International Journal of Cyber and IT Service Management (IJCITSM) p-ISSN: 2797-1325
Vol. 3 No. 2 October 2023 e-ISSN: 2808-554X

Application of Digital Technology Risk Management Models in Banking Institutions Reflecting The Digital Transformation of Indonesian Banking BLUEPRINT

Kento Mazayo[1], Sri Agustina[2], Riska Asri[3]
Business Administration[1], Computerized Accounting[2,3]
University of Tsukuba[1], Telkom University[2,3]
1 Chome-1-1 Tennodai, Tsukuba, Ibaraki 305-8577[1], Jl. Telecommunication. 1, Buah Batu Canal - Bojongsoang, Telkom University, Sukapura, Kec. Dayeuhkolot, Bandung Regency, West Java 40257[2,3]
Japan[1], Indonesia[2,3]
e-mail: kento_mazayo@yahoo.com[1], tina92697@gmail.com[2], riska.asri@gmail.com[3]

Author Notification
10 October 2023
Final Revised
29 October 2023
Published
31 October 2023

To cite this document:
Mazayo, K., Agustina, S. ., & Asri, R. . (2023). Application of Digital Technology Risk Management Models in Banking Institutions Reflecting The Digital Transformation of Indonesian Banking BLUEPRINT. *International Journal of Cyber and IT Service Management, 3(2)*. *Retrieved from https://iiast.iaic-publisher.org/ijcitsm/index.php/IJCITSM/article/view/137*

DOI:
https://doi.org/10.34306/ijcitsm.v3i2.137

Abstract

This article discusses trends in the use of digital technology in the banking industry that are occurring in the world, specifically in Indonesia. This study found that the use of digital technology (digitization) has made the global financial ecosystem change rapidly. This happens because people's demand for digital services continues to increase. This opens up opportunities for the banking industry to increase the number of customers and increase profits. However, on the other hand, there are a number of channels through which banking institutions have the potential to experience potential losses because cybercrime will continue to increase. The authors therefore suggest that banking institutions continue to seek to reinvent their risk management function, especially through the development of digital risk management, to protect themselves, their customers and their place in the market. In Indonesia, the Financial Services Authority (OJK) has actually created a blueprint and road map that helps the banking industry implement digitalization and develop digital risk management in a targeted and effective manner.

Keywords*: Cybersecurity in Banking, Financial Digitization Strategies, Digital transformation, Digital Transformation Blueprint, Digital Risk Management*

1. Introduction

Since 2010, around 200 banks in the world, which are preparing for long-term change, have taken the initiative to adopt digital technology of these, 46 are in Asia Pacific [1]. At that time they believed that in the next ten years, banking risk management would be subject to an unprecedented transformation, and they would face completely new risks [2].

The rapid development of information technology has brought world society's lives into a new era which is often called the era of industrial revolution 4.0 [3]. This era is marked by the development of various technological innovations such as the Internet of Things (IoT), Cloud Computing, Artificial Intelligence (AI), Cyber Security, Additive Manufacturing, System Integration and Machine Learning [4].

In 2020, when various economic and business sectors were paralyzed by the COVID-19 pandemic, banking circles thought that in 2025 or the next five years, the risk function in banks would likely be fundamentally different from before [5]. Because, it is estimated that by 2025 more than half of the people in the world, including in Southeast Asia, will switch to neobanks or digital banks [6]. Therefore, the banking industry must move quickly in adopting digital technology so that it can quickly evolve into a digital bank with minimal risk [7].

The Covid-19 pandemic has forced changes in people's behavior and orientation from the previous physical economy to a virtual economy [8]. This condition creates a blessing in the form of acceleration and becomes a momentum for change in various aspects of society's life as a whole and creates digital behavior, including behavior in financial transactions. The shift in society's behavior and orientation towards a virtual economy has of course given rise to different expectations and needs than before. At this point, Banks are forced to accelerate digital transformation, carry out extraordinary innovations, work more effectively, more efficiently and more productively in order to meet customer expectations and needs amidst increasingly fierce business competition [9].

The use of various technologies in the financial services sector has brought significant changes to the banking industry. These changes can be seen from 4 (four) aspects which then drive changes in the future banking landscape as follows:

First, changes in consumer expectations for banking products and services. In general, as information technology develops, consumer expectations for products and services have led to products and services that are easy and safe, personalized, not left behind trends, and consumers have the convenience of comparing the quality of various products and services.

Second, the use of data to improve the quality of products and services (data enhanced products and services). The use of large volumes of data, known as big data, is able to provide information which banks can then use to create many opportunities and give rise to new business categories.

Third, the emergence of new partnerships with big companies and start-ups. Technological developments have led to the formation of a new digital ecosystem with the Bank becoming one of the players in this ecosystem. The Bank's partnerships with players in the digital ecosystem such as fintech and bigtech are able to provide opportunities for the Bank to gain new consumers, take advantage of partner innovation, and gain access to data for developing Bank products and services.

Fourth, change the operational model to a digital business model. The development of information technology accompanied by changes in consumer behavior forces banks to immediately carry out digital transformation. For the Bank, the transformation to become a fully digital bank presents an efficient and effective business model, which is expected to increase the Bank's penetration and reach to all levels of society, thereby ultimately encouraging increased profitability, inclusiveness and maintaining business existence amidst increasingly tight competition in the financial services sector.

The application of digital technology will differentiate a bank from its competitors [10]. The right technology will not only increase the speed and reliability of services, but also ensure data security [11]. At the very least, it will determine the bank's ability to deliver world-class digital application experiences [12]. However, the risk management function of banks that adopt digital technology will have a different character from the risk management function of conventional banks [13].

2. Research Method

In this research, the method used is Literature Review or literature review. Literature reviews are descriptions of theories, findings and other research materials obtained from reference materials to serve as a basis for research activities [14]. Literature reviews contain reviews, summaries and the author's thoughts about several library sources (articles, books, slides, information from the internet, etc.) about the topic being discussed [15]. A good literature review must be relevant, up-to-date and adequate [16]. Theoretical basis, theoretical review, and literature review are several ways to conduct a literature review.

2.1 Formulation of The Problem

Based on the description above, the main questions that can be asked are as follows:

1. What are the trends in the application of digital technology in banking institutions in Indonesia?
2. What is the function of risk management, especially digital technology risk management in the banking industry?

2.2 Literature Review

2.2.1 Banking Risk Management

In essence, risk in the banking context is a potential event, both predictable and unpredictable, which has a negative impact on bank income and capital [17]. Risk can also be considered as an obstacle in achieving a goal.

To achieve the goals expected by shareholders and fulfill the promise to the public to be more than just a bank, each bank develops what is called Enterprise Risk Management (ERM), which is a unit or division that is responsible for establishing risk supervision, monitoring and reporting that encourages risk integration [18].

The Bank's ERM policy and amendments thereto require board approval. The Risk Management Division is responsible for enforcing the Bank's risk policy by continuously monitoring risk, to identify and measure significant risk exposures and act on such exposures if necessary [19].

A bank's overall risk tolerance is set in the context of its earnings power, capital and diversified business model [20]. Organizational structure and business strategy, on the other hand, are aligned with risk management philosophy [21].

For this purpose, the Bank uses periodic reviews of risk exposure limits and risk controls as well as self-assessment to position itself against adverse scenarios [22]. This is an invaluable tool with which the Bank predicts and successfully manages local and global recessions that continue to impact the macro economy. ERM identifies opportunities, assesses the risks inherent in these opportunities and actively manages these risks in a cost-effective manner.

2.2.2 Types of Banking Risks

It is often said that profit is the reward for successfully bearing risk. And, this is very true in the banking industry [23]. Banks are literally exposed to various types of risk. A successful banker is one who can mitigate these risks and create significant profits for shareholders on a consistent basis [24]. Risk mitigation begins by first correctly identifying the risk, why it exists and what damage it can cause. It is generally known that banks have several main types of risks as follows:

Credit Risk: Credit risk is the risk that arises from the possibility of non-payment of the loan by the borrower. Although credit risk is largely defined as the risk of not receiving payment, banks also include the risk of late payment in this category.

Market Risk: Banks face market risk in various forms. For example if they hold large amounts of equity then they are exposed to equity risk. Also, banks by definition must hold foreign exchange which exposes them to Forex risk. Similarly banks lend against commodities like gold, silver and real estate which exposes them to commodity risks as well.

Operational Risk: Occurs as a result of business process failures in daily bank activities. Examples of operational risks would include payments being credited to the wrong account or executing the wrong order when transacting in the markets. None of the departments in a bank is immune from operational risks.

Moral Hazard: Recent bank bailouts by many countries have created another type of risk called moral hazard. This risk is not faced by the bank or its shareholders. In turn, these risks are faced by taxpayers in the countries where the bank operates. Banks are used to taking excessive risks. If their risk pays off, they can maintain their returns. However, if the risk backfires, then the losses will be borne by taxpayers in the form of bailout funds.

Liquidity Risk: Liquidity risk is another type of risk inherent in the banking business. Liquidity risk is the risk that the bank will not be able to fulfill its obligations if depositors come to withdraw their money. This risk is inherent in the fractional reserve banking system.

Business Risks: Today's banking industry is very advanced and diversified. Banks today have a variety of strategies they have to choose from. Once the strategy is selected, banks need to focus their resources on achieving their strategic goals in the long term.

Reputation Risk: Reputation is a very important intangible asset in the banking business. Banks such as JP Morgan bank, Chase bank, Citibank, Bank of America or at the national level Bank BCA, Bank BRI, Bank Mandiri etc. have all been in this business for hundreds of years and have an extraordinary reputation. This reputation allows them to generate more business more profitably.

Systemic Risk: Systemic risk arises due to the fact that the financial system is one complex and connected network. Therefore, the failure of one bank has the possibility of causing the failure of many other banks as well. This is because banks are each other's counterparties in many transactions. Therefore, if one bank fails, a credit risk event for other banks becomes a reality.

Digital Risks: Apart from various financial risks, there are several non-financial banking risks. Technological risk is one of them. These include cybersecurity risks, risks of non-compliance with data protection regulations, and risks of legacy systems [25]. While banks develop comprehensive plans to address financial risks, they may not be aware of technology risks. Banks may face several challenges as they try to mitigate technology risks.

In recent years, as digital technology advances, digitalization has become firmly embedded in banking strategies, as almost all businesses and activities have been scheduled for digital transformation. The significant benefits of digitalization, with respect to customer experience, revenue and costs, are becoming increasingly compelling. Momentum to adopt the new technologies and operating models needed to capture these benefits continues to increase. However, the use of digital technology has the potential to pose risks.

They also suggest that risk management in banks has begun to change substantially over the last ten years. According to them, non-financial risk management is becoming more important because compliance and behavioral standards are tightening, and the trend of utilizing digital technology continues to strengthen rapidly. They even state that despite not having a magic crystal ball that will tell us what bank risk functions will look like in 2025 and beyond, or what kind of financial crises or technological changes may disrupt bank risk management, we believe that the trend towards leveraging digital technology is likely to fundamentally change bank risk management over the next ten years.

2.2.3 Digitalization Trends in the Banking Industry

The digital era has brought the financial sector kicking and screaming into the modern era. Although technology and customer participation have been slow to catch on, things may finally be making progress. Furthermore, digital technology has enabled the birth of Open programming interfaces (API). Open X Banking relies on banks' technological capabilities to control data and create a collaborative environment to develop and deliver banking services through partnerships with financial and non-financial companies, providing the creation of new and better products for banking users.

So, today there are three banking models coexisting – traditional, digital and open banking. Traditional banking is represented in countries where the development of FinTech is low and there is no demand for digital services among consumers, that is, these countries are mainly developing countries with low economies. At the same time, statistical analysis shows that there is a high level of demand for digital banking or the coexistence of traditional and digital forms of banking in a global dimension. Among the three European countries taken for analysis (UK, Germany and France), only in France do consumers prefer the physical presence of banks over digital services. At the same time, it is worth noting that at least 57 percent of consumers gave a positive answer about the importance of digital banking in all countries considered and on average in the world.

According to a banking consumer survey conducted in 2016 in 32 countries, it is known that having a variety of digital banking services for consumers is much more important than the physical presence of its subdivisions. Although, in fact, between 2010 and 2018, FinTech companies in Europe have seen the potential of digital technology because they have been able to reap almost 92 billion US dollars by leveraging digital technology.

The speed of digital, mobile-first and app-based banking has succeeded in attracting customers impressively. In December 2017, London-based NeoBank Revolut was reported to be the first to implement a digital system. In February 2018, the number of Revolut customers had changed to around 1.5 million customers, and in 2020 it had become 12 million customers. Similar growth was seen with N26 based in Berlin, Germany.

Globally, the use of online and mobile banking continues to grow. In 2018, across the European Union there were 141 million people using online banking regularly. It is expected to continue increasing between 2020 and 2024, with the Asian market being the largest. In 2020, the Far East and China accounted for more than 800 million active online banking users. This figure is expected to reach almost one billion by 2024. In 2020, as many as 1.9 billion people worldwide actively used online banking services with this number expected to reach 2.5 billion in 2024.

Meanwhile, according to the Financial Services Authority (OJK), the development of digital banking services is driven by the following: 1). the rapid development of information technology; 2). changes in people's lifestyles according to developments in information technology; 3). the public's need for banking services that are effective, efficient, accessible from anywhere and at any time, comprehensive and easy; 4). banking industry competition to provide services according to community needs; and 5). banking needs for efficient and integrated operations.

The presence of digital banks in the Indonesian financial ecosystem was marked by the launch of the 'Jenius' digital banking platform from PT Bank BTPN Tbk. (BTPN) in 2017. BTPN's steps this year have been followed by a number of other commercial banks in Indonesia such as Wooke, a digital banking application in Indonesia developed by Bank Bukopin; Digibank, a digital banking product owned by DBS Bank; and TMRW, a subsidiary of Bank UOB Indonesia which was launched in 2020.

Furthermore, throughout 2021, a number of banks such as PT Bank Jago Tbk. officially launched the Jago application on April 15 2021. This Neo Commerce Bank was launched in March 2021 on the App Store and Google Play Store. The neobank application presents various features with a user-friendly display, starting from Neo WOW Savings, Neo WOW Deposits, to Neo Jurnal.

Furthermore, PT Bank MNC Internasional Tbk officially launched a digital banking service application called MotionBanking on June 3 2021. Then, following, PT Bank Central Asia Tbk. launched a digital bank called blu, which officially launched on July 2 2021. This application from PT BCA Digital is present as a digital bank ecosystem without branch offices and can be accessed from anywhere and at any time.

Finally, PT Bank KEB Hana Indonesia (Bank Hana) in collaboration with LINE Corporation officially launched LINE Bank by Hana Bank or LINE Bank on June 10 2021 and can now be downloaded on the Play Store and App Store.

As of June 15 2021, OJK stated that Indonesia had 14 digital banks, seven were already operating, and the remaining seven were currently preparing. Digital banking services bring several benefits, such as the following:

First, inclusive financial services. Digital banks provide inclusive or comprehensive financial services. This means that digital banks can reach people from all walks of life, including groups who do not yet use conventional banks.

Second, consumers can get efficient service 24 hours a day. If you need financial services, you don't have to wait for the bank to open and you don't have to queue for a long time.

Third, admin costs are cheaper. The digital banking business model apparently also influences the bank's operational costs. This also affects the administration costs charged to customers. With a digital system, operational costs are lower, so bank admin costs are also lower than conventional banks.

3. Findings

3.1 Blueprint for Digital Transformation of Indonesian Banking

To respond to substantial and structural changes in the banking industry as a result of

the application of digital technology (digitalization), the Indonesian Financial Services Authority (OJK) has prepared, among other things, the Indonesian Financial Services Sector Master Plan 2021-2025 (MPSJKI) Pillar 3 and the Indonesian Banking Development Roadmap 2020- 2025 (RP2I) Pillar 2 which has directed banks to accelerate digital transformation.

One of the pillars that is the direction of policy is the acceleration of banking digital transformation. This pillar is further explained through the 'Banking Digital Transformation Blueprint'. The Banking Digital Transformation Blueprint was prepared by prioritizing the principle of balance between digital banking innovation and prudential aspects to maintain banking performance in a healthy condition (prudent, safe, and sound banking). Apart from that, this Blueprint also carries the principle of technology neutrality, that is, it does not regulate technical aspects related to technology.

The Banking Digital Transformation Blueprint contains a draft OJK policy to encourage the acceleration of banking digital transformation in Indonesia. This Blueprint is expected to become the basis for developing digitalization in national banking so that it is more resilient, competitive and contributive.

The Banking Digital Transformation Blueprint will provide a more concrete reference for future banking digitalization in the context of accelerating digital transformation, as well as being a policy response to mitigate various challenges and risks from banking digital transformation. It is hoped that the implementation of this Blueprint can encourage national banking to be more resilient, competitive and contributive.

According to the OJK, something that is quite important to pay attention to in accelerating digital transformation is that the adoption of information technology needs to be followed by initiatives to implement adequate information technology governance and risk management.

The Banking Digital Transformation Blueprint contains 5 (five) main elements, namely data, technology, risk management, collaboration and institutional order in the banking industry. These five elements are strategic steps to encourage banks to create innovative financial products and services that can meet consumer expectations and are oriented towards consumer needs (customer centric orientation).

1) Data

In the digital era, data has become a new type of wealth that is much more valuable than gold or oil. With the development of the use of information technology, collecting, processing and transferring data will become easier to do. Data exchange will become increasingly common along with the development of open banking by utilizing API technology. However, banks need to be careful about the customer data they have. A number of crucial elements related to data, namely data protection, data exchange arrangements (data transfer), and data governance in banking are important things. Good implementation of these elements will increase public trust in banking in the digital era. Adequate protection of data will be able to give customers confidence to provide their data for various greater purposes without misuse or violating personal rights.

Data protection policies, data exchange regulations and data governance in banking are important aspects needed to increase public trust in digital banking services. In addition to 26 Ibid. matter. 22-24, banks need to fulfill 7 (seven) principles in collecting and processing consumer data, namely 1) valid, fair and transparent, 2) specific objectives, 3) data minimization, 4) accountability, 5) integrity and confidentiality, 6) consumer storage restrictions namely, and 7) accurate.

Data governance at the Bank is in principle a business strategy initiative. The data governance process includes people, processes and technology needed to ensure that data management is in accordance with the intended objectives. To achieve data governance objectives and obtain optimal benefits from the data governance program, Banks need to pay attention to 8 (eight) principles in governance. Data management, namely 1) integrity, 2) transparency, 3) stewardship, 4) checks-and-balances, 5) auditability, 6) accountability, 7) standardization, and 8) change management.

2) Technology

Technology continues to change along with the rapid development of innovation. This causes the focus on a particular technology to quickly become obsolete. However, a number of aspects that greatly influence the selection, use and management of technology tend not to change much and therefore need to be implemented properly. These aspects include information technology governance, information technology architecture, and principles of information technology adoption. Information technology governance will provide alignment of business strategy and IT investment in order to create business value from these investments. The IT Governance System refers to IT governance in accordance with the 2019 COBIT framework issued by ISACA and carries 6 (six) principles, namely 1) Provide Stakeholder Value; 2) Holistic Approach; 3) Dynamic Governance System; 4) Governance Distinct from Management; 5) Tailored to Enterprise Need; and 6) End-to-End Governance System.

3) Risk Management

The utilization and use of information technology needs to be supported by the implementation of effective risk management to mitigate various potential risks including outsourcing risks and cyber security risks.

Information technology is a valuable asset for the Bank so that its management is not only the responsibility of the information technology operating unit but also all parties who use it. The implementation of risk management must be carried out in an integrated manner at every stage of IT use from the planning process, procurement, development, operations, maintenance to termination and deletion of IT resources. The risk management process related to information technology includes 1) identify risk, 2) manage risk, 3) mitigate risk, and 4) optimize risk – monitoring and review. This will be discussed specifically in the following sub-topic.

4) Partnership or Collaboration

Technological developments have led to the formation of a new digital ecosystem with the Bank becoming one of the players in this ecosystem. Bank partnerships or collaborations with players in the digital ecosystem such as banking institutions, non-bank financial institutions, non-financial institutions such as financial technology companies or fintech and bigtech are able to provide opportunities for banks to get new consumers, take advantage of partner innovations, and gain access to data for development Bank products and services. Bank collaboration with other institutions can take the form of a sharing platform (super-app), or collaboration between the Bank and other institutions in the form of infrastructure sharing within the Bank Business Group or collaboration in the distribution of services and products.

Furthermore, forms of cooperation with financial and non-financial institutions are divided into sharing services and distribution of products and services. One form of service sharing that can be done is through infrastructure sharing for Bank Business Groups (KUB) which aims to encourage operational efficiency. Synergy between Indonesian Legal Entity Bank (BHI) (as the holding company or implementing holding company) with BHI Bank which is part of the KUB can be in the form of utilizing technological infrastructure such as applications, data centers or data recovery centers.

5) Institutional Order

Changes that occur along with digital transformation need to be accompanied by the readiness of the Bank's institutional structure. This institutional structure includes, among other things, funding and investment, leadership, organizational design, digital culture, and human resource talent. Digital transformation in the banking sector certainly needs to be supported by the Bank's ability to maintain funding sources and invest in information technology. Providing information technology infrastructure to support digital transformation certainly requires significant investment.

Banks must make appropriate investment decisions by considering related aspects so that the investments made provide benefits and profits for the Bank's business processes in the future, and are supported by full commitment from the Bank's management. For this reason, banks can pay attention to investments that generate high value (high-value investments) and

rebalance technology investments and measure the business value of these investments.
In the context of digital banking transformation, banks must have digital leadership, which is defined as strategic leadership that can utilize the company's digital assets to achieve organizational goals. According to research by Capgemini (2018), digital leadership is a combination of developing digital capacity (digital capabilities) and leadership capacity (leadership capabilities). Digital capabilities include the ability to use technology to change the Bank's business processes, including in terms of the Bank's interaction with customers (customer experience), talent and organization development, operationalization of internal processes (operations), and business model formulation (business model innovation). Meanwhile, leadership capabilities include the ability to drive and lead digital transformation in terms of technology and business, vision and goals, workforce empowerment, governance, as well as culture and engagement.

6) Consumer

In addition to customer centric orientation services, banks also need to pay attention to the availability of banking services for all levels of society.

Digital transformation aims to provide products and services that suit consumer needs or achieve customer centric orientation services. Referring to the TM Forum's digital maturity framework, the level of maturity of an organization's digitalization in the customer aspect is measured by 4 (four) things, namely (i) customer engagement is a consumer's attachment or dependence on digital banking services; (ii) customer experience is an indicator of the success of the services provided by the company; (iii) customer insight is a way for the Bank to understand consumer behavior, preferences and needs by utilizing consumer data; and (iv) customer trust and perception is consumer trust and perception towards digital banking services. Banks need to ensure that digital banking services can be accessed by all levels of society in order to increase financial inclusion, including for people with disabilities who have the potential to be marginalized due to technological developments.

3.2 Digital Technology Risk Management in Banking Institutions

The use of information technology carries its own risks for banking. Some of the risks that usually arise when using information technology are cyber attacks which can disrupt the performance of information technology, cracker/hacker attacks which can disrupt the system and even steal confidential company data, errors and damage to supporting systems such as broken power lines, etc.

For this reason, banks need to effectively implement information technology risk management to mitigate these various risks. In line with this, banks also need to implement adequate cyber security. Apart from that, banks also need to implement good outsourcing management in terms of using third parties to provide information technology.

Information Technology Risk Management is the application of risk management principles to companies that utilize information technology with the aim of managing risks related to the company.

Information technology is a valuable asset for the Bank so that its management is not only the responsibility of the information technology operating unit but also all parties who use it. The implementation of risk management must be carried out in an integrated manner at every stage of IT use from planning, procurement, development, operations, maintenance to termination and deletion of IT resources.

3.2.1 Process Risk Management Process Related to Information Technology

The risk management process related to information technology includes 1) identify risk, 2) manage risk, 3) mitigate risk, and 4) optimize risk – monitoring and review.

Figure 1. Information Technology Risk Management Process

The Banking Digital Transformation Blueprint states that in carrying out activities of handing over work to other parties (outsourcing), especially in the field of Information Technology (IT), Banks face various risks that can arise, such as strategic risk, operational risk, regulatory and compliance risk, reputation risk, and concentration risk.

To minimize these various potential risks, the Bank needs to implement risk management for outsourcing activities, especially by paying close attention to outsourcing principles as well as the processes and stages of outsourcing properly. Banks can carry out outsourcing activities optimally while still complying with the principles of prudence and adequate risk management.

Cyber security management provides an overview and guidance for Banks in managing cyber risks that refer to international standards and best practices, including the National Institute of Standards and Technology (NIST) Framework for Improving Cyber Security, NIST Risk Management Framework, ISO 27001 – Information Security Management Standard , ISO 27032 – Guidelines for Cybersecurity, and Financial Stability Board Cyber Incident Response and Recovery Toolkits.

The cyber security risk management framework consists of 4 (four) mutually sustainable pillars which have been adjusted to the provisions relating to the implementation of Commercial Bank risk management so that they can be integrated into aspects of the Bank's risk profile. The four pillars are governance; cyber security risk management process strategy (identification, protection, vigilance, resilience, and information system); and internal control systems.

3.2.2 Implementation of Cyber Security Exercise

Cyber Security Exercises can be carried out periodically according to the Bank's cyber risk needs and profile. Apart from implementing the cyber security framework in question, an adequate cyber reporting system is also needed. This aims to support strengthening cyber resilience by providing an overview of cyber incidents and threats that occur to the authorities, including, among other things, cyber incident reports and Bank cyber security status reports.

Over the last few years the threat of cyber incidents and attacks has become an important issue in the financial services sector, including the banking sector, as reflected in the fairly high number of cyber incidents and attacks in the banking sector in all parts of the world, including in Indonesia.

Teguh Arifiyadi, Plt. The Director of Information Application Control at the Ministry of Communication and Informatics said that along with the increase in internet use since the outbreak of the Covid-10 pandemic in early March 2020, the level of fraud or cyber crime, including in the banking sector, has increased. According to him, there are 5,000 reports of complaints about fraudulent activities submitted to the Ministry of Communication and Information website every week. In fact, since March 2020 until now the total complaints we have received are almost 200,000 fraud reports with the most widely used media being WhatsApp and Instagram.

AKP Jeffrey Bram, Kasubnit 4 Subdit 2 Ditipidsiber Bareskrim Polri said that from 2017 to 2020 there were 16,845 reports of criminal acts of cyber fraud submitted to the Directorate of Cyber Crime (Ditipidsiber) Polri.

The risk management model as recommended by the OJK through the Digital Banking Transformation Blueprint has apparently not been used as a reference by a number of banks in Indonesia. Bank CIMB Niaga, for example, still uses a conventional model by implementing an Enterprise Wide Risk Management (EWRM) policy/framework to manage risk in an integrated manner by aligning risk appetite with business strategy. CIMB Niaga only makes cyber risk management an integral part of operational activities and decision-making processes in an effort to achieve business goals. The implementation of risk management is carried out actively with the aim of maximizing added value for shareholders, managing capital comprehensively and maintaining capital at a strong level, as well as ensuring profitability and sustainable business growth.

For CIMB Niaga, adequate technology and data management support risk management activities. In order to increase the effectiveness of the risk measurement process, the Bank must have an information system that provides accurate and timely reports and data to support decision making by management. The information system must be able to produce reports that are used for continuous risk monitoring to detect and correct deviations from policies and procedures more quickly in order to reduce the potential for loss events to occur.

3.2.3 What are the Key Trends in Banking Digitalization Risk Management?

The risk management function of banks has changed greatly in the last decade. While it is difficult to predict how things will continue to change, there are several key trends that will determine risk management in the future as follows:

- **Rapidly Changing Regulations:** Banking regulations are getting stricter every year. Each country has its own set of regulations that change according to the economic environment. The activities of financial institutions and their relationships with customers are under close scrutiny. Due to the ever-changing nature of regulations, financial institutions are looking for more flexible risk management functions.
- **Rise of Fintech and high Customer Expectations:** With the entry of advanced technology into the banking sector, customers expect faster and better services. There is huge competition in the banking sector to meet the changing needs and demands of customers. Online banking and applications open up new sources of risk for banks.
- **Evolving Technology and Analytics:** The risk function of the future must take advantage of technological advances such as big data, machine learning, artificial intelligence and enhanced analytics. This technology enables the risk function to make better decisions. They also help create a data infrastructure that allows companies to spend more time analyzing their data than managing it.
- **Emergence of New Risks:** Banks are facing new types of technological risks. One example is model risk, which develops from an organization's reliance on a business model. Cyber risks increase as banks go online and provide their services via third-party APIs. Hacking and banking fraud are increasing, and risk functions must be designed to account for these new types of risk.

Security trends indicate that the banking risk function of the future must be high performing. They must be able to handle various risks and also comply with ever-changing

regulations. The risk function must also adapt to a rapidly changing global economy.

Only a fully digitalized risk function with the following attributes can prepare financial organizations for the challenges of the future:

- Automated risk evaluation and decision making
- Utilization of advanced analytical models
- Integration with efficient data governance models
- Reliance on intelligent data science models

Meanwhile, OJK offers eight principles for information technology outsourcing, including 1) governance, 2) due diligence, 3) contractual requirements, 4) information security, 5) monitoring and control, 6) Business Continuity Plan, 7) access and audit rights, and 8) exit strategies.

According to OJK, the development of digitalization in the banking sector increases the risk of cyber security for banks. The rise of cyber attacks has driven the need to increase cyber resilience through strengthening cyber security. Referring to international standards and best practices from various countries, a framework for strengthening the banking sector's cyber security framework has been prepared, consisting of Cyber Security Management, Cyber Security Exercise and Cyber Security Reporting.

The most pressing digital banking risk management problems are divided into two categories, namely challenges and ways to overcome them. Common challenges encountered are:

- **Outdated company culture:** Entrenched processes and perspectives can hold back digital transformation. Promoting a more forward-thinking culture must start at the top and trickle down so that the entire institution embraces change.
- **Reluctance to change:** KPMG notes that, “Today's executives and professionals will be quick believers or they will hinder your progress.” What's important is to identify categories ahead of time and empower them to lead your digital transformation.
- **Lack of innovative thought leadership:** It takes truly out-of-the-box thinking to compete digitally with big banks and emerging fintech companies.
- **Misguided beliefs:** Discard any notion that mobile banking apps are the only component of a digital strategy, or that digital first means personalization is no longer necessary. Back-end operations and internal processes must fully support a digital environment that effectively identifies and meets individual customer needs based on their actions and behavior.
- **Increasing cyber crime:** A real challenge in risk management for banking digital transformation is the increase in cyber crime. Over the last few years the threat of cyber incidents and attacks has become an important issue in the financial services sector, including the banking sector, as reflected in the fairly high number of cyber incidents and attacks in the banking sector in all parts of the world, including in Indonesia. Teguh Arifiyadi, Plt. The Director of Information Application Control at the Ministry of Communication and Informatics said that along with the increase in internet use since the outbreak of the Covid-10 pandemic in early March 2020, the level of fraud or cyber crime, including in the banking sector, has increased. According to him, there are 5,000 reports of complaints about fraudulent activities submitted to the Ministry of Communication and Information website every week.

In fact, since March 2020 until now the total number of complaints we have received is almost 200,000 fraud reports with the most widely used media being Whatsapp and Instagram.44 AKP Jeffrey Bram, Head of Sub-unit 4 Sub-directorate 2 Ditipidsiber Bareskrim Polri said that from 2017 to 2020 there were 16,845 recorded. reports of criminal acts of cyber fraud submitted to the Directorate of Cyber Crime (Ditipidsiber) of the National Police. Cybercrime modes that occur in the banking sector include hacking, skimming (copying information), defacing (replacing or modifying web pages), phishing (phishing), BEC (business email compromise), and social engineering. Business Email Comprise (BEC) also

known as Email Account Compromise or EAO Fraud is a fraud that targets a company's financial managers to make legal transfer payments by posing as company officials, colleagues or vendors. Meanwhile, based on incoming reports, social engineering is the method most frequently used this year. Social engineering usually occurs when the victim is less alert and is tricked into providing personal data such as a PIN or password so that the criminal can access the account and take over customer funds at the bank.

Speakers in the webinar "Challenges and Strategies for Overcoming Cyber Crime" proposed a number of ways to overcome the various challenges mentioned above. Among others are:

- **Improve digital compliance and cybersecurity.** This means that banks operating in a digital environment must still comply with all applicable laws and regulations. This includes paying special attention to unique digital processes covered by special rules, such as electronically signing documents in accordance with applicable Cyber Laws.
- **Third party risk management;** Out of necessity, many banks are outsourcing all or part of their digital strategy to fintechs and other third-party vendors. However, institutions are ultimately still responsible for all functions, whether carried out internally or externally. A strong vendor management program is key to ensuring that no unqualified third-party providers are hired. Providers must understand applicable regulatory requirements, be able to comply with them and guarantee compliance.
- **Be alert to fraud and identity theft:** More banking without face-to-face interaction may increase the risk of synthetic identity fraud, traditional identity theft, and account takeover. Banks can address this challenge by reviewing and strengthening Bank Secrecy/anti-money laundering laws.
- **Raising awareness:** Irwan Tisnabudi, Digital Banking Head of Bank BTPN said that it is the wrong way to carry out various security awareness both in business and in collaboration with bank and non-bank institutions in the Datamu Secret collaborative campaign as well as participating in the FKDKP discussion forum held between Compliance Director institutions in the banking environment Indonesia. In order to optimize public understanding of banking security, Jenius also introduced the page www.jenius.com/pages/jeniusaman which contains the latest digital security information.

4. Conclusion

Based on the discussion above, it is clear that the role of digital technology has rapidly changed the global financial ecosystem. Along with this, public demand for digital financial services continues to increase, providing a great opportunity for the banking industry to increase its customer base and optimize their profits. However, on the other hand, the increasing threat of cybercrime opens up the potential for significant losses for banking institutions.

To meet these challenges, the authors recommend a proactive approach. Banking institutions must restructure their risk management strategies, especially through the development of strong digital risk management. This not only involves protecting the banking institutions themselves, but also involves the security of their customers and their position in the market. Effective digital risk management must be based on the eight principles of information technology outsourcing recommended by the Financial Services Authority (OJK), namely governance, due diligence, contractual requirements, information security, monitoring and control, Business Continuity Plan, access and audit rights, and exit strategies.

By implementing this approach, banking institutions will be able to build a solid foundation in facing the challenges of the digital era. This will not only protect them from potential losses, but also ensure operational continuity, customer confidence and continued growth in this ever-changing market.

References

[1] M. R. Miah *et al.*, “Innovative Policy Approach to Environmental Resource Management Through Green Banking Activities,” *Am. J. Econ.*, vol. 13, no. 2, pp. 35–51, 2023.
[2] U. Beck, “From industrial society to the risk society: Questions of survival, social structure and ecological enlightenment,” in *Risk Management*, Routledge, 2020, pp. 17–44.
[3] Ö. Önday, “Society 5.0-its historical logic and its structural development,” *J. Sci. Reports*, vol. 2, no. 1, pp. 32–42, 2020.
[4] S. Mishra and A. K. Tyagi, “The role of machine learning techniques in internet of things-based cloud applications,” *Artif. Intell. internet things Syst.*, pp. 105–135, 2022.
[5] T. Ibn-Mohammed *et al.*, “A critical analysis of the impacts of COVID-19 on the global economy and ecosystems and opportunities for circular economy strategies,” *Resour. Conserv. Recycl.*, vol. 164, p. 105169, 2021.
[6] D. James and P. Ghosh, “The Evolution Of Neo-Banking In India Study On Growth And Challenges,” *Strateg. Bus. Decis. Sustain. Dev.*, vol. 134, 2023.
[7] H. S. Pramanik, M. Kirtania, and A. K. Pani, “Essence of digital transformation—Manifestations at large financial institutions from North America,” *Futur. Gener. Comput. Syst.*, vol. 95, pp. 323–343, 2019.
[8] A. G. Prawiyogi, M. Hammet, and A. Williams, “Visualization Guides in the Understanding of Theoretical Material in Lectures,” *Int. J. Cyber IT Serv. Manag.*, vol. 3, no. 1, pp. 54–60, 2023.
[9] K. Kano and E. Dolan, “Data Compression Analysis of Multimedia Video on Demand and DEMAND TV Broadcast Systems on the Network,” *Int. J. Cyber IT Serv. Manag.*, vol. 3, no. 1, pp. 48–53, 2023.
[10] E. Suandi, H. Herri, Y. Yulihasri, and S. Syafrizal, “An empirical investigation of Islamic marketing ethics and convergence marketing as key factors in the improvement of Islamic banks performance,” *J. Islam. Mark.*, vol. 14, no. 6, pp. 1438–1462, 2023.
[11] S. Demirkan, I. Demirkan, and A. McKee, “Blockchain technology in the future of business cyber security and accounting,” *J. Manag. Anal.*, vol. 7, no. 2, pp. 189–208, 2020.
[12] O. Popelo, M. Dubyna, and N. Kholiavko, “World experience in the introduction of modern innovation and information technologies in the functioning of financial institutions,” *Balt. J. Econ. Stud.*, vol. 7, no. 2, pp. 188–199, 2021.
[13] P. Dzhaparov, “Application of blockchain and artificial intelligence in bank risk management,” *Икономика и управление*, vol. 17, no. 1, pp. 43–57, 2020.
[14] J. A. Luft, S. Jeong, R. Idsardi, and G. Gardner, “Literature reviews, theoretical frameworks, and conceptual frameworks: An introduction for new biology education researchers,” *CBE—Life Sci. Educ.*, vol. 21, no. 3, p. rm33, 2022.
[15] I. Walsh and F. Rowe, “BIBGT: combining bibliometrics and grounded theory to conduct a literature review,” *Eur. J. Inf. Syst.*, vol. 32, no. 4, pp. 653–674, 2023.
[16] M. Gusenbauer and N. R. Haddaway, “Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google Scholar, PubMed, and 26 other resources,” *Res. Synth. Methods*, vol. 11, no. 2, pp. 181–217, 2020.
[17] H. H. Shubbar, “BANKING RISKS IN THE CONTEXT OF THE FINANCIAL CRISIS 2008,” *World Bull. Manag. Law*, vol. 19, pp. 136–142, 2023.
[18] R. Spanò and C. Zagaria, “Enterprise risk management systems: Emerging issues and future trends,” *Integr. Perform. Manag. Enterp. Risk Manag. Syst. Emerg. Issues Futur. Trends*, pp. 35–68, 2022.
[19] M. M. N. Ahmed and M. M. J. Alam, “Reading Material on Risk Management in Financial Institutions (RMFI),” 2023.
[20] M. Naili and Y. Lahrichi, “The determinants of banks’ credit risk: Review of the literature and future research agenda,” *Int. J. Financ. Econ.*, vol. 27, no. 1, pp. 334–360, 2022.
[21] V. Korphaibool, P. Chatjuthamard, and S. Treepongkaruna, “Scoring sufficiency economy philosophy through GRI standards and firm risk: A case study of thai listed companies,” *Sustainability*, vol. 13, no. 4, p. 2321, 2021.
[22] J. Ruiz-Canela López, “How can enterprise risk management help in evaluating the

operational risks for a telecommunications company?," *J. Risk Financ. Manag.*, vol. 14, no. 3, p. 139, 2021.

[23] F. Alfiana *et al.*, "Apply the Search Engine Optimization (SEO) Method to determine Website Ranking on Search Engines," *Int. J. Cyber IT Serv. Manag.*, vol. 3, no. 1, pp. 65–73, 2023.

[24] H. Do, T. Ngo, and Q. Phung, "The effect of non-performing loans on profitability of commercial banks: Case of Vietnam," *Accounting*, vol. 6, no. 3, pp. 373–386, 2020.

[25] A. Eiji and S. Mehta, "Simulation-Based 5G Femtocell Network System Performance Analysis," *Int. J. Cyber IT Serv. Manag.*, vol. 3, no. 1, pp. 74–78, 2023.