Asia Pacific Fraud Journal
E-ISSN: 2502-695X, ISSN: 2502-8731
Volume 11, Issue 1 (January-June) 2026
*Asia Pacific Fraud Journal now has been accredited "**SINTA 3**" by Ministry of Research and Technology of The Republic of Indonesia (No SK. 225/E/KPT/2022).*
Available online at: http://apfjournal.or.id/index.php/apf

An Integrated Framework of Fraud Risk Assessment in ICOFR Implementation to Enhance Internal Controls Against Fraud Risks

✉[A-F]Indah Kurnia
Senior Auditor at a Subsidiary of State-Owned Company, Jakarta, Indonesia

ARTICLE INFORMATION
Article History:
Received November 24, 2025
Revised April 21, 2026
Accepted June 5, 2026

DOI:
10.21532/apfjournal.v11i1.463

A – Research concept and design
B – Collection and/or assembly of data
C – Data analysis and interpretation
D – Writing the article
E – Critical revision of the article
F – Final approval of article

ABSTRACT
The increasing prevalence of financial statement manipulation, corruption, and asset misappropriation within the Indonesian business community has necessitated the implementation of Internal Control over Financial Reporting (ICOFR) as a critical mechanism for ensuring financial reliability and safeguarding organizational stability against fraudulent activities. This paper examines the integration of fraud risk assessment (FRA) into the ICOFR framework to strengthen internal controls against fraud risks. Using a qualitative descriptive case study approach at an Indonesian energy SOE subsidiary, this research provides implementation recommendations for organizations. The study utilized focus group discussions (FGDs) and interviews to gather insights from 18 selected participants involved in ICOFR execution, ensuring data triangulation through the review of historical audit and investigation reports. Findings suggest that ICOFR, while traditionally focused on operational risk, appears to be more effective when a fraud risk assessment framework is integrated into its design. This process involves identifying specific fraud schemes within business operations, aligning them with the existing Risk Control Matrix (RCM), and performing inherent and residual risk assessments. The study confirms that such integration is feasible and appears to be effective; by utilizing the COSO Framework as a theoretical anchor, the organization successfully lowered its residual fraud risk across all business segments. Notably, the assessment validated a reduction in risk scores across ten critical business processes, effectively transitioning the company from a state of general operational control to a specialized, fraud-resilient reporting environment.

Keywords: *COSO Framework, Financial Statements, Fraud Risk, Internal Control Over Financial Reporting (ICOFR).*

How to Cite:
Kurnia, I. (2026). An Integrated Framework of Fraud Risk Assessment in ICOFR Implementation to Enhance Internal Controls Against Fraud Risks. *Asia Pacific Fraud Journal, 11*(1), 137-153. https://doi.org/10.21532/apfjournal.v11i1.463.

✉Corresponding author :
Email: indahkurnia@gmail.com

1. INTRODUCTION

Fraud is a pervasive and escalating issue in Indonesia, rising from the third to the second most significant emerging risk between 2024 and 2025 as its prevalence jumped from 50% to 59% (Institute of Internal Auditors, 2025). The most common schemes include asset misappropriation, which occurs in 89% of global cases but yields the lowest median loss, and corruption, which affects 48% of cases and severely erodes public trust and institutional effectiveness. While financial statement fraud is the rarest at only 5%, it is the most financially devastating, with a median loss of USD766,000 per case (ACFE, 2024). Ultimately, these fraudulent activities ranging from bribery and embezzlement to the manipulation of reports not only cause immense financial damage but also threaten the survival of businesses by destroying reputations and diminishing market share. Because of the significant impact on financial loss that affects financial statements, organizations should invest in robust fraud risk management and internal controls. One of the activities carried out by the organization is the implementation of internal control over financial reporting (ICOFR).

ICOFR relates to the controls established to reduce the risks associated with financial reporting. It comprises measures that provide reasonable assurance about the accuracy of a company's financial statements in compliance with IFRS. ICOFR gained significant traction globally after the Enron scandal in 2001. Before 2024, only a few Indonesian companies had implemented ICOFR due to the lack of regulations to publish their state of implementation. However, ICOFR has recently emerged as a standardamong state-owned enterprises following the introduction of the Ministry of SOE Decree (SK-5/DKU.MBU/11/2024) and OJK Regulation No. 15/2024 for these entities (Virginia & Hermawan, 2023). Research concerning the implementation of ICOFR in Indonesia during that period was primarily restricted to literature reviews and surveys focusing on the effects of internal control on different facets of fraud and financial reporting (Kristianti, 2025; Amarullah, 2025). Concurrently, extensive analyses on the incorporation of fraud risk management within ICOFR have been scarce. Examining the adoption of ICOFR in Indonesian companies and its success in curbing fraud is difficult, as there were no regulations mandating companies to report the effectiveness of their ICOFR to external parties at that time. To generalize the hypothetical theory, many researchers utilized secondary data to assess the effectiveness of ICOFR in various organizations (Bimo et al., 2019). Thus, this study aims to explore he integration of ICOFR and fraud risk managementto offer recommendations for organizations to strengthen their internal controls against fraud risks.

2. LITERATURE REVIEW AND HYPOTHESIS

In the global landscape, ICOFR has transitioned from a compliance-heavy "SOX 404" era into a phase of digital optimization. Recent studies emphasize the integration of Big Data, AI, and continuous monitoring to enhance the precision of fraud detection. Globally, the research focus is no longer just on whether controls exist, but on their sustainability and efficiency. Modern theoretical frameworks now explore "Data-Driven Internal Controls," where automated audit trails reduce the reliance on human intervention, thereby mitigating the risk of management override a primary cause of material misstatement in financial reporting (KPMG, 2024).

Conversely, the Indonesian landscape is currently defined by a regulatory surge. Following the issuance of the Ministry of SOE Decree Number SK-5/DKU. MBU/11/2024 (BUMN, 2024) and OJK Regulation Number 15/2024 (OJK, 2024), the actual number of HF hospitalizations remains >1 million annually. More than 80% of patients who are hospitalized are

initially seen in the emergency department ED, ICOFR has become a strategic mandate rather than a voluntary best practice (PwC Indonesia, 2024).

However, current Indonesian research reveals a significant maturity gap (Amarullah, 2025). Unlike global firms that focus on automation, many Indonesian organizations are still struggling with foundational issues. Key findings from 2019–2025 studies Bimo et al. (2019); Kristianti (2025); Farradhi & Hartanti (2023); Virginia & Hermawan (2023); Afifah & Siswantoro (2025); ACFE (2023); Kristianti (2025) indicate:

a. Recurring audit findings highlight overpayment, contract disecrepancies, project fraud and weak monitoring mechanism.
b. Weakness in control design to reduce misstatement and fraudulent reporting
c. Organizational complexity affected financial reporting quality.
d. A "Control Environment" that is strong on paper but weakened by high power distance and cultural reluctance to report fraud (whistleblowing lag).

While global literature provides a "Standard of Excellence," it often assumes a high level of technological maturity and institutional stability that may not exist in Indonesian corporations. On the other hand, Indonesian studies have been largely descriptive, focusing on compliance levels.

There is a profound lack of process-level insights on how Indonesian companies move from "Initial" to "Optimized" maturity. Most existing research tells us what is missing process (e.g., "no risk and control design"), but not how to effectively implement these controls within a complex, hierarchical Indonesian organizational culture that faces unique operational and fraud risks.

This study employs an exploratory case study approach to bridge this gap for several reasons:

a. Contextual Depth
   Unlike quantitative surveys, a case study allows for an in-depth exploration of the "interplay of political and bureaucratic factors that influence control behavior (Afifah & Siswantoro, 2025; Nugrahanti et al., 2023).
b. Process Mapping
   It is necessary to observe how fraud schemes are identified and mapped into a risk control matrices in real-time within an Indonesian corporate environment
c. Triangulation
   By comparing FGD results with secondary internal audit findings, this method provides a "grounded" understanding of how to implement ICOFR effectively, moving beyond symbolic compliance toward substantive financial integrity.

3. METHODS

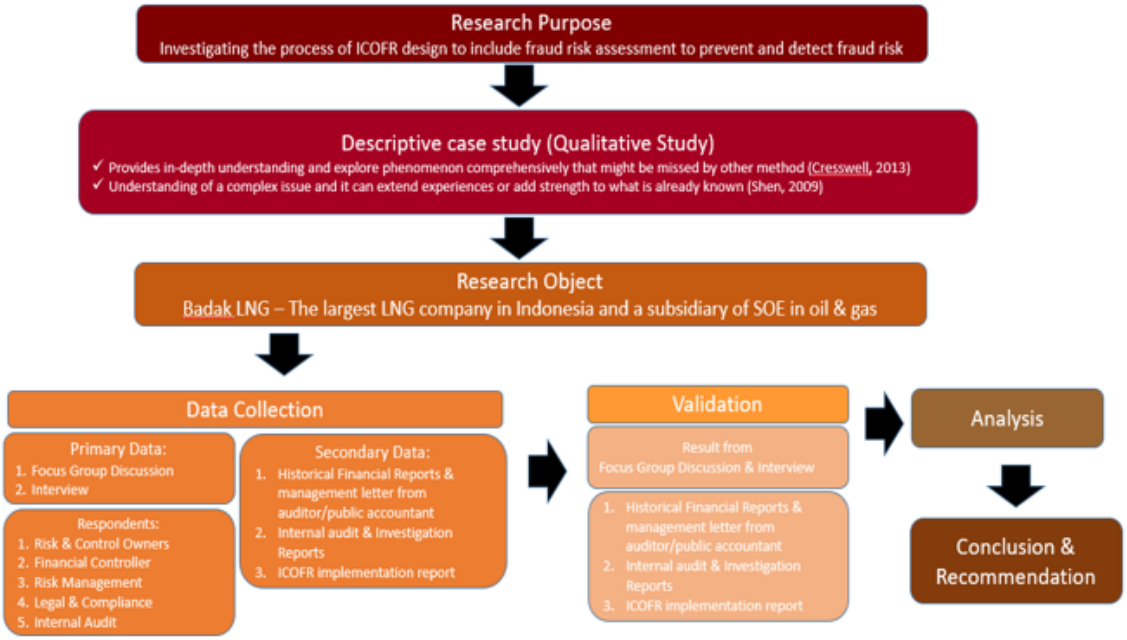
Research Methods

A descriptive case study was selected as the research method because it is suitable for research purposes to provide an in-depth understanding of what is being studied. It enables researchers to investigate a phenomenon thoroughly and reveal details and complexities that may be overlooked by alternative methodologies (Cresswell, 2013). Qualitative research yields an understanding of a complex issue and enhance existing knowledge or reinforce established insights (Lim, 2025).

The focus of this study was to investigate how fraud risk management can be implemented in the ICOFR framework. The research utilizes both primary and secondary data. Primary data were obtained by carrying out a Focus Group Discussions (FGDs) engaged key stakeholders from each department within the ICOFR task force to map business processes and identify potential fraud risks within their respective areas. FGDs and interviews with 18 Respondents from certain areas as explained in the Appendix 1.

While secondary data consisted of available documents, such as previous audited financial statements, internal control memorandum, internal audit

Figure 1. **Research Methodology**



reports, investigation reports, and related data. Data verification was performed by comparing the results of interviews and FGD with secondary data in the form of internal audit report, investigation report and audit report from external public accountants during the year of 2020 to 2025. The aim is to confirm and test the alignment between the data sources. The next stage is presenting the data to be analyzed to understand the problem, root cause, and proposed recommendations.

Research Object

This research focuses on an energy company that is a subsidiary of the state-owned enterprise (SOE) in Indonesia. The company's primary business is operating a plant and providing services to other companies. During our observation, the company has implemented ICOFR and intends to enhance its control levels to include fraud risk management. The need to improve its ICOFR implementation to incorporate fraud risk management was driven by the policies issued by its parent SOE. The company must implement ICOFR according to the regulation of the SOEs Minister Number PER-2/MBU/03/2023 concerning the guidelines for governance and risk management of SOEs, where Article 69 references the internal control system in risk management. To support this regulation, the Ministry of SOEs issued another guideline for ICOFR implementation in SOEs through SK-5/DKU.MBU/11/2024. This guideline encourages SOEs to adopt the COSO internal control framework, which comprises 5 components and 17 principles (COSO, 2013). One of COSO's principles regarding the control environment requires the company to conduct a risk assessment, including a fraud risk assessment, and to prepare control activities to mitigate the impact on financial reports.

The company has already established a complete set of ICOFR implementation, including policy and guidelines. The company implements entity-level controls, information technology general controls, and transaction-level controls that consist of 8 business process cycles, including revenue, expenditure, treasury, inventory, payroll, asset, taxation, and financial closing. The organization adopted the Three Lines Model by establishing an ICOFR task force comprising control owners (first line), a control group (second line), and internal audit (third line).

The company also conducts the design of internal controls through business process mapping (BPM) and risk control matrix (RCM), implementation of internal control and continuous monitoring, evaluation through control self-assessment (CSA), and internal audit. Afterwards, the company performed remediation activities over control weaknesses and reported the effectiveness of ICOFR. The final stage of the ICOFR cycle is providing independent assurance from the external auditor.

Data Collection

Data collection was conducted through FGD, interview, and document review for triangulation purposes. A fraud risk assessment was performed during the FGD with control owners at each section or department of the company. Data collected from respondentswere validated with the Control Group as ICOFR supervisor and Internal Auditor. All control owners explained their business process mapping (BPM) and their existing risk control matrix (RCM), and their bribery risk assessment. All control owners were requested to describe any potential fraud schemesin their BPM and review their existing RCM and perform risk assessment.

Data Analysis

Once the data has been gathered, the subsequent step involves analyzing it through a qualitative lens. The initial phase involves synthesizing business process interview results pertaining to entity-level controls (ELC), transaction-level controls (TLC), and IT general controls (ITGC). Subsequently, each process is categorized based on operational and fraud risks, as well as the efficacy of existing controls. Fraud schemes and their associated risks are then identified within each process and documented in a Risk Control Matrix (RCM). Finally, the findings are verified by triangulating the FGD results with secondary data, including internal audit findings, investigative reports, and external audits conducted by certified public accountants. This step aims to verify and assess the consistency between the various data sources. The following phase entails presenting the data in a descriptive narrative format. Finally, conclusions will be drawn to address the questions formulated for this study.

4. RESULTS AND DISCUSSION

This section presents the analysis of data gathered through FGDs with the ICOFR task force and departmental representatives. The analysis evaluates how the integration of fraud risk assessment (FRA) into the existing ICOFR framework enhances organizational resilience against fraudulent activities.

The primary objective of this study was to examine the approach for integrating fraud risk assessment into the ICOFR framework. The FGD results reveal that while the company possesses a structured control environment, the transition from general compliance to fraud-specific oversight requires a systematic mapping of business processes.

Participants identified that the most effective approach for integration involves:

a. Granular Process Mapping
   Breaking down departmental work-flows to identify custody areas where assets are most vulnerable.
b. Scenario-Based Identification
   Moving beyond checklist-style auditing to brainstorm specific fraud schemes during the Risk Control Matrix (RCM) development.
c. Cross-Functional Synergy
   FGD participants highlightedthat the ICOFR task force serves as a bridge, allowing the process owners (who understand the risks) to collaborate with control owners (who design the safeguards).

These findings provide empirical evidence for the theoretical proposition that significant opportunities exist to embed fraud risk assessment within the ICOFR infrastructure. This alignment is directly rooted in Principle 8 of the COSO 2013 Framework, which mandates that an organization must explicitly consider the potential for fraud in its risk assessment.

Figure 2. **ICOFR Governance Based On Ministry of SOEs Regulation**

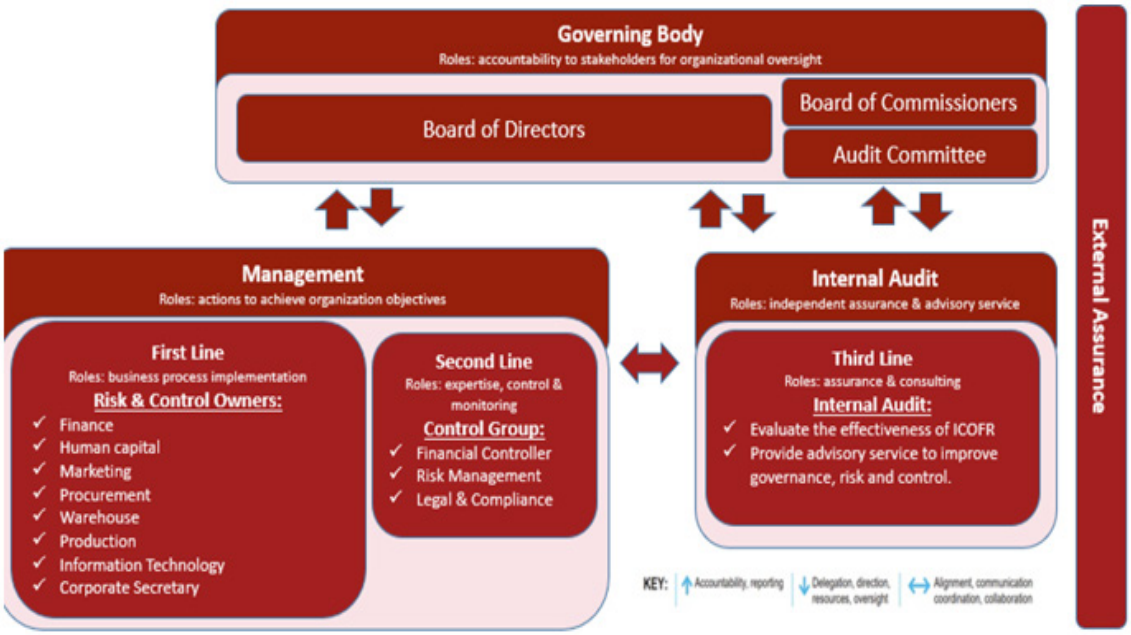
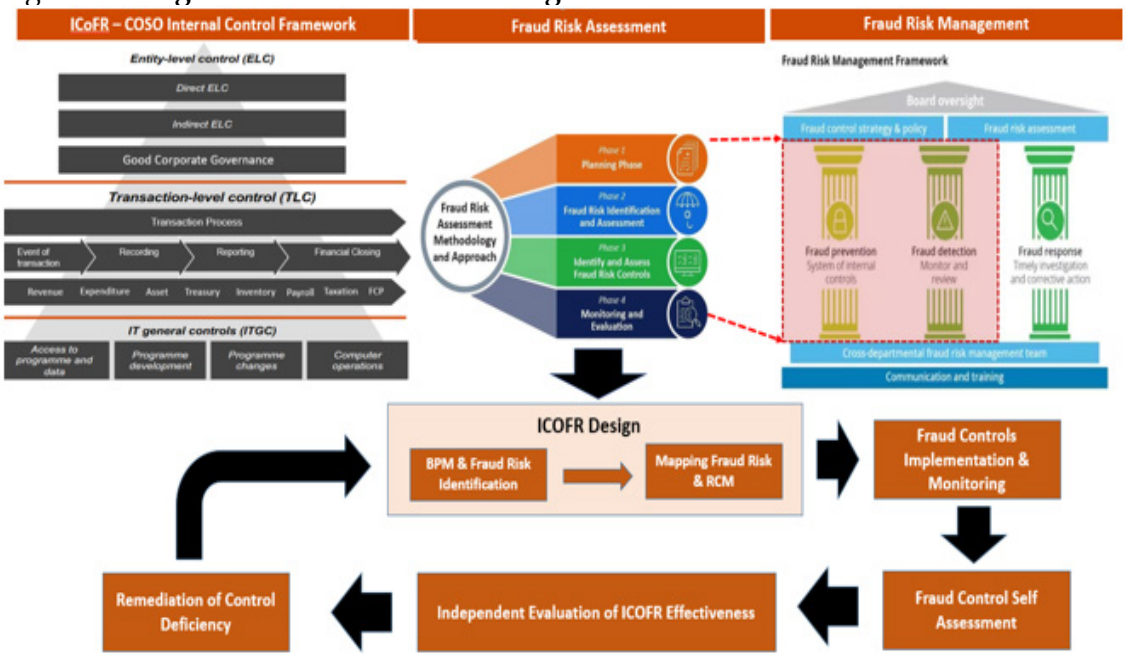


Figure 3. **Integration of Fraud Risk Management and ICOFR Framework**



The integration of FGDs into the ICOFR framework significantly shifted the organizational perception of risk from a compliance-driven exercise to a proactive, fraud-conscious methodology. Originally, the company's internal controls were centered on mitigating general operational risks and ensuring clerical accuracy in financial reporting. However, the FGDs facilitated a transition toward scenario-based identification, allowing the ICOFR task force and process owners to move beyond standard checklists and brainstorm 60 specific fraud schemes, such as fictitious contracts, procurement collusion, and ghost employees. By engaging 18 key stakeholders across various departments including revenue, expenditure, and IT the

sessions fostered cross-functional synergy. This collaborative environment bridged the gap between process owners, who possess detailed knowledge of operational vulnerabilities, and control owners, who design safeguards. Consequently, the perception of risk evolved from a "static annual audit" to a "continuous lifecycle," where the Risk Control Matrix (RCM) is viewed as a living document capable of adapting to intentional manipulation rather than just accidental errors. This aligns with the argument that ICOFR should not merely ensure clerical accuracy but must also safeguard against intentional manipulation.

The FGD findings suggests that when fraud risk identification and control is treated as a subset of ICOFR, rather than a separate silo, the organization achieves a more holistic defense. By embedding fraud assessment into the Risk Assessment component of COSO, the company moves from a reactive stance to a proactive prevent and detect methodology.

According to the data presented on Appendix 2 and Appendix 3, the implementation of three-way matching serves as a robust detective and preventive control specifically designed to neutralize complex expenditure fraud schemes such as fictitious purchasing, invoice forgery, and the manipulation of goods receipts. By systematically cross-referencing the purchase order (authorized requirement), the receiving report (actual quantity and quality delivered), and the vendor invoice (amount billed), the organization ensures that payments are only disbursed for legitimate, authorized transactions. This mechanism directly mitigates risks where employees or vendors might attempt to overstate prices, forge performance bonds, or alter bank account details, as any discrepancy between these three critical documents triggers an immediate exception for review.

The efficacy of data triangulation in this study serves as the primary mechanism for transforming subjective stakeholder insights into a validated, evidence-based internal control framework. By cross-referencing primary data from FGDs with historical secondary data such as internal audit reports, investigation reports, and external public accountant memorandums from 2020 to 2025 the research ensures that the identified fraud schemes are not merely theoretical but are grounded in actual organizational vulnerabilities. This triangulation is most evident in the analysis of the expenditure cycle, where the "three-way matching" control was identified as a critical safeguard. During FGDs, control owners identified specific expenditure fraud schemes, such as fictitious purchasing and the forgery of invoice documents. These concerns were triangulated against historical audit findings, which highlighted previous weaknesses in how goods receipts and invoices were verified. To address these validated risks, the organization implemented a rigorous three-way matching process verifying the purchase order against the goods/service handover and the vendor invoice to ensure that no payment is disbursed for unreceived or unauthorized items. Within the studied Indonesian company, this specific control when paired with a clear segregation of duties among the buyer, receiver, and payable officer appeared to be effective, contributing to a substantial reductionin the expenditure residual risk score from an inherent value of 16 to a residual value of 2 (as seen on Table 1).

The integration of a specialized fraud risk assessment into the ICOFR framework directly addresses the maturity gap prevalent in Indonesian state-owned enterprises (SOEs), where internal controls often exist as symbolic compliance rather than substantive safeguards. While global standards have moved toward digital optimization and automated audit trails, many Indonesian organizations particularly in the construction and government-related sectors continue to struggle with foundational deficiencies,

such as the absence of formal Risk Control Matrices (RCM) and the lack of systematic Tests of Effectiveness (ToE).

Current research highlights that even when a "Control Environment" appears strong on paper, it is frequently weakened by a high power distance and a cultural reluctance to report fraud. This study bridges that gap by demonstrating a transition from "Initial" to "Optimized" maturity through the following evidence-based outcomes:

a. Formalization of the RCM: By layering 60 identified fraud schemes onto the existing ICOFR infrastructure, the organization moved beyond a basic operational checklist to a specialized, "fraud-conscious" architecture.
b. Systematic Validation: The research replaced descriptive "maturity scores" with a rigorous process of triangulating FGD results against historical internal audit and investigation reports, ensuring that the RCM reflected real-world vulnerabilities.
c. Empirical Risk Reduction: The effectiveness of these controls was validated through a significant drop in risk scores; for example, the expenditure process saw its inherent risk scores decreased from 16 to a residual score of 2, confirming that the newly implemented ToE were capable of mitigating high-impact fraud schemes.

This transition underscores that closing the maturity gap in the Indonesian context requires moving away from annual audits toward a continuous lifecycle of quarterly Control Self-Assessments (CSA) and inter-departmental synergy. The overall study suggest that incorporating fraud risk assessment into the ICOFR framework is both feasible and highly effective. By utilizing the COSO Framework as a theoretical anchor, the organization successfully lowered its residual fraud risk across all business segments, moving from a state of general operational control to a specialized, fraud-resilient reporting environment.

The study offers several critical implications for corporation to treat ICOFR as a continuous lifecycle management. Managers must move away from annualaudits. The study's model of quarterly CSA ensures that the RCM remains a living document that adapts to new fraud schemes. The remediation stage should be viewed not as a failure, but as a design loop. The interdepartmental synergy is needed to achieve effective implementation. The role of the Control Group as a bridge between operational

Table 1. **Summary of Inherent and Residual Fraud Risks Assessment Validation**

Business Process	IF	IS	IR	RF	RS	RR	Remarks
Revenue	3	4	12	1	2	2	Decreasing residual risk
Expenditure	4	4	16	1	2	2	Decreasing residual risk
Treasury	3	4	12	1	2	2	Decreasing residual risk
Inventory	3	3	9	1	2	2	Decreasing residual risk
Payroll	3	4	12	1	2	2	Decreasing residual risk
Asset	3	3	9	1	2	2	Decreasing residual risk
Taxation	3	4	12	1	2	2	Decreasing residual risk
Financial Closing & Reporting	3	5	15	1	3	3	Decreasing residual risk
Information Technology	3	3	9	1	2	2	Decreasing residual risk
Entity level control	3	5	15	1	2	2	Effective to eliminate risk

Note: IF (inherent risk), IS (inherent severity), IR (inherent risk), RF (residual frequency), RS (residual severity), RR (residual risk)

Source: Processed Data

owners and Internal Audit is vital. Managers should foster this collaboration to ensure that process owners understand the reason behind fraud controls implementation.

While the case study methodology facilitates a granular, longitudinal analysis of internal control mechanisms, its idiographic nature inherently constrains the generalizability of the findings. As the data are derived from a single organizational context, the observed outcomes may be influenced by site-specific cultural or operational idiosyncrasies that lack universal applicability across diverse industries or organizational scales. Consequently, the theoretical framework developed herein for identifying fraud vulnerabilities remains exploratory. To establish broader generalizability and confirm the robustness of these propositions across varying corporate landscapes, further empirical validation via large-scale quantitative analyses or comparative multi-case designs is required.

5. CONCLUSION

This study utilizes an exploratory case study approach to bridge the existing maturity gap in Indonesian corporate governance, offering a nuanced perspective that quantitative methodologies often overlook. This study demonstrates that the integration of fraud risk assessment into the Internal Control over Financial Reporting (ICOFR) framework is not only operationally feasible but also effective in strengthening corporate governance. By adopting the COSO Framework as a definitive theoretical anchor, the organization successfully mitigated residual fraud risks across all business segments. The transition from a generalized operational control state to a specialized, fraud-resilient reporting environment underscores the strategic value of aligning process-level fraud identification with financial oversight. This approach allowed for real-time process mapping, demonstrating how specific fraud schemes were identified and integrated into a specialized Risk Control Matrix (RCM). Furthermore, the triangulation of FGD results with historical internal audit and investigation reports from 2020 to 2025 provides a validation of control efficacy. Consequently, these findings suggest that a unified framework significantly enhances the integrity of financial assertions and provides a robust defense against intentional organizational misstatements.

REFERENCES

ACFE. (2023). *Persepsi dan Implementasi Fraud Risk Management. Hasil Survei Nasional The Institute of Internal Auditors Indonesia dan Association of Certified Fraud Examiners Indonesia Chapter*. Association of Certified Fraud Examiners Indonesia.

ACFE. (2024). *The Nations Occupational Fraud 2024 : A Report to the Nations*. Association of Certified Fraud Examiners.

Afifah S, F. N., & Siswantoro, D. (2025). Evaluation of the Implementation of Internal Control of Financial Reporting (ICOFR) on Maintenance Expenditure: Case Study of State Institution "X". *Eduvest-Journal of Universal Studies, 5*(10), 12819–12836. https://doi.org/10.59188/eduvest.v5i10.51353.

Amarullah, K. (2025). Pemetaan Literatur Ilmiah Mengenai *Internal Control over Financial Reporting* (ICOFR): Pendekatan Bibliometrik Berbasis Database *Scopus*. *EKOMA: Jurnal Ekonomi, Manajemen, Akuntansi, 4*(6), 8594–8610. https://doi.org/10.56799/ekoma.v4i6.9924.

Bimo, I. D., Siregar, S. V., Hermawan, A. A., & Wardhani, R. (2019). Internal Control Over Financial Reporting, Organizational Complexity, and Financial Reporting Quality. *International Journal of Economics and Management, 13*(2), 331-342.

BUMN. (2024). *Guideline for ICOFR Implementation in SOEs through SK-5/ DKU.MBU/11/2024.* Badan Usaha Milik Negara (BUMN).

COSO. (2013). *Internal Control-Integrated Framework.* COSO. 1–20. https:// www.coso.org/Pages/ic.aspx.

Cresswell, J. W. (2013). *Qualitative Inquiry & Research Design, Third Edition*. SAGE.

Farradhi, M., & Hartanti, D. (2023). Efektivitas *Internal Control Over Financial Reporting* (ICFR) pada Project Konstruksi Perusahaan BUMN Karya. *Fair Value: Jurnal Ilmiah Akuntansi dan Keuangan, 5*(7), 3081-3094. https://journal.ikopin. ac.id/index.php/fairvalue

Institute of Internal Auditors (IIA). (2025). *Indonesia 2025 Risk In Focus. Hot Topics for Internal Auditors*. Institute of Internal Auditors Indonesia.

KPMG. (2024). *The Future of SOX : Trends in ICOFR Programs.* KPMG. https:// kpmg.com/kpmg-us/content/ dam/kpmg/pdf/2024/the-future-of-sox-icofr-trends.pdf.

Kristianti, I. (2025). Literatur Review : Dampak *Implementasi Internal Control Over Financial Reporting, Whistleblowing System* dan Internal Audit terhadap *Fraud Prevention. Media Akuntansi Perpajakan, 10*(2), 295–304. https://doi.org/10.52447/ map.v10i2.8858.

Lim, W. M. (2025). What Is Qualitative Research? An Overview and Guidelines. *Australasian Marketing Journal, 33*(2), 199–229. https://doi. org/10.1177/14413582241264619.

Nugrahanti, T. P., Sudarmanto, E., Andani, M., & Judijanto, L. (2023). The Effect of Audit Quality, Auditor Independence, and Financial Reporting Transparency on Internal Control Effectiveness: A Case Study of a Public Company in Indonesia. *West Science Accounting and Finance, 1*(03), 108–118. https://doi. org/10.58812/wsaf.v1i03.370.

OJK. (2024). *POJK No.15 Tahun 2024 concerning The Integrity of Bank Financial Report.* Otoritas Jasa Keuangan (OJK).

PwC Indonesia. (2024). *Signifikansi Internal Controls over Financial Reporting (ICOFR) dalam Lingkungan Regulasi di Indonesia.* PwC Indonesia. https://www.pwc.com/id/en/ publications/soe/internal-controls-over-financial-reporting.pdf.

Virginia, E., & Hermawan, A. A. (2023). *Contemporary Accounting Case Studies*. Article, 8(1), 150–165.

Appendix 1. **Respondents for Focus Group Discussion**

ICOFR Type	Position of Repondents	#	Experience	Gender	Edu	FGD Freq	Duration	Topic Discussion
Entity level controls	Corporate Secretary	1	3	F	B	2	2 days	BPM, RCM, FRA
	Risk Management	1	2	M	B		2 days	BPM, RCM, FRA
	Financial Control	1	1	F	B	2	2 days	BPM, RCM, FRA
	Legal & Compliance	1	1	F	B	2	2 days	BPM, RCM, FRA
	Internal Auditor	1	3	F	B	2	2 days	BPM, RCM, FRA
Information technology controls	Information Technology	1	5	M	B	2	3 days	BPM, RCM, FRA
Transaction level controls								
Revenue	Revenue Accountant	1	3	F	B	3	3 days	BPM, RCM, FRA
	Marketing	1	2	M	B	3	3 days	BPM, RCM, FRA
Expenditure	Expenditure Accountant	1	4	F	B	3	3 days	BPM, RCM, FRA
	Procurement Buyer	1	3	F	B	3	3 days	BPM, RCM, FRA
Treasury	Treasury Accountant	1	3	F	B	3	3 days	BPM, RCM, FRA
Inventory	Warehouse	1	3	M	B	3	3 days	BPM, RCM, FRA
	Financial Accountant	1	10	M	B	3	3 days	BPM, RCM, FRA
Payroll	Human Capital	1	5	F	B	3	3 days	BPM, RCM, FRA
	Payroll Accountant	1	3	F	B	3	3 days	BPM, RCM, FRA
Asset	Asset Accountant	1	3	M	B	3	3 days	BPM, RCM, FRA
Taxation	Tax Accountant	1	10	M	B	3	3 days	BPM, RCM, FRA
Financial Closing	Financial Accountant	1	10	M	B	3	3 days	BPM, RCM, FRA
	Total	18						

Note: Education: Bachelor Degree; BPM: Business Process Management; RCM: Risk Control Matrices; FRA: Fraud Risk Assessment

Source: Processed Data

Apendix 2. **Mapping of Fraud Risks Across ICOFRBusiness Processes and Key Activities**

No	ICOFR Type/Business Process	Key Activities	Fraud Risks/Schemes
1	Revenue	1. Obtain customer/ contract 2. Sales & Service delivery 3. Invoicing & billing 4. Payment receipt 5. Account receivable 6. Revenue recognition	1. Fictitious contract 2. Unrecorded sales 3. False invoice void 4. Manipulation of billing to overstate/understate sales quantity or amount. 5. Concealing uncollectable revenue 6. Unauthorized write-off of uncollectable revenue 7. Premature revenue recognition 8. Improper adjustment or estimation of accrued revenue
2	Expenditure	1. Purchase requisition 2. Supplier selection 3. Purchase order 4. Good/service receipt 5. Invoice verification 6. Payment authorization 7. Expenses recognition	9. Fictitious purchasing/expenses 10. Procurement fraud (collusion, bid rigging, kickback, conflict of interest, extortion, overstating price) 11. Manipulating goods/service receipts to alter quantity/quality/promised delivery to avoid penalty or payment deductions. 12. Forgery of invoice documents 13. Forging VAT invoice documents 14. Forging performance bond documents 15. Altered payee/bank account 16. Unauthorized expense approval 17. Mischaracterized reimbursement for personal purchase 18. Multiple reimbursements 19. Overstated expense amount 20. Improper adjustment or estimation of accrued expenses
3	Treasury	1. Cash forecast 2. Cash call 3. Bank account management 4. Manage expenses & receivable payment 5. Foreign exchange	21. Unauthorized use of the Company's e-banking account 22. Forged payment authorization 23. Cash theft 24. Check tampering 25. Deposit lapping 26. Unrecorded cash revenue 27. Foreign exchange manipulation
4	Inventory	1. Inventory planning 2. Goods receiving 3. Inventory issuing 4. Stock count	28. Fictitious inventory purchasing/ receiving/ issuing 29. Manipulating stock opname data to overstate/understate inventory quantity or value 30. Inventory theft 31. Unauthorized inventory write-off

No	ICOFR Type/Business Process	Key Activities	Fraud Risks/Schemes
5	Payroll	1. Define payroll policy 2. Data gathering 3. Input data validation 4. Statutory compliance 5. Payment distribution 6. Recording & reporting	32. Manipulation of employee data related to salary or other benefit payment 33. Ghost/fictitious employee 34. Intentional failure to deduct tax and other statutory compliance (i.e BPJS, etc) 35. Unauthorized payroll payment 36. Cash theft when distributing payroll 37. Overstate/understate payroll
6	Asset	1. Planning 2. Acquisition 3. Operation 4. Maintenance 5. Disposal	38. Overstate/understate asset capitalization 39. Unauthorized asset acquisition 40. Unauthorized asset disposal 41. Improper asset estimation & valuation 42. Asset theft 43. Asset misuse for personal purpose
6	Taxation	1. Tax planning 2. Transaction recording & tax calculation 3. Payment/provision 4. Reconciliation & adjustment 5. Recording & reporting	44. Overstated expenses 45. Understated revenue 46. Falsified tax payment document
7	Financial Closing	1. Identify event of transaction 2. Recording 3. Reporting 4. Financial closed	47. Improper asset valuation 48. Timing differences (improper period recognition of revenues and expenses) 49. Concealed liabilities and expenses 50. Fictitious revenues 51. Recording fictitious asset 52. Failure to disclose information of transactions or accounting practices that violate GAAP
8	IT General Control	1. Access to programme and data 2. Programme development 3. Programme changes 4. Computer operations	53. Violation of access control to data and applications. 54. Failure to maintain data and application integrity 55. Failure to provide data and application availability 56. Cybersecurity attack
9	Entity level control	1. Control environment 2. Risk assessment 3. Control activities 4. Information & communication 5. Monitoring activities	57. Management override 58. Conflict of interest 59. Bribery & kickback 60. Economic extortion

Source: Processed Data

Appendix 3. **Mapping Fraud Risks and Risk Control Matrices (RCM)**

No	ICOFR Type/ Business Process	Fraud Risks/Schemes	Internal Controls
1	Revenue	1. Fictitious contract from customer 2. Bribery & kickback 3. Unrecorded sales 4. False invoice void 5. Manipulation of billing to overstate/understate sales quantity or amount. 6. Concealing uncollectable revenue 7. Unauthorized write-off of uncollectable revenue 8. Premature revenue recognition 9. Improper adjustment or estimation of accrued revenue	• Match revenue transaction records with documents of contracts, evidence of goods/service handover, invoices, and receipts. • Anti-bribery management system • Perform regular reconciliation on revenue, cash, and receivables. • Segregation of duties between people to initiate billing, approve invoices, record revenue, and reconcile transactions. • Perform revenue or billing confirmation to customers. • Transaction limit for each authorization level. • Receivables and billing confirmation from customer • Accrued revenue based on GAAP rules
2	Expenditure	10. Fictitious purchasing/expenses 11. Procurement fraud (collusion, bid rigging, kickback, conflict of interest, extortion, overstating price) 12. Manipulating goods/service receipts to alter quantity/ quality/promised delivery to avoid penalties or payment deductions. 13. Forgery of invoice documents 14. Forging VAT invoice documents 15. Forging performance bond documents 16. Altered payee/bank account 17. Unauthorized expense approval 18. Mischaracterized reimbursement for personal purchase 19. Multiple reimbursements 20. Overstated expense amount 21. Improper adjustment or estimation of accrued expenses	• Perform three-way matching to verify expenditure transaction records with payment requisition documents such as contracts, evidence of goods/service handover, invoices, and receipts. • Segregation of duties between user purchase requester, estimator, buyer, and bid committee to avoid procurement fraud. • Anti-bribery management system • Segregation of duties between purchasing, goods/services receiver, and payable officer. • Perform regular reconciliation on expenses, cash payment, prepaid/ advance, and payables. • Create a checklist of supporting documents needed for expense payment. • Transaction limit for each authorization payment level. • Using the government's Core Tax application to verify VAT invoice documents • Accrued payables based on GAAP rules

No	ICOFR Type/ Business Process	Fraud Risks/Schemes	Internal Controls
3	Treasury	22. Unauthorized use of the Company's e-banking account 23. Unauthorized payment without approval 24. Cash theft 25. Check tampering 26. Deposit lapping 27. Unrecorded cash revenue 28. Foreign exchange manipulation	• Maintain access to the e-banking account only for the treasurer and authorized managers • Use multifactor authentication for e-banking, such as token or other authentication methods. • Maintain the payment limit for each authorization level. • Avoid single approval for payment. • Cashless transactions through electronic payment and maintaining records of transactions. • Segregation of duties between treasury, sales, payable and purchasing. • Enhance collaboration with banks for fraud prevention • Perform bank reconciliation regularly
4	Inventory	29. Fictitious inventory purchasing/ receiving/issuing 30. Manipulating stock opname data to overstate/understate inventory quantity or value 31. Inventory theft 32. Unauthorized inventory write-off	• Segregation of duties between the person who handle purchasing and the person who received goods/inventory and the person who issue goods/inventory. • Limit access to inventory application and data and keep user access log to be reviewed regularly. • Stock opname report should be witnessed by several people from warehouse, user, finance and auditor. • Perform inventory regular reconciliation to analyze any data inconsistencies between stock value & quantity recorded and actual condition. • Install surveillance cameras or CCTV and physical security to prevent inventory theft. • Inventory write-off should be approved by authorized person.

No	ICOFR Type/ Business Process	Fraud Risks/Schemes	Internal Controls
5	Payroll	33. Manipulation of employee data related to salary or other benefit payment 34. Ghost/fictitious employee 35. Timesheet fraud 36. Intentional failure to deduct tax and other statutory compliance (i.e BPJS, etc) 37. Unauthorized payroll payment 38. Cash theft when distributing payroll	• Limit access to employee data on HRIS and keep user access log to be checked regularly. • Increase monitoring and approval of any alteration of employee data variable input data and formula or changes in payroll application that impact to salary and benefit. • Using electronic attendance for timesheet that processed by payroll system • Perform regular payroll reconciliation to analyze any data inconsistencies. • Segregation of duties between the person who prepare payroll calculation and the person who perform payment. • Payroll calculation and payment should be verified and approved by authorized person. • Payroll distribution using registered employee bank account. Any alteration should be approved by authorized person.
6	Asset	39. Overstate/understate asset capitalization 40. Unauthorized asset acquisition 41. Unauthorized asset disposal 42. Improper asset estimation & valuation 43. Asset theft 44. Asset misuse for personal purpose	• Maintain database of asset and its capitalization value including depreciation or amortization rate. • Asset transaction approval based on authorization table. • Use certified consultant to provide accurate asset estimation & valuation. • Install surveillance cameras or CCTV and physical security to prevent inventory theft. • Clear policy for employee in order not to misuse company asset for personal purposes.
6	Taxation	45. Tax evasion and illegal tax avoidance 46. Falsified tax payment document	• Tax recording and regular tax reconciliation to match taxable transaction with actual payment. • Using tax consultant to advise appropriate tax treatment in accordance with tax regulation. • Using the government's Core Tax application.

No	ICOFR Type/ Business Process	Fraud Risks/Schemes	Internal Controls
7	Financial Closing	47. Improper asset valuation 48. Timing differences (improper period recognition of revenues and expenses) 49. Concealed liabilities and expenses 50. Fictitious revenues 51. Recording fictitious asset 52. Failure to disclose information of transactions or accounting practices that violate GAAP	• Establish accounting policy and procedures • Perform regular reconciliation of all accounts and analyze any inconsistencies. • Ensure that all transaction records are supported with appropriate documents to justify accounting treatment • Use certified consultant to provide accurate asset estimation & valuation.
8	IT General Control	53. Violation of access control to data and applications. 54. Failure to maintain data and application integrity 55. Failure to provide data and application availability 56. Cybersecurity attack	• Information security management system • Control objective for information and related technology (COBIT)
9	Entity level control	57. Management override 58. Conflict of interest 59. Bribery & kickback 60. Economic extortion	• Code of conduct • Code of good corporate governance • Board manual • Enterprise Risk Management system • Whistleblowing system • Anti-Bribery Management System

Source: Processed Data