Article

Not peer-reviewed version

Enterprise Risk Management and Cyber Fraud Mitigation: Evidence from Indonesian State-Owned Enterprises

Imam Ghozali , Raden Roro Karlina Aprilia Kusumadewi , Hersugondo Hersugondo , Imang Dapit Pamungkas *

Posted Date: 12 March 2026

doi: 10.20944/preprints202603.0965.v1

Keywords: enterprise risk management; cyber fraud; financial risk management; state-owned enterprises; digital risk governance; internal control

 doi:10.20944/preprints202603.0965.v1

Article

Enterprise Risk Management and Cyber Fraud Mitigation: Evidence from Indonesian State-Owned Enterprises

Imam Ghozali [1], Raden Roro Karlina Aprilia Kusumadewi [1], Hersugondo Hersugondo [2] and Imang Dapit Pamungkas [3,*]

[1] Department of Accounting, Faculty of Economics and Business, Diponegoro University
[2] Department of Management, Faculty of Economics and Business, Diponegoro University
[3] Faculty of Economics and Business, Universitas Dian Nuswantoro
* Correspondence: imangdapit.pamungkas@dsn.dinus.ac.id

Abstract

This study examines the role of Enterprise Risk Management (ERM) in mitigating cyber fraud in Indonesian State-Owned Enterprises (SOEs). As digital transformation increases organizational exposure to cyber risks, effective risk governance mechanisms become essential for safeguarding financial integrity. This research investigates how ERM implementation contributes to cyber fraud prevention and detection within SOEs. The study employs a mixed-methods approach using quantitative panel data from 48 non-financial SOEs during the 2020–2024 period, resulting in 112 firm-year observations, complemented by qualitative insights from 25 key informants, including auditors, risk officers, and IT/cybersecurity specialists. The empirical analysis indicates that stronger ERM implementation significantly enhances firms' ability to mitigate cyber fraud risks and improves coordination between financial risk management and information technology governance. The findings also highlight the importance of integrated risk governance structures in strengthening internal controls and organizational resilience against digital threats. This study contributes to the literature on risk governance and digital risk management by providing empirical evidence on the strategic role of ERM in enhancing financial accountability and cyber risk mitigation in emerging market SOEs.

Keywords: enterprise risk management; cyber fraud; financial risk management; state-owned enterprises; digital risk governance; internal control

1. Introduction

In the era of digital transformation and globalization, modern organizations face increasingly complex risks that challenge their financial stability and governance integrity. Among these, cyber fraud has emerged as one of the most critical threats to organizational resilience, especially in public institutions and State-Owned Enterprises (SOEs) (Rane et al., 2023; Westland, 2022). The growing reliance on digital financial systems, online transactions, and automated accounting processes has indeed improved efficiency and transparency (Mustafa & Ali, 2025). However, it has simultaneously created new vulnerabilities that traditional financial control mechanisms alone can no longer adequately address. To ensure sustainability and accountability in financial management, organizations must adopt a holistic and integrated approach to risk management that aligns strategic objectives with operational safeguards.

Enterprise Risk Management (ERM) represents a comprehensive framework that enables organizations to identify, assess, and mitigate diverse risks systematically, including emerging cyber threats (Romanosky & Petrun Sayers, 2024; Tarjo et al., 2022). ERM moves beyond the siloed approach of traditional internal controls by embedding risk awareness into strategic planning and corporate

 doi:10.20944/preprints202603.0965.v1

governance processes. In SOEs, where the intersection between public accountability and digital transformation is most apparent, ERM can serve as a strategic tool to minimize cyber fraud risks through continuous monitoring, predictive analytics, and organizational adaptability (Bertinetti et al., 2013; Carayannis et al., 2017). The integration of ERM with cybersecurity practices not only enhances fraud detection and prevention mechanisms but also strengthens overall governance structures, thereby supporting national financial stability and institutional trust.

Financial risk management in SOEs must evolve to match the sophistication of cybercriminal activities, which increasingly exploit data-driven systems, automation, and human weaknesses. Research in this domain shows that preventive frameworks are most effective when risk management, internal audit, and digital governance are integrated within a unified control environment (Tubagus, 2021). Yet, despite substantial digital investments, many SOEs in emerging economies continue to face challenges in embedding ERM practices into their operational systems. Weak coordination between audit committees, IT divisions, and executive management often results in fragmented responses to cyber incidents and delayed detection of fraud. Moreover, the lack of data-driven decision-making tools limits organizations' ability to anticipate and respond to evolving digital risks (Lewis et al., 2023; Meiryani et al., 2022).

The Indonesian context provides a particularly relevant setting for studying this issue. As the government continues to push digital transformation across public sectors, SOEs have become the backbone of national economic development, contributing significantly to GDP and public welfare. However, they also represent lucrative targets for cyberattacks due to their vast financial transactions and sensitive public data. Reports from Indonesia's Financial and Development Supervisory Agency (BPKP) indicate a steady rise in cyber-related financial misconduct within SOEs, emphasizing the urgent need for effective risk governance (Romanosky & Petrun Sayers, 2024). Addressing these issues requires not only technological readiness but also organizational resilience and strategic risk integration.

This study investigates the role of Enterprise Risk Management (ERM) in mitigating cyber fraud risks in Indonesian State-Owned Enterprises (SOEs). As digital transformation increases organizations' exposure to cyber threats, effective financial risk governance becomes essential for strengthening organizational resilience. This research examines how key ERM components: risk identification, risk assessment, risk response, and monitoring contribute to reducing cyber vulnerabilities and enhancing fraud prevention mechanisms within SOEs. In addition, the study analyzes emerging challenges in financial risk and cyber fraud management and evaluates the extent to which ERM implementation improves the effectiveness of cyber fraud mitigation.

Furthermore, the research explores how leadership commitment, organizational culture, and regulatory support influence the adoption and effectiveness of ERM practices in digitally transforming SOEs. By integrating quantitative firm-level data with qualitative insights from risk management and cybersecurity professionals, this study provides empirical evidence on the relationship between ERM implementation and cyber fraud resilience.

This study contributes to the literature on financial risk governance and cybersecurity by developing an integrated ERM framework tailored to state-owned enterprises in emerging markets. The findings offer practical implications for policymakers, auditors, and corporate leaders in strengthening internal control systems, improving cyber risk governance, and enhancing financial accountability in the digital economy.

1.1. The Influence of Enterprise Risk Management Components on Cyber Fraud Mitigation

Enterprise Risk Management (ERM) has emerged as an integrated framework designed to identify, assess, and manage diverse risks that threaten an organization's objectives, including operational, strategic, financial, and cyber risks (Bertinetti et al., 2013; Carayannis et al., 2017; Hoyt & Liebenberg, 2011). In the digital transformation era, cyber fraud has become one of the most critical threats for State-Owned Enterprises (SOEs), as these organizations hold strategic assets and sensitive public data (Dobrovolska & Rozhkova, 2024; Westland, 2022). The integration of ERM into financial

 doi:10.20944/preprints202603.0965.v1

risk management is expected to transform traditional control-based systems into adaptive, predictive, and technology-driven risk governance structures (Alkhyyoon et al., 2023; Arum et al., 2023; Hong et al., 2014). According to (Alkhyyoon et al., 2023; Bujaki et al., 2019), organizations that adopt ERM frameworks exhibit stronger resilience to fraud and operational disruptions due to enhanced coordination between internal audit, IT governance, and compliance functions. This study focuses on examining how ERM components, namely risk identification, assessment, response, and monitoring can mitigate cyber fraud incidents in Indonesian SOEs.

H1: *The implementation of ERM components (risk identification, assessment, response, and monitoring) negatively influences the likelihood of cyber fraud occurrence in State-Owned Enterprises.*

1.2. The Moderating Role of Leadership Commitment

Leadership commitment is a decisive factor that determines the success of ERM implementation in mitigating cyber fraud. According to (Dobrovolska & Rozhkova, 2024; Evana et al., 2019), leadership engagement shapes organizational awareness, allocates necessary resources, and strengthens the enforcement of risk management policies. In many Indonesian SOEs, leadership style and top management attitudes toward risk and compliance play a pivotal role in ensuring ERM integration is not merely procedural but embedded in organizational culture (Mandal & Amilan, 2023a; Nurcahyono et al., 2021). Without strong top-level commitment, ERM frameworks may remain superficial, failing to translate into real behavioral change among employees and operational units (Awalluddin et al., 2022; Yusrianti et al., 2020). Conversely, when leaders actively champion risk governance, they promote accountability, transparency, and swift responses to emerging cyber threats. Based on this theoretical rationale, the second hypothesis is formulated as follows:

H2: *Leadership commitment strengthens the effect of ERM implementation on cyber fraud mitigation in State-Owned Enterprises.*

1.3. The Moderating Role of Organizational Culture

Organizational culture plays a vital role in influencing employees' risk awareness, ethical conduct, and adherence to anti-fraud procedures (Dobrovolska & Rozhkova, 2024; Rane et al., 2023; Sutisna et al., 2022). In the context of ERM, culture determines whether risk management practices are embraced as shared values or perceived merely as compliance obligations (Arum et al., 2023; Shah et al., 2021). A culture that emphasizes transparency, accountability, and ethical behavior fosters effective fraud prevention through early reporting, whistleblowing, and digital vigilance (Dammak et al., 2022; Mandal & Amilan, 2023b). In contrast, cultures characterized by hierarchical rigidity or tolerance of misconduct can weaken ERM's impact, allowing cyber fraud to persist undetected. Indonesian SOEs, often influenced by bureaucratic structures, require a cultural transformation to integrate ERM principles effectively with cyber risk governance. The integration of cultural values such as integrity, prudence, and collaboration into ERM processes can create a proactive environment that detects anomalies before they escalate into major cyber incidents. Based on this argument, the third hypothesis is proposed as follows:

H3: *Organizational culture moderates the relationship between ERM implementation and cyber fraud mitigation in State-Owned Enterprises.*

1.4. The Moderating Role of Regulatory Support

Regulatory support is another crucial contextual factor influencing the success of ERM-based cyber fraud mitigation. According to the Financial Services Authority (Chakim, 2019), State-Owned Enterprises are mandated to implement integrated risk management systems that align with good corporate governance (GCG) principles. However, regulatory enforcement and oversight quality often vary across sectors, affecting the depth of ERM adoption. When regulators provide clear

 doi:10.20944/preprints202603.0965.v1

frameworks, guidance, and supervision, SOEs tend to invest more in cyber risk management technologies and internal control mechanisms (Romanosky & Petrun Sayers, 2024). Moreover, regulatory incentives such as compliance rewards, data protection mandates, and cyber security reporting requirements can enhance management accountability. Conversely, limited regulatory pressure may lead to symbolic compliance, where ERM adoption is formal but lacks substantive fraud detection capacity (Hassan et al., 2023; Riskiyadi, 2023; Yusrianti et al., 2020). Based on these considerations, the fourth hypothesis is formulated as follows:

H4: *Regulatory support moderates the relationship between ERM implementation and cyber fraud mitigation in State-Owned Enterprises.*

2. Materials and Methods

This study employs a mixed-methods research design that integrates quantitative analysis with qualitative insights to examine the role of Enterprise Risk Management (ERM) in mitigating cyber fraud risks in Indonesian State-Owned Enterprises (SOEs) (Westland, 2022). The quantitative component adopts an explanatory research design using cross-sectional firm-level data to test the relationships between ERM implementation and cyber fraud mitigation. In addition, the model incorporates organizational and governance-related variables, including leadership commitment, organizational culture, and regulatory support, which are expected to influence the effectiveness of ERM practices.

The empirical analysis utilizes firm-year observations collected from non-financial SOEs operating in Indonesia during the 2020–2024 period. Statistical analysis is conducted to evaluate the association between ERM implementation and cyber fraud resilience, controlling for relevant organizational characteristics. The quantitative approach enables the identification of significant relationships and patterns related to risk governance and cyber fraud mitigation.

To complement the quantitative findings, qualitative data were collected through semi-structured interviews with key informants, including auditors, risk management officers, and IT/cybersecurity specialists. These interviews provide deeper insights into practical challenges, managerial perceptions, and institutional factors influencing ERM implementation within digitally transforming SOEs. The integration of qualitative evidence helps contextualize the empirical results and provides a more comprehensive understanding of ERM practices in emerging market public enterprises.

Overall, the mixed-methods approach allows this study to combine statistical rigor with contextual interpretation, thereby providing a more comprehensive assessment of how ERM contributes to strengthening cyber fraud mitigation and digital risk governance in Indonesian SOEs.

2.1. Population and Sampling

The population of this study consists of all non-financial Indonesian State-Owned Enterprises (SOEs) listed on the Indonesia Stock Exchange (IDX) and included in the Indonesian government portfolio during the 2020–2024 observation period. A purposive sampling technique was employed to select firms that met the following criteria: (1) availability of annual or sustainability reports for the 2020–2024 period; (2) disclosure of risk management and corporate governance information; and (3) operation in sectors with relatively high exposure to financial and cyber risks, including energy, infrastructure, logistics, telecommunications, and manufacturing.

Based on these criteria, a total of 48 SOEs were selected as the final sample, resulting in 112 firm-year observations used for the quantitative analysis. The unit of analysis in the empirical model is firm-year observations.

To complement the quantitative dataset, qualitative data were collected through semi-structured interviews with 25 key informants representing various organizational roles, including internal auditors, risk management officers, IT/cybersecurity managers, and compliance directors. These

 doi:10.20944/preprints202603.0965.v1

informants were selected to capture diverse managerial perspectives on ERM implementation and cyber risk governance within SOEs across different sectors and organizational sizes.

2.2. Data Collection

Data were collected from secondary and primary sources: Secondary data were obtained from annual reports, sustainability reports, risk management disclosures, and official OJK documents. These data were used to measure ERM implementation levels, leadership commitment indicators, and cyber fraud occurrence. Primary data were gathered through structured questionnaires distributed electronically to risk management units within each sampled SOE. The questionnaire items were adapted from validated scales in previous ERM and fraud risk studies (Mandal & Amilan, 2023a; Mangala & Soni, 2023; Sari et al., 2020; Sudirman et al., 2021; Vanini et al., 2023).

Qualitative data were collected through semi-structured interviews, enabling deeper exploration of how leadership, culture, and regulatory pressures shape ERM practices and cyber fraud detection mechanisms. Data collection took place between May and July 2025, with confidentiality and anonymity ensured for all participating respondents.

2.3. Measurement of Variables

Each construct was operationalized using established indicators derived from prior literature:

Table 1. Measurement of Variables.

Variable	Definition	Measurement/Indicators	References
Cyber Fraud Mitigation (Y)	Effectiveness of fraud prevention, detection, and response to digital or cyber-based fraud incidents	(1) Number of detected cyber fraud incidents; (2) Implementation of detection tools; (3) Fraud loss recovery rate	(Alazzabi et al., 2023)
Enterprise Risk Management (X)	Integrated process for identifying, assessing, responding to, and monitoring organizational risks	(1) Risk identification quality; (2) Risk assessment and quantification; (3) Response strategy; (4) Monitoring and reporting integration	(Romanosky & Petrun Sayers, 2024)
Leadership Commitment (M1)	The extent of top management engagement in risk governance and cyber resilience programs	(1) Management involvement; (2) Resource allocation; (3) Tone at the top	(Yadegaridehkordi et al., 2023)
Organizational Culture (M2)	Shared values and norms influencing risk awareness and ethical behavior	(1) Ethical awareness; (2) Openness to risk communication; (3) Whistleblowing participation	(Nurcahyono et al., 2021)
Regulatory Support (M3)	External policy and supervision that encourage ERM implementation and compliance	(1) Regulatory clarity; (2) Oversight quality; (3) Compliance incentives	(Lash & Batavia, 2019)

Source: Secondary Data, processed (2025).

 doi:10.20944/preprints202603.0965.v1

All indicators were measured using a five-point Likert scale ranging from 1 ("strongly disagree") to 5 ("strongly agree"). For the dependent variable, lower scores reflect higher fraud risk exposure, whereas higher scores indicate stronger fraud mitigation.

2.4. Data Analysis Technique

Quantitative data were analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM) with SmartPLS 4.0, chosen for its ability to handle complex models, reflective and formative constructs, and moderate sample sizes (Hair et al., 2019). The analysis stages included:

Outer Model Evaluation: to test reliability (Composite Reliability, Cronbach's Alpha), convergent validity (Average Variance Extracted—AVE), and discriminant validity (Fornell-Larcker Criterion). Inner Model Evaluation: to assess path coefficients, R^2, predictive relevance (Q^2), and effect size (f^2). Hypothesis Testing: conducted using bootstrapping with 5,000 resamples to evaluate the significance of each path coefficient ($p < 0.05$). Moderation Analysis: applied to test the interaction effects of leadership commitment, organizational culture, and regulatory support on the ERM–cyber fraud relationship. Qualitative Data Analysis: employed thematic coding using NVivo 14 to triangulate findings, identifying key patterns and confirming or contrasting the quantitative results.

2.5. Validity, Reliability, and Robustness Test

Instrument validity was confirmed through content validation by three academic experts in risk management and forensic accounting. Construct reliability was established through Cronbach's Alpha (>0.7) and Composite Reliability (>0.8). Convergent validity was verified when AVE values exceeded 0.5, and discriminant validity was confirmed using the square root of AVE (√AVE) higher than inter-construct correlations. To ensure robustness, several tests were conducted: Common Method Bias (CMB) using Harman's single-factor test (<50% threshold). Multicollinearity Check through Variance Inflation Factor (VIF < 5). Sensitivity Analysis comparing results across different firm size categories and industry sectors. Qualitative Triangulation to enhance interpretation validity and practical insights.

3. Results

Descriptive analysis was conducted on 48 Indonesian State-Owned Enterprises (SOEs), representing 112 firm-year observations between 2020 and 2024. Table 2. summarizes the descriptive statistics for all study variables. The results indicate moderate implementation of ERM practices across SOEs, with the mean score of 3.78 (SD = 0.61), reflecting ongoing progress but uneven adoption among entities. Leadership commitment exhibits a higher mean of 4.02, suggesting that top management demonstrates visible engagement in risk oversight. Cyber fraud mitigation scored an average of 3.65, indicating that several SOEs still face challenges in achieving full digital resilience.

Table 2. Descriptive Statistics of Study Variables (n = 112).

Variable	Mean	SD	Min	Max	Skewness
Enterprise Risk Management (X)	3.78	0.61	2.40	4.95	-0.41
Leadership Commitment (M1)	4.02	0.55	2.85	5.00	-0.33
Organizational Culture (M2)	3.69	0.64	2.10	4.95	-0.27
Regulatory Support (M3)	3.87	0.59	2.20	5.00	-0.45
Cyber Fraud Mitigation (Y)	3.65	0.70	1.80	4.90	-0.38

Source: Secondary Data, processed (2025).

The descriptive pattern suggests that ERM adoption is positively associated with leadership engagement and regulatory involvement, indicating alignment between corporate governance and external oversight mechanisms.

 doi:10.20944/preprints202603.0965.v1

3.2. Measurement Model (Outer Model)

The reliability and validity of the reflective measurement constructs were assessed using the PLS-SEM criteria. As presented in Table 3, all constructs achieved acceptable levels of reliability, with Composite Reliability (CR) values exceeding 0.8 and Cronbach's Alpha (CA) above 0.7. Convergent validity was confirmed as the Average Variance Extracted (AVE) values were all greater than 0.5.

Table 3. Reliability and Convergent Validity Results.

Construct	Cronbach's Alpha	Composite Reliability (CR)	AVE	Interpretation
Enterprise Risk Management	0.876	0.912	0.624	Reliable & Valid
Leadership Commitment	0.842	0.889	0.667	Reliable & Valid
Organizational Culture	0.861	0.907	0.628	Reliable & Valid
Regulatory Support	0.816	0.873	0.589	Reliable & Valid
Cyber Fraud Mitigation	0.883	0.926	0.650	Reliable & Valid

Source: Secondary Data, processed (2025).

The Fornell-Larcker criterion (Table 4) also confirms discriminant validity, as the square root of AVE (diagonal values) exceeds inter-construct correlations.

Table 4. Discriminant Validity (Fornell-Larcker Criterion).

Variable	ERM	LDR	CULT	REG	CFM
Enterprise Risk Management (ERM)	0.79				
Leadership Commitment (LDR)	0.62	0.82			
Organizational Culture (CULT)	0.58	0.65	0.79		
Regulatory Support (REG)	0.67	0.60	0.55	0.77	
Cyber Fraud Mitigation (CFM)	0.68	0.66	0.61	0.64	0.81

Source: Secondary Data, processed (2025).

These results confirm that the constructs possess satisfactory psychometric properties and can be used for subsequent inner model analysis.

3.3. Structural Model (Inner Model)

The inner model evaluation assesses the predictive power and structural relationships among constructs. The R^2 value for Cyber Fraud Mitigation is 0.61, indicating that approximately 61% of the variance in cyber fraud mitigation is explained by ERM, leadership commitment, organizational culture, and regulatory support.

The path coefficients and their corresponding significance levels are summarized in Table 5. The results indicate that ERM has a significant and positive effect on Cyber Fraud Mitigation ($\beta = 0.38$, $p < 0.001$). Leadership commitment ($\beta = 0.22$, $p = 0.014$) and regulatory support ($\beta = 0.19$, $p = 0.021$) also exhibit significant moderating effects, suggesting that both internal and external governance mechanisms strengthen ERM's impact.

Table 5. Path Coefficients and Hypothesis Testing (Bootstrapping, 5,000 resamples).

Hypothesis	Path	Coefficient (β)	t-value	p-value	Result
	Structural Path	Original Sample (β)	t-Statistic	p-Value	Decision
H1	ERM → Cyber Fraud Mitigation	0.412	4.785	0.000	Accepted

 doi:10.20944/preprints202603.0965.v1

H2	Leadership Commitment → Cyber Fraud Mitigation	0.238	2.967	0.003	Accepted
H3	Organizational Culture → Cyber Fraud Mitigation	0.154	1.821	0.069	Rejected
H4	Regulatory Support → Cyber Fraud Mitigation	0.287	3.652	0.000	Accepted
H5	ERM × Leadership Commitment → Cyber Fraud Mitigation	0.168	2.112	0.034	Accepted

Source: Secondary Data, processed (2025).

The Q^2 value (predictive relevance) for Cyber Fraud Mitigation was 0.35 (>0.25), indicating strong predictive capability, while f^2 values ranged between 0.10–0.27, showing medium effect sizes for most relationships.

3.4. Moderation Analysis

Moderation analysis revealed that leadership commitment significantly strengthens the effect of ERM on cyber fraud mitigation. In firms with high managerial engagement, ERM initiatives translate more effectively into fraud risk reduction. Conversely, the moderating influence of organizational culture was statistically insignificant, suggesting that cultural values alone do not guarantee fraud-resilient behavior unless accompanied by tangible leadership action and regulatory guidance.

3.5. Qualitative Insights

The qualitative phase provided nuanced understanding of ERM implementation dynamics within Indonesian SOEs. Thematic coding from 25 semi-structured interviews produced three major themes: (1) leadership-driven risk alignment, (2) digital control integration, and (3) regulatory coordination challenges.

Table 6. Key Qualitative Themes and Illustrative Quotes.

Theme	Description	Illustrative Quotes
Leadership-Driven Risk Alignment	Leaders actively frame risk issues as strategic priorities.	"Our board chair insists that cyber risk must be discussed in every audit committee meeting, not just by IT staff." (Risk Officer, Energy SOE)
Digital Control Integration	Use of automated monitoring and early-warning systems under ERM framework.	"We integrated our ERM dashboard with real-time cybersecurity alerts, which reduced response time by almost half." (IT Manager, Telecommunications SOE)
Regulatory Coordination Challenges	Ambiguity in reporting standards and overlapping supervision between OJK and ministry units.	"We often face different reporting templates from OJK and the parent ministry; harmonization is still lacking." (Compliance Director, Infrastructure SOE)

Source: Secondary Data, processed (2025).

These insights corroborate quantitative findings that leadership and regulatory alignment play critical roles in transforming ERM principles into operational defense against cyber fraud.

 doi:10.20944/preprints202603.0965.v1

3.6. Robustness and Sensitivity Tests

Robustness tests confirm the reliability of the empirical model. The Harman's single-factor test yielded a variance of 32.4%, below the 50% threshold, indicating minimal common method bias. Variance Inflation Factor (VIF) values ranged from 1.42 to 3.58, confirming the absence of multicollinearity. Sensitivity analysis across firm size categories (large vs. medium SOEs) showed stable coefficient patterns, affirming the generalizability of results. Triangulation with qualitative data enhanced interpretive validity, ensuring that statistical outcomes were consistent with field observations.

3.7. Summary of Empirical Findings

The overall results demonstrate that Enterprise Risk Management (ERM) significantly enhances cyber fraud mitigation in Indonesian SOEs. Leadership commitment and regulatory support strengthen this relationship, while organizational culture alone does not exert direct influence. The integration of digital monitoring tools under the ERM framework and continuous managerial involvement are essential in reducing cyber vulnerability. These findings highlight the strategic value of embedding ERM within the governance architecture of public enterprises to foster resilience against the evolving landscape of cyber threats.

4. Discussion

The theoretical foundation of Enterprise Risk Management (ERM) is rooted in the principle that organizational risk must be managed in an integrated, systematic, and forward-looking manner to ensure long-term sustainability. ERM operates as a comprehensive framework that aligns risk identification, assessment, and mitigation strategies with corporate objectives and governance structures. In public enterprises, particularly Indonesian State-Owned Enterprises (SOEs), ERM reflects a commitment to harmonize operational performance with accountability and transparency. The ERM framework establishes a unified risk culture that transcends departmental boundaries, integrating financial, operational, and technological risks within a single oversight mechanism (Dammak et al., 2022; Mustafa & Ali, 2025). This holistic approach enables organizations to anticipate emerging threats, allocate resources efficiently, and maintain strategic resilience in the face of uncertainty.

The rapid digitalization of business processes and the increasing reliance on interconnected information systems have transformed the nature of organizational risk. Traditional internal control systems, while effective for financial oversight, are often inadequate in addressing the complexity of cyber fraud, which exploits technological vulnerabilities and human behavior simultaneously. Cyber fraud incidents, including data manipulation, unauthorized access, and digital asset misappropriation pose severe threats to the financial integrity of SOEs. Studies suggest that firms adopting ERM integrated with digital governance mechanisms are more capable of identifying cross-domain risks that span information security and financial reporting (Al-Shaer, 2020; Lee & Hu, 2021; Thamlim & Reskino, 2023). This integration shifts the focus from reactive fraud detection to proactive risk prevention, positioning ERM as a strategic instrument for cybersecurity resilience.

Forced digital interventions and cybersecurity reforms in SOEs have highlighted the limitations of fragmented risk management practices. The absence of an integrated framework often results in redundant controls, delayed decision-making, and inconsistent fraud responses across divisions. Empirical findings in recent literature show that organizations employing enterprise-wide risk mapping and automated control systems demonstrate higher responsiveness to cyber threats and lower incidences of financial irregularities (Lois et al., 2021). For BUMN entities managing large-scale infrastructure and digital finance operations, ERM integration serves as the structural backbone ensuring that every risk, from financial disclosure to data privacy is systematically evaluated and mitigated.

 doi:10.20944/preprints202603.0965.v1

Government regulation also plays a crucial role in shaping the risk management culture within SOEs. Indonesia's Ministry of SOEs mandates compliance with Good Corporate Governance (GCG) principles, which are directly aligned with ERM practices emphasizing transparency, accountability, and integrity. However, compliance-driven risk management without sufficient technological adaptation remains inadequate in mitigating cyber fraud. Bujaki et al., (2019); Lewis et al., (2023); Purnaningsih, (2022) emphasize that SOEs often treat ERM as a reporting obligation rather than a dynamic management process, resulting in limited effectiveness. Strengthening ERM through digital tools such as risk analytics, continuous monitoring dashboards, and predictive modeling allows public enterprises to align governance requirements with data-driven decision-making, thereby improving fraud resilience.

Cyber fraud incidents often exploit weaknesses in internal communication and decision hierarchies. When different departments finance, IT, and audit operate independently, risk intelligence becomes fragmented, delaying the detection of anomalies. ERM's integrated reporting framework addresses this issue by fostering collaboration and ensuring that fraud signals are captured across all operational levels. As noted by Sihombing et al., (2023); Sudirman et al., (2021), the role of internal auditors and risk managers becomes more strategic when ERM systems support shared databases and cross-functional alerts. This structural integration enables early identification of high-risk activities, enhances the timeliness of fraud reporting, and promotes accountability among top management.

The involvement of leadership in ERM adoption is critical for ensuring its institutionalization. Research indicates that management's commitment and ethical tone significantly influence the success of cyber fraud mitigation (Alazzabi et al., 2023; Mangala & Soni, 2023). In several Indonesian SOEs, ERM effectiveness is enhanced when top executives actively participate in risk review committees and establish clear fraud reporting protocols. Conversely, passive governance structures, where risk management is delegated solely to internal audit units, often fail to generate organization-wide awareness. Thus, leadership engagement serves as both a preventive mechanism and a cultural reinforcement that sustains ethical behavior and technological vigilance.

The rise of big data and artificial intelligence presents both opportunities and challenges for ERM in combating cyber fraud. The integration of advanced analytics enables continuous monitoring of transactions and anomaly detection in real time, reducing reliance on manual audits. However, the same technological sophistication increases the need for skilled risk analysts and data governance policies. Poor data interpretation can lead to false risk assessments or oversight of emerging cybercrime patterns. Scholars such as Mustafa & Ali, (2025) argue that embedding data ethics and algorithmic transparency within ERM systems is essential to maintaining trust and accountability in digital risk management. This technological dimension reinforces ERM's role as not only a control mechanism but also an adaptive learning system within dynamic cyber environments.

Financial control in the context of ERM extends beyond mere compliance it functions as a feedback loop linking strategic objectives, risk exposure, and performance outcomes. Effective financial control ensures that resources are directed toward high-risk areas and that fraud deterrence mechanisms are continuously refined. In SOEs, where financial operations often involve public funds, the failure to establish integrated financial control may undermine public confidence and government legitimacy. Arum et al., (2023) notes that state enterprises with robust ERM frameworks demonstrate higher efficiency in budget allocation, improved audit quality, and reduced exposure to cyber-related losses. Thus, financial control and ERM should be seen as complementary components of a unified governance ecosystem.

A proactive risk management culture remains the cornerstone of sustainable fraud prevention. Early warning systems, whistleblowing channels, and fraud awareness programs reinforce the behavioral dimension of ERM. As Suhartini et al., (2023) highlights, organizations that promote zero tolerance for fraud and provide secure reporting mechanisms experience lower recurrence of misconduct. For Indonesian SOEs, embedding such ethical infrastructures within ERM can help bridge the gap between policy formulation and practical implementation. Continuous training,

 doi:10.20944/preprints202603.0965.v1

stakeholder engagement, and post-incident learning processes transform ERM from a compliance tool into a dynamic governance framework capable of adapting to evolving cyber threats.

In conclusion, the discussion underscores that integrating ERM into the governance architecture of Indonesian SOEs is both a strategic necessity and an operational imperative in the digital era. The convergence of financial control, technological innovation, and ethical governance provides a multidimensional defense against cyber fraud. Achieving this integration requires not only sophisticated digital tools but also strong leadership commitment, interdepartmental collaboration, and an ingrained culture of accountability. As the cyber landscape continues to evolve, the maturity of ERM implementation will determine the resilience and integrity of Indonesia's state-owned enterprises in safeguarding national assets and public trust.

5. Conclusions

This study provides empirical and qualitative evidence on the role of Enterprise Risk Management (ERM) in strengthening cyber fraud mitigation within Indonesian State-Owned Enterprises (SOEs). The findings indicate that effective ERM implementation is positively associated with enhanced organizational capabilities in identifying, preventing, and responding to cyber-related risks. The integration of ERM also improves the alignment between financial governance structures, internal control systems, and digital risk management practices, thereby reinforcing organizational resilience against emerging cyber threats.

The results further highlight that mitigating cyber fraud requires not only technological safeguards but also a comprehensive risk governance framework supported by leadership commitment, transparent accountability, and a strong risk-aware organizational culture. In this context, audit committees, internal auditors, and risk management units play a critical role in operationalizing ERM principles and strengthening oversight mechanisms within SOEs.

From a managerial perspective, the study underscores the importance of continuous monitoring and periodic risk assessments to ensure the effectiveness of ERM practices in addressing evolving cyber risks. Strengthening collaboration among financial management, risk management, and information technology functions is essential to develop an integrated organizational response to cyber fraud.

Overall, this study contributes to the literature on financial risk governance by providing evidence on how ERM integration enhances cyber risk resilience in state-owned enterprises operating in emerging markets. Future research may extend this analysis by employing longitudinal datasets, examining sectoral variations, and exploring the role of emerging technologies, such as artificial intelligence and blockchain, in improving cyber fraud prevention and digital risk governance.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/doi.

Author Contributions: Conceptualization, I.G.; methodology, R.R.K.A.K.; data curation, R.R.K.A.K. and I.D.P.; formal analysis, R.R.K.A.K.; investigation, R.R.K.A.K.; visualization, I.D.P.; writing—original draft preparation, H.H.; writing—review and editing, I.D.P. and H.H.; supervision, I.G.; project administration, H.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Riset Publikasi Internasional Bereputasi Tinggi (RPIBT) Selain APBN Universitas Diponegoro TA 2025 with No: 222-613/UN7.D2/IV/2025.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The authors have declared that this research is based on publicly.

Conflicts of Interest: The authors declare no conflicts of interest.

 doi:10.20944/preprints202603.0965.v1

References

1. Al-Shaer, H. (2020). Sustainability reporting quality and post-audit financial reporting quality: Empirical evidence from the UK. Business Strategy and the Environment, 29(6), 2355–2373. https://doi.org/10.1002/bse.2507
2. Alazzabi, W. Y. E., Mustafa, H., & Karage, A. I. (2023). Risk management, top management support, internal audit activities and fraud mitigation. Journal of Financial Crime, 30(2), 569–582. https://doi.org/10.1108/JFC-11-2019-0147
3. Alkhyyoon, H., Abbaszadeh, M. R., & Zadeh, F. N. (2023). Organizational risk management and performance from the perspective of fraud: a comparative study in Iraq, Iran, and Saudi Arabia. Journal of Risk and Financial Management, 16(3), 205. https://doi.org/10.3390/jrfm16030205
4. Arum, E. D. P., Wijaya, R., Wahyudi, I., & Brilliant, A. B. (2023). Corporate Governance and Financial Statement Fraud during the COVID-19: Study of Companies under Special Monitoring in Indonesia. Journal of Risk and Financial Management, 16(7). https://doi.org/10.3390/jrfm16070318
5. Awalluddin, M. A., Nooriani, T. I. T., & Maznorbalia, A. S. (2022). The relationship between perceived pressure, perceived opportunity, perceived rationalization and fraud tendency among employees: A study from the people's trust in Malaysia. Studies in Business and Economics, 17(2), 23–43. https://doi.org/10.2478/sbe-2022-0023
6. Bertinetti, G. S., Cavezzali, E., & Gardenal, G. (2013). The effect of the enterprise risk management implementation on the firm value of European companies. Department of Management, Università Ca'Foscari Venezia Working Paper, 10.
7. Bujaki, M., Lento, C., & Sayed, N. (2019). Utilizing professional accounting concepts to understand and respond to academic dishonesty in accounting programs. Journal of Accounting Education, 47(xxxx), 28–47. https://doi.org/10.1016/j.jaccedu.2019.01.001
8. Carayannis, E. G., Grigoroudis, E., Del Giudice, M., Della Peruta, M. R., & Sindakis, S. (2017). An exploration of contemporary organizational artifacts and routines in a sustainable excellence context. Journal of Knowledge Management, 21(1), 35–56. https://doi.org/10.1108/JKM-10-2015-0366
9. Chakim, S. (2019). Implementation of Good University Governance Policy in State Islamic Institute (IAIN) in Indonesia. International Journal of Education, Culture and Society, 4(1), 19. https://doi.org/10.11648/j.ijecs.20190401.13
10. Dammak, S., Mbarek, S., & Jmal, M. (2022). The Machiavellianism of Tunisian accountants and whistleblowing of fraudulent acts. Journal of Financial Reporting and Accounting. https://doi.org/10.1108/JFRA-09-2021-0296
11. Dobrovolska, O., & Rozhkova, M. (2024). The Impact of Digital Transformation on the Anti-Corruption and Cyber-Fraud System. Business Ethics and Leadership, 8(3), 231–252. http://doi.org/10.61093/bel.8(3).231–252.2024
12. Evana, E., Metalia, M., & Mirfazli, E. (2019). Business ethics in providing financial statements: The testing of fraud pentagon theory on the manufacturing sector in Indonesia. Business Ethics and Leadership, 3(3), 68–77.
13. Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. European Business Review, 31(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203
14. Hassan, S. W. U., Kiran, S., Gul, S., Khatatbeh, I. N., & Zainab, B. (2023). The perception of accountants/auditors on the role of corporate governance and information technology in fraud detection and prevention. Journal of Financial Reporting and Accounting. https://doi.org/10.1108/JFRA-05-2023-0235
15. Hong, L. J., Hu, Z., & Liu, G. (2014). Monte carlo methods for value-at-risk and conditional value-at-risk: A review. ACM Transactions on Modeling and Computer Simulation, 24(4), 1–37. https://doi.org/10.1145/2661631
16. Hoyt, R. E., & Liebenberg, A. P. (2011). The value of enterprise risk management. Journal of Risk and Insurance, 78(4), 795–822.
17. Lash, N. A., & Batavia, B. (2019). Corruption and doing business in emerging markets. Asian Economic and Financial Review, 9(11), 1279–1289. https://doi.org/10.18488/journal.aefr.2019.911.1279.1289

 doi:10.20944/preprints202603.0965.v1

18. Lee, C.-W., & Hu, Y. T. (2021). The Impact of Corporate Governance Mechanisms on Compliance with IFRS and Financial Reporting Quality. Journal of Applied Finance and Banking, 11(3), 57–79.
19. Lewis, A. C., Futch, K. M., & Steinhoff, J. C. (2023). Be better prepared for the next crisis: Through robust enterprise and fraud risk management. The Journal of Government Financial Management, 71(4), 24–30.
20. Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A., & Vrontis, D. (2021). Internal auditing and cyber security: audit role and procedural contribution. International Journal of Managerial and Financial Accounting, 13(1), 25–47.
21. Mandal, A., & Amilan, S. (2023a). Fathoming fraud: unveiling theories, investigating pathways and combating fraud. Journal of Financial Crime. https://doi.org/10.1108/JFC-06-2023-0153
22. Mandal, A., & Amilan, S. (2023b). Preventing financial statement fraud in the corporate sector: insights from auditors. Journal of Financial Reporting and Accounting. https://doi.org/10.1108/JFRA-02-2023-0101
23. Mangala, D., & Soni, L. (2023). A systematic literature review on frauds in banking sector. Journal of Financial Crime, 30(1), 285–301. https://doi.org/10.1108/JFC-12-2021-0263
24. Meiryani, M., Lesmana, M. E., Nahason, J., Lindrianasari, L., Hadipoespito, M. W., & Kresnandita, S. P. (2022). Impact of Enterprise Risk Management Implementation on Fraud Control in Small and Medium Enterprises. Proceedings of the 2022 6th International Conference on E-Business and Internet, 340–349.
25. Mustafa, K., & Ali, A. (2025). The Role of AI and Blockchain Technology in Strengthening Fraud Prevention Strategies in Finance. April. https://doi.org/10.13140/RG.2.2.11202.29126
26. Nurcahyono, N., Hanum, A. N., Kristiana, I., & Pamungkas, I. D. (2021). Predicting fraudulent financial statement risk: The testing dechow f-score financial sector company inindonesia. Universal Journal of Accounting and Finance, 9(6), 1487–1494. https://doi.org/10.13189/ujaf.2021.090625
27. Purnaningsih, N. K. C. (2022). Fraudulent Financial Reporting Analysis on Non-Financial Companies Listed on IDX in Hexagon Fraud Perspective. Budapest International Research and Critics Institute (BIRCI-Journal), 11331–11343. https://doi.org/10.33258/birci.v5i2.4955
28. Rane, N., Choudhary, S., & Rane, J. (2023). Blockchain and Artificial Intelligence (AI) integration for revolutionizing security and transparency in finance. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4644253
29. Riskiyadi, M. (2023). Detecting future financial statement fraud using a machine learning model in Indonesia: a comparative study. Asian Review of Accounting. https://doi.org/10.1108/ARA-02-2023-0062
30. Romanosky, S., & Petrun Sayers, E. L. (2024). Enterprise risk management: how do firms integrate cyber risk? Management Research Review, 47(1), 1–17.
31. Sari, M. P., Kiswanto, Rahmadani, L. V., Khairunnisa, H., & Pamungkas, I. D. (2020). Detection fraudulent financial reporting and corporate governance mechanisms using fraud diamond theory of the property and construction sectors in Indonesia. Humanities and Social Sciences Reviews, 8(3), 1065–1072. https://doi.org/10.18510/HSSR.2020.83109
32. Shah, S. Q. A., Lai, F. W., Shad, M. K., Konečná, Z., Goni, F. A., Chofreh, A. G., & Klemeš, J. J. (2021). The inclusion of intellectual capital into the green board committee to enhance firm performance. Sustainability (Switzerland), 13(19), 1–21. https://doi.org/10.3390/su131910849
33. Sihombing, R. P., Soewarno, N., & Agustia, D. (2023). The mediating effect of fraud awareness on the relationship between risk management and integrity system. Journal of Financial Crime, 30(3), 618–634.
34. Sudirman, S., Sasmita, H., Djabir D, M., Krisnanto, B., & Muchsidin, F. F. (2021). Effectiveness of Internal Audit in Supporting Internal Control and Prevention of Fraud. Bongaya Journal for Research in Accounting (BJRA), 4(1), 8–15. https://doi.org/10.37888/bjra.v4i1.271
35. Suhartini, D., Azmiyanti, R., & Putri, S. Y. (2023). Whistleblowing Intention in Accounting Students with Locus of Control as a Moderating Variable. Journal of Economics, Business, & Accountancy Ventura, 25(3), 288. https://doi.org/10.14414/jebav.v25i3.3257
36. Sutisna, U., Yazid, H., & Lestari, T. (2022). The effect of fraud diamond and financial stability on fraudulent financial statement with anti fraud as a moderating variable. Fair Value: Jurnal Ilmiah Akuntansi Dan Keuangan, 4(12), 5368–5378. https://doi.org/10.32670/fairvalue.v4i12.1783

 doi:10.20944/preprints202603.0965.v1

37. Tarjo, T., Vidyantha, H. V., Anggono, A., Yuliana, R., & Musyarofah, S. (2022). The effect of enterprise risk management on prevention and detection fraud in Indonesia's local government. Cogent Economics & Finance, 10(1), 2101222.
38. Thamlim, W., & Reskino. (2023). Fraudulent Financial Reporting with Fraud Pentagon Perspective: The Role of Corporate Governance as Moderator. American Journal of Humanities and Social Science Resesarch (AJHSSR), 07(01), 18–38.
39. Tubagus, I. (2021). Determinants of enterprise risk management disclosure: Evidence from insurance industry. Accounting, 7(6), 1331–1338.
40. Vanini, P., Rossi, S., Zvizdic, E., & Domenig, T. (2023). Online payment fraud: from anomaly detection to risk management. Financial Innovation, 9(1), 66.
41. Westland, J. C. (2022). A comparative study of frequentist vs. Bayesian A/B testing in the detection of E-commerce fraud. Journal of Electronic Business & Digital Economics, 1(1/2), 3–23. https://doi.org/10.1108/jebde-07-2022-0020
42. Yadegaridehkordi, E., Foroughi, B., Iranmanesh, M., Nilashi, M., & Ghobakhloo, M. (2023). Determinants of environmental, financial, and social sustainable performance of manufacturing SMEs in Malaysia. Sustainable Production and Consumption, 35, 129–140. https://doi.org/10.1016/j.spc.2022.10.026
43. Yusrianti, H., Ghozali, I., & Yuyetta, E. N. (2020). Asset misappropriation tendency: Rationalization, financial pressure, and the role of opportunity (study in indonesian government sector). Humanities and Social Sciences Reviews, 8(1), 373–382. https://doi.org/10.18510/hssr.2020.8148