Evaluation of Cybersecurity Implementation in the Master Plan for Information Technology (RITI) of Indonesian Banking in the Digital Era

Erlangga Faezal *[1], Lukman Abdurrahman[2],

* [1] Universitas Telkom, Bandung, Jawa Barat, Indonesia
[2] Universitas Telkom, Bandung, Jawa Barat, Indonesia

A R T I C L E I N F O

Jurnal Economic Resources

ISSN: 2620-6196
Vol. 8 Issues 1 (2025)

Article history:
Received – 07 Juni 2025
Revised – 13 Juni 2025
Accepted – 15 Juni 2025

Email Correspondence:
faezalerlangga@gmail.com

Keywords:
Bank Indonesia, Cybersecurity, Digital Banking, OJK (Indonesia's Financial Services Authority, RITI (Master Plan for Information Technology)

A B S T R A C T

The purpose of this study is to evaluate the implementation of cybersecurity policies outlined in the Master Plan for Information Technology (RITI) within Indonesia's digital banking sector, with a specific focus on assessing their effectiveness in mitigating increasingly sophisticated cyber threats. Employing a descriptive qualitative research design, this study uses a literature review approach based on credible sources, including peer-reviewed scientific articles, regulatory policy documents, and case studies involving cyberattacks on Indonesian banks. The findings indicate that while the regulatory frameworks established by Otoritas Jasa Keuangan (OJK) and Bank Indonesia (BI) serve as a solid foundation for cybersecurity governance, their implementation remains inconsistent across institutions, particularly due to resource disparities between large and small banks. Smaller banks often face significant obstacles such as limited IT infrastructure, insufficient human resources, and lack of technical oversight, which hinder the full adoption of cybersecurity standards. The discussion highlights the need for more proactive supervision, tailored technical support, and the adoption of AI-driven solutions for real-time threat detection and rapid incident response. The study concludes that fostering stronger collaboration between regulatory bodies, financial institutions, and private technology providers is crucial for creating an integrated and resilient cybersecurity ecosystem. These efforts are essential not only for strengthening system resilience but also for increasing customer trust in digital banking services.

INTRODUCTION

The rapid advancement of digital technology has significantly transformed the global financial landscape, including Indonesia's banking sector, which is transitioning from conventional to technology-based systems. This transformation enables the widespread use of digital banking services such as mobile banking, offering the public unprecedented convenience in accessing financial products and conducting transactions at any time and from any location. While digital technology provides clear operational advantages, it also presents major risks—particularly in the form of cyber threats. These threats include malicious activities such as hacking, data theft, and malware attacks that compromise the integrity, confidentiality, and availability of digital systems. In the context of digital banking, such threats are particularly critical due to the sensitivity of financial data and the digital infrastructure involved, making banks prime targets for cybercriminals (Dermawan et al., 2023). In Indonesia, despite the implementation of various cybersecurity policies, challenges persist. Increasingly sophisticated cyberattacks such as the 2023 ransomware attack on Bank Syariah Indonesia (BSI), which led to the theft of 1.5 terabytes of sensitive data, and the DDoS attack on Bank Central Asia (BCA) that disrupted services for hours, underscore the sector's vulnerability and the urgent need for robust security mechanisms (Parulian et al., 2021). These events highlight the pressing necessity to critically evaluate the effectiveness of

cybersecurity implementation within the framework of the Master Plan for Information Technology (RITI) in Indonesian banking (Bank Indonesia, 2023).

Recent studies have examined various aspects of cybersecurity implementation in Indonesia's banking sector, providing foundational insights while also illustrating the need for further analysis. Putra et al. (2020) evaluated cybersecurity maturity in the human resource management domain of Bank Indonesia using the C2M2 framework, revealing that the institution had not yet achieved the highest level of maturity. Meanwhile, Fitri et al. (2024) explored how the national values derived from the 1945 Constitution are integrated into Bank BRI's security management, emphasizing the centrality of customer data protection in digital banking. Ula & Fuadi (2017) developed a governance framework to assess Information Security Governance (ISG) in banking, categorizing components into governance, managerial, and technical dimensions, and applying mathematical modeling validated through expert assessments. These studies collectively underscore the multifaceted nature of cybersecurity challenges in Indonesian banks and the ongoing efforts to align practices with regulatory and ethical standards. Additionally, Kharisma et al. (2024) have pointed out that the surge in digital transactions introduces significant cybersecurity and consumer protection issues. The sector—including Islamic banks—is increasingly exposed to cybercrime that threatens customer trust and institutional credibility (Lubis et al., 2025) . While regulatory mechanisms such as the Electronic Information and Transactions Law (UU ITE) are in place, their effectiveness is hampered by vague provisions and inconsistent enforcement (Aprilianti, 2024). Other studies have called attention to the importance of data security, the role of big data in cybercrime mitigation, and the broader cybersecurity ecosystem within fintech (Maliha, 2024). Solutions proposed include implementing encryption, continuous monitoring, staff training, and regulatory harmonization to bolster the resilience of Indonesia's digital banking infrastructure (Kharisma et al., 2024; Lubis et al., 2025).

Despite the expanding body of research on cybersecurity in Indonesia's banking sector, several empirical and theoretical gaps persist that warrant further investigation. Many previous studies have emphasized the importance of cybersecurity frameworks, national values, and technical safeguards, yet few have comprehensively evaluated the implementation of strategic cybersecurity policies such as those outlined in the Master Plan for Information Technology (RITI). For instance, Putra et al. (2020) provided valuable insights into cybersecurity maturity at Bank Indonesia, but their analysis was limited to workforce management without addressing cross-sectoral implementation or systemic interdependencies. Similarly, the governance-oriented model developed by Ula & Fuadi (2017) offers a strong theoretical foundation for assessing information security but lacks empirical validation across a broader spectrum of banking institutions. Meanwhile, Fitri et al. (2024) emphasized ethical dimensions and constitutional values, but their work did not evaluate technical readiness or operational resilience in the face of actual cyberattacks. On a broader level, while studies by Lubis et al. (2025) and Kharisma et al. (2025) identified key cybersecurity concerns—such as data security, regulatory inconsistencies, and the need for digital literacy—there remains limited empirical analysis connecting these concerns to the real-world effectiveness of RITI-based policy measures. Furthermore, although regulations such as the UU ITE are in place, their ambiguous provisions and uneven enforcement (Aprilianti, 2025) suggest a disconnect between policy intent and practical execution.

This study offers a novel contribution by specifically evaluating the implementation of cybersecurity policies embedded within the Master Plan for Information Technology (RITI) in the context of Indonesia's banking sector—a focus that has been largely overlooked in prior research. Unlike earlier studies that examine isolated frameworks, regulatory principles, or institutional roles, this research adopts a holistic lens to analyze how RITI's cybersecurity strategies are being operationalized across different banking

institutions, including their alignment with regulatory expectations and resilience against actual cyber threats. By integrating perspectives on institutional coordination (OJK, BI, BSSN), technical readiness, and policy enforcement, this study bridges the gap between normative regulatory frameworks and the empirical realities of cybersecurity management. The primary objective is to assess the effectiveness, strengths, and limitations of current cybersecurity implementations under RITI, using a descriptive qualitative method supported by literature review. This research aims to generate actionable insights that can inform strategic improvements, strengthen institutional preparedness, and enhance trust in Indonesia's digital banking ecosystem in the face of increasingly sophisticated cyber threats.

LITERATURE REVIEW

Cybersecurity

Cybersecurity refers to the practice of protecting systems, networks, and programs from digital attacks that are intended to access, change, or destroy sensitive information, extort money from users, or interrupt normal business processes. In the banking sector, cybersecurity has become a critical component of operational integrity, especially as digital banking platforms expand and financial transactions increasingly rely on integrated information systems. In the Indonesian context, the acceleration of digital banking has exposed financial institutions to rising cyber risks such as phishing, ransomware, and distributed denial-of-service (DDoS) attacks. These vulnerabilities have prompted scholars and practitioners to evaluate both the technical and institutional mechanisms that can mitigate cybersecurity threats. For example, Kurnia (2024) highlight that governance structure, particularly board gender diversity, significantly influences the level of cybersecurity disclosure within Indonesian banks, suggesting that internal oversight plays a crucial role in shaping cyber resilience. Similarly, Maulisa et al. (2023) address how national initiatives like the introduction of the digital rupiah raise significant cybersecurity concerns, particularly in maintaining monetary sovereignty while managing data protection challenges. The concerns presented by these scholars underscore the importance of institutional readiness, especially within Bank Indonesia and the Financial Services Authority (OJK), to ensure policy alignment with evolving threat landscapes.

Moreover, recent systematic reviews have shed light on the broader dynamics of cybersecurity in financial technology and banking. Waliullah et al. (2025) conducted a comprehensive review of cybersecurity threats in digital banking, identifying prevalent risks such as identity theft, malware, and ransomware, and emphasizing the importance of deploying countermeasures like biometric authentication, AI-based fraud detection, and continuous system monitoring. In the same vein, Javaheri et al. (2024) provide a taxonomy of key cyber threats in the fintech industry and propose nine strategic defense mechanisms, including threat modeling, endpoint security, and regulatory compliance audits, which can be adapted by banking institutions. This evolving body of literature suggests that while technological interventions are critical, regulatory and organizational strategies must also be prioritized. The integration of artificial intelligence (AI) into banking cybersecurity has become increasingly relevant. According to Kovacevic et al. (2024), AI and machine learning have shown promise in detecting anomalies and responding proactively to cyber threats, although their use also introduces new risks such as adversarial attacks and algorithmic manipulation. Complementing these perspectives, Sidik (2020) emphasizes that Indonesia's financial institutions require a more harmonized legal and institutional framework to respond to increasingly sophisticated cybercrimes. His work advocates for the development of proactive national cybersecurity policies, improved coordination among state agencies, and enhanced literacy within the financial sector workforce. These insights collectively support the urgency for a thorough evaluation of cybersecurity

policy implementation, particularly within the Master Plan for Information Technology (RITI), as a foundational step toward building a secure and sustainable digital banking ecosystem in Indonesia.

Digital Banking

Digital banking refers to the digitization of all traditional banking activities and services that were historically only available to customers when physically inside a bank branch. These services include money deposits, withdrawals, fund transfers, and account management, all of which are now accessible via digital platforms such as mobile applications and internet banking. In Indonesia, the proliferation of smartphones, growing internet penetration, and digital transformation policies have led to an accelerated shift toward fully digital banking ecosystems. Windasari et al. (2022) highlight that the younger generations in Indonesia—particularly Gen Y and Gen Z—demonstrate a strong preference for digital-only banking experiences, which offer convenience, speed, and personalized services. This behavioral shift is not only reshaping consumer expectations but also driving banks to reengineer their service models. Similarly, Jaya (2024) examine how fintech and digital banking developments have influenced share prices and trading volumes in Indonesia's digital banks, emphasizing that the integration of technology is now a key determinant of financial market performance. Furthermore, Hidayat & Kassim (2023) reveal that the adoption of digital banking in Islamic financial institutions is influenced by perceived usefulness, ease of access, and trust, suggesting that religious and cultural contexts also shape digital transformation in the banking sector.

Alongside behavioral and cultural factors, institutional performance and technological efficiency have also been major themes in the discourse on digital banking. Amanda & Sudrajad (2023) using a Data Envelopment Analysis (DEA) approach, found that digital banking has significantly improved operational efficiency across several Indonesian banks from 2012 to 2020. Their findings support the notion that digitization can lead to cost savings and optimized service delivery. Complementing this efficiency narrative, Latiff et al. (2025) argue that fintech research plays an essential role in empowering the financial sector, especially through innovation and consumer-centric product development. Their study underscores the importance of integrating financial technology into traditional banking to maintain competitiveness. Moreover, digital banking is also closely linked to broader socio-economic goals such as financial inclusion. Triwibowo & Nurbasith (2023) that digital financial services, including mobile banking, e-wallets, and online credit platforms, have contributed significantly to increasing financial access among Indonesia's unbanked population. They stress that such progress must be supported by adequate digital infrastructure, regulatory frameworks, and financial literacy initiatives to ensure sustainable inclusion. Taken together, these studies show that digital banking in Indonesia is not merely a technological evolution but a systemic transformation with implications for customer behavior, institutional strategy, financial markets, and social equity.

Information Technology Master Plan (RITI)

An Information Technology Master Plan (RITI) is a comprehensive strategic framework designed to guide the development, governance, and implementation of information technology systems within an institution or sector. In the context of Indonesia's banking industry, RITI serves as a blueprint to ensure that digital infrastructure, cybersecurity measures, data governance, and innovation strategies are aligned with national objectives and global best practices. The plan provides structured direction to institutions such as Bank Indonesia and the Financial Services Authority (OJK), particularly in coordinating policy implementation, ensuring cybersecurity readiness, and enhancing institutional digital resilience. According to Maulisa et al. (2023), initiatives such as the development of the Digital Rupiah, which are

embedded within broader RITI objectives, underscore the importance of maintaining cybersecurity and data sovereignty while modernizing the national payment system. These authors argue that RITI is not merely a technical roadmap but also a strategic instrument for economic security in an increasingly digital environment. Moreover, the implementation of RITI in banking systems requires a balance between policy enforcement and institutional capacity building. Ilma (2022) point out that while several banks in Indonesia have integrated cybersecurity practices aligned with RITI directives, disparities in enforcement and internal control maturity remain significant challenges. Their study further emphasizes that effective cybersecurity implementation must be institutionalized through continuous auditing, workforce training, and technological investment, all of which are guided by the principles outlined in the IT Master Plan.

Additionally, the alignment of RITI with international digital banking and cybersecurity standards has been critically examined in recent literature. Waliullah et al. (2025) conducted a systematic literature review to assess global best practices in cybersecurity within the digital banking sector and highlighted several key mechanisms—such as multifactor authentication (MFA), biometric verification, and AI-driven threat detection—that align closely with the RITI strategic direction. These technologies, when embedded into RITI implementation, are essential in mitigating advanced persistent threats and securing customer data. The study by Maulisa et al. (2023) also reinforces the importance of building cross-sectoral collaboration in policy implementation. In Indonesia, coordination among Bank Indonesia, the OJK, and BSSN (National Cyber and Crypto Agency) is mandated within RITI to ensure timely incident response and threat intelligence sharing. However, this coordination still faces operational constraints. Ilma (2022) noted that the lack of integration between risk management systems and regulatory supervision frameworks often results in fragmented cyber policy execution. Therefore, RITI must not only provide strategic policy direction but also offer flexible and scalable implementation models adaptable to the rapidly evolving digital threats facing the banking sector. Collectively, these studies demonstrate that the effectiveness of RITI lies in its ability to translate strategic intent into enforceable action plans, supported by institutional readiness, technological competence, and inter-agency collaboration.

RESEARCH METHOD

This study employs a descriptive qualitative method with a literature review approach to evaluate the implementation of cybersecurity policies in Indonesia's banking sector in the digital era. The descriptive qualitative method was chosen by the researcher to analyze and understand the phenomenon within a broader context without involving statistical measurements, focusing instead on an in-depth understanding of the policies being implemented.

This method aims to provide a comprehensive overview of the implementation of cybersecurity policies in Indonesia's banking sector, particularly the policies outlined in the Master Plan for Information Technology (RITI) issued by the Financial Services Authority (OJK) and Bank Indonesia (BI) (Azmi et al., 2024).

The data used in this study is sourced from secondary literature, including scientific articles, policy reports, and case studies related to cyberattacks. Relevant case examples include the data breach at Bank Syariah Indonesia (BSI) in May 2023 and the DDoS attack on Bank Central Asia (BCA). The collected data will be analyzed to understand the strengths and weaknesses of the implemented policies and to provide recommendations for policy enhancement and the development of cybersecurity defense systems in Indonesia's banking sector (Zulfahmi et al., 2023).

RESULTS AND DISCUSSION

Cybersecurity Implementation in the RITI

1. Cybersecurity in the Master Plan for Information Technology (RITI) of Indonesia's Digital Banking Sector

   The Master Plan for Information Technology (RITI), developed by the Financial Services Authority (OJK) and Bank Indonesia (BI), includes a series of policies aimed at strengthening cybersecurity in Indonesia's digital banking sector. These policies are designed to ensure secure Information Technology (IT) infrastructure to prevent cyberattacks and protect customer data and digital transactions, which are critical components of digital banking services. OJK and BI establish policies that must be followed by digital banks to effectively manage cyber risks, ensure transaction security, and safeguard customer data.

   Cybersecurity in the RITI is a top priority because the rapid growth of Indonesia's digital banking sector brings with it increasing potential threats. The successful implementation of these policies will ensure that digital banks have adequate security systems to cope with the fast-evolving cyberattacks. In addition, these policies provide a clear framework for managing cyber risks, protecting personal data, and securing digital transactions within the banking sector.

   The following are the policies issued by OJK and BI that are part of the RITI and aim to strengthen cybersecurity in Indonesia's digital banking sector:

   A. OJK Regulation No. 11/POJK.03/2022

   This regulation governs the implementation of information technology in digital banking. It aims to ensure that the IT infrastructure used by financial institutions can protect customer data and the security of digital transactions, which are essential components of digital banking services. Under this regulation, OJK requires digital banks to implement encryption technology to protect data confidentiality and maintain the integrity of transaction systems. In addition, the regulation mandates that banks manage cyber risks by assessing potential cyber threats and ensuring effective security systems to monitor and mitigate existing risks. Overall, this regulation is designed to strengthen the resilience and security of information systems so that digital banks can face increasingly complex threats and maintain customer trust in transactions conducted through digital platforms (Otoritas Jasa Keuangan (OJK), 2022a).

   B. OJK Policy No. 29/SEOJK.03/2022

   This policy mandates that banks ensure the implementation of cybersecurity systems capable of protecting customer data and securing digital transactions. It stipulates that each bank must conduct vulnerability testing on their information technology systems and assess potential cyber threats that could impact operational continuity. In addition, banks are required to have effective system recovery procedures in place following an attack and implement mitigation measures to reduce the impact of such attacks on systems and customer data. The policy aims to strengthen cybersecurity resilience in the banking sector by ensuring that digital banking systems remain secure in the face of increasingly complex threats. Through this policy, OJK encourages banks to enhance their emergency response capabilities and improve their ability to identify and respond to cyber threats in real time. The main goals of this policy are to ensure the security of customer

data, increase customer trust in digital banking services, and maintain the integrity of digital payment systems against evolving cyber threats (Otoritas Jasa Keuangan (OJK), 2022b).

C. Bank Indonesia Regulation (PBI) No. 22/23/PBI/2020

This regulation governs the security of payment systems used by digital banks and other payment system providers in Indonesia. It was established to ensure that the payment systems used in digital banking transactions operate securely and are protected from cyber threats. To achieve this, Bank Indonesia requires digital banks to implement two-factor authentication (2FA) and data encryption to safeguard customer transaction data and ensure the integrity of the payment system. Additionally, the regulation mandates that banks proactively manage cyber risks by detecting potential threats early and ensuring proper system recovery procedures are in place following a cyberattack. The primary goal of this regulation is to strengthen the resilience of digital payment systems in facing increasingly complex threats such as DDoS attacks, hacking, and data theft, which could damage the reputation and trust in digital banking services. Through this policy, Bank Indonesia aims to ensure that transactions conducted through digital platforms remain secure while also promoting the development of a safe and reliable digital banking ecosystem, so that customers feel confident using these services (Hasanah et al., 2024).

Case Study of Cyberattacks on Indonesian Banking

1. Case of Bank Syariah Indonesia (BSI): Data Breach and Ransomware Attack

The data breach and ransomware attack on Bank Syariah Indonesia (BSI) in May 2023 was a significant incident in the landscape of Indonesia's digital banking sector. In this case, the LockBit ransomware group successfully accessed and stole approximately 1.5 terabytes of sensitive customer data, including highly confidential personal information.

The attack disrupted the operations of various BSI digital services. Mobile banking, ATMs, and teller services experienced access issues, hindering customers' banking activities. Although BSI made extensive efforts to ensure the security of customer data and funds, this incident revealed vulnerabilities in the implemented digital banking security systems.

The immediate impact of this incident was a decline in customer trust regarding the safety of their personal data and concerns about the potential misuse of leaked information. Additionally, the incident resulted in significant operational losses, including the costs of system recovery and repair.

BSI's reputation as a digital banking institution in Indonesia was also affected, particularly in regard to its ability to safeguard the confidentiality and integrity of digital transactions. This event underscored the importance of stricter cybersecurity policy implementation in the digital banking sector. Digital banks need to enhance their security infrastructure and establish more efficient and responsive recovery systems to address evolving threats.

Moreover, this incident reinforces the need to strengthen cybersecurity policies and risk management to anticipate similar threats in the future and maintain customer trust in using digital banking services (Putri et al., 2023).

2. Case of Bank Central Asia (BCA): DDoS Attack

In the same year, Bank Central Asia (BCA) experienced a Distributed Denial of Service (DDoS) attack that disrupted mobile banking, internet banking, and several ATM functions. The attack aimed to shut down the bank's operations by overwhelming the system with excessive data traffic, preventing customers from accessing services to perform transactions or check their account information.

Although the attack did not result in financial loss or customer data breaches, its impact on customer trust was significant. Customers began to question the bank's ability to manage cyber threats and protect critical digital services.

This incident served as an important lesson regarding the vulnerability of BCA's IT infrastructure in facing DDoS attacks, which are becoming an increasingly real threat in the digital banking sector. Nevertheless, BCA successfully restored its services in a short time and enhanced its security measures to address similar threats in the future.

The case highlights the importance of strengthening cybersecurity and system resilience to maintain service operations in Indonesia's digital banking sector. Furthermore, it reinforces the need for better protection of customer transactions, especially given the growing reliance on digital banking services by the public (Alfarizi et al., 2024).

Cybersecurity Weaknesses in the RITI

1. OJK Regulation No. 11/POJK.03/2022 on the Implementation of Information Technology

The main weakness of OJK Regulation No. 11/POJK.03/2022 lies in the uneven implementation of the policy between large banks and smaller banks, as well as in the lack of effective supervision. Smaller banks operating in the digital banking sector often lack adequate infrastructure and human resources to fully implement this regulation, which makes them more vulnerable to cyberattacks.

As the issuer of this regulation, OJK is not always able to provide sufficient support to help smaller banks meet the required standards. This weakness has the potential to create security gaps in the digital banking sector, thereby increasing the risk of cyberattacks that could harm both the banks and their customers (Aini et al., 2024).

2. OJK Policy No. 29/SEOJK.03/2022 on Resilience and Security

The customer data breach at Bank Syariah Indonesia (BSI) resulting from a ransomware attack revealed significant weaknesses in the implementation of this policy. The incident demonstrated that banks still undergoing digital transformation face serious challenges in conducting comprehensive vulnerability testing and risk assessments.

A major barrier lies in the limited availability of human resources with cybersecurity expertise and the inadequacy of existing IT infrastructure. In addition, the lack of sufficient technical support to combat increasingly sophisticated cyberattacks further exacerbates the situation.

System recovery procedures implemented by banks in general have also proven insufficient to effectively mitigate the impact of such attacks, as reflected in prolonged service disruptions and the potential for greater losses. The BSI case serves as a clear example of the weaknesses in the

implementation of this policy, where resilience and cybersecurity are already regulated, yet the enforcement heavily depends on each bank's internal capacity to adopt and uphold the policy (Putri et al., 2023).

3. Bank Indonesia Regulation No. 22/23/PBI/2020

   Bank Indonesia Regulation (PBI) No. 22/23/PBI/2020 faces several significant weaknesses in practice, particularly in the inability of financial institutions especially smaller banks and newer payment system providers to adopt the latest security technologies.

   Limited resources in both technology and skilled personnel capable of operating and managing security systems effectively remain major obstacles in the implementation of this policy. Many banks and digital payment system providers still lack adequate detection and mitigation mechanisms for cyberattacks, leaving a high potential for security breaches.

   These weaknesses indicate that while data protection is relatively well-addressed, the overall system resilience needs to be strengthened in order to withstand increasingly complex and sophisticated cyber threats (Luthfah, 2024).

Strengthening Cybersecurity in the RITI to Confront Digital Threats

Strengthening cybersecurity policies within the Master Plan for Information Technology (RITI) is essential to address the growing cyber threats in Indonesia's digital banking sector. The policies issued by the Financial Services Authority (OJK) and Bank Indonesia (BI) provide a strong foundation to confront these threats. However, improvements in implementation, supervision, and technological adaptation are needed to ensure the effectiveness of these policies.

The following are steps to strengthen cybersecurity policies in Indonesia's digital banking sector:

1. OJK Regulation No. 11/POJK.03/2022 on the Implementation of Information Technology

   The information system security of digital banks still faces several weaknesses in its implementation, particularly regarding the uneven application of policies between large and small banks. To strengthen this policy, OJK needs to enhance its supervision and provide more support to smaller banks that struggle to fully implement the policy due to limited IT infrastructure and human resources.

   OJK's supervision of the implementation of this policy has not been optimal in assisting smaller banks. Therefore, OJK must improve collaboration with relevant institutions and offer more intensive technical assistance. This is crucial to ensure that all banks especially smaller ones can meet the required security standards.

2. OJK Policy No. 29/SEOJK.03/2022 on Cyber Resilience and Security

   OJK Policy No. 29/SEOJK.03/2022 mandates banks to ensure cybersecurity in their operations. This policy provides guidelines related to cybersecurity in banking operational services. However, there are still significant challenges related to uneven implementation and insufficient oversight. Banks that have recently undergone digital transformation, such as BSI, often face difficulties in implementing vulnerability testing and risk assessments for existing threats.

The main issue here lies in the limited number of human resources with cybersecurity expertise and inadequate IT infrastructure. To strengthen this policy, OJK needs to enhance technical support and introduce the latest security technologies, such as AI-based threat detection systems, which can help smaller banks detect threats in real-time and recover systems more quickly after an attack.

3. Bank Indonesia Regulation (PBI) No. 22/23/PBI/2020 on Payment Systems

   Bank Indonesia Regulation (PBI) No. 22/23/PBI/2020 governs the security of digital payment systems with the aim of ensuring that digital transactions can be carried out safely. Although two-factor authentication (2FA) and data encryption have been implemented, vulnerabilities still exist, such as DDoS attacks and hacking that target service availability. Many banking payment system providers still lack the ability to detect threats in real-time and effectively mitigate attacks.

   Therefore, strengthening this policy should include improving attack detection capabilities and post-attack system recovery across the digital banking sector. One of the steps that can be taken is the implementation of AI-based technologies for faster threat detection. Bank Indonesia also needs to enhance collaboration with the private sector and international institutions to build a more integrated cybersecurity ecosystem, so that digital payment systems are better prepared to face increasingly sophisticated cyberattacks.

CONCLUSION

This study underscores the critical importance of evaluating the implementation of cybersecurity policies embedded within the Information Technology Master Plan (RITI) in Indonesia's digital banking sector as a response to increasingly complex cyber threats. While policies issued by the Financial Services Authority (OJK) and Bank Indonesia (BI) provide a solid regulatory foundation, findings indicate that their implementation remains hindered by disparities between large and small banks, particularly in terms of infrastructure readiness and institutional capacity. Additionally, the lack of consistent oversight and technical support—especially for smaller banks—continues to pose a significant challenge to achieving a resilient digital banking ecosystem.

From a scholarly and practical perspective, this study contributes original insights into the effectiveness and limitations of cybersecurity policy execution within a strategic national framework. It offers a policy-relevant analysis that is valuable for regulators, financial institutions, and industry stakeholders. Practically, the research implies the need for OJK and BI to strengthen regulatory supervision and extend more targeted technical assistance to ensure compliance and resilience across all banking institutions. Furthermore, the study highlights the managerial imperative of integrating advanced technologies such as AI-based real-time threat detection, as well as fostering multi-stakeholder collaboration between public institutions and the private sector to build a cohesive and trustworthy cybersecurity ecosystem.

This study is limited in scope as it relies primarily on secondary data and literature-based analysis, which may not fully capture the operational complexities experienced by diverse banking entities. It also does not include empirical insights from industry practitioners or end-users. Therefore, future research is encouraged to adopt a mixed-methods approach that incorporates primary data from conventional banks, digital banks, and supervisory bodies to yield a more comprehensive understanding of cybersecurity implementation under RITI. Additionally, subsequent studies should explore the adoption and impact of emerging technologies—such as artificial intelligence, blockchain, and zero-trust frameworks—within the

broader policy execution landscape, and how these innovations influence public trust and digital financial literacy over time.

REFERENCE

Aini, A. N., Girsang, R., Putri, A. J., & Suwarsit, S. (2024). Efektivitas Pengawasan Otoritas Jasa Keuangan (OJK) Dalam Menjamin Keamanan Dana Nasabah di Era Perbankan Digital: Studi Kasus Bank Syariah Indonesia. *Media Hukum Indonesia (MHI)*, *2*(4), 359–363. https://doi.org/10.5281/zenodo.14195708

Alfarizi, R., Satrio, A. J., Praseyto, Y. O., & Syahputra, M. F. (2024). ANALISIS PERKEMBANGAN TEKNOLOGI M-BCA DAN KEAMANAN SIBER DI BANK CENTRAL ASIA. *Jurnal Akademik Ekonomi Dan Manajemen*, *1*(4), 43–53. https://doi.org/10.61722/jaem.v1i4.3204

Amanda, P., & Sudrajad, O. Y. (2023). Evaluation of Digital Banking Efficiency in Indonesian Banking Sector using Data Envelopment Analysis (DEA) Approach. *International Journal of Current Science Research and Review*, *06*(08), 5345–5353. https://doi.org/10.47191/ijcsrr/v6-i8-01

Aprilianti, A. (2024). Efektivitas dan Implementasi Undang-Undang Informasi dan Transaksi Elektronik sebagai Hukum Siber di Indonesia: Tantangan dan Solusi. *Begawan Abioso*, *15*(1), 41–50. https://doi.org/10.37893/abioso.v15i1.1002

Azmi, M. N. A., Saifudin, H., Purba, C. T., Suryaningtyas, A., & Situmorang, U. S. (2024). Analisa Kasus Kebocoran Data pada Bank Indonesia Dalam Sistem Perbankan: Indonesia. *Jurnal Multidisiplin Ilmu Akademik*, *1*(6), 448–458. https://doi.org/10.61722/jmia.v1i6.3267

Dermawan, I., Baidawi, A., & Dewi, S. M. (2023). Serangan Cyber dan Kesiapan Keamanan Cyber Terhadap Bank Indonesia. *Jurnal Informasi Dan Teknologi*, 20–25. https://doi.org/10.60083/jidt.v5i3.364

Fitri, D., Soesanto, E., & Winny, W. (2024). Implementasi Nilai-Nilai Kebangsaan yang Bersumber UUD 1945 dan NKRI dalam Mengacu Peran Manajemen Sekuriti Menunjang Keamanan Data Nasabah di Era Digital pada PT Bank Rakyat Indonesia. *Sammajiva: Jurnal Penelitian Bisnis Dan Manajemen*, *2*(2), 84–105. https://doi.org/10.47861/sammajiva.v2i2.986

Hasanah, N., Sayuti, M. N., & Lisnawati, L. (2024). Optimalisasi regulasi perbankan syariah oleh Bank Indonesia dan Otoritas Jasa Keuangan dalam akselerasi transformasi digital. *Jurnal Manajemen Terapan Dan Keuangan*, *13*(03), 709–723.

Hidayat, A., & Kassim, S. (2023). THE DETERMINANTS OF DIGITAL BANKING ADOPTION AMONG BANKS OFFERING ISLAMIC BANKING SERVICES. *Journal of Islamic Monetary Economics and Finance*, *9*. https://doi.org/10.21098/jimf.v9i4.1688

Ilma, M. A. (2022). Bank role in preventing money laundering and cyber security. *Technium Soc. Sci. J.*, *37*, 287. https://doi.org/10.47577/tssj.v37i1.7595

Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2024). Cybersecurity threats in FinTech: A systematic review. *Expert Systems with Applications*, *241*, 122697. https://doi.org/10.48550/arXiv.2312.01752

Jaya, A. (2024). How Do Fintech and Digital Banking Affect Indonesia Digital Bank Share Prices and Trading Volumes? *Revenue Journal: Management and Entrepreneurship*, *2*. https://doi.org/10.61650/rjme.v2i2.222

Kharisma, D., Tobing, W. T. M. L., Susanti, E., & Aprili, R. (2024). Evaluasi Kebijakan Perlindungan Konsumen dalam Transaksi Digital di Indonesia: Studi Kebijakan dan Analisis SWOT. *Perkara: Jurnal Ilmu Hukum Dan Politik*, *2*(4), 565–578. https://doi.org/10.51903/perkara.v2i4.2228

Kovacevic, A., Radenkovic, S. D., & Nikolic, D. (2024). Artificial intelligence and cybersecurity in

banking sector: opportunities and risks. *ArXiv Preprint ArXiv:2412.04495*. https://doi.org/10.48550/arXiv.2412.04495

Kurnia, P., & Ardianto. (2024). Board gender diversity and cyber security disclosure in the Indonesian banking industry: a two-tier governance context. *Corporate Governance: The International Journal of Business in Society*, *24*(7), 1614–1637. https://doi.org/10.1108/CG-01-2023-0010

Latiff, A. R., Alqudah, M. Z., Samara, H., & Alslaibi, N. (2025). Empowering the financial sector: the role of fintech research development trends. *Future Business Journal*, *11*(1), 92. https://doi.org/10.1186/s43093-025-00512-y

Lubis, A. M., Jelita, G., Wirya, S. O. V., & Nurbaiti, N. (2025). Tantangan dan Keamanan Teknologi Informasi pada Manajemen Bank Syariah. *Switch: Jurnal Sains Dan Teknologi Informasi*, *3*(1), 148–162. https://doi.org/10.62951/switch.v3i1.344

Luthfah, D. (2024). Penguatan Keamanan Siber Pada Sektor Jasa Keuangan Indonesia. *Jurnal Penelitian Dan Karya Ilmiah Lembaga Penelitian Universitas Trisakti*, 259–267. https://doi.org/10.25105/pdk.v9i1.18643

Maliha, H. (2024). Cybersecurity and Fintech Studies in Academic Discussion. *Journal of Islamic Economics Literatures*, *5*(2). https://doi.org/10.58968/jiel.v5i2.578

Maulisa, N., Mahardika, Z., & Permana, R. B. (2023). Going Digital Rupiah: Some Considerations from Sovereignty, Cybersecurity and Resilience Perspective. *Journal of Central Banking Law and Institutions*, *2*(1), 25–54. https://doi.org/10.21098/jcli.v2i1.42

Otoritas Jasa Keuangan (OJK). (2017). Surat Edaran Otoritas Jasa Keuangan Nomor 21/SEOJK.03/2017 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum.

Otoritas Jasa Keuangan (OJK). (2022a). Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum.

Otoritas Jasa Keuangan (OJK). (2022b). Surat Edaran Otoritas Jasa Keuangan Nomor 29/SEOJK.03/2022 tentang Ketahanan dan Keamanan Siber bagi Bank Umum.

Parulian, S., Pratiwi, D. A., & Yustina, M. C. (2021). Studi tentang ancaman dan solusi serangan siber di indonesia. *Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT)*, *1*(2), 85–92. https://ejournal.upi.edu/index.php/TELNECT/article/view/40866.

Putra, A. P. G., Humani, F., Zakiy, F. W., Shihab, M. R., & Ranti, B. (2020). Maturity assessment of cyber security in the workforce management domain: A case study in Bank Indonesia. *2020 International Conference on Information Technology Systems and Innovation (ICITSI)*, 89–94. https://doi.org/10.1109/ICITSI50517.2020.9264982

Putri, D. F., Sari, W. R., & Nabbila, F. L. (2023). Analisis Perlindungan Nasabah Bsi Terhadap Kebocoran Data Dalam Menggunakan Digital Banking. *Jurnal Ilmiah Ekonomi Dan Manajemen*, *1*(4), 173–181. https://doi.org/10.61722/jiem.v1i4.331

Sidik, M. (2020). Cyber Security Applied For Financial Sector In Indonesia. *Jurnal Pajak Dan Bisnis (Journal of Tax and Business)*, *1*(1), 30–47. https://doi.org/10.55336/JPB.V1I1.6

Triwibowo, S., & Nurbasith, N. (2023). *Measuring Financial Inclusion in Indonesia: Asserting the Role of Digital Financial Services BT - Economics and Finance Readings* (E. Lau, R. K. Brahmana, & L. M. Tan (eds.); pp. 119–140). Springer Nature Singapore.

Ula, M., & Fuadi, W. (2017). A method for evaluating information security governance (ISG) components in banking environment. *Journal of Physics: Conference Series*, *812*(1), 12031. https://doi.org/10.1088/1742-6596/812/1/012031

Waliullah, M., George, M. Z. H., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital

banking: a systematic literature review. *ArXiv Preprint ArXiv:2503.22710*. https://doi.org/10.48550/arXiv.2503.22710

Windasari, N. A., Kusumawati, N., Larasati, N., & Amelia, R. P. (2022). Digital-only banking experience: Insights from gen Y and gen Z. *Journal of Innovation & Knowledge*, *7*(2), 100170. https://doi.org/10.1016/j.jik.2022.100170

Zulfahmi, E., Lilisdar, R., Ferdianti, P., Nurita, C., & Puspita, D. F. (2023). Perkembangan Industri Perbankan Di Era Digital. *Al-Iqtishad: Jurnal Perbankan Syariah Dan Ekonomi Islam*, *1*(1), 34–43. https://ejournal.staindirundeng.ac.id/index.php/aliqtishad/article/view/2213.