JOURNAL OF INFORMATION TECHNOLOGY AND ITS UTILIZATION, VOLUME 8, ISSUE 1, JUNE 2025
EISSN 2654-802X ; PISSN 2985-4067
DOI: https://doi.org/10.56873/jitu.8.1.6019. SUBMITTED: 9 JUNE, 2025; REVISED: JUNE 20, 2025; ACCEPTED: JUNE 26, 2025

Evaluating Bank DJX's Cybersecurity Maturity Level from Indonesia's Regulatory Perspective

Rahmat Rian Hidayat[1*], Juniana Husna[2], Son Ali Akbar[3]

[1,2] Sekolah Tinggi Multi Media, Yogyakarta, Indonesia
[3]Universitas Ahmad Dahlan, Yogyakarta, Indonesia
rianhidayat.r2h@mmtc.ac.id[1*]
*Corresponding author

***Abstract*--In the digitalization era of banking, cybersecurity has become a critical priority as the frequency and sophistication of cyber-attacks rise. This study evaluates Bank DJX's cybersecurity maturity (a pseudonym), focusing on compliance with POJK PTI and SEOJK regulations on cyber resilience in commercial banks. Using a qualitative approach, it assesses inherent cybersecurity risks and the effectiveness of risk management. Findings show a maturity score of 2.1, indicating effective and satisfactory practices, alongside an inherent risk score of 1.9 with a narrow gap (+0.20), suggesting that while current controls address existing threats, the capacity to manage emerging risks remains limited without further enhancements. Given the rapidly evolving threat landscape, continuous improvement is essential. Aligned with recommendations, Bank DJX is well-positioned to strengthen its cybersecurity resilience to meet regulatory demands and proactively address future threats. This study offers empirical insights into cybersecurity practices in Indonesia's digital banking sector, underscoring the importance of regulatory compliance and proactive risk management.**

Key words: **Digital bank; Maturity level; POJK PTI; Risk assessment; SEOJK.**

I. INTRODUCTION

The global banking sector has undergone a profound transformation driven by digital technologies. Innovations such as mobile banking, cloud computing, open APIs, and artificial intelligence have revolutionized customer experience, streamlined operations, and enabled data-driven decision-making [1]-[4]. However, this digital transformation has also introduced unprecedented cybersecurity risks, particularly for digital-first institutions wholly reliant on technology for service delivery and internal operations. One example is Bank DJX (a pseudonym), a digital-native banking institution that operates without a traditional branch network and leverages digital platforms as its primary customer interface. While such a model offers agility and scalability, it also presents complex cybersecurity challenges that can undermine service continuity, financial integrity, and public trust [5].

Cyberattacks on financial institutions have become more frequent, complex, and damaging. Threat vectors such as phishing, ransomware, credential stuffing, insider threats, and Distributed Denial of Service (DDoS) attacks have targeted critical assets, including payment systems, customer databases, and identity management platforms [6]. The consequences of these attacks are wide-ranging; Financially, they result in direct losses, fraud, legal penalties, and recovery costs. Reputationally, they erode consumer confidence and market competitiveness. Institutionally, they can impair regulatory relationships and investor perceptions [7]. More critically, cyberattacks on financial infrastructure can threaten systemic stability, as the interconnectivity of banking systems means a breach in one institution could have ripple effects across the economic ecosystem [8], [9]. The World Bank has also emphasized that strengthening cybersecurity supervision is now an essential element of safeguarding financial sector integrity [10].

As cybersecurity incidents continue to rise, regulatory bodies have increasingly recognized cyber risk as a fundamental element of financial stability and institutional soundness. The World Economic Forum (2023) emphasizes that cyber resilience has become as critical as capital adequacy and liquidity for the long-term sustainability of financial institutions [11]. In response to this global shift, many countries have introduced national regulations and frameworks to govern the secure use of information technology in banking operations. Moreover, protecting critical digital infrastructures such as central bank

EISSN 2654-802X ; PISSN 2985-4067
DOI: https://doi.org/10.56873/jitu.8.1.6019. SUBMITTED: 9 JUNE, 2025; REVISED: JUNE 20, 2025; ACCEPTED: JUNE 26, 2025

digital currency (CBDC) systems has emerged as a top priority. This urgency is further amplified by the anticipated disruption from emerging technologies like quantum computing, which may significantly alter the cybersecurity landscape [12].

In Indonesia, this responsibility falls on the *Otoritas Jasa Keuangan* (OJK), or the Financial Services Authority, which regulates and supervises the banking sector. OJK has issued several key policies to fortify banks' digital resilience. Among them, POJK: 11/POJK.03/2022 governs the Implementation of Information Technology by Commercial Banks (POJK PTI), while SEOJK: 29/SEOJK.03/2022 provides technical guidelines for implementing cyber-security and resilience measures [13], [14]. These instruments mandate banks to establish robust processes across the cybersecurity lifecycle-identification, protection, detection, response, and recovery. They also emphasize board-level accountability, organizational readiness, risk-based control implementation, and continuous monitoring. Beyond being compliance tools, these regulations serve as benchmarks to measure institutional maturity in cybersecurity governance.

Cybersecurity maturity has gained prominence as institutions seek structured methods to evaluate and to improve their cyber defenses. Cybersecurity maturity models (CMMs) provide a tiered approach to assessing an organization's capability, ranging from ad hoc or reactive practices to optimized and adaptive systems [15]. Maturity is often measured across multiple domains such as governance, risk management, operational controls, incident response, and workforce awareness. Maturity frameworks allow organizations to benchmark their current state, to identify gaps, and to implement a roadmap for continuous improvement. Models such as the NIST Cybersecurity Framework (CSF), COBIT, and CMMI are widely adopted globally [16]. Scholars have also adapted these for specific industries. For example, Alayo et al. [17] propose a governance-integrated maturity model tailored for financial institutions in Peru to improve service provision. Ozkan et al. [18], on the other hand, introduce the Cybersecurity Focus Area Maturity Model (CYSFAM), a generic framework based on 11 technical and organizational focus areas, tested in a large financial institution to validate its applicability. Meanwhile, Watkins and Hurley [19] emphasize the use of evidence-based metrics to measure cybersecurity maturity more scientifically.

Despite these advancements, the implementation gap between regulatory mandates and real-world practices remains a persistent issue. In Indonesia, this gap is particularly concerning in the context of digital banks. Unlike traditional banks, digital banks often operate with leaner teams, faster deployment cycles, and a stronger emphasis on user experience and market expansion. As a result, cybersecurity governance may be underdeveloped, decentralized, or reactive. Banks may sometimes view compliance with POJK and SEOJK as a checkbox exercise, focusing on documentation rather than building resilient infrastructure and a cyber-aware culture. This misalignment between compliance and actual resilience increases exposure to threats and undermines the strategic intent of regulation [20].

Research into cybersecurity governance in Indonesian banking remains limited. While several studies have explored IT governance and digital transformation, few have empirically assessed how banks particularly digital-native institutions implement national cybersecurity regulations. Even fewer have examined whether regulatory compliance is a valid proxy for cyber maturity. This knowledge gap is critical, especially as Indonesia promotes financial inclusion and digital banking as key pillars of economic growth. Without clear insights into the current state of cybersecurity maturity among banks, regulators may struggle to calibrate policies, and banks may remain unaware of systemic weaknesses until a significant breach occurs [7], [20].

This study seeks to address that gap by evaluating the cybersecurity maturity of Bank DJX using a diagnostic framework derived from POJK PTI and SEOJK. The evaluation encompasses strategic, operational, and technical dimensions, assessing how well the bank's cybersecurity practices align with regulatory expectations and industry standards. In doing so, it aims to uncover implementation strengths and vulnerabilities, offering a balanced assessment of current performance and future needs.

EISSN 2654-802X ; PISSN 2985-4067
DOI: https://doi.org/10.56873/jitu.8.1.6019. SUBMITTED: 9 JUNE, 2025; REVISED: JUNE 20, 2025; ACCEPTED: JUNE 26, 2025

The study is guided by a central research question: To what extent does Bank DJX exhibit cybersecurity maturity in accordance with Indonesian regulatory standards, and what strategic measures can be implemented to further enhance its cyber resilience?

In answering this question, the study will contribute to three main objectives. First, it will generate empirical evidence on cybersecurity governance in a leading Indonesian digital bank. Second, it will evaluate the practical application of OJK's regulatory frameworks, identifying enablers and barriers to effective implementation. Third, it will provide actionable recommendations for strengthening cybersecurity maturity that can inform banking policy, industry best practices, and internal strategy development.

By adopting a case-study approach with regulatory alignment at its core, this research offers both academic and practical value. It provides a template for evaluating other digital banks in Indonesia and potentially in other emerging markets with similar regulatory landscapes. More broadly, the findings support Indonesia's financial sector modernization agenda by aligning innovation with safety, speed with security, and growth with governance.

II. METHOD

This research employs a qualitative approach to analyze Bank DJX's cybersecurity maturity level. The method was selected to provide an in-depth understanding of the practices and policies related to cybersecurity risk management. It includes detailed interviews with key stakeholders at Bank DJX and an analysis of relevant cybersecurity documents.

Interviews were conducted to gain deeper insights into implementing the POJK PTI and SEOJK regulations and the challenges faced during this process. Additionally, document analysis was employed to validate the qualitative data obtained from the interviews. Focus Group Discussions (FGDs) with various departments were also held to gather collective perspectives on the implemented cybersecurity policies' effectiveness and identify areas for improvement.

The data collected from interviews, document analysis, and FGDs will undergo thematic analysis. The qualitative analysis technique is used to identify patterns, themes, and relationships among the policies, practices, and cybersecurity maturity level at Bank DJX.

The cybersecurity maturity assessment involves three key components that are interrelated and collectively provide a comprehensive picture of the Bank DJX's cyber risk exposure and its capability to manage and respond to cyber threats.

The first component is Cyber-related Inherent Risk Assessment, which evaluates the level of risk naturally present in the DJX Bank's operations before any security controls are applied. This assessment focuses on factors as shown in Table I, essentially establishing a baseline of the Bank's vulnerability to cyber risks based on its inherent characteristics.

TABLE I
Cyber-related Inherent Risk Assessment

Domain	Assessment
Technology	IT environment, network connectivity, cloud usage, software and EOL, BYOD and third-party access policy.
Product	The Bank's digital services: Online and mobile channels, ATMs, and IT-based card products.
Organizational Characteristics	The cybersecurity framework covers organization, roles, turnover, IT changes, and access control.
Cyber Incident Track Record	Number of cybersecurity incidents in the past 12 months.

The second component, Quality of Cybersecurity Risk Management Implementation, evaluates how effectively Bank DJX applies its cybersecurity controls and reflects its capability to mitigate or manage inherent risks. The specific control items are presented in Table II.

The third component is Quality of Cyber Resilience Process Implementation, evaluates the organization's effectiveness in responding to and recovering from cyber security incidents, as presented in Table III. Rather than focusing solely on preventive measures, this component emphasizes the bank's preparedness to sustain operations and recover swiftly in the event that preventive controls fail.

These three components are interrelated: inherent risk reflects the initial level of risk; cyber security risk management aims to reduce this risk

DOI: https://doi.org/10.56873/jitu.8.1.6019. SUBMITTED: 9 JUNE, 2025; REVISED: JUNE 20, 2025; ACCEPTED: JUNE 26, 2025

through controls; and cyber resilience ensures the organization can detect, respond to, and recover from incidents even if some controls fail. Notably, all the components tested for Bank DJX in this case study are based on POJK regulations.

TABLE II
Cybersecurity Risk Management Implementation

Domain	Bank's Control
Governance	Cyber-risk oversight by the Board through an independent structure with competent personnel, promoting shared responsibility and policy compliance.
Cyber Security Risk Management.	Annual documentation and review of cyber risks, roles, policies, gaps, and third-party governance.
Risk Management Process and ISRM.	RM based on ISO 27001:2013, with regular identification, assessment, and monitoring, supported by audits and a disaster recovery plan (DRP), and aligned with business complexity.
Internal Control System	Conducting regular internal controls and risk management evaluations through a dedicated internal audit unit and implementing a formal routine job rotation policy

TABLE III
Cyber Security Resilience Process Implementation

Domain	Cybersecurity Resilience
Asset, Threat & Vulnerability Identification	Effective asset management with regular vulnerability assessments and cyber security testing.
Asset Protection	Security controls aligned with ISO 27001:2013, including regular updates, secure coding, and consistent patching.
Cyber Incident Detection	SIEM supports key security functions, enabling continuous threat monitoring, detection, and analysis.
Cyber Incident Response & Recovery	Clear response and recovery plans, well-defined team roles, and structured escalation and reporting processes.

III. RESULT AND DISCUSSION

The inherent cybersecurity risk assessment, derived from in-depth interviews with key stakeholders, is rated on a scale of 1 to 5, where 1 denotes minimal risk and 5 indicates severe risk. The evaluation covers multiple dimensions, including technological infrastructure, banking products and services, organizational attributes, and the institution's history of cybersecurity incidents. The assessment results are summarized in Table IV.

TABLE IV
Cyber-related Inherent Risk Assessment Results

No.	Assessment Factor	Rating
1	Technology	2.7
2	Bank Products	2.2
3	Organizational Characteristics	1.8
4	Cyber Incident Track Record	1
Inherent Cyber Security Risk Rating		1.9

Table IV presents the inherent cybersecurity risk rating of 1.9, reflecting Bank DJX's overall awareness and preparedness in addressing cyber threats. The score is derived from multiple assessment dimensions, with the following key contributing factors:

1. Technology (2.7): This dimension received the highest risk rating, indicating that while Bank DJX employs secure and up-to-date technologies, the fast-evolving and complex nature of IT systems poses significant inherent risks. Ongoing investment in resilient infrastructure and advanced security solutions remains essential.
2. Bank Products and Services (2.2): This moderate score indicates that although the bank's digital offerings are generally secure, there is still room for improvement, especially in enhancing the security of digital transaction features.
3. Organizational Characteristics (1.8): This rating highlights the need to strengthen security culture and employee awareness. Ongoing training and awareness programs are crucial to mitigating human-related risks.
4. Cyber Incident Track Record (1.0): The lowest risk rating among all dimensions, indicating Bank DJX's strong track record in effectively managing cyber incidents, demonstrating the success of its mitigation and response efforts.

The Cybersecurity Maturity Level is assessed on a five-point scale, where a lower rating indicates higher maturity: Rating 1 (Strong),

EISSN 2654-802X ; PISSN 2985-4067
DOI: https://doi.org/10.56873/jitu.8.1.6019. SUBMITTED: 9 JUNE, 2025; REVISED: JUNE 20, 2025; ACCEPTED: JUNE 26, 2025

Rating 2 (Satisfactory), Rating 3 (Fair), Rating 4 (Marginal), and Rating 5 (Unsatisfactory). The cybersecurity maturity rating for Bank DJX is presented in the Table V.

TABLE V
Cybersecurity Maturity Assessment Results

No.	Assessment Factor	Rating
1	Quality of Cybersecurity Risk Management Implementation	2.16
2	Quality of Cybersecurity Resilience Process Implementation	2.04
	Cybersecurity Maturity Level Rating	2.10

The cybersecurity maturity level of Bank DJX is rated at 2.10, as shown in Table V. This rating is derived from two key components:

1) Cybersecurity Risk Management Quality (2.16): This indicates that Bank DJX has a well-structured system with systematic processes for identifying, assessing, and mitigating cyber risks, forming a strong foundation for information security.
2) Cyber Resilience Process (2.04): This shows that Bank DJX has implemented adequate measures to support post-incident recovery and ensure operational continuity.

Based on the average scores from Table IV (1.9) and Table V (2.10), Bank DJX falls into the "Low to Moderate" Cybersecurity Risk category, as illustrated in Fig. 1. This reflects a solid risk management approach supported by effective mitigation measures and a strong awareness of potential threats.

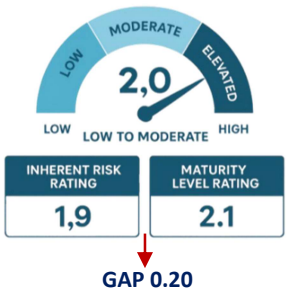

Fig. 1. Bank DJX Cyber Security Risk Level

However, the gap between the inherent risk level (1.9) and the cybersecurity maturity level (2.10) is relatively narrow (gap = +0.20), suggesting that while current controls are sufficient to address existing risks, there is limited buffer to accommodate emerging or escalating threats. Ideally, a more substantial maturity margin is recommended to ensure resilience, especially for digital-first institutions operating in high-threat environments.

The gap indicates that although some controls exist, they are not yet fully optimized or consistently applied. Strategic alignment between cybersecurity and business objectives needs reinforcement, and incident response processes require further testing, automation, and integration. Security awareness remains uneven, while monitoring practices tend to be reactive. Addressing these gaps requires targeted improvements in governance, technical measures, and organizational culture. By increasing maturity, especially in medium to high-risk areas, Bank DJX can strengthen its cybersecurity resilience to meet regulatory demands and anticipate future threats.

In light of the evolving cyber threat landscape, ongoing adaptation is imperative. To build upon its current maturity, Bank DJX should consider implementing several key enhancements: First, the establishment of a cybersecurity steering committee, alongside the integration of security metrics into leadership dashboards, will help ensure governance is aligned with strategic objectives. Second, risk management practices can be strengthened through regular threat modeling, quarterly updates to risk registers, and consistent assessments of third-party and vendor risks. Third, incident response capabilities should be reinforced by conducting frequent simulation exercises and developing a comprehensive crisis communication plan involving public relations and legal teams. Fourth, advancing technical controls requires the deployment of advanced threat detection tools, automation of log correlation, and adoption of Zero Trust Architecture principles. Fifth, enhancing the human factor involves implementing role-based cybersecurity training and phishing simulation programs, supported by reward mechanisms. Sixth, continuous improvement can be driven by adopting automated control validation frameworks and conducting annual benchmarking using updated standards such as NIST CSF or ISO/IEC 27001, in alignment with POJK

DOI: https://doi.org/10.56873/jitu.8.1.6019. SUBMITTED: 9 JUNE, 2025; REVISED: JUNE 20, 2025; ACCEPTED: JUNE 26, 2025

regulations. Lastly, regulatory compliance should be ensured through the development of a centralized compliance tracking system and the execution of regular independent audits.

By implementing these recommendations, Bank DJX can transform from a compliance-focused approach into a dynamic, risk-aware, and forward-looking cybersecurity ecosystem, better equipped to address evolving digital threats and maintain the trust of customers, regulators, and stakeholders.

IV. CONCLUSION

Based on the inherent risk assessment and cybersecurity maturity evaluation, Bank DJX demonstrates a strong commitment to managing cybersecurity risks. The implementation of effective policies and procedures, supported by investments in security technologies, has contributed to a relatively high maturity level. Nevertheless, like other banks, Bank DJX must continue adapting to the evolving cyber threat landscape.

V. REFERENCES

[1] Accenture, The Future of Banking: It's Time for a Change of Perspective, Dublin, Ireland, 2021.
[2] Deloitte, Digital Banking Maturity 2022, London, UK, 2022. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-digital-banking-maturity-report-sep-22.pdf.
[3] IBM, AI in Banking: Transforming Financial Services, Armonk, NY, USA, 2021. [Online]. Available: https://www.ibm.com/think/topics/ai-in-banking
[4] PwC-Cloud for Financial Services, Cloud is the Engine Required to Drive the Next Wave of Innovation within Financial Services, London, UK, 2023.
[5] O. Gulyás and G. Kiss, Impact of cyber-attacks on the financial institutions, Procedia Computer Science, Volume 219, 2023, pp. 84-90.
[6] Verizon, 2025 Data Breach Investigations Report, Verizon Enterprise Solutions, 2025.
[7] A. T. Oyewole, C. C. Okoye, O.C., Ofodile, and C.E. Ugochukwu. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio. World Journal of Advanced Research and Reviews. *21(3),* pp. 625-643.
[8] G. Birindelli & A.P. Iannuzzi. (2025). The Systemic Importance of Cyber Risk in Banks. In: Pacelli, V. (eds) Systemic Risk and Complex Networks in Modern Financial Systems. New Economic Windows. Springer.
[9] L. Liyanage, N. Arachchilage, G. Russello, A Novel Framework to Assess Cybersecurity Capability Maturity, arXiv:2504.01305, 2025, doi: https://doi.org/10.48550/arXiv.2504.01305. [Online]. Available: https://arxiv.org/abs/2504.01305
[10] The World Bank, Financial Sector's Cybersecurity: A Regulatory Digest, Washington, DC, USA, 2020.
[11] World Economic Forum, Global Cybersecurity Outlook 2023, Geneva, Switzerland, 2023. [Online]. Available: https://www.weforum.org/reports/global-cybersecurity-outlook-2023/
[12] World Economic Forum, Safeguarding central bank digital currency systems in the post-quantum computing age, Geneva, Switzerland, 2024.
[13] Otoritas Jasa Keuangan (OJK), Peraturan OJK No.11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum, Jakarta, Indonesia, 2022.
[14] Otoritas Jasa Keuangan (OJK), Surat Edaran OJK No.29/SEOJK.03/2022 tentang Ketahanan dan Keamanan Siber Bagi Bank Umum, Jakarta, Indonesia, 2022.
[15] G. Büyüközkan and M. Güler. Cybersecurity maturity model: Systematic literature review and a proposed model, Elsivier Technological Forecasting and Social Change, Volume 213, 2025, 123996, ISSN 0040-1625.
[16] National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, Gaithersburg, MD, USA, 2018.
[17] J. G. Alayo, P. N. Mendoza, J. Armas-Aguirre and J. M. Molina, "Cybersecurity maturity model for providing services in the financial sector in Peru," 2021 Congreso Internacional de Innovación y Tendencias en Ingeniería (CONIITI), Bogotá, Colombia, 2021, pp. 1-4
[18] B. Y. Ozkan, S. van Lingen, & Spruit, M. (2021). The Cybersecurity Focus Area Maturity (CYSFAM) Model. Journal of Cybersecurity and Privacy, *1(1),* pp. 119-139. https://doi.org/10.3390/jcp1010007.
[19] L. Watkins and J. S. Hurley. The Next Generation of Scientific-Based Risk Metrics: Measuring Cyber Maturity, International Journal of Cyber Warfare and Terrorism (IJCWT) *6(3),* pp. 43-52. https://doi.org/10.4018/IJCWT.2016070104.
[20] M. Perdana Karim, Archandra Viryasatya Sugama, 2023, Cyber Security Landscape of Indonesia's Banking and Financial Sector 2022, Center for Digital Society, Yogyakarta, Indonesia.