DEVOTION Journal of Research and Community Service
Volume 6, Number 1, January 2025
e-ISSN: 2797-6068 and p-ISSN: 2777-0915

Implementation of Prudential Principles in Risk Management in Digital Banking Business Models

Fatika Redita Suryadarma, Pujiyono
Universitas Sebelas Maret, Indonesia
fatikaredita@student.uns.ac.id, pujifhuns@staff.uns.ac.id

KEYWORDS
digital transformation; prudential principles; risk management

ABSTRACT
The rapid advancement of digital transformation has brought significant challenges to the banking sector, including increased risks related to cybersecurity, operational disruptions, and reputational damage. These risks underscore the urgency of implementing the principle of prudence in risk management for digital banking business models to ensure financial stability and customer trust. This study aims to analyze how the principle of prudence is applied in risk management within digital banking frameworks. Employing normative research methods, the study utilizes a legislative approach and a conceptual analysis to explore the role of prudence in addressing emerging risks. The findings reveal that the principle of prudence is indispensable for mitigating risks in the digital banking sector. It serves as a critical safeguard for maintaining the stability and integrity of financial institutions by ensuring robust risk management practices. Furthermore, this principle fosters stronger relationships between banks and customers by reinforcing trust and accountability in financial interactions. The study concludes that adopting the principle of prudence in digital banking is essential for navigating the complexities of the digital era, ensuring the sustainable growth of financial institutions, and safeguarding the interests of customers and stakeholders alike.

INTRODUCTION

The economy is a fundamental principle that functions in building a country. In this context, the economic aspect of a country is inseparable from the role of banking institutions which is one of the important pillars supporting and driving the economy. As an intermediary institution, banks play a role as a support for the national payment system which acts as the main support for the movement and improvement of the economy in the context of national development. Departing from this, banks can be said to be agents *of development* that function as positive catalysts in accumulating development capital.

The rapid advancement of information technology, especially the digitalization of the banking industry 4.0, has an impact on all countries, including Indonesia, preparing to face the digital banking era where all future services will be carried out *online* and no longer require physical branch offices (Galazova & Magomaeva, 2019). The concept of digital banking is a project of the government's efforts to advance the economic sector through technological resources that support the banking industry 4.0. The banking era 4.0 prioritizes the ease of transactions, which was initially "face-to-face" , now more flexible, where customers can enjoy and use bank services anywhere.

The transformation process towards the digital banking era requires continuous cooperation starting from regulations, operational standards, procedures or SOPs and the role of the community, and to meet public expectations for digital transformation in the banking sector, the Government realizes it in POJK No. 12/POJK/03/2018 concerning the Implementation of Digital Banking Services by Commercial Banks, which was then updated with POJK No. 12/POJK.03/2021.

The digital transformation process provides an opportunity for digital banks to make comprehensive internal changes, including work processes and systems that have been ongoing so far. In addition, customers also benefit from new interaction experiences during the transformation process. Starting from *Mobile banking services, Internet banking,* and payments through *virtual accounts*, it has now developed into artificial intelligence applications known as *super apps.*

The principle of prudence (*prident priciple)* in risk management of digital banking business models is an urgency that cannot be ignored. Digital banks must be able to balance innovation with good risk management to maintain operational integrity and stability. The principle of prudence is for banks to have a risk management strategy, which not only anticipates existing risks, but can also identify potential risks in the future. The implementation of this principle is the key to maintaining customer trust and ensuring the sustainability of the bank's business in the midst of increasingly complex challenges.

The use of technology in banking requires a strong legal framework to ensure that these innovations do not compromise the security and stability of the financial system. Existing regulations must be able to keep pace with technological advances while maintaining customer interests and market integrity. One of the relevant approaches in this context is the application of the prudential principle which emphasizes the importance of effective risk management in banking operations.

This study has been compared with 2 (twoa) previous studies. *First*, research conducted by Muhammad Akbar Suharbi and Hendro Margono with the research title "The Need for Transformation of Indonesian Digital Banks in the Era of Revolution 4.0" in the Scientific Journal of Accounting and Finance Volume 4, No. 10. In 2022. This research shows that transforming into a digital bank provides many advantages for banks to be able to continue *to survive* in running their business, such as increasing more customers and *fee base income* for banks because they can collaborate with *fintech* and *e-commerce* and can manage bank assets which can ultimately increase the bank's profits exponentially. However, in transforming into a digital bank, banks must have a strong foundation, especially in terms of infrastructure and security of customer data that is vulnerable to *hacking attacks (cybercrime),* so that in the era of the Industrial Revolution 4.0, technology is the main key in winning the competition and remaining *sustainable* in running its business. *Second*, research conducted by Muhammad Urfi Amrilla with the research title "The Urgency of *Digital Banking* Regulation for Sharia Banking in Indonesia (Analysis of Law Number 21 of 2009 concerning Sharia Banking and POJK No. 12/POJK/03/2018)" in the 2021 Thesis of the Islamic University of Indonesia. This study concludes that *digital banking* for Islamic banking in Indonesia has weaknesses, namely prone to identity theft, online crimes, *malware* attacks, and inaccessible to all groups. With the absence of synchronization between regulations and realities on the ground, the implementation mechanism for Islamic banking cannot be equated with the implementation of conventional banks as stated in POJK No. 12/POJK/03/2018.

There is a difference in this study with the 2 (two) studies that were juxtaposed previously. The novelty in this study provides a legal perspective on technological developments in the banking sector, especially during the transformation period to digital banking. This perspective is then related to how the strategy of preparing risk management in the digital banking sector is based on the principle of prudence. This is because in Indonesia, digital banking is growing rapidly, but it still faces challenges in implementing its regulations, so the principle of prudence is very important in dealing with risks faced by digital banks, such as cyber risks, operational risks, and reputational risks. Therefore, this study aims to analyze the extent to which the prudential principle can be implemented in risk management.

The banking industry plays a pivotal role in driving economic stability and growth by facilitating financial transactions, providing credit, and supporting national development initiatives. In the digital era, banks are evolving from traditional institutions into dynamic entities offering innovative services that cater to the growing demands of digital-savvy customers. This shift is characterized by the adoption of mobile banking, internet banking, and artificial intelligence-based applications, creating a seamless, borderless banking experience. However, with these advancements come new challenges, particularly in maintaining operational security and customer trust.

Digital transformation in the banking sector has introduced heightened risks, including cyber threats, data breaches, and operational vulnerabilities, which could significantly impact financial stability. For instance, cyberattacks targeting customer data and critical financial systems are becoming more sophisticated and frequent. Such threats emphasize the need for robust risk management strategies and regulatory frameworks to ensure the integrity of banking operations. In Indonesia, the Financial Services Authority (OJK) has implemented key regulations, such as POJK No. 12/POJK.03/2021, to guide the development of digital banking practices while prioritizing prudential principles.

The principle of prudence is integral to managing these risks effectively, acting as a safeguard to ensure that banks operate within acceptable risk levels while upholding customer trust. As digital banking models continue to grow, the ability to balance innovation with stringent risk management practices has become crucial. The emphasis on regulatory compliance and proactive risk mitigation underlines the need for banks to implement comprehensive frameworks tailored to the complexities of digital transformation.

Given the rapid adoption of digital banking in Indonesia, it is imperative to develop risk management strategies that address the unique challenges posed by technology. This involves not only protecting against cyber risks but also ensuring operational continuity, data security, and adherence to regulatory standards. The transformation of banking into digital platforms demands a nuanced understanding of how prudential principles can be applied to mitigate risks without stifling innovation.

By incorporating prudential principles into risk management frameworks, digital banks can strengthen their resilience against operational disruptions and cyber threats. Such frameworks promote transparency, accountability, and customer trust, ultimately ensuring the sustainability of digital banking in a competitive and volatile financial environment. This study aims to analyze the application of prudential principles in digital banking risk management, offering insights into how these principles can enhance operational efficiency and safeguard financial stability.

This research is urgent because the rapid expansion of digital banking introduces significant risks, including cybersecurity breaches, operational inefficiencies, and customer trust erosion. These risks, if not managed effectively, can undermine the stability of financial systems and hinder public confidence in digital banking. Addressing these challenges through the application of prudential principles is crucial to ensure sustainable growth and the integrity of digital financial services in Indonesia.

While extensive research exists on digital banking and its associated risks, there is limited focus on integrating prudential principles into risk management frameworks specifically tailored to the digital banking landscape in Indonesia. Most studies emphasize technological innovations but lack a comprehensive analysis of how regulatory and prudential approaches can mitigate emerging risks in this sector. This research seeks to fill that gap by exploring the role of prudential principles in addressing cybersecurity, operational, and reputational risks.

The novelty of this study lies in its interdisciplinary approach, combining legal, financial, and technological perspectives to analyze the implementation of prudential principles in digital banking risk management. It offers a unique focus on the Indonesian context, considering local regulatory frameworks such as POJK No. 12/POJK.03/2021 and their application in mitigating risks associated with digital transformation. This study provides a new lens for understanding how prudential principles can be operationalized effectively in the evolving digital banking sector.

The primary objective of this research is to analyze the application of prudential principles in managing risks within digital banking business models. The findings aim to provide actionable recommendations for banks to strengthen their risk management frameworks. Benefits include enhanced operational security, improved customer trust, and better regulatory compliance, contributing to the overall stability and sustainability of digital financial services. This research will also serve as a valuable resource for policymakers, academics, and banking practitioners seeking to navigate the complexities of digital transformation.

RESEARCH METHOD

In this study, it applies a type of normative legal research, namely legal research that is often interpreted or written in laws and regulations (*law in book),* or as a rule or norm that becomes a reference for good behavior in social life, but does not exclude what is manifested in action (*law in action*) (Efendi & Ibrahim, 2018). The focus of this research is the study of regulations on the transformation of digital banking implementation, describing the problems that occur in society related to the use of digital banks, and explaining and formulating an ideal regulatory model related to digital banking for the realization of legal protection. The method of approach used is the statute *approach*, which is carried out by thoroughly reviewing laws and regulations related to legal issues that are the focus of the research (Mahmud Marzuki, 2018), especially Article 24 of the Financial Services Authority Regulation Number 12/POJK.03/2021 concerning Commercial Banks, and the conceptual approach) which is carried out by reviewing books and research related to legal issues that are the focus of the research. Therefore, the data collection technique in this study uses a literature study. After all the data is collected, analysis is carried out using a descriptive method, which is carried out by formulating and proposing guidelines and rules that are critical and then applied to solve the problems faced, by concluding the problems accompanied by offering solutions.

RESULTS AND DISCUSSION

Trust is the main element that is the key to all forms of bank operations, because trust is related to the bond between the bank and the parties involved. As a service provider, banks must foster trust in related parties in order to maintain obligations that will be or have been agreed. Therefore, the application of the prudential principle is very important for banks to maintain their stability and integrity as a financial institution. In addition to maintaining its stability and integrity as a fundamental financial institution, the prudential principle can also help banks manage risk more effectively so that the relationship between banks and customers is maintained.

Prudential principles are often used to describe the measures that will be applied in bank operations. The prudential principle also serves as the basis for bank operational supervision which ensures that the bank is a financial institution that maintains public funds and trust through its functions and business activities that are carried out with great care (*prudent*), so that it can protect the interests of the bank and its partners without sacrificing the welfare of the bank itself. Thus, the prudential principle acts as a bridge that connects the elements of bank supervision with bank management.

The concept that is the basis for the principle of prudence is one of the main constituent factors in the establishment of digital banks, as stated in Article 24 Paragraph (1) letters (b) and

(c) of POJK Number 12/POJK.03/2021 concerning Commercial Banks which states that the consideration of digital banks is *"having the ability to manage a prudent and sustainable digital banking business model;"* Then continued with *"having adequate risk management"*.

Referring to letters (b) and (c) in Article 24 Paragraph (1) of POJK Number 12/POJK.03/2021 concerning Commercial Banks, we can know that the digital banking business model must prioritize the principle of prudence in its operations. This is because the prudential principle has significant implications for the stability and sustainability of the banking sector. The prudential principle in the digital bank's business model aims to manage financial and operational risks more effectively and ensure that the technological innovations used do not override customer trust and data security. By applying the principle of prudence in designing risk management, digital banks can increase their resilience to cyberattacks and maintain their business integrity.

The concept of prudence in managing a digital bank's business can include various aspects, such as the implementation of strict security policies to protect customer data to ensure legal compliance in all transactions and operational activities. Pro-active risk management management, such as the implementation of regular and periodic internal audits, as well as the implementation of anomaly detection technology are key in preventive efforts to deal with potential cyber threats. In addition, digital banks must have a mature scenario in dealing with emergency situations such as sudden cyber attacks or unexpected operational disruptions to ensure the continuity of wealth to customers.

A digital bank can be said to have a prudent business model if it meets several important criteria, including: *first*, a digital bank must have effective risk management, including identification, assessment, monitoring, and mitigation of risks on an ongoing basis. *Second,* comply with existing regulations, follow all regulations set by the OJK, Bank Indonesia and international banking institution standards. *Third*, transparency in reporting, including financial reporters, must be in accordance with applicable protocol standards. *Fourth,* have a strict security system to protect customer data from cybercrime. *Fifth,* digital banks must ensure that they have sufficient liquidity to meet their short- and long-term obligations. In addition, having strong capital to cover potential losses and meet the minimum requirements set by the Financial Services Authority and Bank Indonesia is very important. Responsible innovation in the development of new products and services, efficient operational management, and good and ethical customer service are integral parts of a prudent business model. Finally, there is internal oversight to ensure that all operations and transactions are in accordance with the established policies and procedures.

Developing risk management means that it involves supervising and controlling the operational activities of digital banks to manage existing risks in order to achieve common goals. This includes financial planning, risk management, asset and liability management, customer relationship management, and risk-taking strategy planning. Risk management involves identifying, assessing, and mitigating different types of risks using techniques such as risk diversion, avoidance, reduction, and management.

The planning and preparation of risk management protocols for digital banks must of course prioritize the principle of prudence to ensure the stability of the bank's security and operational systems. The principle of prudence is a fundamental foundation that plays an important role in identifying, evaluating, supervising, and controlling various risks faced by digital banks. This includes cyber risk, operational risk, compliance risk, and credit risk. In the context of digital banks, cyber risk is very important considering the high threat to customer data and digital transactions.

In response to this, the Financial Services Authority (OJK) has issued various regulations, such as POJK No. 12/POJK.03/2021 concerning Commercial Banks and Financial Services Authority Circular Letter No. 29/SOJK.03/2022 concerning Cybersecurity Resilience and

Security, to ensure that digital banks have clear guidelines regarding risk management and data security. OJK is also preparing a digital transformation blueprint that more firmly regulates cybersecurity and customer data protection.

An article written by Costerat, a company engaged in *software development* in 2023 titled *Risk Management for Digital Banks* stated that digital banking requires a strong risk management strategy which includes periodic risk assessments and the development of risk management frameworks. This is intended to ensure that all potential threats are continuously monitored and addressed effectively. Therefore, the function of the prudential principle not only helps banks in managing risk but also in building business trust and credibility in the eyes of customers and other stakeholders. Prioritizing the principle of prudence in the preparation of risk management protocols is an essential step for digital banks to survive and thrive in the midst of rapidly changing financial industry dynamics.

Risk management is one of the alternatives carried out by a company in managing obstacles or risks arising from uncertainties that pose threats and a series *of human activities*, including risk assessment, development of strategies to manage and mitigate risks using existing resources (Suroso & Fakhrozi, 2018).

The risk management process is carried out with 3 (three) major approaches known as *the Three Lines of Defense*, where each of these lines has its own role. In *the Three Lines of Defense, management control* is the first line in the implementation of the Company's risk management, followed by the second line consisting of risk control and *compliance over-sight functions*, and the third line is independent *assurance* (Auditors, 2013).

The three lines contained in the *Three Lines of Defense* work together to build effective risk management within a company. If there is one component that does not exist, then there is the potential for overlapping responsibilities between one line and another which can result in the implementation of management running not optimally.

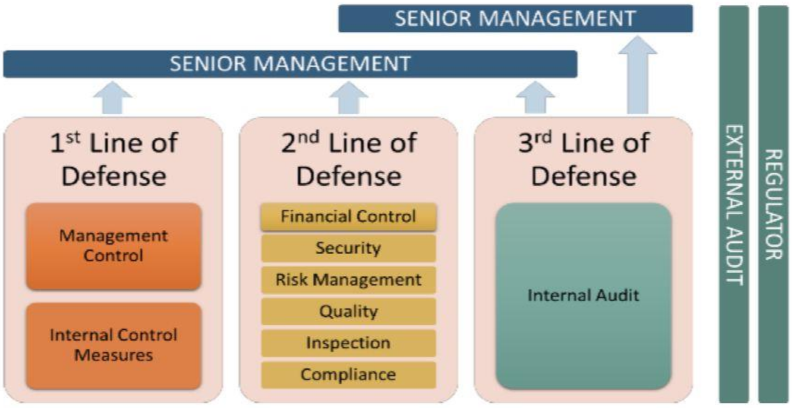

Figure 1. Three Lines Of Defense

(Source: Sihab, I. N., & Diyanti, V. (2019). Three lines of defense in the application of risk management in natural gas trading companies. Journal of Management & Business Sciences, 10(2), 169.)

The Three Lines of Defense in risk management is interpreted as a layered defense mechanism to manage and assess risks. If the company has the maturity and effectiveness of implementing *Enterprise Risk Management* (ERM), it will be reflected in the effectiveness of implementing this 3LD model. The more mature this model is applied, the more intense it will be to create an integrated risk management culture across all processes and all lines of the entity, towards a level *of* organizational resilience that is solid and comprehensive (Suryandari, 2018).

The Three Lines *of Defense* model divides the functions within a company involved in risk management into three groups or layers. The three layers are risk *owners*, risk overseers, and independent *assurance providers*. In addition, companies can also involve external parties as an additional layer (Khristian et al., 2021).

In July 2020, IIA has updated the *Three Lines of Defense Model* to *Three Lines Models* which is a defense mechanism that describes the functions and responsibilities of effective risk management and control. The renewal of the three-line model adapts to the complexity and agility of today's business world. The Three-Line Model is more about the principles of the responsibilities and roles of each function and organization involved in managing risk management in the company. The emphasis of the Three *Lines of Defense* reform is the need for close coordination between each front.

Through the principles contained in *the Three Lines of Defense*, it is hoped that there will be more flexible space and the selection of applications that can be adjusted to the applicable regulations and legal requirements in accordance with each industry. In the *Three Lines of Defense* there are arrows that interconnect management (first and second lines) with Internal Audit (Third Line), so that there is an *interaction* model between internal audit and management that can provide clues or input to the organization's business. *Three Lines of Defense* is also expected to help organizations to capture existing business opportunities, not only in terms of protection and can increase value to *stakeholders* (Casmeliana et al., 2022).

One of the implementation of the principle of bank prudence is by applying the principles of banking risk management. The essence of the implementation of risk management is the adequacy of risk management procedures and methodologies so that the bank's business activities can still be controlled at acceptable limits and benefit the bank. In order to create pre-conditions and risk management infrastructure, banks are required to take steps to prepare for the implementation of risk management, transparency is one of the aspects that need to be considered in controlling the risks faced by banks. Improving the quality of risk management implementation will support the effectiveness of the risk-based bank supervision framework (Mulyati, 2018).

The *prudential principle* plays a role in the preparation of risk management for digital banks by ensuring that operational and financial risks are managed effectively and efficiently. This principle encourages active oversight from management and the board of commissioners to ensure that all risks associated with digital operations, including technology risks, cybersecurity risks, and compliance risks, are identified, measured, and properly managed. The prudential principle emphasizes the importance of compliance with relevant regulations, such as those regulated by the Financial Services Authority (OJK) and Bank Indonesia, in order to protect customers and maintain financial system stability. Transparency in financial reporting and risk disclosure is also part of this principle, ensuring that all stakeholders have the necessary information to make informed decisions. If these principles are applied properly, digital banks can reduce operational risks and maintain customer confidence and the stability of the financial system as a whole.

In the preparation of risk management strategies for digital banks, the principle of prudence that must be considered includes several important aspects. *First*, compliance with applicable regulations, including rules set by the Financial Services Authority (OJK). Digital banks must ensure that all policies and procedures implemented are in line with existing legal and regulatory standards to minimize risks and maintain the integrity and reputation of banks (Wijayanti, 2024). *Second,* strengthening cybersecurity is a top priority. Digital banks need to implement adequate security systems and conduct regular risk assessments to protect customer data from cyber threats (Ferdynandus et al., 2024). *Third,* effective operational controls, including assessing operational risks that may arise from the use of new technologies and ensuring that adequate mitigation measures are in place. The prudential principle emphasizes that digital banks can maintain customer stability and trust in the long term (Abubakar & Handayani, 2022).

In Indonesia, the harmonization of the preparation of risk management strategies in digital banks has become an important focus for the Financial Services Authority (OJK) and Bank Indonesia. OJK has released a banking Digital Transformation Blueprint that includes a risk management approach that is balanced with banks' vulnerabilities and exposures. This strategy aims to ensure that digital banks have a capable framework for managing cybersecurity risks, which is in line with their risk tolerance and risk appetite. This arrangement supports banks to be more responsive to dynamic changes in the digital landscape (Suharbi & Margono, 2022).

In addition, Bank Indonesia also encourages the strengthening of risk management in line with the rapid pace of digital innovation. This includes the formulation of harmonious policies to maintain financial system stability. With this approach, banks are expected to be able to balance innovation with operational security and reliability. This harmonization is important so that banks not only pursue growth and profitability, but also ensure that the risks arising from the use of new technologies can be managed properly (Astuti, Rini Puji, Al Karimatus Sa'idah, Bahrur Rosi, 2022).

Article 24 Paragraph (1) letters (b) and (c) of POJK Number 12/POJK.03/2021 concerning Commercial Banks emphasizes the importance of digital banks in Indonesia to manage their business models in a prudent and sustainable manner. This indicates that banks must have a clear and sustainable strategy that not only focuses on growth and innovation, but also considers the risks that may arise from the use of information technology. The relationship with POJK Number 13/POJK.03/2020 concerning Amendments to Financial Services Authority Regulation Number 38/POJK.03/2016 concerning the Implementation of Risk Management in the Use of Information Technology by Commercial Banks lies in the mandated framework to ensure that all banks, including digital banks, adopt risk management practices in the use of information technology. This ensures that banks have adequate controls to identify, measure, monitor, and control risks associated with technology.

POJK Number 13/POJK.03/2020 concerning Amendments to Financial Services Authority Regulation Number 38/POJK.03/2016 concerning the Implementation of Risk Management in the Use of Information Technology by Commercial Banks requires banks to implement effective risk management in the era of technological development. This includes the development and assessment of policies, procedures, and controls designed to protect customer information systems and data from the threat of cyberattacks and operational disruptions. This provision is in line with the requirements in POJK Number 12/POJK.03/2021 concerning Commercial Banks which requires digital banks to have adequate risk management. Therefore, these two regulations together become the foundation for digital banks to not only develop innovative new products and services but also maintain the security and integrity of their operations.

Departing from the relationship between these two regulations, digital banks in Indonesia are expected to build a business model that is not only innovative but also resilient to risks. Adequate risk management allows banks to anticipate and respond to threats more effectively, ensuring continuous operations and protection for customers.

POJK Number 13/POJK.03/2020 concerning Amendments to Financial Services Authority Regulation Number 38/POJK.03/2016 concerning the Implementation of Risk Management in the Use of Information Technology by Commercial Banks is a regulation issued by the Financial Services Authority (OJK) that focuses on the application of risk management in the use of information technology by commercial banks. In the context of digital banks, this regulation reinforces the importance of a risk management strategy that prioritizes the principle of prudence. Digital banks that rely more on information technology must ensure that their systems are secure, reliable, and can protect customer data from cyber threats (Wahyudi & Arbay, 2021). The implementation of strict risk management allows banks to assess and mitigate potential risks related to cybersecurity and data integrity, which is important for maintaining customer trust and operational stability.

In addition, POJK Number 13/POJK.03/2020 concerning Amendments to Financial Services Authority Regulation Number 38/POJK.03/2016 concerning the Implementation of Risk Management in the Use of Information Technology by Commercial Banks encourages digital banks to adjust their risk policies in accordance with technological developments. This includes ensuring that there are adequate risk mitigations in place to deal with new threats that may arise as technology advances. By paying attention to the prudential principle, digital banks are expected to develop strategies that focus not only on profitability but also on protection against risks that may affect their long-term operations and reputation in the eyes of the public. Overall, the regulation emphasizes the need for a balance between digital innovation and operational security.

Both POJK Number 12/POJK.03/2021 concerning Commercial Banks and POJK Number 13/POJK.03/2020 concerning Amendments to Financial Services Authority Regulation Number 38/POJK.03/2016 concerning Implementation, both encourage banks to not only focus on technological innovation, but also ensure that every innovative step taken has gone through a rigorous risk evaluation process. Digital banks can operate safely and efficiently, providing certainty to customers and other stakeholders (Gitazia & Muhaimin, 2023).

In the context of digital banking, the integration of risk management with information technology is becoming increasingly crucial as cyber threats and operational complexity increase (Pertiwi et al., 2023). These two regulations direct digital banks to develop adaptive risk management, to ensure that the technology used supports the goals of digital banks as prudent and sustainable business models. Adaptive risk management initiates digital banks to continue to innovate while maintaining customer integrity and trust.

The process of harmonizing the preparation of risk management strategies in digital banks in Indonesia involves several strategic steps coordinated by the Financial Services Authority (OJK) and Bank Indonesia. OJK has issued a Digital Transformation Blueprint for banking that underscores the importance of implementing integrated and balanced risk management. This involves adjusting risk policies to match technological developments and rapid market dynamics. This strategy ensures that digital banks have a solid framework in place to manage risks associated with the use of information technology and cybersecurity (Ramadhenta & Priyono, 2024).

In addition, Bank Indonesia also plays an active role in directing digital banks to implement best practices in risk management. Bank Indonesia encourages the strengthening of governance structures and decision-making processes based on existing data. This is done by providing guidance and evaluation tools that help banks assess their digital maturity level, including in terms of risk management. With this approach, banks can be more proactive in identifying and addressing complex risks, ultimately supporting the stability of the financial system as a whole (Israhadi & Surateman, 2024).

In the harmonization process, digital banks in Indonesia are also encouraged to increase the capacity of human resources in developing risk management strategies. This includes training and skill development for employees to better understand the risks associated with digital technology and how to assess and manage them. OJK and Bank Indonesia also encourage collaboration between banks and technology providers to ensure that the technology solutions used are safe and compliant with regulatory standards. This harmonization process will not only focus on policies and regulations, but also on strengthening the bank's internal to face increasingly complex risk challenges.

Furthermore, periodic supervision and evaluation by the authorities can help ensure whether digital banks are implementing effective risk management practices. This includes a regular audit process and regular risk assessments to ensure that banks continue to update their strategies in line with the changing business and technology environment. Through this approach, the harmonization of risk management strategies in digital banks in Indonesia aims to create a safe, innovative, and sustainable banking ecosystem.

The conclusion of the preparation of a risk management strategy for digital banks based on the principle of prudence and POJK Number 13/POJK.03/2020 concerning Amendments to Financial Services Authority Regulation Number 38/POJK.03/2016 concerning the Application of Risk Management in the Use of Information Technology by Commercial Banks is that digital banks in Indonesia must integrate strong risk management with technological innovation. POJK Number 13/POJK.03/2020 emphasizes the importance of implementing risk management which includes cybersecurity, operational, and compliance risk management. The regulation encourages banks to adopt adequate and adaptive technology to help monitor and manage risks, while ensuring that digital banks' operational systems comply with the principle of prudence to protect customer trust and maintain financial system stability.

Given the importance of the prudential principle as a fundamental foundation for operations, digital banks are expected to be able to balance the need to innovate and the need to maintain operational security and integrity. A structured risk management strategy allows banks to actively identify and address potential risks, both internal and external. This not only protects the interests of customers, but also ensures that banks can operate well and sustainably in the dynamics of a challenging business environment.

CONCLUSION

The prudential principle in the digital banking sector serves as a fundamental foundation for maintaining the stability and integrity of financial institutions. This principle not only helps in risk management, but also ensures a strong relationship between the bank and the customer, which is based on trust. Article 24 Paragraph (1) letters (b) and (c) of POJK Number 12/POJK.03/2021 concerning Commercial Banks emphasizes the need for prudent and sustainable management of digital bank business models, in line with POJK Number 13/POJK.03/2020 concerning Amendments to Financial Services Authority Regulation Number 38/POJK.03/2016 concerning the Implementation of Comprehensive Risk Management Practices. An ethical and responsible bank culture is key in the dynamic digital banking environment. The OJK has issued regulations to ensure that digital banks have clear guidelines regarding risk management and data security. The Three Lines of Defense serves as an important mechanism in risk management, ensuring that each line in the organization functions effectively in managing risk. The integration of strong risk management with technological innovation is the key for digital banks to maintain stability and customer trust.

REFERENCES

Abubakar, L., & Handayani, T. (2022). Penguatan Regulasi: Upaya Percepatan Transformasi Digital Perbankan Di Era Ekonomi Digital. *Masalah-Masalah Hukum*, *51*(3), 259–270.

Astuti, Rini Puji, Al Karimatus Sa'idah, Bahrur Rosi, And S. R. N. (2022). "Payment System In Indonesia." *Gudang Jurnal Multidisciplinary*, *51*(3), 533–537.

Auditors, I. Of I. (2013). *The Three Lines Of Defense In Effective Risk Management And Control*.

Casmeliana, C., Ayu, F. D., Saraswati, R., Firdiyah, H., & Ananda, C. (2022). Pengaruh Penerapan Model Tiga Lini Terhadap Efektivitas Pengendalian Internal Pada Rs Pusat Otak Nasional Jakarta. *E-Prosiding Akuntansi*, *3*(1).

Efendi, J., & Ibrahim, J. (2018). Legal Research Methods: Normative And Empirical. *Jakarta: Kencana Prenamedia Group, Cet*, *2*.

Ferdynandus, F., Prihanto, J. N., & Winarno, W. (2024). Implementing Nist Framework And The People, Process, Technology Approach In Indonesian Financial Services. *International Journal Of Engineering Continuity*, *3*(1), 172–182.

Galazova, S. S., & Magomaeva, L. R. (2019). *The Transformation Of Traditional Banking Activity In Digital*.

Gitazia, A. R., & Muhaimin, M. (2023). Tinjauan Yuridis Bank Digital Dalam Perspektif Bank Indonesia. *Commerce Law*, *3*(1).

Israhadi, E. I., & Surateman, S. (2024). Implementation Of Balance Score Card To Improve Employee Performance At Pt Gaya Makmur Tractors. *International Journal Of Engineering Business And Social Science*, *2*(03), 1102–1107.

Khristian, E., Karamoy, H., & Budiarso, N. S. (2021). Analisis Manajemen Risiko Dalam Mewujudkan Good Corporate Governance (Studi Kasus Pada Pt Angkasa Pura I (Persero)). *Jurnal Riset Akuntansi Dan Auditing" Goodwill"*, *12*(2), 112–128.

Mahmud Marzuki, P. (2018). Pengantar Ilmu Hukum. *Kencana, Jakarta*.

Mulyati, E. (2018). Penerapan Manajemen Risiko Sebagai Prinsip Kehati-Hatian Dalam Pemberian Kredit Perbankan. *Supremasi: Jurnal Hukum*, *1*(1), 34–48.

Pertiwi, D., Suyitno, A., Rochmiatun, E., Anisa, W. N., & Handayani, D. L. (2023). Bank Digital Sebagai Peradaban Lembaga Keuangan Syariah Di Indonesia. *Indonesian Scientific Journal Of Islamic Finance*, *1*(2), 172–182.

Ramadhenta, M. R., & Priyono, F. J. (2024). Harmonization Of Authority In The Investigation Of The Financial Services Sector In Indonesia. *International Journal Of Multicultural And Multireligious Understanding*, *11*(5), 352–360.

Suharbi, M. A., & Margono, H. (2022). Kebutuhan Transformasi Bank Digital Indonesia Di Era Revolusi Industri 4.0. *Fair Value: Jurnal Ilmiah Akuntansi Dan Keuangan*, *4*(10), 4749–4759.

Suroso, J. S., & Fakhrozi, M. A. (2018). Assessment Of Information System Risk Management With Octave Allegro At Education Institution. *Procedia Computer Science*, *135*, 202–213.

Suryandari, W. D. (2018). The Reform Of Legal Protection For Creditors In The Implementation Of Fiduciary Guarantee Registration Policy In Indonesia Based On Justice Value. *Thematics Journal Of Law*, *2*(1).

Wahyudi, C. A., & Arbay, E. A. (2021). The Impact Of Ojk Regulation No. 48/Pojk. 03/2020 On The Quality Of Credit And Risk Management Of Banking Credit. *Journal Of Economics And Business*, *4*(1).

Wijayanti, Y. (2024). Banking Risk Management And Digital Transformation.". *Mercu Buana University*. Https://Doi.Org/Https://Doi.Org/10.13140/Rg.2.2.12629.23524.