.

Republik Indonesia. (2008). Peraturan Pemerintah Nomor 60 Tahun 2008 tentang Sistem Pengendalian Intern Pemerintah.

Republik Indonesia. (2019). Peraturan Pemerintah Nomor 12 Tahun 2019 tentang Pengelolaan Keuangan Daerah.

Roussy, M. (2013). Internal auditors' roles: From watchdogs to helpers and protectors of the top manager. Critical Perspectives on Accounting, 24(7–8), 550–571. https://doi.org/10.1016/j.cpa.2013.08.004

Safkaur, O., Hanasbey, L., & Sakti, E. (2025). The role of political pressure, fraud risk management and organizational culture in moderating public governance on Indonesian local government financial performance. Pacific Accounting Review, 37(3), 455–476. https://doi.org/10.1108/PAR-08-2024-0183

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Spira, L. F., & Page, M. (2003). Risk management: The reinvention of internal control and the changing role of internal audit. Accounting, Auditing & Accountability Journal, 16(4), 640–661. https://doi.org/10.1108/09513570310492335

Sumiyana, S., Susanto, E. A., Rahajeng, D. K., & Winardi, R. D. (2025). Indonesia's local government internal auditors (LGIAs): Reflecting on low motivation in enhancing their dynamic capabilities while being the spearhead of responsible auditing. Journal of Accounting & Organizational Change, 21(1), 24–47. https://doi.org/10.1108/JAOC-10-2022-0159

Tarjo, T., Anggono, A., Alim, M. N., Said, J., & Mohd-Sanusi, Z. (2024). Religiosity, ethical leadership and local wisdom in moderating the effect of fraud risk management on asset misappropriation: Evidence from local government in Indonesia. Journal of Islamic Accounting and Business Research. Advance online publication. https://doi.org/10.1108/JIABR-09-2022-0227

Tarjo, T., Vidyantha, H. V., Anggono, A., Yuliana, R., & Musyarofah, S. (2022). The effect of enterprise risk management on prevention and detection fraud in Indonesia's local government. Cogent Economics & Finance, 10(1), 2101222. https://doi.org/10.1080/23322039.2022.2101222

Vousinas, G. L. (2019). Advancing theory of fraud: The S.C.O.R.E. model. Journal of Financial Crime, 26(1), 372–381. https://doi.org/10.1108/JFC-12-2017-0128

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

Woods, M. (2009). A contingency theory perspective on the risk management control system within Birmingham City Council. Management Accounting Research, 20(1), 69–81. https://doi.org/10.1016/j.mar.2008.10.003

Zahra, F., Abdullah, M. I., Kahar, A., Din, M., & Nurfalah, N. (2021). Preventing procurement fraud in e-purchasing for Indonesian local governments. The Journal of Asian Finance, Economics and Business, 8(2), 505–511. https://doi.org/10.13106/jafeb.2021.vol8.no2.0505