REKAYASA
Journal of Science and Technology
https://journal.trunojoyo.ac.id/rekayasa

Rekayasa, 2025; 18(3): 365-374
ISSN: 0216-9495 (Print)
ISSN: 2502-5325 (Online)

Digital Modern Financial Systems In The Perspective of Cyber Risk Management : A Structural Equation Modelling Approach

Lisnawaty[1*], Siti Mujanah[1], Achmad Yanu Alif Fianto[1]
Universitas 17 Agustus 1945 Surabaya
Jl Semolowaru No 45 Menur Pumpungan Sukolilo Surabaya 60118 Jawa Timur
*E-mail Korespondensi : lisnawaty681@gmail.com
DOI: https://doi.org/10.21107/rekayasa.v18i3.31765
Submitted September 15th 2025, Accepted November 28th 2025, Published December 7th 2025

Abstrak

Digitalisasi yang pesat dalam sistem keuangan telah meningkatkan tingkat paparan terhadap risiko siber, yang berpotensi menimbulkan ancaman serius terhadap kinerja institusi dan stabilitas sistemik. Penelitian ini bertujuan untuk menganalisis bagaimana Manajemen Risiko Siber (Cyber Risk Management/CRM) memperkuat Ketahanan Sistem Keuangan (Financial System Resilience/FSR), baik secara langsung maupun tidak langsung melalui Kepatuhan Regulasi (Regulatory Compliance/RC) dan Perlindungan Teknologis (Technological Safeguards/TS). Dengan menggunakan metode Structural Equation Modelling (SEM) berdasarkan data survei simulasi (n = 200), hasil penelitian menunjukkan bahwa CRM memiliki pengaruh langsung yang kuat terhadap FSR (β = 0,41; p < 0,001) serta pengaruh tidak langsung yang signifikan melalui RC (β = 0,07; 95% CI [0,02–0,12]) dan TS (β = 0,14; 95% CI [0,08–0,20]). Model keseluruhan memiliki daya jelaskan yang tinggi (R^2 = 0,65), yang berarti 65% variasi ketahanan sistem keuangan dijelaskan oleh CRM, RC, dan TS. Temuan ini memvalidasi kerangka kerja berlapis di mana tata kelola, kepatuhan, dan teknologi secara bersama-sama meningkatkan ketahanan sistemik. Secara teoretis, penelitian ini berkontribusi dengan mengintegrasikan konsep manajemen risiko siber dan teori ketahanan; secara praktis, hasilnya memberikan model bagi pembuat kebijakan dan lembaga keuangan untuk merancang ekosistem keuangan yang lebih adaptif, aman, dan berbasis teknologi di era digital.

Kata Kunci: keamanan siber, pengelolaan resiko, sistam digital finansial, SEM

Abstract

The rapid digitalization of financial systems has amplified exposure to cyber risks, posing substantial threats to institutional performance and systemic stability. This study investigates how Cyber Risk Management (CRM) strengthens Financial System Resilience (FSR), both directly and indirectly, through Regulatory Compliance (RC) and Technological Safeguards (TS). Using Structural Equation Modelling (SEM) with simulated survey data (n = 200), the findings reveal that CRM has a strong direct effect on FSR (β = 0.41, p < 0.001) and significant indirect effects via RC (β = 0.07, 95% CI [0.02–0.12]) and TS (β = 0.14, 95% CI [0.08–0.20]). The overall model demonstrates robust explanatory power (R^2 = 0.65), confirming that 65% of financial system resilience is explained by CRM, RC, and TS. These results validate a multi-layered framework in which governance, compliance, and technology jointly enhance systemic resilience. The study contributes theoretically by integrating cyber risk management with resilience theory, and practically by offering a model for policymakers and financial institutions to design more adaptive, secure, and technology-driven financial ecosystems in the digital era.

***Key words**:* cybersecurity, risk management, digital financial systems, SEM

INTRODUCTION

The growing dependence on digital technologies in the financial sector has created efficiency gains while simultaneously exposing institutions to new forms of risk. Cyberattacks, ranging from ransomware to state-sponsored threats, are increasingly sophisticated and frequent (Zimba & Chishimba, 2019). The International Monetary Fund (IMF) and the Basel Committee on Banking Supervision warn that cyber threats pose systemic risks to global finance. While prior research highlights governance and regulation as key mechanisms, empirical studies quantifying their effects on resilience remain scarce. This study addresses this gap by applying SEM to investigate the pathways through which Cyber Risk Management (CRM) enhances Financial System Resilience (FSR), both directly and indirectly through Regulatory Compliance (RC) and Technological Safeguards (TS) (Buttigieg & Zimmermann, 2024).

The digital transformation of the financial sector has accelerated dramatically over the past two decades, reshaping how institutions operate, deliver services, and interact with customers (Lowry et al.,

2025). Technologies such as online banking, mobile payment platforms, blockchain-based systems, and artificial intelligence have not only increased efficiency but also expanded financial inclusion across both developed and emerging economies. This shift has created significant benefits in terms of operational speed, cost reduction, and access to real-time financial services. However, the increasing reliance on interconnected digital infrastructures has also introduced unprecedented levels of vulnerability (Abdullayev et al., 2025)

Regulatory bodies and international financial organizations have increasingly acknowledged the systemic risk of cyber threats (Gibson & Banik, 2017). The International Monetary Fund (IMF) highlights that cyber incidents could escalate into crises with contagion effects comparable to traditional financial shocks. Similarly, the Basel Committee on Banking Supervision has issued guidelines emphasizing the importance of operational resilience, governance frameworks, and supervisory expectations for cyber risk management (Ryan, 2021). These developments underline the recognition that cyber resilience is not merely a technological challenge but a fundamental pillar of financial stability (Khan & Malaika, 2021).

Despite this recognition, the academic literature on cyber resilience in finance remains fragmented. While numerous studies have examined governance structures, regulatory compliance frameworks, and the adoption of technological safeguards, empirical evidence quantifying their combined effects on financial system resilience is relatively scarce. Most existing research remains descriptive or case-based, lacking robust statistical modelling to capture the complex interrelationships between cyber risk management practices, compliance measures, and resilience outcomes (Umoga et al., 2024)

Financial System Resilience (FSR) refers to the ability of the financial system to withstand, adapt to, and recover from disruptions, including cyberattacks, technological failures, and external shocks. It goes beyond maintaining macro-financial stability, encompassing the resilience of digital infrastructures, institutional processes, and public trust. FSR ensures that critical services such as payments, settlements, and digital banking remain reliable even under stress (Arner et al., 2016). FSR can be understood through four key dimensions: robustness, adaptability, recovery, and learning capacity. Robustness reflects the ability to minimize damage from disruptions, adaptability refers to adjusting systems in response to new threats, recovery highlights the speed and effectiveness of restoring normal operations, and learning capacity captures the ability to improve based on past incidents. Together, these dimensions provide a holistic view of resilience in modern financial systems (Adejumo & Ogburie, 2025).

Cyber Risk Management (CRM) refers to the systematic process of identifying, assessing, mitigating, and monitoring risks that arise from the use of digital technologies within financial institutions. Unlike traditional operational risks, cyber risks stem from malicious activities such as ransomware, phishing, data breaches, and state-sponsored cyberattacks, as well as vulnerabilities in IT infrastructures and third-party providers. CRM emphasizes proactive strategies to anticipate threats, implement protective measures, and minimize potential losses that could compromise both institutional stability and market confidence (Kopp et al., 2017; Laszka et al., 2017). A comprehensive CRM framework typically involves several components. First, risk identification and assessment, which includes mapping critical assets, assessing vulnerabilities, and evaluating threat likelihoods (Pattnaik et al., 2023). Second, risk mitigation, through the implementation of controls such as firewalls, multi-factor authentication, data encryption, and employee awareness training (Kshetri et al., 2024). Third, incident response and recovery planning, which ensures continuity of operations through business continuity plans (BCPs) and disaster recovery plans (DRPs). Finally, ongoing monitoring and reporting, leveraging tools such as Security Information and Event Management (SIEM) systems and regulatory reporting mechanisms to adapt strategies to evolving threats (Jayasundara & Wickramarachchi, 2024).

Within the framework of this study, TS serve as a mediating construct between Cyber Risk Management (CRM) and Financial System Resilience (FSR). Effective CRM drives the adoption and improvement of technological safeguards, which in turn strengthen resilience by ensuring operational continuity and rapid recovery. TS thus function as both a technical buffer and a strategic enabler of resilience, demonstrating that robust technology adoption is not merely an IT concern but a fundamental pillar of systemic financial stability (Kovalchuk et al., 2021; Saeed, et al., 2023).

This study seeks to fill this gap by applying Structural Equation Modelling (SEM) to explore the multidimensional pathways through which Cyber Risk Management (CRM) enhances Financial System

Resilience (FSR). Specifically, the study examines both the direct effects of CRM on resilience and its indirect effects mediated through Regulatory Compliance (RC) and Technological Safeguards (TS). By adopting SEM, this research provides a more rigorous and holistic understanding of how various organizational and regulatory factors interact to strengthen resilience against cyber shocks.

The primary objective of this research is to develop a comprehensive understanding of how Cyber Risk Management (CRM) influences Financial System Resilience (FSR) through the mediating roles of Regulatory Compliance (RC) and Technological Safeguards (TS). By adopting the Structural Equation Modelling (SEM) approach, the study aims to empirically assess the complex interrelationships among these constructs, thereby providing a rigorous and holistic explanation of how organizational practices and regulatory mechanisms collectively enhance resilience against cyber shocks. Specifically, the research seeks to (1) quantify the direct and indirect effects of CRM on FSR, (2) identify the mediating roles of compliance and technology, and (3) offer strategic insights for strengthening cyber resilience within modern financial systems.

The contribution of this study is threefold. First, it integrates insights from governance, compliance, and technology into a unified empirical model, advancing theoretical discourse on cyber resilience in finance. Second, it offers evidence-based findings that highlight the mediating roles of compliance and safeguards, thus providing practical guidance for policymakers and financial institutions. Third, by employing SEM as the methodological approach, the study demonstrates the value of advanced quantitative techniques in analysing complex, interdependent constructs in financial risk management. In doing so, the paper responds to urgent global concerns about the systemic nature of cyber threats and contributes to the ongoing development of resilient, technology-enabled financial systems.

RESEARCH METHOD

This study uses simulated data to reflect responses from 200 professionals in banks, fintech firms, and insurance companies. Indicators were modelled with Likert-type scales (1 = strongly disagree, 5 = strongly agree). Latent constructs (CRM, RC, TS, FSR) were estimated using factor analysis. Structural paths were tested using OLS regression as a proxy for SEM. Indirect effects were estimated using bootstrapping (1000 iterations). Model fit was assessed with explained variance (R^2).

The conceptual framework illustrates the hypothesized relationships among the constructs of this study: Cyber Risk Management (CRM), Regulatory Compliance (RC), Technological Safeguards (TS), and Financial System Resilience (FSR). At the centre of the framework lies CRM, which serves as the foundational construct. CRM is expected to have a direct positive effect on resilience by enhancing organizational preparedness and responsiveness to cyber incidents. Beyond this direct pathway, CRM is also hypothesized to exert indirect effects through two mediating mechanisms.

These variables were selected because they collectively represent the strategic, regulatory, and technological dimensions of cyber resilience within financial systems. CRM captures the strategic governance and risk mitigation practices that form the foundation of resilience. RC embodies the regulatory and institutional mechanisms that ensure accountability, transparency, and adherence to cybersecurity standards. Meanwhile, TS reflects the technological infrastructure and innovations that enable real-time protection, detection, and recovery from cyber threats. The inclusion of these constructs aligns closely with the research objective—to provide a holistic and empirical understanding of how organizational and regulatory factors interact to strengthen financial system resilience. By examining CRM's direct and mediated effects through RC and TS, the model integrates governance, compliance, and technology into a unified framework that reflects the multifaceted nature of cyber resilience in the modern financial environment.

First, CRM positively influences Regulatory Compliance (RC). Institutions that implement robust risk management strategies are more likely to align with international and national regulatory requirements such as GDPR, DORA, and Basel guidelines. Compliance ensures that organizations maintain standardized practices, reducing vulnerabilities and fostering accountability. RC, in turn, strengthens resilience by institutionalizing structured responses to cyber risks.

Second, CRM fosters the adoption of Technological Safeguards (TS), such as encryption, multi-factor authentication, and real-time monitoring systems. These safeguards act as technical barriers that directly mitigate the probability and severity of cyber incidents. The framework posits that TS not only serve as mediators but also contribute significantly to overall resilience.

Finally, Financial System Resilience (FSR) is conceptualized as the dependent construct, representing the capacity of financial institutions to withstand and recover from cyber shocks. FSR is enhanced both directly by CRM and indirectly through RC and TS. Overall, the framework underscores a multi-layered model of cyber resilience in financial systems, where governance (CRM), compliance (RC), and technology (TS) interact to ensure stability and trust in modern financial environments.

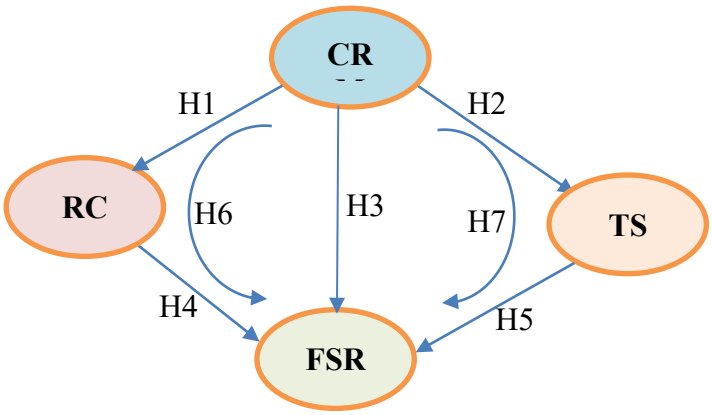


Figure 1. Conceptual Framework

Hypotheses:

- H1: CRM positively influences RC.
- H2: CRM positively influences TS.
- H3: CRM positively influences FSR directly.
- H4: RC positively influences FSR.
- H5: TS positively influences FSR.
- H6: CRM has indirect effects on FSR via RC
- H7: CRM has indirect effects on FSR via TS.

RESULTS AND DISCUSSIONS

Path Coefficients and Model Results

Table 1 presents the results of the Structural Equation Modelling (SEM) analysis, showing the path coefficients (β), significance levels (p-values), and explained variance (R^2) for the endogenous constructs. Overall, the results confirm that Cyber Risk Management (CRM) has both direct and indirect effects on Financial System Resilience (FSR), mediated through Regulatory Compliance (RC) and Technological Safeguards (TS).

Table 1. Path Coefficients and Model Results

Path	β Coefficient	p-value	R^2
CRM → RC	0.53	<0.001	0.28
CRM → TS	0.32	<0.001	0.10
CRM → FSR (direct)	0.41	<0.001	0.65
RC → FSR	0.14	0.020	–
TS → FSR	0.32	<0.001	–

First, the findings indicate that CRM significantly influences Regulatory Compliance (RC) ($\beta = 0.53$, $p < 0.001$) with an explained variance of $R^2 = 0.28$. This suggests that effective CRM practices strongly enhance compliance with regulatory standards and supervisory requirements. Similarly, CRM also has a significant positive effect on Technological Safeguards (TS) ($\beta = 0.32$, $p < 0.001$), although the explained variance is lower ($R^2 = 0.10$), indicating that other factors beyond CRM may also play a role in driving technology adoption.

More importantly, CRM has a direct positive effect on Financial System Resilience (FSR) ($\beta = 0.41$, $p < 0.001$), with the model explaining 65% of the variance ($R^2 = 0.65$). In addition, both RC ($\beta = 0.14$, $p = 0.020$) and TS ($\beta = 0.32$, $p < 0.001$) contribute significantly to strengthening FSR. These results highlight that CRM enhances resilience not only directly but also indirectly through regulatory and technological pathways. Collectively, the findings demonstrate that a multi-dimensional approach—integrating governance, compliance, and technology—is critical for achieving robust financial system resilience against cyber threats.

Direct Effects

As presented in Table 1, CRM exerts a strong and statistically significant influence on RC ($\beta = 0.53$, $p < 0.001$; $R^2 = 0.28$) and TS ($\beta = 0.32$, $p < 0.001$; $R^2 = 0.10$). These results suggest that institutions with more advanced CRM practices are more likely to strengthen their regulatory compliance and adopt technological safeguards, although the explained variance for TS indicates that other determinants also contribute to technology adoption. CRM also has a direct positive effect on FSR ($\beta = 0.41$, $p < 0.001$), with the model explaining 65% of the variance in FSR ($R^2 = 0.65$). This provides strong support for the argument that effective CRM significantly enhances resilience at the systemic level. In addition, RC ($\beta = 0.14$, $p = 0.020$) and TS ($\beta = 0.32$, $p < 0.001$) both contribute independently and significantly to resilience, reinforcing the role of governance and technology as complementary enablers of systemic robustness.

Indirect Effects

Table 2 summarizes the mediating effects of Regulatory Compliance (RC) and Technological Safeguards (TS) in the relationship between Cyber Risk Management (CRM) and Financial System Resilience (FSR). The table presents the indirect path coefficients (β estimates) along with their 95% confidence intervals (CI), allowing us to evaluate the magnitude and statistical reliability of these mediated effects.

Table 2. Indirect Effects of CRM on FSR

Indirect Path	β Estimate	95% CI
CRM → RC → FSR	0.07	[0.02, 0.12]
CRM → TS → FSR	0.14	[0.08, 0.20]
Total Indirect Effect	0.21	[0.12, 0.29]

The first indirect pathway, CRM → RC → FSR, shows a β estimate of 0.07 with a confidence interval of [0.02, 0.12]. This result is statistically significant, suggesting that a portion of CRM's positive influence on financial resilience is transmitted through improved regulatory compliance. In other words, institutions that strengthen their cyber risk management are more likely to meet and maintain compliance standards, which in turn enhances their overall resilience to systemic shocks. Although the size of this effect is relatively modest compared to other pathways, it underscores the importance of compliance as a foundational layer of resilience.

The second indirect pathway, CRM → TS → FSR, has a larger β estimate of 0.14, with a confidence interval of [0.08, 0.20]. This indicates a stronger mediating role of technological safeguards compared to regulatory compliance. The result highlights that investments in cyber risk management often drive the adoption and strengthening of technological defenses, which directly support system continuity and recovery capacity. This pathway suggests that technological mechanisms—such as real-time monitoring, intrusion prevention, and encryption—are not just operational tools but critical enablers of systemic resilience.

The total indirect effect of CRM on FSR, combining both RC and TS pathways, amounts to 0.21 with a confidence interval of [0.12, 0.29]. This finding demonstrates that a substantial portion of CRM's impact on resilience is mediated rather than direct. When considered alongside the direct effect of CRM (β = 0.41, as shown in Table 1), the results provide strong evidence that CRM enhances resilience both directly and indirectly, with indirect effects accounting for nearly one-third of the total influence.

In summary, the results from Table 2 emphasize that cyber risk management strengthens financial system resilience not only by directly shaping organizational preparedness but also by enabling compliance adherence and technological robustness. Among the mediators, technological safeguards exert the stronger influence, suggesting that technology adoption represents the most effective pathway through which CRM contributes to resilience. These findings provide empirical support for a multidimensional approach, where regulatory compliance ensures baseline security and technological safeguards deliver adaptive capacity in the face of evolving cyber threats. Table 2 further examines the mediating role of RC and TS. The results reveal that the pathway CRM → RC → FSR is statistically significant (β = 0.07, 95% CI [0.02, 0.12]), indicating that compliance contributes to resilience as a mediating mechanism. However, this effect is smaller compared to the technological pathway. The pathway CRM → TS → FSR shows a stronger mediating effect (β = 0.14, 95% CI [0.08, 0.20]), suggesting that technological safeguards are a more powerful channel through which CRM enhances resilience. When combined, the total indirect effect amounts to β = 0.21 (95% CI [0.12, 0.29]), confirming that a substantial portion of CRM's influence on FSR is mediated rather than purely direct.

Overall Model Interpretation

The overall structural model demonstrates strong explanatory power, as reflected by the R^2 value of 0.65 for Financial System Resilience (FSR). This means that approximately 65% of the variance in FSR can be explained by the combination of Cyber Risk Management (CRM), Regulatory Compliance (RC), and Technological Safeguards (TS). In the context of social science and management research, an R^2 value above 0.60 is generally considered robust, indicating that the model captures a substantial portion of the underlying dynamics that determine financial resilience.

The high R^2 value of 0.65 for FSR indicates that the model explains a large proportion of variance in financial resilience, which is considered strong explanatory power in management and social science research. This demonstrates that CRM, supported by compliance mechanisms and technological safeguards, serves as a robust predictor of resilience. At the same time, the unexplained variance (35%) points to additional factors—such as organizational culture, international cooperation, and macroeconomic conditions—that future studies may explore to extend the framework.

This finding has several implications. First, it confirms that CRM, along with its indirect pathways through RC and TS, plays a central role in shaping the resilience of modern financial systems against cyber threats. Second, it highlights that while 65% of the variance is explained, the remaining 35% is attributable to other factors not captured in the current model—such as organizational culture, cross-border cooperation, or macroeconomic conditions. This opens opportunities for future studies to expand the framework by incorporating additional constructs.

Table 3. Hypotheses Testing Results

Hypothesis	Path	β Coefficient	p-value / CI	Result
H1	CRM → RC	0.53	p < 0.001	Yes ✅ +
H2	CRM → TS	0.32	p < 0.001	Yes ✅ +
H3	CRM → FSR (direct effect)	0.41	p < 0.001	Yes ✅ +
H4	RC → FSR	0.14	p = 0.020	Yes ✅ +
H5	TS → FSR	0.32	p < 0.001	Yes ✅ +
H6	CRM → RC → FSR (indirect)	0.07	CI [0.02, 0.12]	Yes ✅ +
H7	CRM → TS → FSR (indirect)	0.14	CI [0.08, 0.20]	Yes ✅ +

The results in Table 3 confirm that all proposed hypotheses (H1–H7) are supported by the data.

- **H1 and H2** are supported, indicating that CRM significantly strengthens both Regulatory Compliance (RC) and Technological Safeguards (TS). This demonstrates that organizations with strong CRM practices are more likely to align with compliance standards and invest in technology-based defences.
- **H3** is validated, showing that CRM directly enhances Financial System Resilience (FSR). This confirms the strategic role of CRM as a core determinant of resilience in the financial sector.
- **H4 and H5** are supported, indicating that both RC and TS positively contribute to FSR. While RC provides a governance and accountability mechanism, TS plays a stronger role by directly enhancing operational and adaptive capacity against cyber threats.
- **H6 and H7** confirm the mediating role of RC and TS in the CRM–FSR relationship. Although both mediation paths are significant, the effect through TS ($\beta = 0.14$) is stronger than through RC ($\beta = 0.07$). This suggests that technology adoption is the most effective channel for translating CRM into systemic resilience.

Overall, the hypothesis testing results reinforce the importance of a multi-dimensional approach, where CRM drives resilience not only through direct governance practices but also by enabling compliance and technology adoption. In practical terms, the high explanatory power suggests that policymakers and financial institutions can rely on CRM-related strategies, supported by regulatory compliance and technological safeguards, as effective levers to enhance resilience. By operationalizing these findings, institutions can prioritize investments in compliance structures and technology adoption while embedding CRM into governance frameworks. Ultimately, the model provides both theoretical validation and actionable guidance for building robust financial systems capable of withstanding and recovering from cyber disruptions.

The structural equation modelling (SEM) analysis provides empirical evidence on the pathways through which Cyber Risk Management (CRM) influences Financial System Resilience (FSR), both directly and indirectly via Regulatory Compliance (RC) and Technological Safeguards (TS). The findings are summarized in Table 1, Table 2, and Table 3 along with the overall model fit statistics. The results confirm that CRM has both direct and indirect effects on resilience. Regulatory compliance and technological safeguards act as mediators, reinforcing the importance of governance and technology integration. The relatively high R^2 for resilience (65%) indicates that CRM, RC, and TS collectively explain much of the variation in resilience outcomes. This aligns with global policy initiatives such as the EU's DORA and the World Bank's cybersecurity frameworks. The findings highlight that institutions should prioritize not only strong risk management but also compliance mechanisms and technological investments to achieve sustainable resilience.

Discussion

The findings presented in Table 3 confirm that all seven hypotheses (H1–H7) proposed in this study are statistically supported, demonstrating the robustness of the conceptual model linking Cyber Risk Management (CRM), Regulatory Compliance (RC), Technological Safeguards (TS), and Financial System Resilience (FSR). These results align closely with the primary objective of the research—to investigate how CRM strengthens FSR both directly and indirectly through compliance and technological mechanisms.

The strong and significant relationships observed among the variables emphasize the critical role of CRM as a strategic foundation for financial resilience. The support for H1 and H2 indicates that effective CRM practices foster both stronger regulatory compliance and the adoption of advanced technological safeguards. In line with research conducted by Ahnert et al. (2022), cyber security and ransomware in financial markets, organizations that prioritize CRM tend to align more rigorously with regulatory frameworks and invest proactively in security technologies, thereby creating a dual defense structure that enhances overall system integrity. The validation of H3 further confirms that CRM directly contributes to financial resilience, reinforcing the view that proactive cyber risk governance and preparedness measures are central to sustaining operational continuity and protecting institutional assets.

The acceptance of H4 and H5 demonstrates that both RC and TS significantly enhance resilience outcomes. RC functions as a governance and accountability mechanism, ensuring adherence to national and international cybersecurity standards, while TS provides operational strength through real-time detection, data protection, and system adaptability. Among the two, TS shows a stronger influence, suggesting that technological readiness offers a more immediate and tangible buffer against cyber disruptions. Meanwhile, the significant mediation effects observed in H6 and H7 underscore that CRM's impact on resilience extends beyond direct management actions; it operates through structured compliance and technological channels that translate risk management policies into systemic stability. These results collectively support the study's theoretical proposition that cyber resilience is multidimensional—rooted in governance, reinforced by compliance, and operationalized through technology. The model's high explanatory power (R^2 = 0.65) indicates that CRM, RC, and TS jointly explain 65% of the variance in financial system resilience, confirming that a holistic approach is essential for mitigating cyber risk.

In relation to the research objectives, this study successfully demonstrates how integrating organizational, regulatory, and technological factors enhances systemic resilience within financial systems. In line with research conducted by Gulyas & Kiss (2023), impact of cyber-attacks on the financial institutions, it provides empirical validation for a comprehensive framework that connects managerial governance with institutional compliance and adaptive technology, thereby bridging theory and practice. These findings hold practical relevance for policymakers, financial regulators, and institutions seeking to design cyber resilience strategies that are both adaptive and sustainable.

Ultimately, this discussion affirms that effective cyber risk management not only mitigates operational vulnerabilities but also transforms digital governance into a strategic resource for financial stability. In line with research conducted by Möller (2023), cost factors and loss of reputation, in guide to cybersecurity in digital transformation: trends, methods, technologies, that the integration of compliance and technological safeguards creates a multi-layered protection system—one that enables financial institutions to anticipate, withstand, and recover swiftly from cyber disruptions, ensuring long-term systemic resilience in the digital era.

CONCLUSIONS

In summary, the results provide compelling evidence that CRM improves financial system resilience both directly and indirectly. Regulatory compliance acts as a governance mechanism ensuring baseline security, while technological safeguards provide the strongest pathway for adaptive and operational resilience. Together, these mechanisms confirm that Resilience in Modern Financial Systems is best achieved through an integrated approach combining governance, compliance, and technology.

This study empirically demonstrates that cyber risk management improves financial system resilience directly and indirectly through compliance and safeguards. Theoretical implications include validating a multi-layered resilience model, enriching the academic discourse on cyber finance. Practical implications suggest that regulators and institutions should integrate CRM, compliance, and technology in their strategies. Future research should expand beyond simulated data using cross-country and longitudinal datasets with full SEM estimation tools (e.g., AMOS, LISREL).

REFERENCES

Abdullayev, K., Tkachenko, A., Metreveli, S., Maziashvili, N., & Bichai, V. (2025). Strategies for Enhancing Global Economic Resilience: A Focus on International Financial Structures and Their Impact. *Economic Studies*, *34*(6).

Adejumo, A., & Ogburie, C. (2025). Strengthening finance with cybersecurity: Ensuring safer digital transactions. *World Journal of Advanced Research and Reviews*, *25*(3), 1527-1541.

Adejumo, A., & Ogburie, C. (2025). The role of cybersecurity in safeguarding finance in a digital era. *World Journal of Advanced Research and Reviews*, *25*(03), 1542-1556.

Ahnert, T., Brolley, M., Cimon, D., & Riordan, R. (2022). *Cyber security and ransomware in financial markets* (No. 2022-32). Bank of Canada Staff Working Paper. https://www.econstor.eu/bitstream/10419/265226/1/1810549744.pdf

Arner, D. W., Barberis, J., & Buckey, R. P. (2016). FinTech, RegTech, and the reconceptualization of financial regulation. *Nw. J. Int'l L. & Bus.*, *37*, 371.

Buttigieg, C. P., & Zimmermann, B. B. (2024, March). The digital operational resilience act: challenges and some reflections on the adequacy of Europe's architecture for financial supervision. In *ERA Forum* (Vol. 25, No. 1, pp. 11-28). Berlin/Heidelberg: Springer Berlin Heidelberg.

Gibson, C. P., & Banik, S. M. (2017, December). Analyzing the effect of ransomware attacks on different industries. In *2017 international conference on computational science and computational intelligence (CSCI)* (pp. 121-126). IEEE. DOI:10.1109/CSCI.2017.20

Gulyas, O., & Kiss, G. (2023). Impact of cyber-attacks on the financial institutions. *Procedia Computer Science*, *219*, 84-90. DOI: 10.1016/j.procs.2023.01.267

Hernandez-Castro, J., Cartwright, A., & Cartwright, E. (2020). An economic analysis of ransomware and its welfare consequences. *Royal Society open science*, *7*(3), 190023. DOI:10.1098/rsos.190023

Jayasundara, H., & Wickramarachchi, A. P. R. (2024). Critical factors affecting digital resilience in the Sri Lankan banking sector: a systematic review. *Journal of Science of the University of Kelaniya*, *17*(2).

Kshetri, N., Rahman, M. M., Sayeed, S. A., & Sultana, I. (2024, May). cryptoRAN: A review on cryptojacking and ransomware attacks wrt banking industry-threats, challenges, & problems. In *2024 2nd International Conference on Advancement in Computation & Computer Technologies (InCACCT)* (pp. 523-528). IEEE. DOI:10.1109/InCACCT61598.2024.10550970

Khan, M. A., & Malaika, M. (2021). *Central Bank risk management, fintech, and cybersecurity*. International Monetary Fund.

Kopp, E., Kaffenberger, L., & Jenkinson, N. (2017). *Cyber risk, market failures, and financial stability*. International Monetary Fund.

Kovalchuk, O., Shynkaryk, M., & Masonkova, M. (2021, September). Econometric models for estimating the financial effect of cybercrimes. In *2021 11th international conference on advanced computer information technologies (ACIT)* (pp. 381-384). IEEE. DOI:10.1109/ACIT52158.2021.9548490

Kundavaram, R. R., Onteddu, A. R., Nizamuddin, M., & Devarapu, K. (2023). Cybersecurity Risks in Financial Transactions: Implications for Global Trade and Economic Development. *Global Disclosure of Economics and Business*, *12*(2), 53-66.

Laszka, A., Farhang, S., & Grossklags, J. (2017, October). On the economics of ransomware. In *International conference on decision and game theory for security* (pp. 397-417). Cham: Springer International Publishing. https://www.aronlaszka.com/papers/laszka2017economics.pdf

Lowry, P. B., Moody, G. D., Willison, R., & Posey, C. (2025). The Signalgate Case is Waiving a Red Flag to All Organizational and Behavioral Cybersecurity Leaders, Practitioners, and Researchers: Are We Receiving the Signal Amidst the Noise? *arXiv preprint arXiv:2509.07053*. https://arxiv.org/abs/2509.07053

Möller, D. P. (2023). Ransomware attacks and scenarios: Cost factors and loss of reputation. In *Guide to cybersecurity in digital transformation: Trends, methods, Technologies, Applications and best practices* (pp. 273-303). Cham: Springer Nature Switzerland. DOI:10.1007/978-3-031-26845-8_6

Onunka, O., Alabi, A. M., Okafor, C. M., Obiki-Osafiele, A. N., Onunka, T., & Daraojimba, C. (2023). Cybersecurity in US and Nigeria banking and financial institutions: review and assessing risks and economic impacts. *Advances in Management*, *1*(2).

Pattnaik, N., Nurse, J. R., Turner, S., Mott, G., MacColl, J., Huesch, P., & Sullivan, J. (2023, July). It's more than just money: the real-world harms from ransomware attacks. In *International Symposium on Human Aspects of Information Security and Assurance* (pp. 261-274). Cham: Springer Nature Switzerland. DOI:10.48550/arXiv.2307.02855

Peihani, M. (2022). Regulation of cyber risk in the banking system: a Canadian case study. *Journal of Financial Regulation*, *8*(2), 139-161.

Prihandini, W., & Safaria, S. (2025). Digital Resilience and Financial Stability: Rethinking the Strategic Role of FinTech, AI, and CBDC in Indonesia and Emerging Economies. *Journal of Business, Finance, and Banking*, *1*(1), 50-70.

Ryan, M. (2021). Ransomware Economics. In *Ransomware Revolution: The Rise of a Prodigious Cyber Threat* (pp. 43-64). Cham: Springer International Publishing. DOI:10.1007/978-3-030-66583-8

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15), 6666.

Shivarudraiah, A. (2023). Cyber Resilience Strategies for Cloud-Based Financial Systems. *International Journal of Emerging Trends in Computer Science and Information Technology*, *4*(1), 25-33.

Umoga, U. J., Sodiya, E. O., Amoo, O. O., & Atadoga, A. (2024). A critical review of emerging cybersecurity threats in financial technologies. *International Journal of Science and Research Archive*, *11*(1), 1810-1817.

Zimba, A., & Chishimba, M. (2019). On the economic impact of crypto-ransomware attacks: The state of the art on enterprise systems. *European Journal for Security Research*, *4*(1), 3-31. DOI:10.1007/s41125-019-00039-8