

Review Article

# Risk-Based Internal Audit for the Oversight of Village Funds in Remote Areas

(A Literature Review on Risk Mapping, Early Warning, and Fraud Prevention)

Edizon Mirino <sup>1</sup>, Dian Ferriswara <sup>2\*</sup>, Fedianty Augustinah <sup>3</sup>, Sri Kamariyah <sup>4</sup>

<sup>1</sup> Prodi Ilmu Administrasi Jenjang S2, Fakultas Ilmu Administrasi, Universitas Dr. Soetomo Surabaya, Indonesia: [mirinoedison@gmail.com](mailto:mirinoedison@gmail.com)

<sup>2</sup> Prodi Ilmu Administrasi Jenjang S2, Fakultas Ilmu Administrasi, Universitas Dr. Soetomo Surabaya, Indonesia: [dianferriswara@unitomo.ac.id](mailto:dianferriswara@unitomo.ac.id)

<sup>3</sup> Prodi Ilmu Administrasi Jenjang S2, Fakultas Ilmu Administrasi, Universitas Dr. Soetomo Surabaya, Indonesia: [fedianty.augustinah@unitomo.ac.id](mailto:fedianty.augustinah@unitomo.ac.id)

<sup>4</sup> Prodi Ilmu Administrasi Jenjang S2, Fakultas Ilmu Administrasi, Universitas Dr. Soetomo Surabaya, Indonesia: [sri.kamariyah@unitomo.ac.id](mailto:sri.kamariyah@unitomo.ac.id)

\* Corresponding Author: Dian Ferriswara

**Abstract:** The governance of village funds represents a critical dimension of decentralized public financial management, particularly in remote and capacity-constrained regions where oversight mechanisms face structural limitations. This literature review examines the role of Risk-Based Internal Audit (RBIA) as a strategic instrument for strengthening the supervision of village fund management through risk mapping, early warning mechanisms, and fraud prevention. Adopting a state-of-the-art literature review design, the study synthesizes peer-reviewed journal articles, conference proceedings, and authoritative institutional reports published primarily within the last five years. The review integrates the analytical lenses of RBIA as articulated in the International Professional Practices Framework, Enterprise Risk Management (ERM) based on ISO 31000 and COSO ERM, the COSO Internal Control–Integrated Framework, and the Fraud Triangle and Fraud Diamond theories. Thematic synthesis reveals that effective village fund oversight depends on the systematic identification and prioritization of risk, the alignment of audit planning with high-risk areas, and the integration of internal control and risk management processes into audit assurance. Furthermore, the literature highlights the growing relevance of early warning systems and audit analytics in enabling proactive detection of emerging risks and potential fraud, although their implementation in remote areas remains constrained by limited data quality, digital infrastructure, and administrative capacity. This review contributes theoretically by consolidating fragmented strands of audit, risk management, and fraud literature into an integrated conceptual framework tailored to village fund governance. Practically, it offers evidence-based insights for auditors, policymakers, and local governments seeking to enhance accountability and risk-responsive oversight in decentralized and remote public finance settings.

**Keywords:** Early Warning System; Enterprise Risk Management; Internal Control System; Risk-Based Internal Audit; Village Fund Governance.

## 1. Introduction

The governance of village funds has become a central pillar of fiscal decentralization and inclusive development policies in many developing countries, including Indonesia, where substantial public resources are transferred to village governments to stimulate local development and reduce territorial disparities. Despite its strategic importance, the management and oversight of village funds—particularly in remote and geographically isolated areas—remain vulnerable to governance failures, misuse of funds, and fraud. Structural challenges such as limited administrative capacity, weak internal control systems, inadequate human resources, and restricted access to oversight institutions exacerbate these risks in peripheral regions. Empirical studies consistently indicate that remoteness amplifies

Received: July 23, 2025

Revised: September 23, 2025

Accepted: November 18, 2025

Online Available: January 19, 2026

Curr. Ver.: January 19, 2026



Copyright: © 2025 by the authors.

Submitted for possible open

access publication under the

terms and conditions of the

Creative Commons Attribution

(CC BY SA) license

(<https://creativecommons.org/licenses/by-sa/4.0/>)

information asymmetry, weakens accountability mechanisms, and constrains effective monitoring, thereby increasing exposure to financial irregularities (Ginting et al., 2023; Putra et al., 2024). Within this context, conventional compliance-oriented oversight mechanisms often prove insufficient to detect emerging risks or prevent fraud proactively. Consequently, there is growing recognition that village fund governance in remote areas requires a more adaptive, risk-oriented, and analytically robust oversight approach that aligns audit practices with the actual risk profile of decentralized public financial management systems.

A substantial body of literature has examined public sector auditing, village fund oversight, and fraud prevention from diverse methodological and theoretical perspectives. Prior studies have highlighted the role of internal audit functions, internal control systems, and governance structures in mitigating corruption and improving accountability at the local government level (Lonto et al., 2023; Shidqi & Arfiansyah, 2025). Empirical research on village fund management has emphasized determinants of fraud such as weak controls, limited transparency, and low accountability, particularly during periods of fiscal stress or crisis (Putra et al., 2024). Other strands of literature have explored the use of whistleblowing systems, audit technology, and data analytics to enhance fraud detection and prevention (Putra et al., 2022; Lubis, 2024). While these studies contribute valuable insights, they tend to address audit, risk management, internal control, and fraud prevention as partially disconnected domains. Moreover, many analyses remain descriptive or compliance-driven, offering limited guidance on how audit planning and execution can be systematically aligned with evolving risk landscapes, especially in remote village contexts.

This fragmentation in the literature reveals a critical research gap concerning the absence of an integrated conceptual and analytical framework that links audit practices explicitly to risk management and fraud prevention in village fund oversight. In particular, the Risk-Based Internal Audit (RBIA) approach—formally articulated within the International Professional Practices Framework (IPPF) of the Institute of Internal Auditors—has not been sufficiently synthesized with Enterprise Risk Management (ERM) frameworks such as ISO 31000 and COSO ERM, nor with the COSO Internal Control–Integrated Framework, in the context of village fund governance. Additionally, although fraud theories such as the Fraud Triangle and Fraud Diamond provide explanatory lenses for understanding fraudulent behavior, they are rarely operationalized within a structured, risk-based audit model that supports early warning and prevention. This gap is particularly salient in remote areas, where resource constraints necessitate prioritization and risk-focused oversight rather than exhaustive compliance checks.

In response to this gap, the present literature review aims to synthesize and critically analyze state-of-the-art research on RBIA as a strategic mechanism for village fund oversight in remote areas. The review explicitly focuses on three interrelated dimensions: (1) risk mapping and the construction of a village fund risk universe informed by ERM principles (ISO 31000 and COSO ERM); (2) the development of early warning mechanisms through RBIA-aligned planning, assurance, consulting, and audit analytics; and (3) fraud prevention strategies grounded in the integration of internal control systems and fraud theories. By systematically reviewing and thematically synthesizing peer-reviewed journal articles, conference proceedings, and authoritative institutional reports, this study seeks to illuminate how RBIA can function not merely as an assurance tool, but as a proactive governance instrument tailored to the realities of remote and capacity-constrained environments.

This article contributes to the literature in several important ways. Theoretically, it advances an integrative framework that connects RBIA, ERM, internal control, and fraud theories within a unified analytical model for village fund oversight. Empirically, it consolidates dispersed findings across audit, risk management, and fraud prevention studies into coherent thematic insights relevant to remote-area governance. Practically, the review offers evidence-based implications for internal auditors, inspectorates, and policymakers seeking to strengthen early warning capabilities and fraud prevention in decentralized public finance systems. Structurally, the article proceeds as follows: after this introduction, the Literature Review section elaborates the theoretical foundations and prior empirical findings; the Materials and Methods section details the review design and synthesis approach; the Results and Discussion section presents and interprets the main thematic findings; the Comparison section contrasts frameworks and contexts; and the Conclusion summarizes key insights, implications, and directions for future research.

## 2. Literature Review

### Risk-Based Internal Audit in the Public Sector

Risk-Based Internal Audit (RBIA) represents a paradigmatic shift in public sector auditing from traditional compliance-oriented approaches toward a strategic, risk-focused model aligned with organizational objectives and public value creation. Within the International Professional Practices Framework (IPPF) issued by the Institute of Internal Auditors, RBIA is conceptualized as an approach that prioritizes audit resources based on the likelihood and impact of risks that may hinder the achievement of organizational goals. In the public sector, this evolution reflects growing demands for accountability, transparency, and performance-oriented governance in increasingly complex and decentralized administrative environments. The Global Internal Audit Standards (2024) emphasize that internal audit functions must adopt a risk-based mindset in planning and execution to remain relevant to governing bodies and stakeholders (The Institute of Internal Auditors [IIA], 2024). Unlike compliance audits that primarily assess adherence to rules and procedures, RBIA focuses on systemic vulnerabilities, governance weaknesses, and emerging risks, thereby enabling public organizations to anticipate problems rather than merely react to violations. This shift is particularly relevant in public finance contexts, where resource constraints and political accountability necessitate targeted and value-adding audit interventions.

A core operational feature of RBIA in the public sector is risk-based audit planning, which links audit priorities directly to an organization's risk universe and strategic objectives. Under IPPF guidance, audit plans are expected to be dynamic, continuously updated, and informed by enterprise-wide risk assessments rather than static annual schedules (IIA, 2024). Empirical studies demonstrate that risk-based planning enhances audit relevance and managerial responsiveness by directing attention to high-risk programs, financial flows, and governance processes (Lonto et al., 2023). In decentralized public sector settings, such as local governments, RBIA enables internal auditors to cope with limited audit capacity by focusing on material and high-impact risks. However, the effectiveness of risk-based planning depends heavily on the maturity of risk management practices and the availability of reliable risk information. Where risk registers are underdeveloped or treated as formalities, RBIA risks degenerating into nominal compliance exercises. This limitation highlights the interdependence between RBIA and broader risk governance structures in public organizations.

Beyond planning, RBIA expands the role of internal auditors through the balanced provision of assurance and consulting services, as explicitly recognized within the IPPF. Assurance engagements provide independent assessments of risk management, control, and governance processes, while consulting activities support management in improving risk responses without compromising auditor independence (IIA, 2024). Recent empirical research indicates that public sector organizations with strong RBIA-oriented internal audit functions exhibit improved fraud prevention and stronger internal control effectiveness (Putra et al., 2022; Shidqi & Arfiansyah, 2025). Consulting roles, when appropriately governed, allow internal auditors to contribute to risk awareness, capacity building, and early warning mechanisms, particularly in organizations with limited managerial expertise. Nevertheless, scholars caution that role ambiguity and insufficient safeguards may threaten objectivity, especially in politically sensitive public sector environments. Effective RBIA implementation therefore requires clear mandates, strong ethical standards, and robust oversight from audit committees or equivalent governance bodies.

Recent empirical literature (2020–2025) further identifies several critical success factors and constraints shaping RBIA implementation in public sector organizations. Key enabling factors include top management support, auditor competence in risk analysis, integration with enterprise risk management systems, and access to audit analytics and information technology (Lubis, 2024; Putra et al., 2022). Conversely, constraints commonly observed in public institutions include limited human resources, weak risk culture, inadequate training, and resistance from audited units. These challenges are more pronounced in decentralized and remote governance contexts, where institutional capacity and data availability are uneven. Despite these limitations, the literature consistently suggests that RBIA enhances public accountability by strengthening oversight quality, improving risk visibility, and supporting proactive fraud prevention strategies. However, existing studies often remain sector-specific or methodologically fragmented, underscoring the need for integrative reviews that synthesize

RBIA theory and empirical evidence within complex public finance settings, such as village fund oversight in remote areas.

### **Enterprise Risk Management (ERM), Risk Assessment, and Risk Mapping for Public-Sector Oversight**

Enterprise Risk Management (ERM) provides a structured governance architecture for identifying, analyzing, evaluating, and treating risks that could undermine the achievement of organizational objectives, while also strengthening accountability and decision transparency in the public sector. ISO 31000 frames risk management as an iterative process anchored in (i) establishing context, (ii) risk assessment—covering identification, analysis, and evaluation—and (iii) risk treatment, supported by continuous communication, consultation, monitoring, and review (International Organization for Standardization, 2018). COSO ERM complements this by explicitly connecting risk considerations to strategy and performance, emphasizing governance and culture, objective-setting, performance, review and revision, and information/communication/reporting as mutually reinforcing components for enterprise-wide risk oversight (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2017). In contemporary scholarship, ERM is also understood as an evolving organizational practice shaped by institutional dynamics, professional roles, and the gradual embedding of “risk thinking” into administrative routines—an important lens for explaining why ERM adoption may be uneven across public organizations and subnational contexts (Jabbour, 2024). Together, ISO 31000 and COSO ERM establish the conceptual foundation for risk mapping as a decision tool for prioritization and resource allocation under constraints. (International Organization for Standardization, 2018; COSO, 2017; Jabbour, 2024)

Risk mapping is the practical translation of ERM into oversight intelligence: it transforms dispersed risk signals into a structured “risk universe,” enabling decision makers to visualize likelihood–impact profiles, risk interdependencies, and control vulnerabilities. Within ISO 31000’s risk assessment logic, risk identification clarifies threat sources and events; risk analysis estimates likelihood and consequence; and risk evaluation ranks risks relative to criteria and risk appetite, producing a defensible basis for prioritization and escalation (International Organization for Standardization, 2018). COSO ERM further strengthens risk mapping by integrating performance metrics and strategic objectives into risk prioritization, enabling public entities to interpret risk not only as compliance exposure but also as impediments to service outcomes and value delivery (COSO, 2017). Recent synthesis research on internal audit and ERM underscores that risk mapping becomes most actionable when it is linked to governance reporting, clearly assigned risk ownership, and periodic review cycles—conditions that move risk registers from symbolic compliance to operational decision support (Nkansa et al., 2025). In public organizations, these features help mitigate fragmented oversight by creating a shared risk language across audit, management, and leadership forums, improving comparability of risks across programs and administrative units. (International Organization for Standardization, 2018; COSO, 2017; Nkansa et al., 2025)

ERM is particularly consequential for Risk-Based Internal Audit (RBIA) because risk mapping supplies the evidentiary base for risk-based audit planning and supervisory decision-making. The IIA’s standards framework emphasizes that internal audit planning should be risk-based and responsive to organizational objectives, implying that high-quality risk assessment outputs (e.g., risk maps, risk registers, heatmaps, and risk appetite statements) are prerequisites for audit relevance and value addition (The Institute of Internal Auditors [IIA], 2024). Empirical literature aligns with this logic: public-sector internal audit is more effective when it focuses on high-risk processes and control breakdowns rather than evenly distributing audit effort across low- and high-risk domains, particularly under resource constraints (Lonto et al., 2023). Moreover, studies in Indonesian local government contexts show that ERM maturity is associated with stronger fraud prevention and detection, suggesting that risk mapping can function as a preventive governance mechanism that strengthens the internal audit function’s ability to target fraud-prone exposures (Tarjo et al., 2022). Taken together, the evidence supports a governance chain in which ERM risk mapping informs RBIA’s audit universe and prioritization, while RBIA assurance and consulting feedback loops refine ERM risk judgments over time. (IIA, 2024; Lonto et al., 2023; Tarjo et al., 2022)

In local government and public fund management, ERM implementation faces persistent constraints that are amplified in resource-limited and remote settings, where data quality, risk expertise, and control infrastructure are often uneven. Evidence from village fund governance indicates that risk management capacity varies substantially across localities, and

weaknesses in administrative systems can reduce risk mapping to a formalistic exercise rather than a functional basis for control strengthening and targeted oversight (Ginting et al., 2023). These constraints matter because risk mapping depends on reliable process documentation, incident reporting, and control monitoring—inputs that may be scarce where staffing is thin and oversight institutions have limited reach. At the same time, empirical findings suggest that when ERM practices are institutionalized—through leadership commitment, risk ownership clarity, and integration with internal control and audit routines—public organizations can better surface fraud risks and prioritize mitigation actions (Tarjo et al., 2022). Accordingly, the literature implies that ERM in local government should be assessed not merely by formal adoption of frameworks, but by operational indicators: risk register usage in decisions, periodic updating, linkages to internal control evaluations, and demonstrable influence on RBIA audit planning. This operational focus is essential for designing ERM-informed oversight of public funds in remote areas. (Ginting et al., 2023; Tarjo et al., 2022; International Organization for Standardization, 2018)

### **COSO Internal Control–Integrated Framework as the Assurance Foundation for Public-Sector Financial Governance**

The COSO Internal Control–Integrated Framework (2013) is widely recognized as a foundational assurance model for strengthening accountability, reliability of financial reporting, compliance, and operational effectiveness in public-sector financial governance. In decentralized public finance settings, COSO’s value lies in its capacity to translate abstract “good governance” expectations into an auditable system of controls that can be assessed, improved, and monitored over time. COSO defines internal control as a process effected by an entity’s board, management, and personnel, designed to provide reasonable assurance regarding the achievement of objectives across operations, reporting, and compliance (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2013). This “reasonable assurance” logic is particularly salient in public fund management, where absolute prevention of misuse is unrealistic, yet robust design and consistent operation of controls can materially reduce the probability and impact of irregularities. As a result, COSO becomes a practical bridge between governance mandates and audit execution: it provides common criteria for assessing control adequacy and for diagnosing why public organizations fail to prevent fraud or inefficiency despite formal rules and procedures. (COSO, 2013; COSO, n.d.)

COSO operationalizes internal control through five components—(1) control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring activities—supported by 17 principles that specify what “effective” control means in practice (COSO, 2013). The control environment sets the ethical tone and accountability architecture; risk assessment requires specifying objectives and analyzing risks (including fraud risk); control activities translate risk responses into policies and procedures; information and communication ensure relevant, timely data flows; and monitoring verifies that controls remain present and functioning. These components are not linear checklists; rather, COSO emphasizes that control effectiveness arises when components are integrated and operate together, producing a coherent control system capable of adapting to changing risk conditions (COSO, 2013). In public-sector budgeting and fund disbursement, this integration is vital: strong control activities (e.g., approvals, segregation of duties) cannot compensate for weak risk assessment or poor monitoring. Accordingly, COSO’s diagnostic logic supports a more rigorous assurance posture by enabling auditors to assess both design and operating effectiveness across the entire control system rather than focusing narrowly on compliance with isolated procedures. (COSO, 2013; COSO, n.d.)

The linkage between COSO and Risk-Based Internal Audit (RBIA) is direct: RBIA depends on credible assessments of governance, risk management, and internal control to prioritize audit work and provide meaningful assurance. The IIA’s standards framework stresses that internal audit must adopt a risk-based orientation and evaluate the effectiveness of governance, risk management, and control processes to remain relevant for oversight bodies (The Institute of Internal Auditors [IIA], 2024). In practice, COSO provides the audit criteria and structure that RBIA uses to translate risk priorities into assurance questions: which controls mitigate the highest risks, where control design is deficient, and where operating failures persist. Empirical evidence from public-sector contexts indicates that stronger internal audit and control systems are associated with improved fraud prevention outcomes, implying that RBIA becomes more effective when grounded in a well-defined internal control framework such as COSO (Lonto et al., 2023). Conversely, where internal control is weak or

inconsistently applied, RBIA planning may be distorted by incomplete risk information and unreliable control performance signals, reducing the value of assurance conclusions for governance decision-making. (IIA, 2024; COSO, 2013; Lonto et al., 2023)

Empirical literature further demonstrates that internal control weaknesses are repeatedly implicated in fraud risk, corruption exposure, and inefficiency in public fund management, including at the local government level. Studies show that deficits in control design (e.g., inadequate segregation of duties, weak documentation, limited supervision) and failures in monitoring and accountability mechanisms increase opportunities for fraud and undermine preventive oversight (Pattawe, 2023; Shidqi & Arfiansyah, 2025). From an integrated governance perspective, combining COSO with ERM strengthens assurance by ensuring that risk identification and prioritization (ERM) are matched with a coherent system of mitigating controls (COSO), and then targeted and tested through RBIA (IIA standards). Empirical evidence from Indonesian local government contexts suggests that ERM maturity is associated with better fraud prevention and detection, reinforcing the argument that risk management and internal control must be mutually reinforcing rather than “siloed” initiatives (Tarjo et al., 2022). Thus, for public fund oversight—including village fund governance—the most defensible assurance logic is a triadic integration: ERM risk mapping → COSO control design and monitoring → RBIA risk-based planning and assurance, enabling more targeted supervision under resource constraints. (Pattawe, 2023; Shidqi & Arfiansyah, 2025; Tarjo et al., 2022; COSO, 2013; IIA, 2024)

### **Fraud Triangle/Fraud Diamond in Public-Sector Financial Management and Village Fund Oversight**

Fraud risk in public-sector financial management is commonly explained through Fraud Triangle theory, which posits that fraudulent behavior emerges when pressure, opportunity, and rationalization converge within a “trusted position” context (Cressey, 1953; Association of Certified Fraud Examiners [ACFE], 2024). In public administration, pressure often relates to financial stress, political patronage, performance demands, or informal obligations in local governance systems; opportunity is created by weak segregation of duties, limited supervision, poor documentation, and low transparency; while rationalization is reinforced by permissive organizational cultures, normalization of deviance, or moral licensing in bureaucratic settings. The Fraud Diamond extends this logic by adding capability—the perpetrator’s skills, access, authority, and resilience to execute and conceal fraud—an element particularly relevant in public entities where insiders may understand procedural loopholes and exploit weak monitoring (Wolfe & Hermanson, 2004). Contemporary evidence indicates that fraud patterns remain persistent across sectors, and prevention is most effective when organizations operationalize these drivers into risk indicators, control design, and monitoring routines rather than treating fraud as isolated misconduct events (ACFE, 2024).

The empirical literature consistently links internal control weaknesses to heightened fraud exposure and inefficiency in public fund administration, including village-level financial management. Studies of village finance show that weak control environments and accountability arrangements—such as insufficient oversight, limited documentation discipline, and inconsistent application of controls—significantly erode fraud prevention capacity (Pattawe, 2023). Similarly, broader local-government evidence demonstrates that deficiencies in internal controls and internal audit functions correlate with corruption-related outcomes and governance failures, underscoring the structural role of control systems in shaping “opportunity” conditions under the Fraud Triangle/Diamond (Shidqi & Arfiansyah, 2025). Research on village fund fraud during crisis periods also illustrates how administrative disruptions and capacity stressors can intensify opportunity structures and weaken monitoring, creating fertile conditions for misappropriation (Putra et al., 2024). Importantly, these findings suggest that fraud is rarely a purely individual-level phenomenon; rather, it reflects systemic control gaps and governance misalignments that allow pressures and rationalizations to translate into actionable opportunities, particularly when individuals possess the capability to exploit institutional vulnerabilities.

From a prevention standpoint, Risk-Based Internal Audit (RBIA) provides a proactive mechanism for translating fraud risk theory into targeted oversight priorities, thereby shifting audit practice from retrospective compliance checking to forward-looking risk anticipation. The Global Internal Audit Standards (2024) emphasize that internal audit should adopt a risk-based orientation and evaluate governance, risk management, and controls to provide value-adding assurance (The Institute of Internal Auditors [IIA], 2024). In fraud-prone public fund

cycles, RBIA strengthens prevention by (i) aligning audit planning to high-risk processes, (ii) testing control design and operating effectiveness at points of greatest exposure, and (iii) using consulting engagements—when appropriately safeguarded—to improve controls and risk awareness. Empirical studies indicate that internal audit, when supported by risk management and enabling infrastructures (including analytics capability), contributes to preventing financial crime behaviors, reinforcing the argument that prevention is maximized when audit functions are integrated with risk governance rather than operating as isolated compliance units (Putra et al., 2022). This RBIA logic is especially salient for village funds, where limited resources require prioritization: auditors must focus on the riskiest transactions and control breakdowns rather than distributing attention uniformly.

A robust anti-fraud architecture is therefore best conceptualized as an integrated triad: ERM risk identification and mapping → COSO internal control design and monitoring → RBIA risk-based assurance and advisory feedback loops. ERM maturity has been shown to improve fraud prevention and detection in Indonesian local government, suggesting that systematic risk assessment and prioritization can reduce blind spots and strengthen organizational vigilance (Tarjo et al., 2022). COSO's Internal Control–Integrated Framework provides the assurance backbone by specifying components and principles that mitigate opportunity and support monitoring, while RBIA operationalizes these risk and control insights into audit scope, testing strategies, and early-warning priorities (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2013; IIA, 2024). In practical terms, this integration enables (1) explicit fraud risk assessment embedded in the risk universe, (2) control activities calibrated to fraud opportunities, and (3) audit plans that prioritize high-impact exposures and recurring anomalies. The literature thus converges on a central implication: fraud prevention in public funds—particularly in capacity-constrained settings—depends less on adding rules and more on strengthening the risk–control–audit system that anticipates, detects, and disrupts fraud drivers before losses materialize.

### 3. Materials and Methods

This study adopts a state-of-the-art literature review design to synthesize and critically assess the evolution of concepts, frameworks, and empirical findings on Risk-Based Internal Audit (RBIA) for the oversight of village funds in remote areas. A literature review approach is appropriate given the study's objective to integrate dispersed strands of scholarship—spanning internal auditing, risk management, internal control, fraud theory, and data-driven oversight—into a coherent analytical framework rather than to test hypotheses or collect primary data. The review is positioned as an interpretive and analytical synthesis that combines a systematic narrative review with thematic analysis and conceptual mapping, enabling both breadth of coverage and depth of interpretation. Methodological rigor is emphasized through transparent search procedures, explicit selection criteria, and a theory-driven synthesis strategy to ensure academic validity and replicability (Tranfield et al., 2003; Snyder, 2019).

The literature search was conducted across multiple academic databases to capture high-quality and contextually relevant sources. Core databases included Scopus, Web of Science, and Google Scholar, complemented by DOAJ and SINTA to ensure coverage of reputable open-access and nationally accredited journals relevant to public-sector contexts. In addition, authoritative institutional reports and standards issued by the Institute of Internal Auditors, the International Organization for Standardization, and the Committee of Sponsoring Organizations of the Treadway Commission were included due to their foundational role in shaping RBIA, ERM, and internal control practices. The review prioritized peer-reviewed journal articles published within the last five years, while allowing selective inclusion of seminal works (e.g., Fraud Triangle/Diamond) strictly for theoretical grounding. All sources were required to provide traceable DOIs or official URLs to ensure verifiability.

The search strategy employed structured keyword combinations and Boolean operators to maximize precision and recall. Keywords included, but were not limited to, “risk-based internal audit,” “enterprise risk management,” “ISO 31000,” “COSO ERM,” “internal control,” “COSO internal control,” “fraud triangle,” “fraud diamond,” “early warning system,” “audit analytics,” “public sector audit,” “village fund,” and “remote areas.” The selection process followed a sequential screening procedure consistent with PRISMA principles, albeit applied narratively: initial identification through database queries, screening of titles and abstracts for relevance, and full-text assessment for eligibility. Inclusion criteria required that studies (i) directly address RBIA, ERM, internal control, fraud prevention, or

data-driven oversight in public-sector settings; (ii) present conceptual frameworks, models, or empirical evidence relevant to oversight and accountability; and (iii) be published in reputable academic outlets or as official institutional standards. Exclusion criteria eliminated non-peer-reviewed opinion pieces, practitioner blogs, and sources lacking methodological transparency or scholarly citation.

Data analysis and synthesis were conducted using thematic analysis and conceptual mapping to organize findings across heterogeneous studies. Thematic analysis enabled the identification of recurrent patterns and analytical categories—such as risk identification and mapping, audit planning and prioritization, early warning mechanisms, fraud drivers, and capacity constraints in remote governance—while conceptual mapping facilitated the integration of these themes into a structured framework. This dual approach allowed the review to move beyond descriptive aggregation toward analytical synthesis, highlighting relationships, complementarities, and tensions across the literature (Braun & Clarke, 2006; Snyder, 2019). The iterative coding and synthesis process was guided by constant comparison across studies to refine themes and ensure internal coherence.

The interpretation of findings was explicitly anchored in four interrelated analytical lenses: (1) RBIA, as articulated in the IIA's IPPF and Global Internal Audit Standards, to frame audit planning, assurance, and consulting roles; (2) Enterprise Risk Management, drawing on ISO 31000 and COSO ERM, to structure risk identification, analysis, evaluation, and risk mapping; (3) COSO Internal Control–Integrated Framework, to assess control design, operation, and assurance linkages; and (4) Fraud Triangle/Diamond, to explain behavioral and systemic drivers of fraud risk in public funds. Using these lenses in combination enabled a theoretically grounded synthesis that connects risk governance, internal control, and audit practice with proactive fraud prevention and early warning—particularly salient for village fund oversight in remote, capacity-constrained settings. Throughout the review, methodological transparency and academic accountability were maintained by ensuring that all conceptual and methodological references are cited in APA 7th edition with active DOIs or official URLs, thereby supporting replicability and scholarly rigor.

## 4. Results and Discussion

### Risk Mapping of Village Fund Management in Remote Areas

The literature converges on the finding that risk mapping is a critical entry point for strengthening oversight of village fund management in remote areas, where administrative capacity, data availability, and supervisory reach are structurally constrained. Empirical studies show that risks in village fund governance are not evenly distributed but clustered around procurement, cash management, beneficiary targeting, and reporting processes, with remoteness amplifying information asymmetry and weakening routine controls (Ginting et al., 2023; Putra et al., 2024). From an ERM perspective, risk identification and evaluation enable the construction of a “village fund risk universe” that prioritizes high-impact and high-likelihood exposures rather than treating all activities as equally risky (International Organization for Standardization [ISO], 2018). The synthesis indicates that villages with rudimentary or symbolic risk assessment practices struggle to anticipate emerging risks, resulting in reactive oversight and post hoc detection of irregularities. Conversely, where risk mapping is institutionalized—through risk registers, periodic review, and linkage to decision-making—it improves risk visibility and provides a rational basis for targeted supervision. These findings extend ERM theory by highlighting that, in remote governance contexts, the process of risk mapping (who participates, how often it is updated, and how it informs action) is as important as the formal adoption of risk frameworks.

### The Role of Risk-Based Internal Audit in Risk-Oriented Oversight Planning

Across the reviewed literature, Risk-Based Internal Audit (RBIA) emerges as a pivotal mechanism for translating risk maps into actionable oversight priorities in decentralized public finance. Consistent with the IPPF and the Global Internal Audit Standards, RBIA shifts audit planning from routine compliance coverage toward selective engagement with high-risk programs and transactions (The Institute of Internal Auditors [IIA], 2024). Empirical evidence indicates that internal audit functions adopting risk-based planning are better positioned to allocate scarce audit resources, enhance managerial responsiveness, and contribute to fraud prevention outcomes (Lonto et al., 2023). In village fund contexts, RBIA

allows inspectorates to focus on risk-prone villages, phases of the budget cycle, or transaction types, rather than applying uniform audit intensity across heterogeneous settings. However, the literature also reveals a dependency effect: RBIA effectiveness is contingent on the quality of upstream risk assessment and governance support. Where risk information is incomplete or politically constrained, RBIA risks becoming nominally “risk-based” without substantively improving assurance. These findings refine RBIA theory in the public sector by underscoring its embeddedness within broader risk governance systems rather than its operation as a stand-alone audit technique.

### **Integrating ERM and COSO Internal Control to Strengthen Assurance**

A central thematic finding is that assurance quality improves when ERM and COSO Internal Control are integrated with RBIA, rather than implemented as parallel or siloed initiatives. COSO’s Internal Control–Integrated Framework provides the structural criteria for evaluating control design and operating effectiveness across five interrelated components, while ERM contributes systematic risk prioritization that informs which controls matter most for achieving objectives (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2013; COSO, 2017). Empirical studies demonstrate that weaknesses in internal control—particularly in monitoring, segregation of duties, and accountability—are strongly associated with fraud risk and inefficiency in public fund management (Pattawe, 2023; Shidqi & Arfiansyah, 2025). The synthesis suggests that RBIA functions most effectively when it leverages ERM outputs to select audit priorities and COSO principles to assess assurance adequacy. This triadic integration (ERM–COSO–RBIA) supports a shift from rule-based oversight toward system-based assurance, which is especially relevant in remote areas where exhaustive compliance checks are infeasible. The findings thus extend assurance theory by positioning internal control not merely as an audit object, but as a dynamic interface between risk governance and audit judgment.

### **Early Warning Systems and Audit Analytics as Proactive Oversight Tools**

The reviewed literature highlights early warning systems (EWS) and audit analytics as emerging innovations that operationalize RBIA’s forward-looking orientation. Studies on continuous auditing and anomaly detection demonstrate that analytics-enabled monitoring can identify irregular patterns earlier than traditional periodic audits, thereby strengthening preventive oversight (Wang & Vasarhelyi, 2024; Hilal et al., 2022). Within a risk-based framework, EWS transforms risk maps into leading indicators—such as unusual spending patterns, delays, or control overrides—that signal heightened fraud or mismanagement risk. However, evidence also points to uneven adoption of audit analytics due to data quality issues, limited technical skills, and weak integration with audit workflows, resulting in partial or symbolic implementation (Krieger et al., 2021). In remote village contexts, these constraints are more pronounced, yet the literature suggests that “minimum viable” analytics—focused on a small set of high-risk indicators—can still enhance oversight credibility and timeliness. These findings contribute to digital governance scholarship by emphasizing that the value of EWS lies less in technological sophistication than in institutional embedding within RBIA planning and escalation processes.

### **RBIA and Fraud Prevention through the Fraud Triangle/Diamond Lens**

The synthesis further demonstrates that RBIA-informed oversight directly addresses the structural drivers of fraud articulated in the Fraud Triangle and Fraud Diamond frameworks. Weak internal controls and ineffective audits expand opportunity, while administrative stressors and political pressures intensify pressure, and normalized practices enable rationalization; capability is reinforced when insiders possess procedural knowledge and unchecked authority (Cressey, 1953; Wolfe & Hermanson, 2004). Empirical studies on village fund fraud confirm that such conditions are prevalent in decentralized and crisis-affected settings (Putra et al., 2024). RBIA mitigates these drivers by prioritizing audits where opportunities are greatest, strengthening controls through assurance and consulting, and supporting early warning mechanisms that disrupt concealment. Evidence linking ERM maturity and internal audit effectiveness to improved fraud prevention outcomes reinforces this logic (Tarjo et al., 2022; Putra et al., 2022). Collectively, the findings suggest that fraud prevention in public funds is most effective when RBIA is embedded within an integrated risk–control–analytics architecture, rather than treated as an episodic detection activity.

## **Integrative Discussion: Implications for Governance and Accountability in Remote Areas**

Taken together, the thematic findings reveal a coherent governance logic in which risk mapping, RBIA, ERM, internal control, and early warning systems function as mutually reinforcing elements of public-sector oversight. The literature supports and extends existing theories by demonstrating that RBIA's value in remote-area governance lies in its capacity to align limited oversight resources with the most consequential risks, while embedding fraud prevention into routine governance processes. Importantly, the synthesis underscores that institutional capacity—not merely framework adoption—determines outcomes: where leadership commitment, risk culture, and data infrastructures are weak, even well-designed RBIA and ERM systems underperform. For village fund governance, this implies that strengthening accountability requires incremental, context-sensitive implementation of RBIA-informed oversight rather than wholesale transplantation of advanced models. From a theoretical standpoint, the findings advance an integrated perspective that links risk governance and audit assurance to behavioral fraud theories, highlighting how systemic design choices shape incentives and opportunities. Practically, the results suggest that policymakers and inspectorates should prioritize risk-based targeting, minimum viable analytics, and control strengthening as realistic pathways to improving accountability and public trust in remote settings.

### **5. Comparison**

Prior research on village fund governance and public-sector financial oversight has provided important empirical insights into fraud risk, accountability weaknesses, and administrative capacity constraints at the local level. Studies focusing on village fund management have consistently documented that remoteness, limited human resources, and weak monitoring structures increase vulnerability to misappropriation and inefficiency (Ginting et al., 2023; Putra et al., 2024). Complementary work emphasizes the role of internal control systems and accountability mechanisms in mitigating fraud risk, demonstrating that deficiencies in control design and monitoring are closely associated with governance failures (Pattawe, 2023). However, much of this literature remains descriptive and control-centric, offering limited guidance on how risk information should be systematically translated into audit priorities. In particular, earlier studies rarely articulate a clear linkage between identified risks in village fund management and the strategic deployment of audit resources, leaving a gap in understanding how oversight can be made adaptive and risk-responsive in heterogeneous and capacity-constrained village contexts.

Research on Risk-Based Internal Audit (RBIA) in the public sector has advanced conceptual and empirical understanding of how audit effectiveness can be improved through risk-oriented planning and execution. International standards emphasize that RBIA enhances audit relevance by aligning assurance activities with the most significant organizational risks (The Institute of Internal Auditors [IIA], 2024). Empirical evidence supports this claim, showing that stronger internal audit functions contribute to fraud prevention and improved governance outcomes (Lonto et al., 2023; Shidqi & Arfiansyah, 2025). Nevertheless, this body of literature often treats RBIA at a generic organizational level, with limited sensitivity to the institutional realities of village fund governance. Prior studies seldom address how RBIA can be operationalized where risk data are fragmented, audit coverage is uneven, and inspectorates face logistical and political constraints—conditions that are characteristic of remote and peripheral regions. As a result, the transferability of RBIA prescriptions to village-level oversight remains underexplored.

Another limitation in earlier scholarship concerns the fragmented treatment of ERM, internal control, and internal audit as parallel governance mechanisms rather than as an integrated assurance system. ERM frameworks based on ISO 31000 and COSO ERM provide systematic approaches to risk identification, analysis, and evaluation, while the COSO Internal Control–Integrated Framework specifies criteria for assessing control effectiveness (International Organization for Standardization, 2018; Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2013, 2017). Although empirical studies suggest that ERM maturity is associated with stronger fraud prevention and detection in local governments (Tarjo et al., 2022), prior research often stops short of explaining how ERM outputs—such as risk maps and risk registers—should inform COSO-based control assessments and RBIA audit planning in practice. This separation is particularly problematic

in remote governance contexts, where oversight institutions must prioritize among competing risks and cannot rely on exhaustive compliance audits.

With respect to early warning systems (EWS) and audit analytics, existing literature demonstrates significant methodological potential but uneven institutional uptake in public-sector auditing. Studies on continuous auditing and monitoring illustrate that data-driven approaches can identify anomalies and emerging risks earlier than traditional periodic audits (Wang & Vasarhelyi, 2024). At the same time, research highlights substantial barriers to analytics adoption, including limited technical capacity, data accessibility issues, and weak integration between analytics outputs and audit decision-making processes (Krieger et al., 2021). While anomaly-detection research provides sophisticated tools for fraud identification (Hilal et al., 2022), most studies do not sufficiently contextualize these tools for village fund oversight or remote-area governance. Consequently, prior work offers limited guidance on how early warning mechanisms can be realistically embedded within RBIA frameworks under conditions of infrastructural and administrative scarcity.

Against this backdrop, the present literature review offers conceptual and practical novelty by integrating RBIA, ERM, COSO Internal Control, and fraud theories into a single, context-sensitive analytical framework tailored to village fund oversight in remote areas. Unlike earlier studies that address these elements in isolation, this review synthesizes them into a coherent governance chain in which ERM-based risk mapping informs COSO-aligned control assurance, which in turn underpins RBIA planning, assurance, and consulting activities. Furthermore, the review extends fraud-focused scholarship by explicitly linking Fraud Triangle and Fraud Diamond drivers to risk-based audit interventions and early warning mechanisms, thereby translating behavioral theory into actionable oversight strategies. By foregrounding remoteness as a structural risk amplifier and emphasizing “minimum viable” analytics for early warning, this review advances a more realistic and operationally grounded model of public-sector oversight, contributing both to theory development and to policy-relevant audit practice.

## 6. Conclusion

This literature review synthesizes state-of-the-art scholarship on Risk-Based Internal Audit (RBIA) as a strategic mechanism for strengthening the oversight of village fund management in remote areas. The review identifies a consistent pattern across the literature: effective oversight is most likely to emerge when RBIA is embedded within an integrated governance architecture that combines Enterprise Risk Management (ERM) frameworks (ISO 31000 and COSO ERM), the COSO Internal Control–Integrated Framework, and fraud-oriented analytical lenses such as the Fraud Triangle and Fraud Diamond. The synthesis shows that risk mapping functions as the critical entry point for oversight, enabling the prioritization of high-impact and high-likelihood risks in capacity-constrained settings. RBIA translates these risk insights into focused audit planning, assurance, and consulting activities, while early warning systems and audit analytics extend the audit function from retrospective detection toward proactive risk anticipation. Collectively, the literature demonstrates that such integration not only improves audit relevance and efficiency, but also strengthens fraud prevention by systematically reducing opportunities, enhancing monitoring, and disrupting concealment mechanisms in decentralized public finance systems.

In relation to the study’s objectives, this review contributes theoretically by consolidating fragmented bodies of knowledge—public-sector auditing, risk management, internal control, fraud theory, and data-driven oversight—into a unified analytical framework tailored to village fund governance. Unlike prior studies that examine these elements in isolation, this article advances an integrative perspective that clarifies how ERM-based risk identification informs COSO-aligned control assurance and how both are operationalized through RBIA. By explicitly situating these relationships within the context of remote and peripheral regions, the review extends audit and governance theory beyond generic organizational settings. It highlights remoteness not merely as a contextual variable, but as a structural risk amplifier that shapes the feasibility, sequencing, and effectiveness of oversight mechanisms. In doing so, the article strengthens the conceptual foundations of public-sector audit literature by linking risk governance and assurance frameworks to behavioral explanations of fraud and to the realities of decentralized fiscal administration.

From a practical and policy perspective, the findings underscore several implications for internal auditors, local governments, and village-level stakeholders. First, inspectorates and internal audit units should prioritize the development of risk-based planning capabilities

grounded in credible risk mapping rather than relying on uniform or compliance-driven audit coverage. Second, policymakers should promote the integration of ERM and internal control systems as enablers of RBIA, ensuring that risk registers, control assessments, and audit plans are mutually reinforcing. Third, the literature suggests that early warning systems and audit analytics should be implemented pragmatically, focusing on “minimum viable” indicators that are feasible under local data and infrastructure constraints. Such targeted approaches can enhance accountability and public trust without imposing unrealistic technological demands. Overall, the review indicates that strengthening village fund oversight in remote areas requires incremental, context-sensitive reforms that align governance ambition with institutional capacity.

Despite its contributions, this literature review is subject to limitations inherent in review-based research. The analysis depends on the scope, quality, and availability of existing studies, many of which remain cross-sectional, sector-specific, or descriptive in nature. Empirical evidence on RBIA implementation, early warning systems, and audit analytics in village fund contexts—particularly in remote areas—remains limited. Future research should therefore pursue empirical and mixed-methods studies that test the integrated RBIA–ERM–Internal Control framework in practice, including comparative analyses across regions with differing capacity levels. There is also a clear agenda for advancing research on audit analytics, digital oversight tools, and adaptive early warning systems suited to low-resource environments. Such studies would not only validate and refine the conceptual synthesis advanced in this review, but also provide actionable evidence to support more resilient, risk-responsive, and accountable governance of village funds in remote settings.

**Author Contributions:** “Conceptualization, E.M.; F.A.; Methodology, E.M.; D.F.; Formal analysis, E.M.; S.K.; Writing, E.M. The authors has read and agreed to the published version of the manuscript”

**Funding:** “This research received no external funding”

**Data Availability Statement:** This article is a literature review and does not generate new primary data. All materials analyzed in this study are derived from publicly available secondary sources, including peer-reviewed journal articles and conference proceedings indexed in recognized academic databases.

**Acknowledgments:** “The author gratefully acknowledges institutional and academic support that facilitated the completion of this review. The author also acknowledges the use of artificial intelligence–assisted tools for language refinement and editorial support, applied in accordance with responsible research and publication ethics, without altering the scholarly interpretation or substantive content of the manuscript.”

**Conflicts of Interest:** “The authors declare no conflict of interest.”

## References

- Association of Certified Fraud Examiners. (2024). *Occupational fraud 2024: A report to the nations*. <https://www.acfe.com/-/media/files/acfe/pdfs/rtnn/2024/2024-report-to-the-nations.pdf>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Internal control—Integrated framework: Executive summary*. [https://www.sechistorical.org/collection/papers/2010/2013\\_0501\\_COSOInternal.pdf](https://www.sechistorical.org/collection/papers/2010/2013_0501_COSOInternal.pdf)
- Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management: Integrating with strategy and performance*. <https://www.coso.org/guidance-erm>
- Committee of Sponsoring Organizations of the Treadway Commission. (n.d.). *Internal control—Integrated framework (guidance hub)*. <https://www.coso.org/guidance-on-ic>
- Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. Free Press.

- Ginting, A. H., Widianingsih, I., Mulyawan, R., & Nurasa, H. (2023). Village government's risk management and village fund administration in Indonesia. *Sustainability*, 15(24), 16706. <https://doi.org/10.3390/su152416706>
- Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: A review of anomaly detection techniques and recent advances. *Expert Systems with Applications*, 193, 116429. <https://doi.org/10.1016/j.eswa.2021.116429>
- International Organization for Standardization. (2018). *ISO 31000:2018 risk management—Guidelines*. <https://www.iso.org/standard/65694.html>
- Jabbour, M. (2024). Enterprise risk management: An institutional work perspective. *Australian Accounting Review*. <https://doi.org/10.1080/01559982.2024.2439640>
- Krieger, F., Drews, P., & Velte, P. (2021). Explaining the (non-)adoption of advanced data analytics in auditing: A process theory. *International Journal of Accounting Information Systems*, 41, 100511. <https://doi.org/10.1016/j.accinf.2021.100511>
- Lonto, M. P., Sukoharsono, E. G., Baridwan, Z., & Prihatiningtias, Y. W. (2023). The effectiveness of internal audit for fraud prevention. *Australasian Accounting, Business and Finance Journal*, 17(3), 171–190. <https://doi.org/10.14453/aabfj.v17i3.11>
- Lubis, I. M. (2024). Determining the fraud audit technology and improved audit quality. *Problems and Perspectives in Management*, 22(2), 31–42. [https://doi.org/10.21511/ppm.22\(2\).2024.04](https://doi.org/10.21511/ppm.22(2).2024.04)
- Nkansa, P., Boateng, A., & Ahinful, G. (2025). From compliance to strategic partnerships: The role of internal audit in enterprise risk management and opportunities for future research. *Journal of Risk and Financial Management*, 18(12), 707. <https://doi.org/10.3390/jrfm18120707>
- Pattawe, A. (2023). The influence of the internal control system and accountability on fraud prevention in village financial management. *Atestasi: Jurnal Ilmiah Akuntansi*, 6(1), 217–228. <https://doi.org/10.57178/atestasi.v6i1.652>
- Putra, I., Sulistiyo, U., Diah, E., Rahayu, S., & Hidayat, S. (2022). The influence of internal audit, risk management, whistleblowing system, and big data analytics on financial crime behavior prevention. *Cogent Economics & Finance*, 10(1), 2148363. <https://doi.org/10.1080/23322039.2022.2148363>
- Putra, W. M., Sani, M. K., Putra, A. Z., & Utami, B. B. K. (2024). Factors causing fraudulent management of village funds during the COVID-19 pandemic. *Journal of Accounting and Investment*, 25(2), 460–478. <https://doi.org/10.18196/jai.v25i2.20092>
- Shidqi, F., & Arfiansyah, Z. (2025). Good governance and corruption: The roles of internal controls, internal audit functions, audit opinions, and capital expenditures. *Jurnal Akuntansi dan Auditing Indonesia*, 29(1). <https://doi.org/10.20885/jaai.vol29.iss1.art1>
- 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>
- Tarjo, T., Vidyantaha, H. V., Anggono, A., Yuliana, R., & Musyarofah, S. (2022). The effect of enterprise risk management on prevention and detection of fraud in Indonesia's local government. *Cogent Economics & Finance*, 10(1), 2101222. <https://doi.org/10.1080/23322039.2022.2101222>
- The Institute of Internal Auditors. (2024). *Global internal audit standards (2024 ed.)*. [https://www.theiia.org/globalassets/site/standards/globalinternalauditstandards\\_2024january9.pdf](https://www.theiia.org/globalassets/site/standards/globalinternalauditstandards_2024january9.pdf)

- 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>
- Wang, W., & Vasarhelyi, M. A. (2024). The application of continuous audit and monitoring methodology: A government medication procurement case. *International Journal of Accounting Information Systems*, 55, 100713. <https://doi.org/10.1016/j.accinf.2024.100713>
- Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, 74(12), 38–42. <https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=2546&context=facpubs>