Proceedings of the International Conference on Education, Economics, Business, Entrepreneurship, and Finance (ICEBEF)
Volume 4 (2025)

A Comparative Analysis of Fintech Cybersecurity Governance in Singapore and Indonesia: Regulatory Effectiveness, Risk Exposure, and Policy Implications

Zahra Tazkia[1], Okta Nurul Gina[2], Risa Nur Safitri[3], Syahla Aulia Syahida[4], Zahrah Salsabila[5], Fitrina Kurniati[6], Iqbal Lhutfi[7]
[1234567]Faculty of Economics and Business Education, Universitas Pendidikan Indonesia, Dr Setiabudi Street No. 229, Bandung, West Java, 40154, Indonesia
E-mail: zahratazkia@upi.edu; okta01nurul@upi.edu; risanrsf@upi.edu; syahlaaulia08@upi.edu; zahrahsalsabila30@upi.edu; fitrina.kurniati@upi.edu; iqbal.lhutfi@upi.edu

ABSTRACT
This study compares fintech cybersecurity governance in Singapore and Indonesia, focusing on regulatory effectiveness, risk exposure, and policy implications. A systematic literature review was conducted using data from 2018 to 2024, sourced from Scopus, Web of Science, Google Scholar, and official reports issued by financial regulators, including the Monetary Authority of Singapore (MAS) and the Financial Services Authority of Indonesia (OJK). An inductive thematic analysis was applied to synthesise findings from 52 eligible documents. The results show that Singapore demonstrates stronger regulatory coherence, mandatory technology risk management (TRM) frameworks, and a higher level of digital literacy, contributing to lower cybersecurity risk exposure across the fintech ecosystem. In contrast, Indonesia faces recurring challenges, including inconsistent data protection enforcement, limited consumer awareness, and uneven technological infrastructure. The study highlights that the regulatory gap and governance maturity significantly influence national fintech resilience. The paper contributes to the literature by integrating a cross-country perspective on fintech cybersecurity governance and by proposing policy recommendations for emerging markets, particularly the need for unified data protection enforcement, capacity building, and enhanced public awareness.

Keywords: Intech Governance; Cybersecurity; Regulatory Effectiveness; Risk Management; Comparative Analysis

INTRODUCTION

The rapid expansion of financial technology (fintech) has reshaped the global financial landscape by creating new channels for payments, investment, and credit access (Gai, Qiu, & Sun, 2018). However, this transformation also increases cybersecurity risks, including data breaches, identity theft, fraud, and systemic vulnerabilities (Zveryakov et al., 2019). Fintech-related cyber incidents have risen by more than 45% globally over the past five years, underscoring the growing tension between innovation and security in digital finance (IMF, 2023).

Singapore and Indonesia present contrasting yet interconnected cases within Southeast Asia's fintech ecosystem. As a global fintech hub, Singapore adopts a proactive regulatory approach through the Technology Risk Management (TRM) Guidelines and the Payment Services Act (PSA) to ensure systemic resilience. Conversely, Indonesia, despite being one of the region's fastest-growing fintech markets, faces structural and regulatory challenges, including uneven digital infrastructure, fragmented data protection laws, and limited public cybersecurity awareness. These differences provide a valuable comparative context for assessing how governance quality and regulatory design influence fintech security outcomes.

Existing studies largely emphasise technical solutions such as encryption, blockchain, and authentication systems (Chen et al., 2022; Lim & Tan, 2023). This tendency is also evident in cryptocurrency research, where governance and regulatory frameworks are often treated as secondary despite their importance in mitigating risks such as exchange hacks and key management failures (Benedetti & Nikbakht, 2021). Although technological countermeasures are well documented, governance-oriented analyses examining how regulatory frameworks, institutional coordination, and digital maturity shape fintech resilience remain limited (Anagnostopoulos, 2018; Arner et al., 2017). Moreover, cross-country comparisons between advanced and emerging Asian economies linking regulatory effectiveness to cybersecurity exposure are still scarce.

This study addresses these gaps through a comparative analysis of fintech cybersecurity governance in Singapore and Indonesia, grounded in Regulatory Governance Theory and Technology Risk Management Theory. The former highlights the role of coherent rule design, institutional capacity, and predictable enforcement (Arner et al., 2017; Zetzsche et al., 2017), while the latter emphasises proactive and standardised cyber risk mitigation for systemic resilience (Lee et al., 2019). Using a systematic review of literature and official reports combined with inductive thematic analysis, the study evaluates regulatory effectiveness, assesses national risk exposure, and formulates policy implications for strengthening fintech governance in emerging markets.

This research contributes by developing a structured comparative framework linking regulatory design, governance maturity, and cybersecurity outcomes; synthesising evidence from developed and emerging economies in Southeast Asia; and offering policy recommendations to enhance data protection enforcement, institutional capacity, and public awareness for resilient fintech ecosystems.

METHOD

This study adopts a qualitative comparative design grounded in a systematic literature review and inductive thematic analysis. The research approach was selected to ensure analytical depth and reproducibility in synthesising existing evidence on fintech cybersecurity governance in two distinct yet interconnected Southeast Asian contexts—Singapore and Indonesia. The comparative framework is particularly relevant given that cybersecurity challenges in fintech often reveal common patterns across different markets, though manifested through distinct regulatory and institutional arrangements, as observed in European Union contexts by Faccia & Moşteanu (2019). By comparing these two countries, the study aims to explore how differences in regulatory structure, institutional maturity, and digital infrastructure shape the level of exposure to cybersecurity risks within the fintech ecosystem. Singapore is a mature, tightly regulated financial hub, whereas Indonesia is a rapidly expanding but fragmented fintech landscape.

The research relies exclusively on secondary data drawn from peer-reviewed academic articles, policy reports, regulatory guidelines, and institutional documents published between January 2018 and December 2024. Relevant materials were collected from major academic databases such as Scopus, Web of Science, and Google Scholar, as well as official repositories of financial authorities, including the Monetary Authority of Singapore (MAS), the Financial Services Authority of Indonesia (OJK), and Bank Indonesia (BI). The search process employed combinations of keywords encompassing "fintech," "cybersecurity," "information security," "regulation," "governance," "Singapore," and "Indonesia." Only studies and documents focusing on the governance, regulation, or management of cybersecurity risks in the fintech sector were included. At the same time, those unrelated to financial technology or lacking methodological rigour were excluded.

An initial pool of 231 publications was identified. After careful screening of titles and abstracts, 52 documents met the inclusion criteria and were selected for full-text review. The selection procedure followed the PRISMA framework's principles to ensure transparency and traceability. Each eligible document was examined in detail, and relevant data were systematically extracted into an analytical matrix that included information on publication type, country focus, regulatory framework, identified risks, and mitigation mechanisms. The extracted data were subsequently analysed using inductive thematic analysis to identify patterns and relationships that explain the differences in fintech cybersecurity resilience between the two countries.

The thematic coding process was conducted in three iterative stages: open coding to identify preliminary concepts, axial coding to organise these codes into coherent categories, and selective coding to integrate them into broader themes. These themes were then synthesised into a comparative framework linking three central dimensions: regulatory effectiveness, governance maturity, and risk exposure. Through this framework, the study examines how each country's institutional capacity, policy coherence, and public digital literacy shape its overall fintech security posture. Coding and thematic validation were carried out independently by two reviewers to ensure consistency and reduce potential researcher bias, and any discrepancies were resolved through discussion and consensus.

To strengthen the validity of the findings, triangulation across multiple sources—academic, regulatory, and institutional—was employed, enabling verification of the consistency of factual information across regulatory provisions, reported incidents, and implementation outcomes. Reliability was reinforced by maintaining a transparent coding log and documenting the analytical process in detail. Reflexivity was observed throughout the research to minimise interpretive bias and ensure that conclusions were grounded in verifiable evidence rather than subjective inference. Since the study relies entirely on publicly available data, no ethical concerns involving human participants arise; nonetheless, all materials used are correctly cited to preserve academic integrity and acknowledge intellectual contributions.

RESULTS AND DISCUSSION

The findings of this comparative analysis reveal distinct differences in the governance architecture, regulatory effectiveness, and cybersecurity resilience between Singapore and Indonesia. These variations reflect not only divergent levels of digital maturity but also contrasting regulatory philosophies and institutional capacities. The evidence synthesised from the 52 reviewed documents demonstrates that the relative strength of each country's fintech cybersecurity framework depends mainly on the coherence of its regulatory instruments, the consistency of institutional coordination, and the extent of public engagement in maintaining digital trust. The comparative synthesis of the reviewed literature reveals substantial differences between Singapore and Indonesia in regulatory structures, institutional coordination, and exposure to cybersecurity risks. To illustrate these contrasts more clearly, Table 1 summarises the key dimensions of fintech security governance identified across the analysed sources, including regulatory frameworks, incident frequency, data protection regimes, public literacy levels, and inter-agency coordination.

Table 1. Comparison of Fintech Security Risks in Singapore and Indonesia (compiled from multiple sources, 2018–2024)

Aspect	Singapore	Indonesia	Interpretation / Implication	Source (Year)

Regulatory framework	Comprehensive; unified under MAS; mandatory TRM & PSA	Fragmented; dual authority (OJK, BI); partial enforcement	Singapore benefits from regulatory coherence; Indonesia needs consolidation	MAS (2021); OJK (2023)
Cyber incident frequency	Low; centralised incident reporting	High under-reporting and fragmented data	Indicates gaps in monitoring and enforcement	MAS Annual Report (2023); Kominfo (2022)
Data protection regime	Enforced PDPA with clear sanctions	Draft law until 2022; limited sanctions	Weak deterrence for data misuse in Indonesia	Gov.sg (2021); DPR RI (2022)
Public digital literacy	High (nationwide digital readiness index 0.84)	Moderate (0.61, significant rural gap)	Awareness gap contributes to consumer vulnerability	IMD (2023); BPS (2022)
Institutional coordination	Strong inter-agency synergy (MAS, IMDA, CSA)	Partial coordination (OJK–BI–Kominfo overlap)	Institutional silos increase response delay	MAS (2022); OJK (2023)

As shown in Table 1, Singapore maintains a more coherent and technologically advanced fintech regulatory environment than Indonesia. The integration of the Technology Risk Management (TRM) Guidelines and the Payment Services Act (PSA) has contributed to consistent compliance and centralised oversight (Monetary Authority of Singapore, 2021). In contrast, Indonesia continues to operate under a dual-authority structure led by OJK and Bank Indonesia, which often results in overlapping jurisdiction and partial enforcement (Otoritas Jasa Keuangan, 2023). Furthermore, the absence of a fully operational data protection law before 2022 has weakened consumer safeguards and institutional accountability (Dewan Perwakilan Rakyat Republik Indonesia, 2022). The comparative differences underscore the importance of regulatory coherence, public literacy, and inter-agency coordination in shaping national fintech security resilience.

Singapore's approach exemplifies the successful integration of technology and finance within a robust regulatory framework, aligning with what Nicoletti (2017) describes as the 'future of fintech' - where regulatory sophistication keeps pace with technological innovation. Singapore’s regulatory regime demonstrates a high level of sophistication and institutional alignment in addressing fintech cybersecurity risks. Singapore's regulatory regime demonstrates a high level of sophistication and institutional alignment, a hallmark of advanced regulatory governance (Arner et al., 2017). The Monetary Authority of Singapore (MAS) plays a central and integrated role as both regulator and policy architect, ensuring a unified supervisory framework across banks, payment systems, and fintech operators. The Technology Risk Management (TRM) Guidelines, first introduced in 2013 and continuously updated through 2021, establish detailed technical and operational standards for risk identification, mitigation, and reporting. These are complemented by the Payment Services Act (PSA), which consolidates multiple payment-related legislations and mandates licensing based on risk profiles. The combination of these instruments promotes regulatory clarity and encourages compliance among market participants. Singapore’s regulatory ecosystem is further supported by advanced digital infrastructure, high public literacy, and strong collaboration between government agencies, private actors, and academia. These conditions have collectively produced a stable and resilient fintech environment, with relatively few major data breach incidents reported over the past five years.

In contrast, Indonesia presents a more fragmented regulatory landscape, characterised by overlapping mandates and uneven enforcement capacity. This regulatory lag creates fertile ground for the 'techrisks' described by Buckley et al. (2020), where vulnerabilities in rapidly scaling fintech services can outstrip the capacity of oversight mechanisms, leading to inconsistent enforcement and heightened systemic exposure. This aligns with the concept of 'real-time risk' described by Aldridge & Krawciw (2017), where a lack of robust, automated controls in fast-paced digital environments can turn localized issues into systemic threats, such as widespread fraud in e-wallets or disruptive runs on P2P lending platforms. The Otoritas Jasa Keuangan (OJK) and Bank Indonesia (BI) share regulatory responsibility for fintech operations, yet coordination between the two institutions often remains procedural rather than integrative. Although OJK has issued several circulars and guidelines on digital financial innovation and consumer data protection, enforcement mechanisms are not uniformly applied across sectors. The absence of a comprehensive and enforceable data protection law until recently has also contributed to inconsistent cybersecurity practices among fintech firms. Moreover, technological disparities between urban and rural areas, combined with limited institutional capacity, have heightened systemic vulnerabilities. Public awareness of cybersecurity risks remains low, particularly among users of peer-to-peer lending and e-wallet platforms, where cases of data misuse and digital fraud have been relatively frequent.

The thematic synthesis suggests that regulatory effectiveness in fintech cybersecurity governance depends on three interrelated conditions: the formal coherence of regulatory frameworks, the maturity of institutional governance, and the behavioural dimension of digital trust. Singapore scores highly across all three dimensions.

Regulations are clear, technology standards are regularly updated, and compliance is enforced through mandatory audits and penalties. Institutional maturity is maintained through coordinated oversight, while digital trust is reinforced through continuous public campaigns and transparency in regulatory communication. Indonesia, on the other hand, shows regulatory inconsistency, with several overlapping authorities issuing non-binding guidelines, leading to a weak compliance culture and partial adoption of cybersecurity standards. Governance maturity is evolving but remains hampered by limited cross-agency coordination and resource constraints. At the same time, public trust in fintech systems remains fragile due to recurring incidents of data breaches and fraud.

From a theoretical standpoint, the observed divergence between Singapore and Indonesia aligns with principles of Regulatory Governance Theory, which emphasises that effective governance arises from coherent rule design, institutional capacity, and predictable enforcement mechanisms. Singapore's model demonstrates how regulatory centralisation and technical mandates enhance compliance and reduce systemic risks. Conversely, Indonesia's distributed regulatory model—though adaptive to rapid market growth—reveals the trade-off between innovation and control. Similarly, applying the lens of Technology Risk Management Theory, Singapore's consistent implementation of TRM frameworks fosters proactive identification and mitigation of cyber risks. In contrast, Indonesia's reliance on reactive responses indicates a need for a more preventive, standardised risk management approach. Furthermore, the dimension of Digital Trust provides an interpretive bridge between regulation and user behaviour. In Singapore, high levels of digital literacy and consumer confidence reinforce regulatory success, whereas in Indonesia, limited awareness and low consumer vigilance weaken the overall cybersecurity posture despite formal regulatory progress.

These comparative findings have broader policy implications. For Indonesia, improving fintech cybersecurity governance requires consolidating regulatory mandates into a unified national framework that integrates financial, technological, and data protection functions. Strengthening enforcement mechanisms, mandating incident reporting, and harmonising standards with ASEAN digital security initiatives would significantly enhance institutional credibility. Equally important is investment in digital literacy programmes targeting both fintech operators and consumers, as the human element remains a critical determinant of cybersecurity resilience. For Singapore, the key policy challenge lies not in creating new regulations but in sustaining adaptability amid the growing complexity of cross-border digital finance. Continuous collaboration with regional partners, transparent information sharing, and cross-jurisdictional regulatory alignment will be essential to maintaining its leadership in fintech governance.

Overall, the results of this study reaffirm that effective fintech cybersecurity governance is not merely a function of technological sophistication but a systemic outcome of coherent regulation, institutional maturity, and societal trust. Singapore's experience demonstrates that proactive regulation and coordinated institutional governance can substantially mitigate cybersecurity risks, while Indonesia's evolving framework reflects both the challenges and opportunities inherent in developing digital economies. These findings contribute to the ongoing discourse on digital financial resilience in emerging markets, offering a policy-relevant roadmap for enhancing fintech governance across ASEAN through harmonised standards, capacity building, and public trust reinforcement.

CONCLUSION

This study has examined the comparative governance of fintech cybersecurity in Singapore and Indonesia through a systematic literature review and inductive thematic analysis. The findings indicate that while both countries recognise the importance of digital financial security, their institutional maturity and regulatory coherence differ markedly. Singapore's approach is characterised by a unified and proactive regulatory framework led by the Monetary Authority of Singapore (MAS). The integration of the Technology Risk Management (TRM) Guidelines and the Payment Services Act (PSA) provides a comprehensive basis for risk identification, mitigation, and compliance, supported by high digital literacy and effective inter-agency coordination. As a result, Singapore enjoys relatively low cybersecurity incident frequency and strong consumer trust in fintech operations.

Indonesia, on the other hand, remains in a phase of regulatory consolidation. Conversely, Indonesia's reliance on reactive responses to cyber incidents, rather than proactive risk management, leaves its financial ecosystem more exposed. Oversight is divided between the Otoritas Jasa Keuangan (OJK) and Bank Indonesia (BI), leading to overlapping mandates and inconsistent enforcement. The delayed establishment of a comprehensive data protection law and the limited public awareness of digital security further constrain the effectiveness of Indonesia's fintech governance. Nonetheless, recent developments, including the enactment of the Personal Data Protection Law and initiatives to strengthen coordination among OJK, BI, and Kominfo, mark a positive trajectory towards more coherent cybersecurity regulation.

The comparative results reaffirm that robust fintech cybersecurity governance depends on three interlinked dimensions: regulatory coherence, institutional capacity, and public digital trust. Singapore's experience demonstrates how integrated and enforceable frameworks foster resilience, whereas Indonesia's fragmented system illustrates the risks of regulatory pluralism and uneven implementation. The analysis underscores that

technological innovation must be supported by structured governance and informed user participation to sustain long-term digital trust.

From a theoretical standpoint, this study reinforces the principle that effective governance arises from alignment between regulatory design and institutional competence. Regulatory clarity and predictability encourage compliance, while fragmented structures can undermine enforcement and accountability. Practically, the findings offer actionable lessons for emerging fintech markets. Indonesia and similar economies should prioritise consolidating regulatory authority, introducing mandatory incident-reporting and audit mechanisms, and strengthening regional cooperation to harmonise cybersecurity standards. Public education on digital risk awareness is equally vital, given that behavioural vulnerabilities often amplify technical weaknesses. For Singapore, maintaining regulatory agility amid cross-border digitalisation will be crucial to sustaining its leadership within ASEAN's fintech ecosystem.

In conclusion, the study demonstrates that fintech cybersecurity resilience is shaped not merely by technological sophistication but by the strength of governance systems that regulate, monitor, and educate. As the market reacts to governance and risk events (Dranev et al., 2019), the contrasting regulatory models of Singapore and Indonesia demonstrate that strong cybersecurity is not a cost center but a critical investment for sustaining innovation, protecting consumers, and maintaining stable market valuations. Coherent regulation, institutional maturity, and public trust form the foundation of sustainable digital finance. While Singapore provides a model of centralised, preventive regulation, Indonesia's gradual reforms highlight the opportunities and challenges inherent in the transition of developing economies towards comprehensive fintech governance. These insights contribute to a broader understanding of how national regulatory models can adapt to the evolving risks of digital financial transformation.

REFERENCES

Aldridge, I., & Krawciw, D. (2017). *Real-time risk: What investors should know about FinTech, high-frequency trading, and flash crashes*. Hoboken, NJ: John Wiley & Sons.

Anagnostopoulos, I. (2018). Fintech and regtech: Impact on regulators and banks. *Journal of Economics and Business, 100*, 7-25. http://dx.doi.org/10.1016/j.jeconbus.2018.04.005

Arner, D. W., Barberis, J., & Buckley, R. P. (2017). FinTech, RegTech, and the reconceptualization of financial regulation. *Northwestern Journal of International Law & Business, 37*(3), 371-413.

Benedetti, H., & Nikbakht, E. (2021). Cybersecurity and cryptocurrency: The role of governance and regulation. *Journal of Financial Stability, 57*, 100936. http://dx.doi.org/10.1016/j.jfs.2021.100936

Buckley, R. P., Arner, D. W., Zetzsche, D. A., & Selga, E. (2020). The dark side of digital financial transformation: The new risks of fintech and the rise of techrisk. *University of New South Wales Law Journal, 43*(3), 969-1006.

Chen, L., Gao, S., & Wang, Y. (2022). A secure and efficient blockchain-based data sharing scheme for fintech applications. *Journal of Network and Computer Applications, 207*, 103517. http://dx.doi.org/10.1016/j.jnca.2022.103517

Dranev, Y., Izosimov, A., & Mehlum, H. (2019). The impact of fintech M&A on stock returns. *Research in International Business and Finance, 48*, 353-364. http://dx.doi.org/10.1016/j.ribaf.2019.01.012

Faccia, A., & Moşteanu, N. R. (2019). Cybersecurity and financial technology: The challenges of digital banking in the European Union. *Journal of Financial Studies, 4*(7), 31-48.

Gai, K., Qiu, M., & Sun, X. (2018). A survey on FinTech. *Journal of Network and Computer Applications, 103*, 1-15. http://dx.doi.org/10.1016/j.jnca.2017.10.011

IMF. (2023). *Fintech and the future of finance: Market and policy implications*. In *Global financial stability report, October 2023*. Retrieved from https://www.imf.org/en/Publications/fintech-notes/Issues/2023/10/11/fintech-and-the-future-of-finance-market-and-policy-implications-542417

Lee, J., Ryu, J., & Lee, D. (2019). The effect of risk management on the performance of FinTech companies: A focus on South Korea. *Journal of Risk and Financial Management, 12*(4), 1-15. http://dx.doi.org/10.3390/jrfm12040155

Lim, J., & Tan, K. (2023). Beyond passwords: A multi-modal biometric authentication framework for secure fintech platforms. *Computers & Security, 124*, 102956. http://dx.doi.org/10.1016/j.cose.2022.102956

Nicoletti, B. (2017). *The future of FinTech: Integrating finance and technology in financial services*. Cham, Switzerland: Springer.

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2017). *The RegTech book: The financial technology handbook for investors, entrepreneurs and visionaries in regulation*. Chichester, England: John Wiley & Sons.

Zveryakov, M., Kovalenko, V., & Sheludko, S. (2019). Fintech and the transformation of the financial system: New risks and new opportunities. *Investment Management and Financial Innovations, 16*(4), 69-75. http://dx.doi.org/10.21511/imfi.16(4).2019.07