International Journal of Law Analytics (IJLA)
Vol. 4, No. 1 2026: 17-36

Regulatory Challenges of Digital Banking Supervision in Indonesia

Diana R.W. Napitupulu
Universitas Kristen Indonesia
Corresponding Author: Diana R.W. Napitupulu diana.napitupulu@uki.ac.id

A R T I C L E I N F O

Keywords: Digital Banking, Financial Regulation, Banking Supervision, Consumer Protection, Financial Services Authority (OJK)

Received : 16, October
Revised : 18, December
Accepted: 20, February

©2026 Napitupulu: This is an open-access article distributed under the termsof the Creative Commons Atribusi 4.0 Internasional.

A B S T R A C T

This study examines the legal and regulatory issues surrounding the supervision of digital banking in Indonesia, with particular attention to consumer protection, data security, and supervisory effectiveness. Employing a normative juridical approach, this research analyzes statutory instruments, regulatory policies, and institutional mandates of Bank Indonesia and the Financial Services Authority, as well as recent financial sector reforms under Law Number 4 of 2023 on Financial Sector Development and Strengthening. The findings indicate that the current regulatory framework remains fragmented and largely derived from conventional banking regulation, resulting in legal gaps in addressing digital-specific risks such as cybersecurity threats, technology outsourcing, and real-time supervision limitations. Furthermore, supervisory authorities face institutional and technical constraints in adapting oversight mechanisms to rapidly evolving digital banking models.

DOI: https://doi.org/10.59890/ijla.v4i1.131
E-ISSN: 3032-4041
https://slamultitechpublisher.my.id/index.php/ijla

INTRODUCTION

The rapid digital transformation of the financial sector has fundamentally reshaped the banking industry in Indonesia. Driven by technological innovation, increased internet penetration, and changing consumer behavior, digital banking services have experienced significant growth over the past decade (Huang et al., 2024). Conventional banking models are increasingly complemented, and in some cases replaced, by digital platforms offering remote account opening, mobile-based transactions, digital lending, and integrated financial services. This development has been further accelerated by the emergence of financial technology (fintech) companies, which introduce new business models characterized by speed, efficiency, and data-driven operations (Chitimira & Ncube, 2023).

In response to these developments, Indonesia has witnessed the rise of fully digital banks and hybrid institutions that operate predominantly through electronic channels. Digital banks are expected to enhance financial inclusion, improve service efficiency, and support national economic growth (Apriani et al., 2024). However, their reliance on complex digital infrastructure, extensive data processing, and third-party technology providers introduces new legal and regulatory risks that differ substantially from those associated with traditional banking operations (Tkachuk et al., 2023).

Recognizing both the opportunities and risks posed by digital banking, Indonesian financial authorities have taken steps to adapt the regulatory framework. Bank Indonesia (BI) plays a central role in regulating and supervising payment systems and monetary stability, while the Financial Services Authority (Otoritas Jasa Keuangan/OJK) is responsible for the prudential regulation and supervision of banking institutions, including digital banks (Febriyanti & Haryanto, 2023; Susilo, 2023). OJK has issued several regulations concerning digital banking operations, risk management, governance, and consumer protection. Meanwhile, BI has strengthened regulations on electronic payment systems, digital financial services, and interoperability standards (Kemp & Buckley, 2017; Nordin et al., 2024).

A significant milestone in Indonesia's financial regulatory reform is the enactment of Law Number 4 of 2023 concerning Financial Sector Development and Strengthening (Undang-Undang Pengembangan dan Penguatan Sektor Keuangan). This law aims to modernize the financial system, enhance regulatory coordination, and improve resilience in the face of technological and systemic risks. While the law provides a broader legal foundation for financial sector reform, its implementation in the context of digital banking supervision raises important questions regarding regulatory adequacy, institutional readiness, and enforcement effectiveness (Halpin & Moore, 2009; Shamraev, 2019).

Despite the progressive regulatory initiatives undertaken by BI and OJK, the supervision of digital banking in Indonesia continues to face substantial legal and regulatory challenges. One of the primary concerns lies in the existence of regulatory gaps and fragmentation within the legal framework governing digital banking activities. Many regulatory instruments applicable to digital banks are adaptations of rules originally designed for conventional banking, which may not fully address the specific risks inherent in digital operations (Berlianty et al., 2025; Dehghan & Haghighi, 2015).

Consumer protection remains a critical issue, particularly in relation to transparency, dispute resolution mechanisms, and liability allocation in cases of system failures, cyber incidents, or unauthorized transactions. Digital banking services rely heavily on automated systems and digital interfaces, which may limit consumers' understanding of contractual terms and increase asymmetry of information. Furthermore, the growing volume of personal and financial data processed by digital banks raises serious concerns regarding data security, privacy protection, and compliance with data protection regulations (Adzmi et al., 2025; Kornelis, 2022).

Another significant challenge relates to supervisory capacity and effectiveness. Digital banking operations are characterized by high transaction volumes, real-time processing, and cross-border technological dependencies. These features require advanced supervisory tools, specialized technical expertise, and effective inter-agency coordination. However, existing supervisory mechanisms may not yet be fully equipped to monitor digital banking risks proactively and comprehensively, particularly in relation to cybersecurity threats, outsourcing arrangements, and the use of cloud computing and artificial intelligence (Jameaba, 2024; Yuspin et al., 2023).

Accordingly, there is a pressing need to critically examine whether the current regulatory and supervisory framework in Indonesia is capable of addressing the complex and evolving risks posed by digital banking. Without adequate legal clarity and effective supervision, digital banking may undermine consumer trust and financial system stability, rather than strengthening them (Kumalasari & Syahyunan, 2024).

This study aims to analyze the regulatory challenges associated with digital banking supervision in Indonesia from a legal perspective. The primary objective is to identify and examine the major regulatory and supervisory issues arising from the digitalization of banking services. This includes an assessment of legal gaps, regulatory inconsistencies, and enforcement limitations within the existing framework.

Furthermore, the study seeks to evaluate the institutional capacity of financial authorities, particularly BI and OJK, in supervising digital banking activities. This evaluation focuses on the adequacy of legal mandates, supervisory tools, and coordination mechanisms in addressing digital risks. By examining the interaction between regulatory norms and supervisory practice, the research aims to provide a comprehensive understanding of the strengths and weaknesses of Indonesia's digital banking oversight regime.

Finally, this research intends to propose legal and regulatory improvements to enhance the effectiveness of digital banking supervision. These proposals are directed toward developing a more adaptive, coherent, and risk-based regulatory framework that balances innovation with consumer protection and financial stability.

METHODOLOGY

This research employs a normative juridical method, focusing on the analysis of legal norms governing digital banking supervision in Indonesia. The study is based on a comprehensive review of relevant laws, regulations, and policy documents issued by BI, OJK, and other competent authorities. In addition, academic literature, journal articles, and comparative regulatory studies are examined to contextualize Indonesia's regulatory approach within broader theoretical and international perspectives. The normative analysis is complemented by a conceptual examination of regulatory challenges associated with digital banking, particularly in relation to consumer protection, data security, and supervisory effectiveness. Through this approach, the study aims to generate legal arguments and policy recommendations that are both doctrinally sound and practically relevant.

RESEARCH RESULTS

Overview of Digital Banking Regulations in Indonesia

1. Key Regulatory Frameworks

   The regulation of digital banking in Indonesia is primarily governed by a multi-layered legal framework involving statutory laws, regulatory instruments, and supervisory policies issued by several authorities. The Financial Services Authority (Otoritas Jasa Keuangan/OJK) and Bank Indonesia (BI) serve as the two principal regulators, each exercising distinct yet complementary mandates in overseeing digital banking activities. This dual regulatory structure reflects the complexity of digital financial services, which simultaneously involve banking operations, payment systems, and technological infrastructure.

OJK holds the primary authority over banking regulation and supervision, including digital banking institutions. Its regulatory framework addresses licensing requirements, governance standards, risk management, and consumer protection obligations applicable to banks operating digital services. OJK regulations require banks providing digital banking services to implement adequate internal controls, information technology risk management, and corporate governance mechanisms. These obligations are designed to ensure that digital banking activities are conducted prudently and in compliance with sound banking principles.

In the area of consumer protection, OJK has issued specific rules mandating transparency, fair treatment, and effective complaint-handling mechanisms for financial service providers. Digital banks are required to disclose relevant information concerning products, fees, and risks in a clear and accessible manner, notwithstanding the absence of physical interaction with customers. Additionally, banks must establish systems for handling consumer complaints and disputes arising from digital transactions. While these rules aim to safeguard consumer interests, their practical enforcement in a fully digital environment remains challenging, particularly where automated decision-making and complex digital interfaces are involved.

Bank Indonesia plays a crucial role in regulating and supervising payment systems, which constitute an essential component of digital banking services. BI exercises authority over electronic money, digital payment instruments, interbank transfer systems, and payment gateways. Its regulatory mandate focuses on ensuring the security, efficiency, and reliability of payment system infrastructure. BI regulations impose technical standards, licensing requirements, and operational obligations on payment system providers, including banks that offer digital payment services as part of their business model.

The regulatory framework is further supported by national legislation governing data protection and digital financial services. The enactment of the Personal Data Protection Law has established general principles for lawful data processing, data security, and individual rights over personal information. These provisions are particularly relevant to digital banks, which process large volumes of sensitive personal and financial data. In addition, broader financial sector legislation, including Law Number 4 of 2023 on Financial Sector Development and Strengthening, seeks to enhance regulatory coordination and strengthen the resilience of the financial system in the digital era. Together, these legal instruments form the foundational framework for digital banking regulation in Indonesia (Haykal, 2025).

2. Scope and Limitations

   The existing regulatory framework provides a relatively comprehensive scope of regulation for digital banking activities, particularly in relation to licensing, operational standards, and risk management. Digital banks are generally subject to the same licensing requirements as conventional banks, with additional obligations related to information technology readiness and digital service delivery. OJK regulations recognize digital banking as a permissible banking model, allowing banks to operate primarily through electronic channels, provided that they meet prudential and governance standards.

The regulatory framework also extends to digital financial services and neo-banks, which often operate through platform-based models and partnerships with technology providers. OJK requires banks engaging in digital innovation to comply with regulatory sandbox mechanisms, which allow for limited testing of new products under regulatory supervision. This approach reflects an attempt to balance innovation with risk mitigation, ensuring that new digital banking services do not undermine financial stability or consumer protection.

Despite these regulatory efforts, significant limitations remain. One of the most notable shortcomings is the absence of a dedicated legal framework that specifically governs digital banks as a distinct category of financial institutions. Current regulations largely treat digital banks as a variation of conventional banks, subject to modified requirements rather than a fundamentally different regulatory regime. As a result, certain digital-specific risks, such as cybersecurity vulnerabilities, algorithmic decision-making, and extensive reliance on third-party technology providers, are not comprehensively addressed.

Moreover, the fragmented nature of the regulatory framework creates challenges in ensuring consistent supervision. While OJK oversees banking activities and BI regulates payment systems, the boundary between these domains is increasingly blurred in digital banking operations. Digital banks often integrate payment services, lending, and data analytics into a single platform, making it difficult to delineate supervisory responsibilities clearly. This fragmentation may lead to regulatory overlap or, conversely, supervisory gaps that weaken oversight effectiveness.

Another limitation concerns the adaptability of existing regulations to rapid technological change. Digital banking innovations evolve at a pace that often outstrips the regulatory process, resulting in rules that may quickly become outdated. The reliance on conventional compliance and reporting mechanisms may also be insufficient for monitoring real-time digital transactions and systemic risks. Consequently, supervisory authorities face challenges in maintaining effective oversight without imposing excessive regulatory burdens that could stifle innovation.

In summary, while Indonesia has established a foundational regulatory framework for digital banking, the scope of existing regulations remains constrained by their conventional orientation and institutional fragmentation. The lack of a specialized legal regime for digital banks underscores the need for more adaptive, coherent, and technology-sensitive regulation. Addressing these limitations is essential to ensuring that digital banking development aligns with the objectives of consumer protection, financial stability, and sustainable innovation.

Major Regulatory Challenges

1. Legal Gaps and Fragmentation

   One of the most significant regulatory challenges in the supervision of digital banking in Indonesia lies in the existence of legal gaps and regulatory fragmentation. The current legal framework governing digital banking services is derived largely from conventional banking regulation, supplemented by sector-specific rules on financial services and data protection. While this approach provides a basic level of legal certainty, it fails to establish a coherent and comprehensive regulatory regime tailored to the unique characteristics of digital banking. Legal protection for digital banking services and personal data is dispersed across multiple statutes and regulatory instruments, each addressing different aspects of financial activity. Banking laws, financial services regulations, payment system rules, and data protection statutes operate in parallel, often without clear normative integration. As a result, digital banks must navigate overlapping compliance obligations, while regulators face difficulties in enforcing consistent standards. This fragmentation increases legal uncertainty, particularly in cases involving cross-sectoral issues such as data breaches, platform-based service delivery, and third-party technology outsourcing.

Furthermore, the absence of unified and adaptive regulatory standards poses challenges in supervising emerging digital banking models, including neo-banks and platform-based banking ecosystems. These models frequently combine banking, payment services, and digital marketplaces into integrated platforms, blurring traditional regulatory classifications. Existing regulations do not sufficiently accommodate these hybrid structures, leading to regulatory arbitrage risks and uneven supervisory treatment among market participants.

2. Consumer Protection and Data Security

   Consumer protection represents a central concern in the digital banking context, particularly due to the increased exposure of customers to digital risks. Digital banking services rely extensively on electronic interfaces and automated processes, which may limit consumers' ability to fully understand contractual terms, service risks, and liability arrangements. This situation exacerbates information asymmetry between service providers and consumers, undermining the principle of informed consent.

Data security and privacy protection constitute critical components of consumer protection in digital banking. Digital banks process vast amounts of sensitive personal and financial data, making them attractive targets for cyberattacks, data breaches, and fraud. Despite the existence of data protection regulations, the practical implementation of data security standards remains uneven. Cybersecurity threats evolve rapidly, while regulatory requirements often lag behind technological developments. This gap exposes consumers to risks of identity theft, unauthorized transactions, and misuse of personal information.

In addition, fraud prevention mechanisms in digital banking face structural limitations. The increasing sophistication of digital fraud schemes challenges existing detection and response systems. Although digital banks are required to implement security measures and transaction monitoring tools, enforcement and supervisory oversight of these obligations remain limited (Yuspin et al., 2024). Another persistent issue is the weak implementation of consumer education obligations. Digital banking providers are generally required to promote consumer awareness and financial literacy; however, such initiatives are often treated as formal compliance requirements rather than substantive protective measures. Insufficient consumer education reduces users' ability to recognize risks, manage digital security practices, and exercise their rights effectively.

3. Supervisory Capacity Constraints
   The effectiveness of digital banking regulation is closely linked to the supervisory capacity of regulatory authorities. In Indonesia, supervisory bodies face increasing challenges in monitoring a growing number of digital banking providers and digital financial services in real time. Digital banking operations generate large volumes of data and transactions at high speed, requiring advanced analytical tools and technical expertise to detect emerging risks.

Regulatory authorities often rely on periodic reporting and traditional audit mechanisms, which may be inadequate for identifying real-time operational, technological, and cybersecurity risks. The lack of integrated supervisory technology limits regulators' ability to conduct continuous monitoring and proactive risk assessment. As a result, supervisory interventions may occur only after significant risks have materialized.

Issues related to audit frequency and enforcement effectiveness further constrain supervisory outcomes. Digital banking activities, particularly those involving outsourced technology services and cross-border data processing, complicate audit processes. Regulators may face difficulties in accessing relevant data, verifying compliance, and imposing timely corrective measures. These constraints weaken deterrence and reduce the overall credibility of the supervisory regime (Endrosava & Afiliasi, 2024).

4. Technology and Innovation Regulatory Framework
   The regulatory framework governing technology and innovation in digital banking presents additional challenges. Regulatory technology (RegTech) and regulatory sandbox initiatives are designed to support innovation while ensuring compliance. However, their implementation in practice remains limited. Regulatory sandboxes often operate within narrow scopes and timeframes, restricting their ability to capture systemic risks associated with large-scale digital banking operations.

Moreover, the integration of RegTech solutions into regulatory practice requires significant investment, institutional adaptation, and technical capacity. Without adequate resources and expertise, regulators may struggle to leverage technological tools effectively for compliance automation and risk monitoring.

There is also a pressing need for updated technical standards governing digital services, cybersecurity, and digital know-your-customer (KYC) procedures. Existing standards may not adequately address emerging technologies such as artificial intelligence, cloud computing, and biometric identification. In the absence of clear and updated technical benchmarks, both regulators and market participants face uncertainty regarding compliance expectations.

5. Institutional Coordination Challenges
   Institutional coordination constitutes a structural challenge in digital banking supervision. The regulatory mandates of Bank Indonesia, the Financial Services Authority, and other state institutions intersect in the digital banking domain. However, coordination mechanisms among these entities are not always sufficiently integrated to address complex digital risks effectively.

As digital banking services increasingly transcend traditional regulatory boundaries, the lack of seamless coordination may result in regulatory overlaps or supervisory gaps. This situation undermines regulatory efficiency and complicates enforcement. Strengthening institutional coordination is therefore essential to ensuring coherent and effective supervision in Indonesia's rapidly evolving digital banking landscape.

Comparative and International Perspectives

1. Regional Regulatory Comparisons
   A comparative analysis of regional regulatory frameworks provides valuable insights into how digital banking supervision can be structured more effectively. Within the ASEAN region, Singapore is often regarded as a leading jurisdiction in regulating digital banking, offering important lessons for Indonesia. Singapore's regulatory approach is characterized by legal clarity, technological adaptability, and strong institutional coordination, particularly under the authority of the Monetary Authority of Singapore (MAS).

Singapore has established a dedicated licensing regime for digital banks, distinguishing clearly between digital full banks and digital wholesale banks. This differentiation allows regulators to tailor prudential requirements, capital thresholds, and risk management obligations according to the specific nature and scale of digital banking activities. By contrast, Indonesia's regulatory framework largely treats digital banks as extensions of conventional banking institutions, resulting in regulatory ambiguity and limited differentiation in supervisory standards. The Singapore model demonstrates the importance of recognizing digital banks as a distinct regulatory category rather than merely a variation of traditional banks.

Another notable feature of Singapore's regulatory model is its strong emphasis on technology risk management and cybersecurity. MAS imposes detailed and enforceable guidelines on technology governance, operational resilience, and outsourcing arrangements. These guidelines require digital banks to implement robust cybersecurity frameworks, conduct regular penetration testing, and ensure accountability at the board and senior management levels. In comparison, ASEAN jurisdictions with less developed digital banking regulation often rely on general risk management rules that lack specificity and enforceability. This contrast highlights the necessity for Indonesia to adopt more granular and technology-specific supervisory standards.

Other ASEAN countries, such as Malaysia and Thailand, have also introduced digital banking licensing frameworks and regulatory sandboxes to accommodate innovation. These jurisdictions emphasize phased licensing, allowing regulators to monitor digital banks' operational readiness before granting full authorization. While Indonesia has adopted regulatory sandbox mechanisms, their scope remains limited and primarily focused on fintech innovation rather than fully integrated digital banking supervision. The regional experience suggests that sandbox frameworks should be embedded within a broader supervisory architecture to ensure continuity between experimentation and long-term regulation.

Overall, regional comparisons indicate that effective digital banking oversight requires legal differentiation, proactive supervision, and regulatory flexibility. The ASEAN experience underscores the importance of harmonizing innovation-friendly policies with strong consumer protection and prudential safeguards (Rozikin, 2025).

2. Global Trends

   At the global level, digital banking supervision is increasingly shaped by international best practices that emphasize risk-based regulation, technological neutrality, and cross-border cooperation. Jurisdictions such as the European Union, the United Kingdom, and Australia have developed comprehensive regulatory approaches that address both financial stability and digital risk governance.

One prominent global trend is the adoption of risk-based supervisory models that focus on identifying and mitigating systemic risks associated with digital banking activities. Regulators prioritize areas such as cybersecurity, data governance, operational resilience, and third-party risk management. Rather than imposing rigid prescriptive rules, these frameworks allow supervisory authorities to adapt regulatory responses based on the risk profile of individual institutions. This approach enables regulators to address emerging risks without constraining technological innovation unnecessarily.

Cybersecurity regulation has become a central pillar of digital financial supervision worldwide. International best practices emphasize mandatory cybersecurity standards, incident reporting obligations, and coordinated response mechanisms. In several jurisdictions, digital banks are required to notify regulators of cyber incidents within strict timeframes and to maintain comprehensive incident response and recovery plans. These measures aim to enhance transparency, accountability, and systemic resilience. Compared to these standards, Indonesia's regulatory approach to cybersecurity remains relatively fragmented and reactive, indicating a need for stronger legal mandates and enforcement mechanisms.

Another significant global development is the increasing use of regulatory technology and supervisory technology (SupTech). Regulators are adopting advanced data analytics, artificial intelligence, and automated reporting systems to enhance real-time supervision and compliance monitoring. These tools enable authorities to process large volumes of transactional data and detect anomalies more effectively. While the adoption of RegTech and SupTech is still uneven across jurisdictions, leading regulators demonstrate that technological integration is essential for supervising complex digital banking ecosystems.

International cooperation also plays a critical role in digital banking supervision, particularly in addressing cross-border risks. Digital banking services often rely on global technology providers, cloud infrastructure, and cross-border data flows. Consequently, regulators are increasingly engaging in information-sharing arrangements and harmonizing standards through international bodies. This trend reflects a growing recognition that digital financial risks cannot be effectively managed through purely domestic regulation. From a comparative perspective, global best practices suggest that effective digital banking supervision requires a holistic regulatory framework that integrates prudential regulation, consumer protection, and technological governance. Legal systems that fail to adapt to these trends risk regulatory obsolescence and reduced supervisory effectiveness.

Comparative Implications for Indonesia

The comparative and international perspectives examined above reveal important implications for Indonesia's digital banking regulation. Regional and global experiences demonstrate that regulatory clarity, technological adaptability, and institutional coordination are essential components of effective supervision. Indonesia's reliance on conventional banking regulation, coupled with fragmented supervisory mandates, limits its ability to respond proactively to digital banking risks.

By learning from Singapore and other advanced regulatory models, Indonesia can develop a more differentiated and adaptive legal framework for digital banking. Incorporating global best practices in cybersecurity regulation, risk-based supervision, and regulatory technology would enhance supervisory effectiveness and strengthen consumer trust. Ultimately, aligning domestic regulation with regional and international standards is crucial for ensuring the sustainability and credibility of Indonesia's digital banking ecosystem in an increasingly interconnected financial environment.

Regulatory Responses and Innovations

1. Regulatory Sandbox and RegTech Adoption
   In response to the rapid expansion of digital banking and financial technology, Indonesian regulatory authorities have introduced a range of regulatory responses aimed at balancing innovation with risk mitigation. One of the most prominent initiatives is the implementation of regulatory sandbox mechanisms. Regulatory sandboxes allow financial institutions and technology-driven service providers to test innovative products, services, and business models within a controlled regulatory environment under the supervision of regulators. This approach reflects a shift from rigid, ex ante regulation toward a more experimental and adaptive supervisory model.

In Indonesia, regulatory sandboxes are primarily administered by the Financial Services Authority and Bank Indonesia, each within their respective regulatory mandates. These initiatives are designed to encourage innovation while enabling regulators to observe operational risks, consumer impact, and compliance challenges before granting full authorization. Through sandbox participation, regulators gain insights into emerging technologies and business practices, allowing them to refine regulatory requirements based on empirical experience.

Despite their potential benefits, regulatory sandboxes in Indonesia face several limitations. Their scope is often restricted to pilot projects and limited participant numbers, which may not adequately capture systemic risks associated with large-scale digital banking operations. Moreover, the transition from sandbox testing to full regulatory compliance is not always seamless, resulting in uncertainty for institutions seeking long-term authorization. Without clear criteria for scaling and integration into the broader regulatory framework, sandboxes risk becoming isolated experimental tools rather than integral components of digital banking supervision.

The adoption of regulatory technology (RegTech) represents another significant regulatory innovation. RegTech refers to the use of technological solutions to enhance compliance processes, risk management, and regulatory reporting. In the context of digital banking, RegTech tools can automate compliance monitoring, improve data accuracy, and facilitate real-time risk detection. For regulators, RegTech enables more efficient supervision by reducing reliance on manual reporting and enabling data-driven oversight.

However, the effectiveness of RegTech adoption is contingent upon institutional capacity and regulatory readiness. Implementing advanced technological solutions requires substantial investment, skilled personnel, and legal frameworks that support digital data sharing and analytics. In Indonesia, disparities in technological capability among regulated entities and regulators limit the uniform application of RegTech solutions. Additionally, overreliance on automated systems may create new risks, including algorithmic bias and reduced human oversight, necessitating careful regulatory calibration.

2. Policy Reforms

   In addition to sandbox and RegTech initiatives, recent policy reforms under the Financial Services Authority and Bank Indonesia reflect a broader effort to strengthen digital banking oversight. These reforms focus on enhancing governance standards, risk management requirements, and supervisory coordination. Regulatory instruments have increasingly emphasized technology risk management, outsourcing controls, and consumer protection obligations for digital banking services.

Bank Indonesia has introduced policies aimed at reinforcing the resilience and security of payment systems, which are integral to digital banking operations. These measures include stricter licensing requirements for payment service providers, enhanced cybersecurity standards, and operational reliability obligations. By strengthening oversight of payment infrastructure, BI seeks to mitigate systemic risks arising from digital transactions and interconnected financial networks.

Similarly, OJK has undertaken reforms to improve the prudential supervision of banks offering digital services. These reforms include requirements for stronger internal controls, clearer accountability of management and boards, and enhanced disclosure obligations. OJK has also sought to improve coordination with other regulatory bodies to address cross-sectoral issues, such as data protection and technology outsourcing.

Notwithstanding these reforms, challenges remain in ensuring that regulatory frameworks remain responsive to rapid technological change. Static regulatory instruments may quickly become outdated, limiting their effectiveness in addressing emerging digital risks. Accordingly, there is a growing need for dynamic and adaptive regulatory frameworks that can evolve alongside technological innovation.

To achieve this objective, regulators should prioritize principles-based regulation that allows flexibility in implementation while maintaining clear supervisory expectations. Enhanced use of regulatory impact assessments and stakeholder consultation can further support regulatory responsiveness. Moreover, strengthening inter-agency coordination and information-sharing mechanisms is essential to addressing the multifaceted risks of digital banking.

In conclusion, regulatory responses and innovations in Indonesia demonstrate a growing awareness of the challenges posed by digital banking. While regulatory sandboxes, RegTech adoption, and policy reforms represent important steps forward, their effectiveness depends on coherent integration, institutional capacity, and adaptive legal frameworks. Continuous regulatory innovation is therefore essential to ensuring effective digital banking supervision that supports innovation, protects consumers, and safeguards financial stability.

DISCUSSION

Synthesis of Key Challenges

The analysis of Indonesia's digital banking regulatory framework reveals a convergence of structural, legal, and institutional challenges that collectively undermine the effectiveness of supervision. At the core of these challenges lies legal incoherence, arising from the fragmented nature of regulations governing digital banking, payment systems, data protection, and financial consumer rights. Existing legal instruments were largely developed within the paradigm of conventional banking and subsequently adapted to accommodate digital services. This incremental approach has resulted in overlapping regulatory mandates and normative ambiguities that complicate both compliance and enforcement.

Supervisory capacity constraints further exacerbate legal incoherence. Digital banking operates in an environment characterized by high transaction volumes, real-time processing, and sophisticated technological infrastructure. Traditional supervisory models, which rely on periodic reporting and ex post audits, are increasingly insufficient to detect and mitigate emerging risks. The limited integration of supervisory technology and data analytics restricts regulators' ability to conduct continuous monitoring and proactive intervention. Consequently, supervisory actions tend to be reactive rather than preventive, reducing their effectiveness in addressing systemic digital risks.

Digital risk governance represents another critical challenge. Digital banks face unique operational risks, including cybersecurity threats, system failures, and dependence on third-party technology providers. While regulatory requirements impose general obligations for risk management, they often lack specificity in addressing digital-specific vulnerabilities. The absence of clear legal standards for technology governance, incident response, and operational resilience creates uncertainty regarding compliance expectations and accountability. This gap undermines the ability of regulators to enforce consistent and effective risk governance practices across the digital banking sector.

Data protection needs also emerge as a central concern. Digital banking services rely heavily on the collection, processing, and storage of personal and financial data. Although data protection legislation establishes general principles for lawful data processing, its integration into financial supervision remains limited. The lack of harmonized standards between financial regulation and data protection law weakens safeguards against data misuse and cyber incidents. As digital banking expands, ensuring robust data protection becomes not only a matter of individual privacy but also a prerequisite for maintaining systemic trust and stability.

Implications for Financial Stability and Consumer Rights

The regulatory weaknesses identified above have significant implications for both financial stability and consumer rights. From a systemic perspective, inadequate digital banking supervision may increase the vulnerability of the financial system to operational and technological shocks. Cyberattacks, system outages, or failures in critical digital infrastructure can have cascading effects across interconnected financial institutions and payment systems. In the absence of effective supervisory oversight, such incidents may escalate into broader systemic disruptions, undermining confidence in the financial system as a whole.

Financial stability is further threatened by regulatory arbitrage and uneven supervisory treatment. Fragmented regulation allows digital banking institutions to exploit gaps between regulatory regimes, potentially engaging in higher-risk activities without adequate oversight. This situation not only distorts competition but also increases systemic risk by concentrating vulnerabilities in less regulated segments of the financial system. Without coherent and comprehensive supervision, the rapid growth of digital banking may amplify rather than mitigate financial instability.

From the perspective of consumer rights, regulatory shortcomings undermine legal protection and trust. Digital banking consumers are particularly exposed to risks related to data breaches, unauthorized transactions, and opaque contractual terms. Weak enforcement of consumer protection obligations reduces access to effective remedies and dispute resolution mechanisms. Moreover, limited consumer education exacerbates information asymmetry, leaving users ill-equipped to assess risks and exercise their rights.

User trust is a foundational element of digital banking adoption. Regulatory failures that result in consumer harm or systemic incidents can erode public confidence in digital financial services. Once trust is compromised, the social and economic benefits of digital banking, including financial inclusion and efficiency gains, may be significantly diminished. Therefore, strengthening regulatory frameworks is not merely a technical or legal exercise but a fundamental requirement for sustaining public trust and legitimacy in the digital financial ecosystem.

Future Regulatory Directions

Addressing the challenges identified above requires a strategic and forward-looking regulatory approach. One key priority is strengthening supervisory frameworks through the adoption of risk-based and technology-enabled supervision. Regulators should invest in supervisory technology that enables real-time monitoring, data analytics, and early detection of digital risks. Integrating SupTech tools into supervisory practice would enhance regulators' capacity to oversee complex digital banking operations more effectively.

Improving institutional capacity is equally essential. Regulatory authorities must develop specialized expertise in digital technology, cybersecurity, and data governance. This objective can be achieved through targeted training programs, recruitment of technical specialists, and collaboration with academic and industry experts. Strengthening internal capacity would enable regulators to engage more effectively with regulated entities and respond to technological developments with greater agility.

Harmonizing laws and regulatory standards represents another critical future direction. A more coherent legal framework should clearly delineate regulatory responsibilities while ensuring normative integration across banking, payment systems, and data protection regimes. Establishing unified standards for digital banking governance, cybersecurity, and data protection would reduce legal uncertainty and improve compliance outcomes. Such harmonization should also address cross-sectoral and cross-border dimensions of digital banking, reflecting the interconnected nature of digital financial services.

Prioritizing digital security standards is indispensable for safeguarding both consumers and the financial system. Regulators should establish clear and enforceable cybersecurity requirements, including mandatory incident reporting, regular security assessments, and accountability mechanisms at the governance level. Aligning domestic standards with international best practices would enhance resilience and facilitate cross-border cooperation.

Finally, regulatory frameworks must remain adaptive and responsive to ongoing technological change. Principles-based regulation, complemented by flexible implementation mechanisms such as regulatory sandboxes and iterative rule-making, can provide the necessary balance between legal certainty and innovation. Continuous dialogue between regulators, industry participants, and consumers is essential to ensure that regulatory responses remain relevant and effective.

In conclusion, the discussion underscores that regulatory challenges in digital banking supervision are multidimensional and interrelated. Legal incoherence, supervisory capacity constraints, digital risk governance gaps, and data protection needs collectively shape the effectiveness of Indonesia's regulatory regime. Addressing these challenges through strategic, coordinated, and adaptive regulation is essential to protecting consumer rights, maintaining financial stability, and ensuring the sustainable development of digital banking in Indonesia.

CONCLUSIONS AND RECOMENDATIONS

This study has examined the regulatory challenges associated with digital banking supervision supervision in Indonesia within the context of an evolving financial and technological landscape. The analysis demonstrates that, while Indonesia has made notable progress in adapting its regulatory framework to accommodate digital banking, significant structural and systemic gaps remain. The existing legal framework continues to rely heavily on conventional banking regulation, resulting in limited differentiation between traditional and digital

banking models. This regulatory approach has contributed to legal fragmentation and uncertainty, particularly in relation to digital-specific risks.

The study further identifies shortcomings in consumer protection and data governance. Despite the presence of regulatory provisions addressing transparency and consumer rights, enforcement remains inconsistent, and the practical protection afforded to digital banking users is often inadequate. Data security and cybersecurity risks pose persistent challenges, exacerbated by fragmented regulatory oversight and insufficient integration between financial supervision and data protection regimes. These vulnerabilities undermine consumer trust and expose the financial system to operational risks.

Supervisory capacity constraints represent another critical finding. Regulatory authorities face difficulties in monitoring digital banking activities in real time, given the scale, speed, and complexity of digital transactions. Traditional supervisory tools and periodic reporting mechanisms are increasingly misaligned with the operational realities of digital banking. Additionally, institutional coordination challenges between supervisory bodies further limit regulatory effectiveness, particularly in addressing cross-sectoral and technology-driven risks.

In light of these findings, this study proposes several strategic recommendations to enhance the effectiveness of digital banking supervision in Indonesia. First, legal reforms are necessary to establish a more coherent and adaptive regulatory framework that recognizes digital banking as a distinct category of financial service. Developing specific legal standards for digital banking governance, technology risk management, and cybersecurity would provide greater legal certainty and improve compliance outcomes.

Second, institutional capacity building should be prioritized. Regulatory authorities must strengthen their technical expertise in areas such as cybersecurity, data analytics, and digital infrastructure. This can be achieved through targeted training, inter-agency collaboration, and the recruitment of specialized personnel. Enhanced institutional capacity would enable regulators to adopt more proactive and risk-based supervisory approaches.

Third, the integration of regulatory technology and supervisory technology frameworks should be expanded. The adoption of advanced data analytics, automated reporting systems, and real-time monitoring tools would improve supervisory efficiency and responsiveness. RegTech solutions can support compliance automation for regulated entities, while SupTech tools can enhance regulators' ability to detect emerging risks and enforce regulatory standards more effectively.

Fourth, international cooperation should be strengthened to address the cross-border dimensions of digital banking. Digital financial services frequently rely on global technology providers and cross-border data flows, making international regulatory coordination essential. Aligning domestic regulatory standards with international best practices and participating in cross-border supervisory networks would enhance regulatory resilience and facilitate information sharing.

ADVACED RESEARCH

While this study provides a normative legal analysis of digital banking supervision, further research is necessary to deepen understanding of regulatory effectiveness in practice. Future studies should focus on empirical assessments of digital banking supervision outcomes, including the effectiveness of regulatory enforcement and compliance mechanisms. Empirical research examining the impact of regulatory reforms on consumer protection, cybersecurity incidents, and financial stability would offer valuable insights into the practical implications of regulatory frameworks.

Additionally, comparative empirical research across jurisdictions could illuminate best practices and lessons applicable to Indonesia. Such studies would contribute to the development of evidence-based regulatory strategies that balance innovation with effective supervision. Ultimately, continued academic inquiry is essential to supporting the evolution of digital banking regulation in a rapidly changing financial environment.

REFERENCES

Adzmi, R., Gustanto, E. S., Lubis, R. R., & Gunardi, S. (2025). Electronic Security and Sharia Compliance: Addressing Legal Challenges in Digital Banking in Indonesia. Jeksyah: Islamic Economics Journal, 5(02), 73–85.

Apriani, M., Antika, R., Haerani, S., & Chaidir, T. (2024). A Systematic Literature Review: The Impact of the Use of E-Money as a Non-Cash Payment Instrument on the Stability of the Indonesian Financial System. Journal of Finance, Economics and Business, 3(2), 1–18.

Berlianty, T., Tjoanda, M., Titahelu, J. A. S., & Sahid, M. M. (2025). Reassessing Islamic Banking Supervision in Indonesia: A Contemporary Islamic and Socio-Legal Perspective on OJK's Integrated Model. MILRev: Metro Islamic Law Review, 4(1), 619–644.

Chitimira, H., & Ncube, M. (2023). The Prospects and Challenges for Mobile Money Regulation and the Promotion of Financial Inclusion in Zimbabwe. Financial Inclusion and Digital Transformation Regulatory Practices in Selected SADC Countries: South Africa, Namibia, Botswana and Zimbabwe, 125–140.

Dehghan, F., & Haghighi, A. (2015). E-money regulation for consumer protection. International Journal of Law and Management, 57(6), 610–620.

Endrosava, A. A., & Afiliasi, S. (2024). Peran Regulasi Modern dalam Menjaga Integritas Sistem Hukum Perbankan Digital. Jurnal Multidisiplin Ilmu Akademik, 1(6), 228–235.

Febriyanti, M., & Haryanto, I. (2023). Perbandingan Regulasi Bank Digital di Indonesia dan Singapura. Ajudikasi: Jurnal Ilmu Hukum, 7 (2), 257–270.

Halpin, R., & Moore, R. (2009). Developments in electronic money regulation–the Electronic Money Directive: A better deal for e-money issuers? Computer Law & Security Review, 25(6), 563–568.

Haykal, H. (2025). Toward a Responsive Legal Framework: Addressing Transaction Security Risks in Indonesia's Digital Banking Services. International Journal of Law and Society (IJLS), 4(2), 234–249.

Huang, Z., Lahreche, M. A., Saito, M., & Wiriadinata, U. (2024). E-money and monetary policy transmission. International Monetary Fund.

Jameaba, M.-S. (2024). Digitalization, emerging technologies, and financial stability: challenges and opportunities for the Indonesian banking sector and beyond. Emerging Technologies, and Financial Stability: Challenges and Opportunities for the Indonesian Banking Sector and Beyond (April 26, 2024).

Kemp, K., & Buckley, R. P. (2017). Resolution powers over e-money providers. University of New South Wales Law Journal, The, 40(4), 1539–1557.

Kornelis, Y. (2022). Digital banking consumer protection: Developments & challenges. Jurnal Komunikasi Hukum (JKH), 8(1), 378–394.

Kumalasari, I., & Syahyunan, H. (2024). Uncovering Legal Gaps in Digital Banking: Customer Protection and Bank Accountability in Indonesia. LITIGASI, 25(2), 301–330.

Nordin, N., Shahwan, S., Ibrahim, N., Nasir, N. M., & Awang, N. (2024). Electronic Money Institution and Protection Framework. International Journal of Business and Technology Management, 6(2), 50–69.

Rozikin, M. (2025). Analisis Kepatuhan Hukum Bank terhadap Regulasi OJK dan BI dalam Implementasi Layanan Digital Banking. Journal of Islamic Finance and Syariah Banking, 3(1), 49–58.

Shamraev, A. (2019). Legal and regulatory framework of the payment and e-money services in the BRiCS countries. BRICS Law Journal, 6(2), 60–81.

Susilo, A. (2023). Regulatory Technology Untuk Digitalisasi Proses Kepatuhan (Studi Kasus Bank Swasta Di Indonesia). INFOTECH Journal, 9(1), 252–258.

Tkachuk, S., Suprunenko, S., & Stender, S. (2023). Regulatory Challenges and Consumer Protection in the Context of the Growth of Electronic Money in Ukraine: A Literature Review. Law, Business and Sustainability Herald, 3(2), 15–29.

Yuspin, W., Putri, A. O., Fauzie, A., & Pitaksantayothin, J. (2024). Digital Banking Security: Internet Phishing Attacks, Analysis and Prevention of Fraudulent Activities. International Journal of Safety & Security Engineering, 14(6).

Yuspin, W., Wardiono, K., Nurrahman, A., & Budiono, A. (2023). Personal data protection law in digital banking governance in Indonesia. Studia Iuridica Lublinensia, 32(1), 99–130.