Journal of Cyber Law and Information Security
Volume 2, Number 1, 2023

A Comparative Analysis of Digital Banking Cybersecurity Regulations in Indonesia and Selected ASEAN Countries

Afifah Dwi Falah[1*]

[1] Universitas Sarjanawiyata Tamansiswa, Yogyakarta, Indonesia

Abstract

Article history:
Received: February 26, 2023
Revised: March 12, 2023
Accepted: April 28, 2023
Published: June 30, 2023

Keywords:
Cyber Resilience, Data Protection, Digital Banking, Institutional Accountability, Legal Comparison.

Identifier:
Zera Open
Page: 40-61
https://zeraopen.com/journal/jclis

Digital banking growth has increased the importance of cybersecurity regulation as banks become more dependent on electronic systems, data processing, cloud infrastructure, and third-party technology providers. This article examines how effective Indonesia's current legal framework on digital banking cybersecurity is compared with selected ASEAN countries in ensuring cyber resilience, data protection, and institutional accountability, and why comparative analysis is necessary for improving Indonesia's cybersecurity governance. Using comparative normative legal research, this study analyzes Indonesian regulations, including OJK regulations, Government Regulation No. 71 of 2019, and Law No. 27 of 2022, alongside regulatory approaches in Singapore, Malaysia, and the Philippines. The discussion shows that Indonesia has established an important legal foundation, but its framework remains fragmented and less operationally specific than selected ASEAN comparators. The article argues that Indonesia needs clearer cyber resilience standards, stronger integration between data protection and banking cybersecurity rules, better third-party risk governance, and more explicit board-level accountability to strengthen trust, legal certainty, and digital banking resilience.

*Corresponding author:
(Afifah Dwi Falah)

1. Introduction

Digital banking has become one of the most important manifestations of financial technology development in Southeast Asia. Banking services that were previously centered on physical branches are increasingly delivered through mobile applications, internet banking platforms, application programming interfaces, and cloud-based infrastructure. This transformation expands access, improves transaction speed, and supports financial inclusion, but it also changes the legal risk profile of banking activities. Digital banks no longer depend only on prudential capital, liquidity, and governance rules; they also depend on the legal capacity of regulators to ensure system resilience, data protection, authentication security, incident response, and accountability for cyber-related losses. As Gomber et al. (2018) explain, financial technology changes the structure of financial intermediation by combining innovation, platform-based services, and new operational dependencies. In the banking sector, this means that cybersecurity is not merely a technical issue, but a legal condition for maintaining trust in digital financial services.

The urgency of cybersecurity regulation becomes clearer when digital banking is understood as a high-risk legal relationship involving banks, customers, third-party technology providers, regulators, and cross-border digital infrastructure. Digital banking customers often submit personal identity data, biometric data, transaction histories, device information, and authentication credentials. These data are valuable for service personalization and fraud prevention, yet they also create exposure to phishing, malware, unauthorized access, identity theft, and large-scale data breaches. Vives (2019) notes that digital disruption in banking increases competition and

efficiency but also creates new regulatory challenges because financial activities become more dependent on data, technology platforms, and non-bank actors. Similarly, Barbu et al. (2021) emphasize that customer trust and experience in financial technology services are strongly influenced by perceived security, reliability, and institutional accountability.

Indonesia has responded to banking digitalization through several regulatory instruments, including the Banking Law, the Electronic Information and Transactions Law, Government Regulation No. 71 of 2019 on Electronic System and Transaction Operation, OJK Regulation No. 38/POJK.03/2016 on risk management in the use of information technology by commercial banks, OJK Regulation No. 12/POJK.03/2018 on digital banking services, OJK Regulation No. 12/POJK.03/2021 on commercial banks, and Law No. 27 of 2022 on Personal Data Protection. These instruments provide a normative basis for electronic system reliability, banking risk management, customer protection, and personal data governance. However, the Indonesian framework still raises questions about whether the rules are sufficiently integrated, specific, and enforceable in the context of digital banks. Yustisia (2022) argues that the development of digital banking services in Indonesia must be followed by regulatory readiness, particularly in relation to customer protection. Tarigan and Paulus (2019) also highlight that legal protection for digital banking customers requires clear responsibility from banks because customers increasingly rely on electronic channels rather than face-to-face transactions.

A comparative perspective is important because ASEAN countries face similar cybersecurity threats but adopt different regulatory designs. Singapore, Malaysia, and the Philippines have developed frameworks that place strong emphasis on technology risk governance, cyber resilience, outsourcing, incident reporting, and operational continuity. Singapore's approach is often associated with detailed technology risk management expectations for financial institutions, while Malaysia's Risk Management in Technology framework emphasizes board responsibility, cyber resilience, and control over technology arrangements. The Philippines formally recognizes digital banks as a distinct banking category through BSP Circular No. 1105, which provides a useful comparison for Indonesia's approach to digital banking within the broader commercial bank framework. These differences make comparative normative legal research relevant because it allows the study to examine not only whether Indonesia has regulations, but also whether the substance, structure, and enforcement orientation of those regulations are adequate when compared with selected ASEAN standards.

Recent cyber incidents further show why this issue requires legal analysis rather than purely technical discussion. The OCBC phishing incident in Singapore, in which customers suffered significant losses through SMS-based impersonation, illustrates how digital banking risks can arise from the interaction between banking systems, customer behavior, telecommunications channels, and fraud networks (Channel NewsAsia, 2022). Such cases demonstrate that cybersecurity regulation must address preventive duties, consumer notification, institutional liability, compensation mechanisms, and supervisory enforcement. In Indonesia, similar

concerns are relevant because digital banking adoption is expanding while legal responsibility for cyber incidents may involve overlapping rules on banking secrecy, consumer protection, electronic systems, and personal data protection.

Based on this background, this article examines two research questions: how effective is Indonesia's current legal framework on digital banking cybersecurity in comparison with selected ASEAN countries in ensuring cyber resilience, data protection, and institutional accountability; and what legal and regulatory factors make comparative analysis necessary for improving Indonesia's digital banking cybersecurity governance? This article uses a comparative normative legal research approach by analyzing statutory instruments, regulatory guidelines, and doctrinal literature. The central argument is that Indonesia has already built an important legal foundation for digital banking cybersecurity, but its effectiveness depends on clearer harmonization between banking regulation, electronic system governance, personal data protection, incident response duties, and enforceable supervisory standards.

2. Research Methods

This article uses a comparative normative legal research method to examine the effectiveness of Indonesia's digital banking cybersecurity legal framework in comparison with selected ASEAN countries. Normative legal research is appropriate because the study focuses on legal norms, regulatory structures, institutional obligations, and doctrinal interpretation rather than field-based measurement. The comparative element is used to evaluate how Indonesia's existing legal framework addresses cyber resilience, data protection, and institutional accountability when

compared with regulatory approaches adopted in Singapore, Malaysia, and the Philippines. These countries are selected because they have relatively developed digital banking or financial technology regulatory frameworks and provide relevant ASEAN-based references for assessing Indonesia's regulatory position.

The primary legal materials used in this study consist of statutory and regulatory instruments related to digital banking, cybersecurity, electronic systems, consumer protection, and personal data protection. For Indonesia, the analysis includes Law No. 27 of 2022 on Personal Data Protection, Government Regulation No. 71 of 2019 on Electronic System and Transaction Operation, OJK Regulation No. 38/POJK.03/2016 on the Implementation of Risk Management in the Use of Information Technology by Commercial Banks, OJK Regulation No. 12/POJK.03/2018 on Digital Banking Services by Commercial Banks, and OJK Regulation No. 12/POJK.03/2021 on Commercial Banks. For comparison, this study examines selected ASEAN regulatory instruments, including Singapore's Technology Risk Management Guidelines, Malaysia's Risk Management in Technology policy document, and the Philippines' digital banking regulatory framework under BSP Circular No. 1105.

Secondary legal materials include peer-reviewed journal articles, academic books, regulatory reports, and scholarly discussions concerning digital banking, financial technology regulation, cybersecurity governance, data protection, and technology risk management. Reputable news sources are used only as supporting materials to illustrate cyber incidents affecting digital banking users, not as the main basis for doctrinal analysis. The materials are selected based on relevance to the

research questions, credibility of publication, and connection to digital banking cybersecurity governance.

The analysis is conducted through statutory, conceptual, and comparative approaches. The statutory approach identifies the rights, duties, obligations, and supervisory mechanisms created by each regulatory framework. The conceptual approach examines key concepts such as cyber resilience, personal data protection, institutional accountability, technology risk management, and consumer protection. The comparative approach evaluates similarities and differences between Indonesia and selected ASEAN countries to identify regulatory gaps and possible lessons for improving Indonesia's digital banking cybersecurity governance. Through this method, the study assesses not only whether Indonesia has relevant regulations, but also whether those regulations are sufficiently integrated, specific, and enforceable in responding to cybersecurity risks in digital banking.

3. Results and Discussion

3.1. How effective is Indonesia's current legal framework on digital banking cybersecurity in comparison with selected ASEAN countries in ensuring cyber resilience, data protection, and institutional accountability?

Indonesia's current legal framework on digital banking cybersecurity can be considered partially effective because it already provides a normative basis for regulating technology risk, electronic system reliability, data protection, and banking supervision. However, its effectiveness remains limited when compared with selected ASEAN countries, particularly Singapore, Malaysia, and the Philippines.

The main issue is not the absence of regulation, but the fragmentation of legal instruments and the lack of a more integrated cybersecurity governance model for digital banking. Indonesia regulates digital banking cybersecurity through several instruments, including OJK Regulation No. 38/POJK.03/2016 on risk management in the use of information technology by commercial banks, OJK Regulation No. 12/POJK.03/2018 on digital banking services, Government Regulation No. 71 of 2019 on electronic system operation, OJK Regulation No. 12/POJK.03/2021 on commercial banks, and Law No. 27 of 2022 on Personal Data Protection. These instruments collectively create legal duties for banks and electronic system operators, but their effectiveness depends on how clearly they interact with one another in practice.

From the perspective of cyber resilience, Indonesia has taken an important step by requiring banks to manage information technology risk. OJK Regulation No. 38/POJK.03/2016 obliges banks to apply governance, risk management, internal control, audit, security management, business continuity, and outsourcing control in the use of information technology. This is relevant because digital banking services rely heavily on mobile applications, internet banking platforms, cloud services, data centers, application programming interfaces, and third-party vendors. Cybersecurity is therefore not merely a technical function but part of banking risk management. Anagnostopoulos (2018) explains that fintech and regtech development changes the relationship between banks, regulators, and technology because financial institutions are increasingly exposed to technology-based risks that require adaptive supervision. This supports the argument that digital banking regulation should not stop at formal

licensing or general compliance, but must also create continuous mechanisms for monitoring cyber risk and institutional preparedness.

Nevertheless, Indonesia's cyber resilience framework remains less detailed than the frameworks adopted by Singapore and Malaysia. Singapore's Technology Risk Management Guidelines and Malaysia's Risk Management in Technology policy document provide more operationally specific standards for technology governance, cyber risk monitoring, incident response, vulnerability assessment, outsourcing, and board-level responsibility. By comparison, Indonesia's framework gives banks general obligations to manage information technology risk, but it does not always specify measurable cyber resilience expectations, such as scenario-based cyber exercises, recovery time objectives, coordinated sectoral incident simulations, or detailed breach escalation procedures. This distinction matters because cyber resilience is broader than cybersecurity. Dupont (2019) defines cyber resilience as the capacity of financial institutions to withstand, recover from, and adapt to cyber shocks, rather than merely preventing attacks. This means that an effective digital banking cybersecurity framework should regulate not only prevention, but also recovery, continuity, adaptation, and institutional learning after cyber incidents.

Indonesia's effectiveness is also mixed in the area of data protection. Law No. 27 of 2022 on Personal Data Protection has strengthened the legal position of customers because it introduces clearer obligations concerning personal data processing, consent, data controller responsibility, data subject rights, breach notification, and sanctions. This is highly relevant for digital banking because banks process sensitive personal and financial information, including identity data,

transaction records, device information, biometric authentication, and behavioral data. Before the PDP Law, data protection in digital banking was scattered across banking secrecy rules, electronic system regulations, consumer protection principles, and internal bank governance duties. The PDP Law therefore creates a more general rights-based framework for protecting customers in digital financial services.

However, the effectiveness of data protection in digital banking still depends on its integration with financial sector cybersecurity rules. Personal data protection cannot be reduced to privacy notices or customer consent. In digital banking, data protection must include secure authentication, encryption, access control, data minimization, breach reporting, vendor control, and accountability for unauthorized access. This is where Indonesia still needs stronger regulatory harmonization. When a digital banking incident causes customer data exposure, the incident may fall under OJK supervision, electronic system operator obligations, PDP Law obligations, and possibly criminal law provisions under the Electronic Information and Transactions Law. Such overlap may strengthen protection if coordination is clear, but it may weaken enforcement if institutions apply fragmented interpretations.

In comparison, Singapore and Malaysia provide useful examples because their technology risk frameworks connect data governance with cybersecurity controls and institutional responsibility. Their regulatory models show that data protection should be embedded into financial technology risk management, not treated as a separate legal issue. This is important because digital banking operations often involve third-party technology providers. Banks may rely on cloud services, cybersecurity vendors, customer verification systems, payment gateways, and

software developers. If these third parties mishandle data or create system vulnerabilities, customers still expect the bank to be accountable. Therefore, data protection effectiveness depends not only on the existence of a privacy law, but also on the ability of banking regulation to allocate responsibility across the entire digital service chain.

The third indicator is institutional accountability. Indonesia already recognizes that banks must be responsible for the security and reliability of their digital banking services. OJK regulations require banks to apply risk management, while Government Regulation No. 71 of 2019 requires electronic system operators to ensure secure and reliable electronic systems. However, institutional accountability remains less explicit than in some selected ASEAN comparators. Singapore's and Malaysia's frameworks emphasize that technology risk is not only the responsibility of the information technology department, but also the responsibility of boards, senior management, risk management units, compliance units, and internal audit. This is important because many cybersecurity failures result from governance weaknesses, such as inadequate investment, poor vendor supervision, weak incident escalation, and insufficient customer warning systems.

Indonesia's accountability framework is also challenged by the multi-institutional nature of digital banking regulation. OJK supervises banks, Bank Indonesia supervises payment systems, the Ministry of Communication and Informatics has authority over electronic system operation, and the PDP Law introduces personal data protection obligations. This regulatory structure reflects the complexity of digital banking, but it also creates potential uncertainty regarding

reporting channels, enforcement authority, and responsibility allocation. The OCBC phishing incident in Singapore illustrates why accountability is important. The case showed that digital banking risks may arise through impersonation, social engineering, and communication-channel manipulation, even when the core banking system itself is not directly hacked. Such incidents raise legal questions about customer education, warning duties, rapid response, fraud monitoring, and compensation standards.

The comparative perspective shows that Indonesia's framework is moderately effective. It is effective in establishing a legal foundation for digital banking cybersecurity, but less effective in providing an integrated and operationally detailed governance model. The Indonesian framework already recognizes cyber resilience, data protection, and institutional accountability, but these elements are distributed across several instruments. In contrast, Singapore and Malaysia provide more consolidated technology risk expectations, while the Philippines provides a specific framework for digital banks through BSP Circular No. 1105. The Philippines' approach is relevant because it recognizes digital banks as a distinct category, which allows regulators to impose requirements that are more closely adapted to digital-only banking models. Indonesia, by contrast, regulates digital banking mainly through the broader commercial banking framework. This approach is not wrong, but it may require more detailed implementing rules to address risks specific to digital banking.

The role of digital finance in ASEAN also supports the need for stronger Indonesian regulation. Banna and Alam (2021) found that digital financial inclusion

can contribute to banking stability in ASEAN, suggesting that digital finance may strengthen the banking sector when it is supported by appropriate governance. However, this positive relationship depends on trust, reliability, and regulatory safeguards. Digital banking can support inclusion and efficiency, but if cybersecurity incidents increase, public confidence may decline. Similarly, Daud et al. (2022) found that fintech may promote financial stability through artificial intelligence, cloud technology, and data technology, but these same technologies also require strong governance to prevent systemic and institutional risks. These studies support the conclusion that digital banking cybersecurity regulation should not be seen as a barrier to innovation. Instead, it is a necessary condition for sustainable digital banking growth.

3.2. What legal and regulatory factors make comparative analysis necessary for improving Indonesia's digital banking cybersecurity governance?

Comparative analysis is necessary because digital banking cybersecurity is no longer a purely domestic regulatory issue. Digital banking services may be offered by Indonesian banks, but the supporting infrastructure often involves cross-border technology providers, cloud systems, payment networks, cybersecurity vendors, and data-processing arrangements. This creates legal risks that cannot be fully understood by examining Indonesian regulation alone. A comparative normative approach allows Indonesia's framework to be assessed against selected ASEAN countries that face similar digital transformation pressures but have developed different regulatory techniques. The purpose of comparison is not to copy another

jurisdiction, but to identify whether Indonesia's legal framework is sufficiently coherent, specific, and enforceable.

The first legal factor is regulatory fragmentation. Indonesia's digital banking cybersecurity governance is built from several legal regimes: banking regulation, electronic system regulation, personal data protection law, consumer protection law, payment system regulation, and cybercrime law. Fragmentation is understandable because digital banking intersects with many legal fields. However, fragmentation becomes a problem when legal obligations overlap without clear coordination. For example, a cyber incident in digital banking may involve OJK as banking supervisor, Bank Indonesia if the incident affects payment systems, the Ministry of Communication and Informatics if it concerns electronic system operation, and personal data protection authorities if customer data are exposed. Comparative analysis is necessary to evaluate whether Indonesia needs a more coordinated supervisory model for financial sector cybersecurity.

The second factor is the need to strengthen cyber resilience standards. Indonesia already requires banks to manage information technology risk, but comparative analysis shows that the next regulatory challenge is to move from general risk management to specific cyber resilience requirements. Dupont (2019) emphasizes that financial institutions must be able to withstand, recover from, and adapt to cyber shocks because complete prevention is impossible. This idea is highly relevant to digital banking because cyberattacks, phishing, malware, credential theft, ransomware, and system disruptions cannot be fully eliminated. Therefore, legal effectiveness should be measured not only by whether banks are required to secure

systems, but also by whether banks are required to test resilience, recover services, notify affected users, document incidents, and improve controls after failures.

The third factor is the growing importance of personal data protection. Digital banking depends on intensive data processing. Customers provide identity data, account data, transaction data, location data, biometric data, and behavioral data. This makes personal data protection central to cybersecurity governance. Indonesia's PDP Law is a major development, but its relationship with financial sector regulation still requires further clarification. Comparative analysis helps show that data protection in digital banking must be connected to cybersecurity controls, vendor accountability, breach notification, and customer remedies. Without this connection, data protection may become formal compliance rather than substantive protection. Singapore and Malaysia offer useful regulatory comparisons because their technology risk frameworks place data security within the broader structure of financial institution governance.

The fourth factor is third-party risk. Digital banking services are rarely operated entirely in-house. Banks may outsource cloud hosting, customer verification, cybersecurity monitoring, application development, payment processing, call centers, and data analytics. This creates a legal problem because customers have a direct relationship with banks, not with the bank's technology vendors. If a third-party provider causes a system failure or data breach, the bank should remain institutionally accountable. Indonesia already regulates outsourcing and electronic system reliability, but comparative analysis shows that third-party technology risk should be more explicitly governed. Malaysia's and Singapore's

frameworks are useful because they place significant attention on technology service providers, outsourcing arrangements, access rights, audit rights, and continuity planning.

The fifth factor is consumer protection. Digital banking customers face information asymmetry because they cannot directly evaluate the security architecture of banking applications. They depend on banks and regulators to ensure that systems are safe. This makes legal protection essential, especially when incidents involve phishing, social engineering, unauthorized transactions, or identity misuse. Tarigan and Paulus (2019) argue that legal protection for digital banking customers must be strengthened because banking relationships increasingly occur through electronic channels. Yustisia (2022) also emphasizes that customer protection in digital banking must address both transaction security and data-related risk. Comparative analysis is useful because it allows Indonesia to evaluate whether its framework provides clear complaint mechanisms, fair liability allocation, compensation standards, and institutional response duties.

The sixth factor is institutional accountability. Effective cybersecurity governance requires clear responsibility before, during, and after cyber incidents. In Indonesia, accountability is shared across banks, regulators, electronic system operators, vendors, and sometimes customers. However, the legal framework still needs clearer rules on senior management responsibility, board oversight, incident reporting, and enforcement consequences. Comparative analysis shows that Singapore and Malaysia place stronger emphasis on board and senior management accountability in technology risk governance. This is important because

cybersecurity failures are often governance failures. If management treats cybersecurity as a technical matter only, the institution may underinvest in controls, delay incident response, or fail to supervise vendors properly.

The seventh factor is regulatory adaptability. Digital banking technology evolves faster than traditional legislation. Artificial intelligence, open banking, biometric verification, cloud computing, digital identity, and application programming interfaces create new opportunities and new vulnerabilities. Anagnostopoulos (2018) explains that fintech and regtech development requires regulators and banks to rethink supervision because technology changes the structure of financial services. This is directly relevant to Indonesia because a static regulatory model may not be sufficient for rapidly changing digital banking risks. Comparative analysis helps identify whether Indonesia should strengthen its framework through technical guidelines, supervisory circulars, regulatory sandboxes, incident reporting protocols, or sector-specific cybersecurity standards.

The final factor is ASEAN financial integration. Digital finance is expanding across the region, and ASEAN countries are increasingly connected through cross-border payments, fintech investment, digital trade, and regional banking activities. Banna and Alam (2021) show that digital financial inclusion has implications for ASEAN banking stability, while Daud et al. (2022) suggest that fintech can support financial stability through technology-based channels. These findings strengthen the argument that Indonesia's digital banking cybersecurity framework should be evaluated regionally, not only domestically. If Indonesia's framework is less specific

or less enforceable than regional comparators, this may affect customer trust, investor confidence, and supervisory cooperation.

Overall, comparative analysis is necessary because Indonesia has entered a new regulatory stage. The country already has important legal instruments for digital banking, electronic systems, and personal data protection. However, the main challenge is improving coherence, specificity, and enforcement. The comparison with Singapore, Malaysia, and the Philippines shows that Indonesia can strengthen its framework by clarifying cyber resilience standards, integrating data protection with banking cybersecurity rules, strengthening third-party risk governance, improving customer remedies, and assigning clearer accountability to boards and senior management. This makes comparative normative legal research important not only for describing regulatory differences, but also for identifying reform directions that can improve Indonesia's digital banking cybersecurity governance.

4. Conclusion

This article concludes that Indonesia's current legal framework on digital banking cybersecurity has established an important normative foundation, but its effectiveness remains partial when compared with selected ASEAN countries. Indonesia already regulates relevant aspects of digital banking cybersecurity through several instruments, including banking risk management regulation, digital banking service regulation, electronic system governance, commercial bank regulation, and personal data protection law. These instruments show that Indonesia has recognized cybersecurity as part of banking governance, electronic system reliability, customer

protection, and data protection. However, the framework is still fragmented because cyber resilience, data protection, and institutional accountability are regulated across different legal regimes. This fragmentation may create uncertainty in determining reporting channels, supervisory authority, responsibility allocation, and remedies when cyber incidents occur in digital banking services. As a result, the existence of several legal instruments does not automatically guarantee a fully coherent cybersecurity governance model.

Compared with Singapore, Malaysia, and the Philippines, Indonesia's regulatory framework is less operationally specific. Singapore's Technology Risk Management Guidelines and Malaysia's Risk Management in Technology framework provide clearer expectations on technology risk governance, incident response, cyber resilience testing, third-party risk management, and board-level accountability. The Philippines also provides a specific regulatory framework for digital banks, which allows cybersecurity and governance requirements to be linked more directly to digital-only banking operations. By contrast, Indonesia mainly places digital banking within the broader commercial banking framework. This approach is legally acceptable, but it requires stronger implementing standards to ensure that digital banking risks are addressed in a more targeted manner. Therefore, Indonesia's framework can be viewed as moderately effective: it provides the basic legal structure, but it still needs clearer harmonization, more detailed supervisory standards, and stronger accountability mechanisms to respond to the practical risks of digital banking operations.

The comparative analysis also shows that digital banking cybersecurity must be treated as a governance issue, not only a technical issue. Cybersecurity failures may result from weak institutional oversight, poor vendor control, unclear incident response, inadequate customer protection, or insufficient coordination among regulators. For this reason, Indonesia should strengthen its digital banking cybersecurity governance by clarifying cyber resilience obligations, integrating the Personal Data Protection Law with financial sector cybersecurity rules, improving third-party technology risk supervision, and assigning clearer responsibility to boards and senior management. These reforms are necessary to support trust, stability, and innovation in Indonesia's digital banking sector. A more integrated regulatory model would help ensure that digital banking growth is accompanied by legal certainty, customer protection, institutional accountability, and resilience against increasingly complex cyber threats. In this sense, comparative normative legal research is useful not only for identifying regulatory differences, but also for formulating reform directions that are relevant to Indonesia's digital financial ecosystem.

References

Anagnostopoulos, I. (2018). Fintech and regtech: Impact on regulators and banks. *Journal of Economics and Business, 100*, 7–25.

Azharuddin. (2019). Legal protection for users of internet banking customers following changes in information and electronic transactions law. *Jurnal Pembaharuan Hukum, 6*(1).

Bangko Sentral ng Pilipinas. (2020). *Circular No. 1105, Series of 2020: Guidelines on the Establishment of Digital Banks*.

Bank Indonesia. (2020). *Peraturan Bank Indonesia Nomor 22/23/PBI/2020 tentang Sistem Pembayaran*.

Bank Negara Malaysia. (2020). *Risk Management in Technology Policy Document*.

Banna, H., & Alam, M. R. (2021). Impact of digital financial inclusion on ASEAN banking stability: Implications for the post-Covid-19 era. *Studies in Economics and Finance, 38*(2), 504–523.

Barbu, C. M., Florea, D. L., Dabija, D. C., & Barbu, M. C. R. (2021). Customer experience in fintech. *Journal of Theoretical and Applied Electronic Commerce Research, 16*(5), 1415–1433.

Channel NewsAsia. (2022, January 30). OCBC says S$13.7 million lost in phishing scams, up from S$8.5 million. *CNA*. Retrieved Jan 14, 2023, from https://www.channelnewsasia.com/singapore/ocbc-phishing-scam-more-losses-victims-reported-2469086

Daud, S. N. M., Khalid, A., & Azman-Saini, W. N. W. (2022). FinTech and financial stability: Threat or opportunity? *Finance Research Letters, 47*, 102667.

Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. *Journal of Cybersecurity, 5*(1), tyz013.

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *Journal of Management Information Systems, 35*(1), 220–265.

Monetary Authority of Singapore. (2021). *Technology Risk Management Guidelines*.

Omarini, A. E. (2018). Banks and fintechs: How to develop a digital open banking approach for the bank's future. *International Business Research, 11*(9), 23–36.

Otoritas Jasa Keuangan. (2016). *Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum*.

Otoritas Jasa Keuangan. (2018). *Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum*.

Otoritas Jasa Keuangan. (2021). *Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2021 tentang Bank Umum*.

Republic of Indonesia. (2019). *Government Regulation No. 71 of 2019 on Electronic System and Transaction Operation*.

Republic of Indonesia. (2022). *Law No. 27 of 2022 on Personal Data Protection*.

Tarigan, H. A. A. B., & Paulus, D. H. (2019). Perlindungan hukum terhadap nasabah atas penyelenggaraan layanan perbankan digital. *Jurnal Pembangunan Hukum Indonesia, 1*(3), 294–307.

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

Yustisia, M. P. (2022). Perlindungan bagi nasabah dalam penyelenggaraan layanan perbankan digital di Indonesia. *Dharmasisya: Jurnal Program Magister Hukum FHUI, 2*, 20.