DIGITAL BANKS IN THE INDONESIAN BANKING SYSTEM: A POST-POJK NO. 12/POJK.03/2021 STUDY

Silvester Magnus Loogman Palit[1*], Tumian Lian Daya Purba[2]
[1,2]Universitas Cenderawasih, Jayapura, Indonesia
silvesterpalit@gmail.com[1*], tlpurba@gmail.com[2]

Received 30 Sep 2025 • Revised 31 Oct 2025 • Published 30 Nov 2025

Abstract

The transformation of digital banking in Indonesia is driven by technological advances and the need for efficiency, but its implementation raises issues of legal certainty and consumer protection following the issuance of POJK No. 12/POJK.03/2021. This study uses a normative juridical method with legislative, conceptual, and limited comparative approaches to assess the adequacy of regulations related to definitions, licensing, supervision, cybersecurity, and sanction regimes. The analysis is reinforced by comparisons with the European Union's Digital Operational Resilience Act (DORA) and the Monetary Authority of Singapore's Technology Risk Management (TRM) Guidelines. The results show that although POJK has provided formal legitimacy and established risk management prerequisites, the regulations are still declarative in nature in terms of data protection and have not set minimum technical standards such as encryption, multi-factor authentication, security audits, penetration testing, and incident reporting deadlines. The absence of technical compliance indicators and lines of legal accountability creates the potential for irregularities in the implementation of data protection. The discussion highlights the limitations of supervision, the potential for a digital divide, and the weak deterrent effect of administrative sanctions. It is concluded that strengthening regulations through integration with the Personal Data Protection Law, establishing prescriptive technical standards, regulating third-party risks, and inter-agency coordination are necessary to create a more adaptive and accountable digital banking ecosystem.
.

Keywords: digital banking; POJK 12/2021; consumer protection; cybersecurity; legal certainty

INTRODUCTION

The development of information and communication technology has driven a massive transformation in the banking sector, shifting the conventional branch-based model towards digital banks that rely entirely on digital platforms. This evolution is not just a technological trend, but part of a global effort to improve efficiency, financial inclusion, and shape an efficient and adaptive digital financial ecosystem. The number and growth of digital banks globally has shown a very significant trend in recent years. According to a Boston Consulting Group report (Pangarkar, 2025) ,there are more than 250 digital banks in the world, with the most rapid growth in the Asian region. It is estimated that global digital bank users will reach more than 2.5 billion people in 2024 and are projected to continue to increase to 3.6 billion by 2027. This figure confirms how digital banking has become one of the elements of transformation in the financial services industry at the global level.

In Indonesia itself, in 2022 the OJK reported that more than 70% of the population had used digital banking services, making Indonesia the largest market in the Southeast Asia region (E-Conomy Sea 2024: Profits on the Rise, Harnessing SEA's Advantage, 2024). This finding is preliminary evidence of how the phenomenon of digital banking is an integral part of the global financial system that requires strong, adaptive regulations oriented toward consumer protection and guaranteed financial system stability.

The development of digitalization in banking is carried out by adopting mobile application technology, artificial intelligence (AI), machine learning, blockchain, biometrics, and cloud computing (Venn, 2023). The adoption of technology in banking is done because it allows banks to accelerate services while reducing operational costs. For customers, these digital innovations also offer a personalized experience (Indriasari et al., 2022). In the banking sector, the use of AI and machine learning includes applications in predictive analytics, fraud detection, and the development of customer service that is more personalized according to customer preferences and needs. On the other hand, blockchain technology contributes to meeting the need for a more secure, transparent, yet accountable transaction infrastructure.

Digitalization in banking enables banks to cut operational costs, expand their service coverage to remote areas, and increase financial inclusion (Tran et al., 2023). According to Tuli (2024), the existence of banking digitization has also shifted the business model of banks from being mere providers of financial services to becoming collaborative digital platforms with fintech and bigtech, enabling them to offer products that are now inseparable from everyday life, such as digital wallets, mobile banking, robo-advisors, and IoT-based financial services.

Although it brings many benefits, it cannot be denied that there are still many risks associated with the adoption of technology in digital banking, such as cyber security threats, data protection, and regulatory compliance. Therefore, an adaptive regulatory framework is needed to maintain a balance between innovation and financial system stability, while ensuring the protection of customers as consumers (Vives, 2019).

In response to this risk assessment, the Financial Services Authority (OJK) ratified Financial Services Authority Regulation Number 12/POJK.03/2021 concerning Commercial Banks (hereinafter referred to as POJK No. 12/POJK.03/2021), which contains specific provisions regarding digital banks as part of commercial banks. The issuance of this regulation is intended to provide regulatory legitimacy to digital bank providers by regulating the technical requirements, risk management, and governance that must be met by digital banks. However, this regulation does not yet provide provisions that accommodate legal certainty, consumer protection, and national financial system stability. Many legal aspects and digital business models have not been specifically regulated (Sulistyandari & Sutrisno, 2023). Thus, the emergence of this regulation raises the question of the extent to which POJK is able to provide legal certainty, consumer protection, and financial stability.

This study contributes to the analysis of digital banking regulations following the issuance of POJK No. 12/POJK.03/2021 by highlighting legal gaps related to consumer protection, cybersecurity standards, and legal sanction mechanisms. In addition to examining regulatory challenges in Indonesia, this study also introduces a comparative approach with digital banking regulations in other countries such as Singapore, South Korea, and India to provide an overview of best practices. This study proposes strengthening regulations at a higher level, harmonization with the Personal Data Protection Law and other banking regulations, and clearer guidelines regarding operational standards for digital banks in Indonesia.

The research gap in this study lies in the absence of normative legal studies that specifically examine legal loopholes in the regulation of digital banks in Indonesia after POJK 12/2021, particularly regarding personal data protection, cybersecurity technical standards, and legal sanctions. Previous

studies, such as that conducted by (Israhadi, 2024) in *"Review of Digital Bank Law in Indonesia: Challenges in the Digital Era,"* focused more on the general challenges of banking digitalization and the need for additional regulations, but did not systematically examine the normative gaps in POJK 12/2021. Meanwhile, the study by (Tribroto et al., 2023) in *"Digital Banking Policy Implementation from the Perspective of Indonesia"* discusses the obstacles to the implementation of digital banking policies more from the perspective of public policy rather than from the perspective of legal certainty. The study (Yuspin et al., 2023) in *"Challenges and Opportunities for Digital Bank Regulation"* emphasizes legal disharmony in digital banking regulations, but has not yet linked this in detail to the need for technical security standards and legal sanctions.

On a global scale, digital banking regulatory standards have moved towards a prescriptive approach by setting minimum technical security standards that must be met. DORA in the European Union and TRM Guidelines in Singapore require digital banks to implement specific encryption, multi-layer authentication, periodic penetration testing, and incident reporting obligations within strict time frames. These provisions serve as an important reference for assessing the normative gap in POJK 12/2021, which does not specify similar technical requirements despite regulating general data protection obligations. This comparison is necessary to concretely demonstrate how technical gaps in Indonesian regulations can reduce legal certainty and the effectiveness of oversight in the digital banking ecosystem.

This study aims to fill this gap by presenting an in-depth analysis of the legal vacuum in the regulation of digital banks after POJK No. 12/POJK.03/2021, and comparing it with regulations in Singapore, which is more established in regulating digital banks, with the hope of providing concrete recommendations to strengthen the legal framework for digital banks in Indonesia to be more adaptive, comprehensive, and responsive to legal risks arising in the digital era.

RESEARCH METHOD

This study uses a normative juridical method through a statute approach, conceptual approach, and comparative legal research. Normative juridical legal research is a legal study conducted by examining theories, concepts, principles, and legislation through legal materials. This research was conducted to analyze the application of rules and norms in positive law (Rony Hanitojo, 1988). Soerjono Soekanto defines the normative legal research method as a legal study that conducts research on library materials or secondary data as the basic material to be examined by conducting a search of regulations and literature on the legal issues being studied (Soerjono Soekanto, 2008).

The legislative approach was carried out by reviewing POJK No. 12/POJK.03/2021 concerning Commercial Banks, Law No. 7 of 1992 in conjunction with Law No. 10 of 1998 concerning Banking, Law No. 21 of 2011 concerning OJK, ITE Law, and Law No. 27 of 2022 concerning Personal Data Protection to determine the extent to which positive regulations govern the existence of digital banks. A conceptual approach was taken by examining the theory of legal certainty and consumer protection theory to assess whether the regulations are able to provide normative guarantees as well as adequate protection for digital bank customers (Israhadi, 2024). Finally, a comparative approach was used in this study by comparing POJK 12/2021 with prescriptive regulatory frameworks, particularly the European Union's DORA and Singapore's TRM Guidelines, to identify minimum technical standards that have not yet been adopted in Indonesian regulations.

RESULTS AND DISCUSSION

Legal Framework for Digital Banks in Indonesia After POJK No.12/2021

Digital banks in Indonesia have officially gained legitimacy through the issuance of Financial Services Authority Regulation Number 12/POJK.03/2021 concerning Commercial Banks (hereinafter referred to as POJK No. 12/POJK.03/2021), which is a derivative regulation of the national banking framework. This regulation is an important milestone because previously, the term “digital bank” was not recognized in banking law. Digital banks in the POJK are defined as

"Indonesian Legal Entity Banks (BHI) that provide and carry out business activities primarily through electronic channels without physical offices other than their Head Office or using limited physical offices."

This provision is clarified in Article 23 of this POJK, which requires digital banks to have at least one physical office as their head office, while their main activities are carried out through electronic channels without additional physical offices. This provision provides flexibility, but on the other hand also raises concerns regarding supervision because the limitation of physical offices greatly affects consumer accessibility and the effectiveness of regulatory control (Israhadi, 2024). There are at least

three aspects affected by the limitation of physical offices in digital banks, namely supervision by the OJK, consumer accessibility, and control effectiveness.

's supervision of digital banks is carried out through two mechanisms, namely on-site (direct inspection at physical locations) and off-site (remote monitoring based on digital data). However, the limited number of physical offices has limited the effectiveness of on-site supervision, so OJK has placed more emphasis on technology-based supervision. This effort is carried out through the use of the OJK Suptech Integrated Data Analytics (OSIDA) system and the application of a regulatory sandbox as an instrument to monitor compliance levels and potential risks. However, in its implementation, digital supervision faces challenges in detecting violations that are not recorded digitally, as well as limitations in reaching customers who experience physical access constraints (Rahmanda et al., 2024).

From the customer's perspective, the lack of physical offices can be difficult for them, especially those in areas with low digital literacy or limited internet access (Rahmanda et al., 2024). This condition can hinder people's access to banking services, from opening accounts, resolving technical issues, to submitting complaints in the event of disputes or transaction problems. Dependence on digital channels, although efficient for users who are familiar with technology, has the potential to deepen the digital divide between urban communities and those in remote areas.

POJK also requires absolute requirements that must be met by every digital bank as stated in Article 24, namely that digital banks must have a business model with innovative yet secure technology, risk resolution mechanisms, accommodative risk management, competent resources in information technology and other fields relevant to operations, guarantees for customer data security, and contributions to financial inclusion. These requirements must be met with due regard for the principle of prudence because, according to Suryadarma & Pujiyono (2025), this principle plays an essential role in digital banking in maintaining the stability and integrity of financial institutions, as well as building and maintaining trust-based relationships between banks and customers. These provisions indicate that sanctions for digital banks are still limited to administrative aspects and do not extend to criminal or civil matters. Thus, in the event of a widespread violation, such as a large-scale customer data leak, there is no legal mechanism in place that can explicitly impose heavier sanctions on the responsible parties. This limitation has the potential to reduce the effectiveness of sanctions as an instrument of law enforcement and weaken the deterrent effect on business actors who are negligent in optimally implementing digital security standards.

According to the theory of legal certainty, regulations must provide clear, firm, and predictable norms for all parties. In the context of digital banking, this requires rules that not only regulate operational requirements but also provide effective legal accountability mechanisms. The lack of certainty regarding the form of sanctions, security standards, and dispute resolution mechanisms has the potential to create legal uncertainty that could undermine public confidence in digital banking (Israhadi, 2024). Although POJK 12/2021 has given the OJK the authority to impose administrative sanctions, the regulation does not comprehensively regulate coordination with law enforcement agencies, thus creating *a legal vacuum* in terms of digital banking crimes.

The lack of legal certainty has serious implications, because without comprehensive and prescriptive rules, regulations lose their enforcement power and weaken the deterrent effect on negligent businesses. This condition not only increases the risk of *cybersecurity breaches* without any guarantee of recovery for victims, but also threatens the stability of the national financial system. Therefore, digital banking regulations must be directed towards fulfilling the element of legal certainty through the formulation of strict security standards, clear complaint mechanisms, and applicable criminal and civil sanctions. (Papathanassiou, 2024) emphasizes that good digital banking regulations must be adaptive as well as prescriptive, i.e., regulating innovation while ensuring clarity of legal responsibility.

In addition to the issues of supervision and legal certainty, another crucial issue lies in the consumer protection framework within the digital banking ecosystem. The lack of physical offices has led to complete dependence on electronic channels for dispute resolution. However, the effectiveness of customer complaints is largely determined by the clarity of easily accessible resolution mechanisms. In practice, the OJK has launched *the OJK Contact Center (OJKCC)* and an *Integrated Complaint Management* system to facilitate consumer complaints, but these mechanisms are still administrative in nature and do not fully guarantee adequate compensation for losses. This situation reinforces the criticism that consumer protection in digital banking is still *compliance-based* rather than *remedy-based,* thus failing to create a sense of security and full public trust. According to recent research, the success of banking digital transformation is not only determined by technological efficiency, but also by the level of legal protection and the clarity of dispute resolution mechanisms that can minimize *the trust deficit*

among customers (Kornelis, 2022). Thus, strengthening regulations in the aspect of consumer remediation is an urgent need so that digital banks are not only innovative, but also accountable and trustworthy.

Implications of Legal Vacuum in POJK 12/2021

One of the fundamental weaknesses in POJK No. 12/POJK.03/2021 concerning Commercial Banks is found in Article 24 letter e, which requires digital banks to "implement protection for customer data security." This norm appears progressive because it explicitly recognizes the importance of customer data protection as a pillar of digital banking sustainability. However, the absence of binding technical standards from the Financial Services Authority (OJK) that provide detailed specifications means this regulation is merely declarative in nature, potentially leading to multiple interpretations and inconsistent implementation.

The provisions of Article 24 letter e in the *a quo* regulation, which does not stipulate minimum technical standards that must be met, creates a very broad scope for interpretation at the implementation level, so that data protection depends on the preferences of each bank. This condition creates legal uncertainty and inconsistency in security standards in the digital banking industry.

In international practice, digital banking regulations tend to set prescriptive provisions in the form of minimum standards that must be applied by all service providers. European Union regulations through the Digital Operational Resilience Act (DORA) and the Technology Risk Management (TRM) Guidelines from the Monetary Authority of Singapore (MAS) have regulated in detail various technical aspects that must be met as part of data protection and cybersecurity (Whardhono, et al., 2024). Unlike these two regulatory frameworks, POJK 12/2021 does not contain a binding list of minimum technical standards, creating gaps in consumer protection and supervisory effectiveness. To clarify these technical gaps, the following minimum standards should be regulated in POJK 12/2012 but have not yet been accommodated:

1. Minimum encryption type to protect sensitive data, both stored and transmitted, such as AES-256, RSA, or ECC encryption.
2. Multi-Factor Authentication (MFA) with certain levels, such as a combination of biometrics, OTP tokens, and device binding, as a prerequisite for high-value transactions or access to core banking systems.
3. Mandatory security audits and penetration tests, at least twice a year, to ensure that system vulnerabilities can be identified and addressed.
4. Mandatory technology incident reporting within a certain time frame, for example, 24–72 hours, as stipulated in DORA.
5. Data protection standards for data in transit and at rest, which must at least meet international standards such as ISO 27001 or PCI DSS.
6. Comprehensive oversight of third-party risk, including the obligation for cloud computing service providers or technology vendors to comply with certain security certifications.
7. The obligation of continuous monitoring and the use of real-time anomaly detection as part of digital operational resilience.

The absence of such standards results in POJK 12/2021 being declarative in nature and not providing normative certainty as prescriptive regulations in other jurisdictions do. Provisions that only stipulate general obligations without minimum technical standards such as data encryption requirements, routine security audits, penetration tests, or incident reporting obligations cause the implementation of data protection to depend on the interpretation of each digital bank. This situation not only leads to multiple interpretations and inconsistencies in the application of security mechanisms, but also weakens the position of consumers, increases the risk of data leaks, and limits the effectiveness of technology-based supervision by regulators. This situation underscores the urgency of developing clear, measurable, and consistent technical standards as the foundation for customer data protection in the digital banking ecosystem. According to Adegbite (2025), these standards include the use of strong data encryption (such as AES-256, RSA, or ECC), the implementation of *multi-factor authentication* (MFA, biometric, and OTP), regular security audits and *penetration testing*, *incident reporting* and *continuous monitoring* obligations, and compliance with international standards, including ISO 27001, PCI DSS, and GDPR (Vishwakarma, 2025). If these technical standards are not explicitly defined, digital banks tend to implement minimal or varying levels of data protection, thereby increasing the risk of data leaks and cyberattacks, while also reducing consumer confidence in digital banking systems (Mahadevan, 2025).

The absence of technical standards also weakens the position of customers in the legal system. In international practice, data protection standards are usually regulated in detail, for example, the General Data Protection Regulation (GDPR) in the European Union, which stipulates obligations for encryption, personal data management, and severe penalties for violations. In contrast, POJK 12/2021 only provides a normative framework without clear compliance indicators. This creates *a regulatory gap,* because even though Indonesia already has Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), its integration with POJK 12/2021 is not specifically regulated. The inconsistency between the PDP Law and POJK has the potential to cause regulatory overlap and create a vacuum in consumer protection mechanisms (Hukom et al., 2025).

Regulatory gaps and inconsistencies in digital banking regulations arise due to the lack of clear synchronization between the provisions of POJK 12/2021 and the Personal Data Protection Law (PDP Law). The lack of synchronization between POJK 12/2021 and the PDP Law is reflected in the provisions of Article 24 letter e of POJK 12/2021, which only requires digital banks to protect customer data in general without clear technical standards. In contrast, Law No. 27/2022 on Personal Data Protection (PDP Law) regulates technical and procedural obligations in detail, including data breach notifications and recovery mechanisms. This difference shows a lack of synchronization, as POJK is declarative in nature while the PDP Law is more prescriptive (Israhadi, 2024). Furthermore, Article 31 of POJK 12/2021 only contains administrative sanctions, while the PDP Law stipulates criminal and civil sanctions for serious violations. This situation creates the potential for overlapping authority between the OJK and the PDP Law enforcement authority, as well as *a legal vacuum* for customers who suffer losses due to data breaches.

This lack of technical integration weakens customer protection because the standards applied may differ between digital banks, leading to multiple interpretations in their implementation. This condition not only opens up loopholes for suboptimal data protection practices, but also creates legal uncertainty regarding accountability mechanisms in the event of violations. As a result, public confidence in the security of digital banking systems may be undermined, while the effectiveness of regulatory oversight becomes limited due to the absence of a consistent and comprehensive normative basis (Anggraini & Putra, 2025). The incoherence between the PDP Law and POJK has the potential to cause regulatory overlap, gaps in consumer protection, and legal uncertainty, while the weak enforcement and sanctions encourage banks to focus more on fulfilling administrative obligations than on the substance of data protection.

This regulatory weakness directly places consumers in a vulnerable position against the risk of loss. Digital banks tend to only fulfill their formal obligations to regulatory requirements. This practice opens up opportunities for *cyber fraud* through phishing, malware, and identity theft based on customer data due to the inadequate protection mandated by regulations for digital banks. Cyber fraud, including the leakage of customers' personal data, can cause losses, both material and immaterial, in the form of identity theft to commit other crimes (Sriono et al., 2024). Limited legal protection due to weak regulations has resulted in uncertainty regarding the bank's responsibility for customer losses, so that consumers often have to go through a long and uncertain legal process to obtain compensation. In this case, it means that the state has failed to guarantee legal certainty for its citizens as customers.

When viewed from the principle of legal certainty, data protection regulations in Indonesia's digital banking sector currently do not meet the principle of legal certainty. The theory of legal certainty requires clear, firm, and predictable rules so that customers understand their rights and banks know their obligations with certainty. However, existing regulations still cause uncertainty and potential for multiple interpretations. On a broader scale, legal uncertainty can hinder innovation in the digital financial ecosystem as a whole. Digital banking innovation requires a regulatory foundation that guarantees security and fairness for all parties. (Papathanassiou, 2024) emphasizes the importance of digital banking regulations being both adaptive and prescriptive, i.e., able to adapt to technological developments while still providing strong and enforceable legal certainty.

Comparison of Digital Banking Regulations with Singapore

To enrich perspectives and identify best practices, it is important to compare the regulatory frameworks for digital banking in countries that have already established their systems. In this context, Singapore is a relevant example for Indonesia because it is known to have a progressive and comprehensive regulatory framework for digital banking in the Southeast Asian region. Regulations under the supervision of the Monetary Authority of Singapore (MAS) emphasize a balance between innovation, security, and consumer protection. The digital banking licensing process in Singapore is strictly designed, with restrictions on the number of licenses, significant minimum capital requirements,

business feasibility tests, and restrictions on activities in the early stages to test business models and minimize systemic risk. Singapore's success is not only based on digital infrastructure support, but also on prescriptive and consistent regulations governing risk management and cybersecurity (Jessa, 2023).

The phased approach implemented by MAS requires digital banks to prove their operational stability before obtaining full licenses, thereby enabling more effective control of systemic risks (Sudirman et al., 2024). Conversely, regulations in Indonesia through POJK No. 12/POJK.03/2021 have indeed provided formal recognition of the existence of digital banks, particularly in Articles 23, 24, and 25, which open up opportunities for the establishment of new digital banks and the transformation of conventional banks. However, these provisions are still general and declarative in nature. For example, Article 24 letter e only requires digital banks to protect customer data without detailed technical standards, while Article 31 limits sanctions to administrative aspects without stronger legal instruments.

In contrast, MAS regulates *incident reporting* obligations through *Technology Risk Management (TRM) Guidelines*, which require banks to immediately report technology incidents and implement mitigation measures within a certain period of time. Research (Shanti et al., 2024) confirms that incident reporting obligations and the existence of comprehensive security standards are key factors in maintaining public trust in digital banks in Singapore. In addition, capital and governance requirements in Singapore are much stricter. Digital banks can only operate fully after meeting significant minimum capital requirements, proving the suitability of their management, and implementing comprehensive information technology risk management. Meanwhile, POJK 12/2021 emphasizes business model flexibility without accompanying minimum technical standards. This fundamental difference creates *a* potential *regulatory gap* in Indonesia, particularly in terms of consumer protection and the stability of the digital financial system (Tan, 2023).

The digital banking regulatory frameworks in Singapore and the European Union provide a clear picture of how minimum technical standards can be applied prescriptively. DORA regulates the obligation to report incidents within 24 hours, applies minimum encryption standards, requires threat-led penetration testing (TLPT), and strictly regulates third-party risk management, including cloud service providers. DORA also requires financial institutions to have operational recovery plans and real-time threat monitoring systems (Aisyah Dinda Ayuni and Imam Asmarudin, 2024).

Meanwhile, the MAS Technology Risk Management (TRM) Guidelines require multi-factor authentication for all sensitive transactions, stipulate the obligation to apply security patches within a certain period, regulate the obligation to conduct periodic technology audits, and require the reporting of material incidents to regulators as soon as possible (Imran Hussain Shah, 2025). The MAS approach is prescriptive and accompanied by auditable compliance indicators, thereby providing clear minimum standards for all financial institutions.

When compared to these two regulatory models, POJK 12/2021 still has a number of shortcomings. Among them are: it does not regulate deadlines for reporting technological incidents, does not set minimum standards for encryption or multi-factor authentication, does not require periodic penetration testing, does not regulate continuous monitoring, and does not regulate security standards that must be met by vendors and technology service providers. These gaps indicate that the regulatory framework for digital banking in Indonesia is still declarative in nature and is not yet compatible with international standards that emphasize operational security, digital resilience, and consumer protection.

As a measure to strengthen digital banking regulations in Indonesia, it is recommended that the OJK adopt the MAS's mandatory *incident reporting* practice, which requires digital financial institutions to immediately report technological incidents (e.g., data breaches, system disruptions) within a certain time frame and implement mitigation measures in accordance with established standards. This policy is in line with Singapore's *Technology Risk Management (TRM) Guidelines,* which form the basis for consumer protection and information technology risk control by the regulator. In addition, Indonesia needs to establish clear technical cybersecurity standards such as encryption, *multi-factor* authentication, periodic security audits, and supervision of third parties, as well as strengthen minimum capital and management competency requirements for digital banks so that less capable players do not damage the reputation of the financial system. In the realm of data protection, Indonesian regulations must provide certainty regarding the legal responsibility of banks for material losses suffered by customers due to security breaches, not just administrative protection. Recent legal studies indicate that customer data protection regulations in Indonesia are currently partial and do not guarantee comprehensive protection against material losses suffered by customers (Sriono et al., 2024). To ensure the effectiveness of this policy, synergy between institutions (OJK, BI, Ministry of

Communication & Information Technology, law enforcement) is needed so that regulations are not only fragmented but integrated within the framework of national digital security and consumer protection.

CONCLUSION

This study shows that although POJK 12/2021 has provided formal legitimacy for digital banks, its regulations are still declarative in nature and do not yet provide the minimum technical standards necessary to ensure legal certainty, consumer protection, and cybersecurity. The absence of prescriptive provisions, including those on encryption, multi-factor authentication, security audits, penetration testing, and incident reporting, has resulted in inconsistent data protection and supervision effectiveness, potentially leading to operational risks and data leaks. This condition shows that the existing regulatory framework is not as comprehensive as international standards such as DORA and TRM Guidelines. Regulatory strengthening is needed through harmonization with the Personal Data Protection Law, more detailed regulations on third-party risks, and the development of prescriptive and auditable technical standards to ensure the operational resilience of digital banks. An integrated and technically-based legal framework is a prerequisite for the formation of a digital banking ecosystem that is more secure, accountable, and consumer-protection oriented.

REFERENCES

Adegbite, M. A. (2025). DATA PRIVACY AND DATA SECURITY CHALLENGES IN DIGITAL FINANCE. *Journal of Digital Security and Forensics*, *2*(1). https://doi.org/10.29121/digisecforensics.v2.i1.2025.40

Anggraini, D. I., & Putra, P. O. H. (2025). Data Protection Impact Assessment Framework in the Banking Sector in Indonesia to Implement Law of Personal Data Protection. *Jurnal Sistem Informasi*, *21*(1), 15–34. https://doi.org/10.21609/jsi.v21i1.1439

Ayuni, A. D., & Asmarudin, I. (2024). *Penggunaan Blockchain dalam Pengelolaan Data: Studi Perbandingan Indonesia dan Singapura.* Penerbit NEM.

e-Conomy Sea 2024: Profits on the Rise, harnessing SEA's Advantage. (2024).

Hukom, S., Humi, N., & Lukman, I. (2025). The Urgency of Legal Regulation for Personal Data Protection in Indonesia in the Big Data Era. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *3*(1), 974–992. https://doi.org/10.51903/hakim.v3i1.2291

Indriasari, E., Prabowo, H., Lumban Gaol, F., & Purwandari, B. (2022). Intelligent Digital Banking Technology and Architecture. *International Journal of Interactive Mobile Technologies (IJIM)*, *16*(19), 98–117. https://doi.org/10.3991/ijim.v16i19.30993

Israhadi, E. I. (2024). Review of Digital Bank Law in Indonesia: Challenges in the Digital Era. *Migration Letters*, *21*(5), 380–392.

Jessa, S. K. (2023). The impact of COVID-19 on digital-only banks: are they winners or losers? *Journal of Banking Regulation*, *24*(3), 310–320. https://doi.org/10.1057/s41261-022-00198-0

Kornelis, Y. (2022). DIGITAL BANKING CONSUMER PROTECTION: DEVELOPMENTS & CHALLENGES. *Jurnal Komunikasi Hukum (JKH)*, *8*(1), 378–394. https://doi.org/10.23887/jkh.v8i1.44477

Mahadevan, G. (2025). Cybersecurity in Banking and Financial Software Solutions. *Economic Sciences*, *21*(1), 334–350. https://doi.org/10.69889/0btn6w55

Pangarkar, T. (2025). *Online Banking Statistics 2025 By Finance, Transactions, Growth*.

Papathanassiou, C. (2024). Digital Innovation and Banking Regulation. *SSRN Electronic Journal*, *351*. https://doi.org/10.2139/ssrn.4860754

Rahmanda, B., Anggayasti, U. H., & Nafi'a, Z. I. (2024). Banking Transformation in the Digital Era: Bank Cooperation with Financial Technology and the Role of the Financial Services Authority in Digital Bank Supervision. *INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND ANALYSIS*, *07*(12). https://doi.org/10.47191/ijmra/v7-i12-04

Rony Hanitojo. (1988). *Metodologi Penelitian Hukum dan Jurumenteri*. Ghalia Indonesia.

Shah, I. H. (2025). Digital Operational Resilience Act (DORA) And Similar Global ICT Risk Management Frameworks Requires a Structured Approach That Balances Theory, Empirical Evidence, And Critical Analysis. *Empirical Evidence, And Critical Analysis (August 13, 2025)*. https://dx.doi.org/10.2139/ssrn.5391781

Shanti, R., Siregar, H., Zulbainarni, N., & Tony. (2024). Revolutionizing Banking: Neobanks' Digital Transformation for Enhanced Efficiency. *Journal of Risk and Financial Management*, *17*(5), 188. https://doi.org/10.3390/jrfm17050188

Silaen, U., Srihandoko, W., & Listari, S. (2025). SUSTAINABLE BANKING MANAGEMENT. *Kesatuan Press*.

Soerjono Soekanto. (2008). *Pengantar Penelitian Hukum*. UI Press.

Sriono, Risdalina, Kusno, Kumalasari M, I., & Syahyunan, H. (2024). LEGAL PROTECTION FOR DIGITAL BANK CUSTOMERS IN INDONESIA: ANALYSIS OF DATA CONFIDENTIALITY REGULATIONS AND BANK RESPONSIBILITY. *LITIGASI*, *25*(2), 301–330. https://doi.org/10.23969/litigasi.v25i2.18538

Sudirman, L., Disemadi, H. S., & Jerryen, J. (2024). Bentuk Pengaturan Perbankan Digital di Negara Indonesia dan Singapura. *Legal Spirit*, *8*(2), 325–340. https://doi.org/10.31328/ls.v8i2.5438

Sulistyandari, & Sutrisno, P. A. (2023). Legal Aspects and Role of Ojk In Bank Digital by Digital Banking Services During Post-Covid 19 Pandemic in Indonesia. *Journal of Law and Sustainable Development*, *11*(12), e2364. https://doi.org/10.55908/sdgs.v11i12.2364

Suryadarma, R. F., & Pujiyono, P. (2025). Implementation of Prudential Principles in Risk Management in Digital Banking Business Models. *Devotion : Journal of Research and Community Service*, *6*(1), 19–29. https://doi.org/10.59188/devotion.v6i1.25408

Tan, A. T. (2023). *Overview of Digital Bank Regulation in Singapore*.

Tran, P. T. T., Le, T. T. H., & Phan, N. H. T. (2023). Digital Transformation of the Banking Industry in Developing Countries. *International Journal of Professional Business Review*, *8*(5), e01503. https://doi.org/10.26668/businessreview/2023.v8i5.1503

Tribroto, G., Hamzah, M. Z., & Hakim, L. (2023). Digital banking policy implementation from the perspective of the banking industry: Case study in Bali province. *OIDA Internation Journal of Sustainable Development*, *16*(11), 23–32.

Tuli, E. (2024). Exploring digital banking adoption in developing Asian economies: Systematic literature review and bibliometric analysis. *International Social Science Journal*, *74*(252), 399–426. https://doi.org/10.1111/issj.12463

Venn, P.-J. Van De. (2023). The evolution of digital banking. *Journal of Digital Banking*, *7*(4), 365. https://doi.org/10.69554/ULOC7565

Vishwakarma, D. (2025). Bank Management System with AES Encryption and Decryption for Secure and Scalable Financial Operations. *International Journal for Research in Applied Science and Engineering Technology*, *13*(5), 2854–2864. https://doi.org/10.22214/ijraset.2025.70814

Vives, X. (2019). Digital Disruption in Banking. *Annual Review of Financial Economics*, *11*, 243–272.

Yuspin, W., Sukirman, A. N., Budiono, A., Pitaksantayothin, J., & Fauzie, A. (2023). Legal Reconstruction of Indonesian Banking Laws: Challenges and Opportunities for Digital Bank Regulation. *Varia Justicia*, *19*(1), 52–69. https://doi.org/10.31603/variajusticia.v19i1.8019