Blockchain-based Risk Management Framework for Digital Asset Exchanges: Bridging COSO ERM with Emerging Technologies

Mahatthakorn Plensamai

Ubon Ratchathani Business School, Ubon Ratchathani University, Ubon Ratchathani, Thailand

Corresponding author. E-mail address: mahatthakorn.p@ubu.ac.th

Received: 28 November 2024; Revised: 24 March 2025; Accepted: 26 March 2025; Available Online: 20 June 2025

Abstract

This study proposes and validates a blockchain-based risk management framework tailored for digital asset exchanges by aligning blockchain-specific risks with the COSO ERM 2017 framework. Data were collected using a convergent mixed-methods approach: qualitative data were gathered through semi-structured interviews with 15-20 industry experts—selected via stratified purposeful and snowball sampling—and document analysis; quantitative data included over 100 survey responses and operational metrics such as downtime incidents, transaction volume, and cyberattack rates. Quantitative analysis utilized descriptive statistics, correlation analysis, regression models, and Monte Carlo simulations, with tools such as SPSS, R, and Python, while qualitative data were thematically analyzed using NVivo. Key findings revealed that the framework led to a 60% reduction in downtime incidents, cyberattack success rates, and compliance breaches, while stakeholder surveys indicated high satisfaction with usability (mean = 4.5) and cybersecurity mitigation (mean = 4.2), though moderate satisfaction with decentralized governance alignment (mean = 3.8). The study concludes that the framework effectively bridges technical, regulatory, and governance gaps in current practices, offering a scalable, adaptable model for enhancing operational resilience and regulatory compliance in blockchain-based ecosystems.

Keywords: Blockchain, Risk Management, COSO ERM Framework, Governance Models, Hybrid Governance, Digital Asset Exchanges

Introduction

Blockchain technology has emerged as a foundational innovation in digital finance, transforming the architecture of digital asset exchanges through its decentralized, immutable, and transparent characteristics. However, these advantages also introduce new types of operational risks that challenge traditional governance and risk management models. In particular, digital asset exchanges face complex threats such as cyberattacks, compliance inconsistencies across jurisdictions, and governance fragmentation (Zhu, 2021; Tangprasert, 2020). These exchanges operate in dynamic environments where real-time transactions, pseudonymous identities, and smart contract logic increase the difficulty of implementing robust Enterprise Risk Management (ERM) practices.

Several studies have attempted to conceptualize risk management in blockchain systems. Vincent and Barkhi (2021) proposed using the COSO ERM framework to assess blockchain governance, while Shah et al. (2025) focused on enhancing risk resilience through technical improvements. Truong and Le (2023) emphasized the importance of cybersecurity frameworks in permissioned blockchains but did not fully address decentralized environments. However, these studies often isolate technical or regulatory elements without integrating them into a comprehensive, adaptable risk governance framework. To address these gaps, researchers have begun advocating for the integration of IT governance models—such as COBIT (Control Objectives for Information and Related Technology)—and cybersecurity frameworks developed by NIST (National Institute of Standards and Technology) to provide more structured guidance for aligning technical, organizational, and compliance risks (ISACA, 2019; Barrett, 2018).

Given the growing complexity of digital asset ecosystems, this study aims to develop and validate a blockchain-based risk management framework for digital asset exchanges that is aligned with the COSO ERM 2017 framework while integrating insights from IT governance models such as COBIT and the NIST Cybersecurity Framework. The research objectives are fourfold: 1) to identify and categorize operational risks specific to digital asset exchanges, 2) to evaluate the effectiveness of existing governance mechanisms in managing such risks, 3) to develop a tailored risk management framework that aligns with COSO ERM and incorporates IT governance perspectives, and 4) to validate the framework through empirical data and stakeholder feedback. Based on qualitative interviews, document analyses, and survey data, the study identifies 22 operational risks commonly observed in digital asset exchanges. These include: cyberattacks, phishing and fraud schemes, smart contract vulnerabilities, system downtime, server overload, transaction delays, inaccurate data feeds, regulatory non-compliance, cross-border regulatory inconsistencies, insider threats, lack of accountability in decentralized governance, inconsistent audit trails, misconfigured smart contracts, insufficient technical documentation, inadequate key management, data privacy violations, inadequate KYC/AML protocols, token listing risks, misaligned incentives in governance, lack of contingency plans, third-party service vulnerabilities, and stakeholder conflict in decision-making. These were later classified into three major categories: cybersecurity risks, regulatory and compliance risks, and governance-related risks. Based on the literature and these identified risks, the research questions guiding this study are:

- How effectively does the COSO ERM framework address blockchain-specific operational risks in digital asset exchanges?
- What enhancements are necessary to align traditional ERM with decentralized governance and technical risk environments?
- Can a tailored framework integrating real-time monitoring and hybrid governance models improve operational resilience?

From these questions, the study proposes the following hypotheses:

H1: The integration of blockchain-specific risk indicators into COSO ERM significantly improves the identification and mitigation of operational risks in digital asset exchanges.

H2: Real-time monitoring and machine learning-based threat detection tools significantly reduce the frequency and impact of cybersecurity incidents.

H3: Hybrid governance models incorporating decentralized decision-making with centralized oversight significantly improve risk management efficiency and stakeholder trust.

In summary, this study bridges critical gaps in the literature by proposing a comprehensive, adaptive risk management framework that merges the strengths of the COSO ERM model with contemporary IT governance principles. By grounding its approach in both theory and empirical validation, the study aims to offer actionable insights for improving the operational resilience of blockchain-based digital asset exchanges.

Methods and Materials

Research Design

This study employed a convergent mixed-methods research design, integrating both qualitative and quantitative approaches to comprehensively explore operational risks in digital asset exchanges and how they can be mitigated through the COSO ERM 2017 framework. The study combined three primary sources of data: Semi-structured interviews with key stakeholders, Document analysis from official publications and risk reports and Survey data and operational metrics from digital exchanges. The qualitative and quantitative findings were integrated during the interpretation stage to ensure a well-rounded and contextually grounded risk management framework.

Sampling Strategy

Key Informants for Qualitative Interviews

Using stratified purposeful sampling, the study selected 18 key informants representing three groups: Blockchain Experts, Compliance Officers, and Risk Managers. The inclusion criteria were: At least 5 years of professional experience in digital asset exchanges or blockchain governance, Active involvement in risk mitigation or regulatory compliance and Representation from at least three geographical regions: Asia, Europe, and North America.

Table 1 Key Informant Profile Summary

Stakeholder Group	Number of Participants	Regions Represented	Selection Criteria
Blockchain Experts	6	Asia, Europe	Technical Knowledge + Project Involvement
Compliance Officers	6	Asia, North America	Regulatory Compliance Experience
Risk Managers	6	Asia, Europe, North America	Operational Oversight Roles

Survey Respondents

A structured online survey was distributed to professionals working in digital asset exchanges. Out of 152 responses, 127 completed responses were retained for analysis (83.5% response rate). The respondents were selected via convenience sampling through industry associations and LinkedIn outreach.

Table 2 Summary of Survey Respondents

Criteria	Number of Respondents	Percentage (%)
Total Received	152	100
Completed & Usable	127	83.5
From Asia	64	50.4
From Europe	35	27.6
From North America	28	22.0

The survey focused on perceptions of operational risk, governance practices, and the effectiveness of existing risk management tools. The 5-point Likert scale was used (1 = Strongly Disagree; 5 = Strongly Agree), and interpretation was based on the following criteria: 1.00-1.80 = Very Low; 1.81-2.60 = Low; 2.61-3.40 = Moderate; 3.41-4.20 = High; 4.21-5.00 = Very High.

Data Sources and Collection

Qualitative Data from Interviews

Semi-structured interviews were conducted via Zoom and in-person, each lasting 45-60 minutes. Questions were designed based on COSO ERM principles, focusing on governance, risk identification, assessment, response, and monitoring.

Document Analysis

A total of 32 documents were reviewed, including white papers, annual risk reports, and regulatory filings from top 10 global digital asset exchanges and international regulatory bodies (e.g., SEC, MAS, and ESMA).

Table 3 Document Sources

Document Type	Number of Documents	Examples of Sources
White Papers	10	Binance, Kraken, Bitkub
Annual Risk Reports	12	Coinbase, Crypto.com, OKX
Regulatory Filings	10	SEC, MAS, ESMA

Operational Metrics

Operational data were collected from public blockchain analytics tools and internal risk reports from three anonymous exchanges (coded A, B, and C). Metrics included transaction volume, downtime frequency, and cyberattack success rate. These were real-world datasets, not simulated.

Data Analysis Techniques

Quantitative Analysis

The following techniques were used Descriptive Statistics: Mean, Standard Deviation, Frequency Inferential Statistics: t-test for comparing perceived risk between regions One-way ANOVA for comparing governance efficiency across exchange sizes Correlation Analysis: To identify relationships between risk perception and governance maturity ($r = 0.65$, $p < 0.01$) Simulation Analysis: Monte Carlo Simulation: Used to evaluate the robustness of real-time monitoring tools (1000 iterations using MATLAB) Regression Models: Logistic regression to predict likelihood of compliance breaches based on governance structure (significant at $p < 0.05$).

Qualitative Analysis

Data were analyzed using thematic analysis (Braun & Clarke framework) with NVivo. Member checking was used with 8 participants to validate findings.

Application of COSO ERM 2017 Framework

This study mapped operational risks to the five components and 20 principles of COSO ERM 2017. For instance: Governance & Culture: Assessed decentralized governance gaps and organizational accountability Strategy & Objective-Setting: Evaluated alignment of blockchain risk strategies with organizational goals Performance: Measured how real-time risk tools improved operational KPIs (e.g., system uptime) Review & Revision: Analyzed how frameworks were revised based on past incidents Information, Communication & Reporting: Reviewed how blockchain platforms documented and reported risks.

Table 4 COSO ERM Components Applied

COSO ERM Component	Key Activities in Study
Governance & Culture	Interviewed experts on decentralized accountability
Strategy & Objective-setting	Analyzed strategic alignment in 127 survey responses
Performance	Used operational metrics to assess framework impact
Review & Revision	Reviewed historical incident reports and changes
Info, Communication, Reporting	Assessed transparency practices in document analysis

Validation and Reliability

Internal Validity: Triangulation of interviews, surveys, and documents Construct Validity: Based on COSO ERM and COBIT principles Instrument Reliability: Cronbach's Alpha for survey items: $\alpha = 0.82$ Inter-coder agreement for interviews: 87% External Validity: Diversity of respondents from 3 continents Simulation Reliability: Cross-validated using randomized input intervals in Monte Carlo models.

Results

This section presents the findings of the study, derived from integrated qualitative and quantitative data sources and aligned with the research objectives. Statistical analyses were conducted to evaluate operational risks, governance effectiveness, and the applicability of COSO ERM principles within digital asset exchanges. Descriptive statistics, correlation, ANOVA, and logistic regression were applied using SPSS and Python, while qualitative themes were derived from thematic analysis of interview transcripts and document reviews.

1. Descriptive Statistics and Perceptions of Operational Risk

From the 127 valid survey responses, the top three perceived operational risks were cybersecurity breaches (reported by 65.4% of respondents), regulatory non-compliance (48.8%), and system downtime (44.1%). Table 5 presents descriptive statistics for key risk management perceptions based on a 5-point Likert scale.

Table 5 Descriptive Statistics of Risk Management Practices in Digital Asset Exchanges

Survey Item	Mean	S.D.	Interpretation
Integration of blockchain-specific risks into ERM framework	2.82	0.91	Moderate
Effectiveness of current risk mitigation strategies	3.26	1.07	Moderate
Use of real-time monitoring tools	3.78	0.86	High
Satisfaction with current governance structure	3.14	0.95	Moderate
Flexibility of governance in cross-border compliance	2.67	0.88	Moderate-Low

The data revealed a moderate level of integration between blockchain-specific risks and traditional ERM frameworks, indicating a need for more tailored approaches.

2. Differences in Governance Efficiency by Exchange Size

To evaluate whether exchange size influenced perceptions of governance efficiency, a one-way ANOVA was conducted. Respondents were grouped based on the size of their exchange: Small (n = 40), Medium (n = 47), and Large (n = 40). The results showed a statistically significant difference among the groups (F = 5.62, p = 0.004), suggesting that medium and large exchanges perceived greater governance efficiency than smaller ones. Post hoc analysis (Tukey HSD) indicated that large exchanges (M = 3.74, SD = 0.88) reported significantly higher governance efficiency than small exchanges (M = 3.12, SD = 0.92), p = 0.003.

3. Correlation between Governance Maturity and Risk Mitigation

A Pearson correlation was performed to examine the relationship between perceived governance maturity and effectiveness in mitigating operational risks. The results showed a strong positive correlation (r = 0.65, $p < 0.01$), suggesting that exchanges with more mature governance structures tend to manage risks more effectively.

4. Predicting Compliance Breaches Using Governance Type

Logistic regression analysis was conducted to assess whether governance type (centralized, hybrid, decentralized) could predict the likelihood of experiencing a compliance breach. The model was statistically significant ($\chi^2(2) = 12.84$, p = 0.002), and governance type was a significant predictor of compliance incidents.

Specifically, decentralized governance was associated with a higher likelihood of experiencing compliance breaches (Odds Ratio = 2.41, p = 0.018) compared to hybrid models. This supports the study’s recommendation for hybrid governance as a balance between flexibility and accountability.

5. Performance Improvement through Real-Time Monitoring

Operational data collected from three partner exchanges (coded A, B, and C) before and after framework implementation demonstrated a reduction in key operational risks. Table 6 summarizes the improvements across core risk metrics.

Table 6 Impact of Real-Time Monitoring on Operational Risk Metrics

Metric	Baseline Value	Post-Framework Value	% Change	Statistical Significance (t-test)
Downtime Incidents (Per Quarter)	5.00 ± 1.12	2.00 ± 0.82	−60%	p = 0.001
Cyberattack Success Rate (%)	25.0 ± 5.1	10.2 ± 3.4	−59.2%	p = 0.003
Compliance Breaches (Per Year)	15.0 ± 3.5	6.2 ± 2.3	−58.7%	p = 0.002

The paired-sample t-tests confirmed statistically significant reductions in all three risk areas after implementation of the proposed risk management framework.

6. Stakeholder Feedback on Framework Effectiveness

A follow-up survey with 42 stakeholders who participated in pilot testing the framework assessed satisfaction across three key dimensions: cybersecurity mitigation, decentralized governance alignment, and usability.

Table 7 Stakeholder Perception of Framework Effectiveness

Evaluation Dimension	Mean	S.D.	Interpretation
Cybersecurity risk mitigation	4.22	0.78	Very High
Alignment with decentralized governance	3.76	0.95	High
Usability and scalability of the framework	4.51	0.68	Very High

Feedback was overwhelmingly positive in terms of usability and cybersecurity performance. Some concerns were raised regarding the complexity of integrating the framework into fully decentralized platforms, which supported the rationale for hybrid governance recommendations.

7. Summary of Key Findings in Relation to Research Objectives

To directly align with the study's objectives, Table 8 summarizes the key results:

Table 8 Summary of Results Based on Research Objectives

Research Objective	Key Result Highlights
Identify and categorize operational risks	22 risks identified; top 3: cybersecurity, compliance, system downtime
Evaluate governance mechanisms and risk response	Statistically significant variation in governance efficiency by exchange size
Develop tailored risk management framework aligned with COSO ERM	Framework mapped to all 5 COSO components; hybrid governance recommended
Validate framework through empirical data and stakeholder feedback	Positive performance outcomes; statistical significance confirmed in risk reduction and satisfaction

Discussion

This study aimed to develop and validate a blockchain-based risk management framework tailored to digital asset exchanges, grounded in the COSO ERM 2017 framework. The results provided clear and empirically supported insights into the operational risks facing digital asset exchanges, the effectiveness of governance structures, and the impact of implementing real-time monitoring tools. While the proposed framework demonstrated potential for reducing operational vulnerabilities, this discussion will focus specifically on interpreting those findings within the scope of the data collected, avoiding overstated claims, and offering reasoned explanations for observed outcomes.

First, the survey and operational metrics confirmed that cybersecurity risks, compliance issues, and system downtimes remain the top operational threats, consistent with findings from previous studies such as Zhu (2021) and Truong and Le (2023). The strong correlation ($r = 0.65$, $p < 0.01$) between governance maturity and effective risk mitigation suggests that a well-structured governance model—particularly hybrid models—can enhance risk responsiveness. This outcome supports the logic that decentralized systems, although innovative, require structured oversight mechanisms to prevent accountability gaps and regulatory breaches.

Second, the statistically significant results from the ANOVA ($F = 5.62$, $p = 0.004$) and logistic regression ($\chi^2(2) = 12.84$, $p = 0.002$) revealed that exchange size and governance model type are important variables affecting risk outcomes. Larger exchanges, with more formalized structures and compliance resources, performed better in governance efficiency and were less likely to experience compliance breaches compared to smaller exchanges or those operating under fully decentralized models. This finding is aligned with COSO ERM's "Governance & Culture" and "Performance" components, which emphasize the role of oversight and process integrity in reducing risks.

Third, the observed 60% reductions in downtime incidents, cyberattack success rates, and compliance breaches after implementing real-time monitoring (t-test, $p < 0.01$ across all indicators) demonstrate the practical benefit of integrating dynamic risk monitoring tools into existing frameworks. However, these results should be interpreted as initial validation rather than definitive proof of long-term success. The improvements could also be partially influenced by increased awareness or short-term behavioral changes following framework adoption, rather than solely by technical interventions.

Fourth, stakeholder feedback provided an important qualitative lens to the study's findings. High satisfaction ratings regarding usability ($M = 4.51$) and cybersecurity risk mitigation ($M = 4.22$) underscore the framework's relevance to practice. However, concerns regarding the framework's compatibility with fully decentralized platforms, reflected in a lower mean score for governance alignment ($M = 3.76$), highlight that universal adoption may require adaptive implementation strategies based on organizational context.

To summarize these discussions, Table 9 presents key findings, their empirical support, interpretations, and implications.

Table 9 Summary of Empirical Findings and Interpretations

Key Finding	Empirical Evidence	Interpretation	Implication
Cybersecurity, compliance, and downtime are top risks	Survey Responses (N = 127); 65%, 49%, 44%	Digital asset exchanges face persistent operational threats	Framework must prioritize these risks in its core structure
Governance maturity correlates with risk mitigation effectiveness	Correlation ($r = 0.65$, $p < 0.01$)	Stronger governance structures improve operational resilience	Hybrid governance is a practical middle ground
Exchange size affects governance performance	ANOVA ($F = 5.62$, $p = 0.004$)	Larger exchanges benefit from more resources and risk controls	Smaller exchanges may need external support or shared frameworks
Governance model predicts compliance breach likelihood	Logistic Regression ($p = 0.002$, OR = 2.41)	Decentralized models face higher compliance risks	Hybrid or dynamic governance structures are recommended
Real-time monitoring reduces operational incidents	t-test ($p < 0.01$ across all metrics)	Proactive detection enables quicker response to incidents	Integration with blockchain analytics tools is critical

Table 9 (Cont.)

Key Finding	Empirical Evidence	Interpretation	Implication
High satisfaction with usability and cybersecurity effectiveness	Stakeholder Survey (M = 4.51 and 4.22)	Framework is practically applicable in industry settings	Potential for industry adoption with training and support
Lower satisfaction with governance alignment	Stakeholder Survey (M = 3.76)	Complexity of decentralized systems remains a barrier	Tailoring of framework needed for high-decentralization environments

In light of these discussions, it is important to recognize that while the framework offers a promising approach to managing blockchain-specific risks, its applicability and effectiveness may vary depending on contextual factors such as organization size, governance culture, and regulatory environment. The COSO ERM 2017 framework proved helpful in structuring the assessment and classification of operational risks, especially under its "Governance & Culture" and "Review & Revision" components. However, extending COSO to suit blockchain ecosystems requires adaptive elements that account for decentralized logic and real-time data processing.

Finally, this discussion acknowledges the study's limitations. The cross-sectional design prevents long-term assessment of framework efficacy, and while statistically significant, the results should not be overgeneralized beyond the sampled exchanges. Future research should adopt longitudinal designs and test the framework across multiple blockchain use cases, possibly including Decentralized Autonomous Organizations (DAOs), to further validate its adaptability and impact.

Conclusion and Suggestions

This study set out to address the challenge of managing operational risks in digital asset exchanges by identifying key risk factors and developing a blockchain-based risk management framework aligned with the COSO ERM 2017 framework. Through a convergent mixed-methods design involving interviews with 18 key stakeholders, analysis of 32 industry documents, and 127 survey responses, the study identified 22 operational risks and validated the effectiveness of the proposed framework using real operational metrics and statistical analyses.

The 22 identified risks were classified into three main categories:

1. **Cybersecurity Risks** - such as system intrusion, phishing attacks, smart contract vulnerabilities, and inadequate encryption.

2. **Regulatory and Compliance Risks** - including lack of standardization across jurisdictions, weak KYC/AML controls, and inconsistent audit trails.

3. **Governance-Related Risks** - such as decision-making conflicts in decentralized structures, lack of clear accountability, and absence of contingency planning.

The framework was empirically validated through observed improvements in key metrics—specifically, a 60% reduction in system downtime, successful cyberattacks, and compliance breaches—supported by statistically significant t-test results ($p < 0.01$). Further, governance type was found to significantly influence risk exposure, with hybrid governance models demonstrating the most effective balance between control and flexibility. Survey data showed high satisfaction with the framework's usability and effectiveness in risk mitigation, although alignment with decentralized systems still requires refinement.

Importantly, the application of the COSO ERM 2017 framework provided a structured approach to risk identification and response. The components of Governance & Culture, Performance, and Review & Revision were most actively utilized in guiding both the design and implementation of the framework in real-world blockchain environments. While COSO provided a foundational structure, integration with elements from IT governance (e.g., COBIT) and cybersecurity frameworks (e.g., NIST) added the necessary technological depth.

Based on these findings, the study proposes the following practical recommendations:

1. **Adopt Hybrid Governance Models**: Digital asset exchanges, especially those operating across jurisdictions, should consider hybrid governance that combines decentralized participation with centralized oversight to reduce compliance risk and increase decision efficiency.

2. **Implement Real-Time Risk Monitoring Systems**: Exchanges should invest in real-time monitoring tools equipped with AI or rule-based alert systems to detect anomalies in transaction behavior, system loads, and regulatory compliance deviations before escalation occurs.

3. **Prioritize Cybersecurity Investment According to Risk Profile**: Smaller or newer exchanges should perform risk-based prioritization and focus limited resources on top-identified vulnerabilities (e.g., smart contract testing, multi-signature wallets).

4. **Customize COSO ERM to Fit Blockchain Contexts**: Organizations should adapt COSO ERM to incorporate elements of blockchain-specific challenges. This includes redefining internal control points, reporting mechanisms, and performance monitoring tools to match the decentralized operational environment.

5. **Establish Cross-Border Regulatory Mapping Tools**: Given the variation in compliance requirements, especially for global exchanges, a real-time regulatory mapping tool (possibly embedded within smart contracts) should be developed to track and auto-adjust processes in response to legal changes.

6. **Design Training Programs for Stakeholders**: Continuous education for compliance officers, developers, and executives on integrated risk governance in blockchain environments should be provided to reduce the human factor as a source of vulnerability.

To conclude, while this research contributes to the literature by bridging blockchain technology and enterprise risk management, its more important value lies in the provision of an evidence-based, practical, and adaptable framework for digital asset exchanges. The framework's validation in actual exchange settings confirms its operational relevance, yet its adaptability across different scales and governance models still requires further testing. Future studies should conduct longitudinal assessments of framework effectiveness, test its integration into Decentralized Autonomous Organizations (DAOs), and explore its scalability across various blockchain platforms beyond exchanges.

Acknowledgments

I would like to express my deepest gratitude to the individuals and organizations whose support and contributions were instrumental in completing this research study. First and foremost, I extend my heartfelt thanks to Ubon Ratchathani University for providing the academic and institutional support necessary for this work. The guidance and encouragement from my colleagues in the Accounting Department have been invaluable throughout this research journey. I am also immensely grateful to Chulalongkorn University for equipping me with the knowledge and skills during my Master's studies, which have been a foundation for my academic pursuits. I wish to acknowledge the insights and expertise shared by blockchain professionals, compliance officers, and risk managers who participated in the interviews and surveys. Your contributions have significantly enriched the depth and scope of this research. Additionally, I appreciate the contributions of industry experts and regulators who provided valuable feedback and perspectives on risk management frameworks for digital asset exchanges. Finally, I am deeply grateful to my family and friends for their unwavering support and encouragement, which have been a constant source of motivation throughout this endeavor.

This research is dedicated to advancing knowledge and practice in the fields of blockchain technology, risk management, and governance, with the hope of contributing positively to the evolving landscape of digital finance.

References

Barrett, M. P. (2018). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST Cybersecurity Framework*. https://doi.org/10.6028/NIST.CSWP.04162018

ISACA. (2019). *COBIT 2019 Framework: Introduction and Methodology*. Illinois, USA.: ISACA.

Shah, S. Q. A., Lai, F.-W., Shad, M. K., Hamad, S., & Ellili, N. O. D. (2025). Exploring the Effect of Enterprise Risk Management for ESG Risks Towards Green Growth. *International Journal of Productivity and Performance Management*, *74*(1), 224-249. https://doi.org/10.1108/ijppm-10-2023-0582

Tangprasert, S. (2020). A Study of Information Technology Risk Management of Government and Business Organizations in Thailand Using COSO-ERM based on the COBIT 5 Framework. *Journal of Applied Science*, *19*(1), 13-24. https://doi.org/10.14416/j.appsci.2020.01.002

Truong, V. T., & Le, L. B. (2023). A Blockchain-based Framework for Secure Digital Asset Management. In *2023 IEEE International Conference on Communications (ICC): Next-Generation Networking and Internet Symposium, Rome, Italy, May 28-June 1, 2023* (pp. 1911-1916). https://doi.org/10.1109/ICC45041.2023.10279622

Vincent, N. E., & Barkhi, R. (2021). Evaluating Blockchain Using COSO. *Current Issues in Auditing*, *15*(1), A57-A71. https://doi.org/10.2308/ciia-2019-509

Zhu, Y. (2021). Research on Digital Finance Based on Blockchain Technology. In *2021 International Conference on Computer, Blockchain and Financial Development (CBFD), Nanjing, China, April 23-25, 2021* (pp. 410-414). Piscataway, NJ: IEEE Service Center. https://doi.org/10.1109/CBFD52659.2021.00089