Journal of Economics, Finance and Management Studies

ISSN (print): 2644-0490, ISSN (online): 2644-0504

Volume 07 Issue 02 February 2024

Article DOI: 10.47191/jefms/v7-i2-28, Impact Factor: 8.044

Page No: 1094-1102

Bank Risk Trends and Integrated Risk Management

I Wayan Budi Artha

Triatma Mulya University

ABSTRACT: The very rapid development of technology, especially information technology, increasingly massive use of the internet and social media, hydrometeorological events/climate change, disease pandemics and very rapid environmental changes, have resulted in bank risks experiencing an increasing and increasingly complex trend. Several common risks, such as operational, credit, strategic, market, liquidity, legal, compliance and reputation risks which previously dominated bank risks, have increased and several new risks have emerged. These new risk trends include cyber risk, climate change, data privacy, third party collaboration/outsourcing. These risks must be integrated into all business processes and mitigated properly so that their impact can be minimized by implementing integrated risk management and effective governance. The implementation of good governance and supported by integrated risk management can encourage improvements in the quality of sound banking management, increase competitiveness, resilience and encourage sustainable growth.

KEYWORDS: Bank Risk Trends, Cyber Risk, Climate Change Risk, Outsourcing Risk, Data Privacy Risk, Integrated Risk Management and Governance.

1. INTRODUCTION

Banks are trust businesses so their business management must be managed carefully by implementing good and effective risk management and governance. Bank risks are very complex and are increasing along with the development of technology, especially information technology and the increasingly massive use of the internet and social media in various areas of our lives, which has an impact on increasing cyber risks, third party collaboration/outsourcing and data privacy. Apart from that, hydrometeorological events and climate change such as earthquakes, the eruption of the Merapi volcano, typhoons/tornadoes and flash floods as well as disease disasters such as the Covid-19 pandemic result in increased risks of climate change, operational risks and other bank risks (EY & IIF, 2021).

According to the Indonesian Bankers Association (2016) banks must be able to identify potential risks that arise in each business process, then determine a risk management strategy to what extent the risk will be taken in accordance with the level of risk tolerance (risk appetite) as well as determine the loss reserves that must be formed and determine funding sources to cover these risks, including risks that cannot be predicted (unexpected loss).

Risk management must be integrated into every business process (Lam, 2006), Hanggraeni, 2016) and (Susilo & Kaho, 2018). Implementation of risk management must be carried out in an integrated manner and combined with the implementation of good governance in order to obtain optimal results.

2. LITERATURE REVIEW

Types of Bank Risk

Bank risk is the risk faced by the banking sector considering the various policies and decisions taken in various fields such as : credit distribution decisions, fund mobilization activities, bank service activities such as transfers, exports, credit card issuance, and various other forms of financial decisions. This causes losses for the banking sector so preventive measures are needed.

In accordance with Financial Services Authority Regulations, namely POJK No: 18/POJK.03/2016 dated 16 March 2016 concerning the Implementation of Risk Management for Commercial Banks, there are 8 (eight) risks that must be implemented, measured and mitigated, namely credit, market, liquidity, operational, legal, reputation, compliance and strategic risks.

According to the OJK, "Credit risk is the risk resulting from the failure of other parties to fulfill their obligations to the Bank, including credit risk due to debtor failure, credit concentration risk, counterparty credit risk and settlement risk. Market risk is the

risk on the balance sheet and administrative account positions, including derivative transactions, due to overall changes in market conditions, including the risk of changes in option prices. Liquidity risk is the risk resulting from the bank's inability to meet maturing obligations from cash flow funding sources and/or from high-quality liquid assets that can be collateralized, without disrupting the bank's activities and financial condition. Operational risk is the risk resulting from inadequacy and/or non-functioning of internal processes, human error, system failure, and/or external events that affect bank operations. Compliance risk is the risk resulting from banks not complying with and/or not implementing laws and regulations. Legal risk is the risk resulting from lawsuits and/or weaknesses in juridical aspects. Reputation risk is a risk resulting from a decrease in the level of stakeholder trust that originates from negative perceptions of the bank. Strategic Risk is the risk resulting from inaccuracy in making and/or implementing a strategic decision as well as failure to anticipate changes in the business environment."

For financial conglomerates there are 2 (two) additional risks, namely intragroup transaction risk and insurance risk (POJK 17, 2014). According to the OJK, "Intra-group transaction risk is the risk resulting from the dependence of an entity, either directly or indirectly, on other entities within a Financial Conglomeration in order to fulfill the obligations of written agreements and unwritten agreements, whether followed by the transfer of funds and/or not followed by the transfer of funds, while insurance risk is the risk resulting from the failure of an insurance company to fulfill its obligations to policyholders as a result of inadequate risk selection processes (underwriting), determining premiums (pricing), use of reinsurance, and/or claims handling." Insurance risks are not required to be managed by Financial Conglomerates which do not have insurance and/or reinsurance companies.

For Sharia banking, there are 2 (two) additional risks, namely return and investment risk (POJK 65, 2016). According to the OJK, "Rate of Return Risk is the risk resulting from changes in the level of return paid by the bank to customers, due to changes in the level of returns received by banks from channeling funds, which can influence the behavior of third party fund customers of the bank, while Investment Risk (Equity Investment Risk) is the risk resulting from the bank taking part in bearing the customer's business losses financed in profit sharing based financing using the net method. revenue sharing or those using the profit and loss sharing method."

Bank Risk Trends

There are several bank risk trends that have emerged as a result of technological developments, especially information technology, increasingly massive use of the internet and social media, disease disasters and hydrometeorological events / climate change, including increasing cyber risks, climate change, data privacy (private data protection) and cooperation. third party / outsourcing (EY and IIF, 2021).

Cyber security risks are risks posed by threats from irresponsible parties who attempt to access, damage or steal sensitive data and information from digital banking systems. Cyber attacks can cause significant financial, reputational and trust losses for customers and banks. Cyber attacks can also disrupt banking operations and services. Data privacy risk (personal data protection) is the risk posed by a breach or leak of customer personal data held by the bank (An Nur, 2023). Outsourcing risk is the risk that arises as a result of outsourcing part of the bank's business to a third party. Potential risks that arise can include strategic risks, operational risks, legal/regulatory and compliance risks, as well as reputation risks (CNBC, 2021).

Climate risk is broadly defined as the potential harm to human life: livelihoods, health and well-being. Also losses to ecosystems and species, economic, social and cultural assets, services (including ecosystem services) and infrastructure due to climate change (CDP, 2022). From an organizational perspective, climate risks are often categorized into two types: physical risks and transition risks. Physical risks refer to the physical impacts of climate change caused by extreme weather events such as floods and storms, as well as severe long-term changes such as rising temperatures and sea levels. Transition risk refers to the transition to a low-carbon economy, which of course requires changes in policy, law, use of technology and broad markets.

Integrated Risk Management

Integrated risk management is a comprehensive, systematic and coordinated approach to identifying, measuring, monitoring and managing (controlling) risks arising from bank operational activities, which have an impact on achieving strategic objectives and corporate profits as well as ensuring and utilizing all available resources used to create and increase company value, both short and long term for stake holders(Indonesian Bankers Association, 2016) and (Susilo and Kaho, 2018).

Corporate governance

Banks are obliged to implement good governance in carrying out business activities at all levels or levels of the organization, in accordance with the provisions of applicable laws and regulations (POJK 17, 2023).This aims to increase banking competitiveness and resilience and encourage stable and sustainable performance growth. The implementation of good governance includes at least the following principles: (a) transparency, (b) accountability, (c) responsibility, (d) independence, and (e) fairness.

Furthermore, Steinberg (2011) stated that the most important element of governance is a corporate culture, which emphasizes the values of integrity and ethics. Companies that operate based on integrity and ethics have a strong foundation for success.

Experience shows that failure to implement good governance in banks is often the main reason why banks are unable to compete in business, and bank failure on a large scale can cause a crisis in the banking sector and the economy.

3. METHODOLOGY

The method used in this research is a qualitative descriptive method with an approachlibrary research (research literature). Library research is a series of activities related to methods of collecting library data, reading and taking notes and processing library materials (Zed, 2014). In library research, literature search is not only the first step in preparing a research framework and research design, but also the use of library sources to collect research data and information.

4. DISCUSSION

Basically, the bank's business is to manage risk, so that all business activities/processes carried out must always be based on risk. In the past, bank risk management was still traditionally carried out in silos, where various types of risks that existed/emerged were seen as separate things so that it was not enough to identify and manage risks as a whole, focusing more on preventing losses. caused by various risks (backward looking), but less attention to risk prevention factors and less attention to the process of creating and protecting value (Indonesian Bankers Association, 2016) and (Susilo and Kaho, 2018). The current bank risk management system has integrated various types of risks in business processes and places greater emphasis on future conditions (forward looking).

Bank Risk Management

Bank risk management should include all types of risk, including credit, operational, market, liquidity, strategic, legal, reputation and compliance risks (POJK 18, 2016). Meanwhile, for financial conglomerate companies, inter-group transaction risks and insurance risks are added (POJK 18, 2014). For Sharia banking, there are 2 (two) additional risks, namely return risk and investment risk (POJK 65, 2016). Management of these risks should be integrated into all business processes to obtain optimal results.

Credit risk management from upstream starting from credit analysis using 5 C analysis or scoring system, supervision and monitoring, portfolio management to downstream, namely problem credit management must be carried out continuously and at each stage it must be carried out with effective mitigation (Indonesian Bankers Association , 2016), Increased operational risk due to the use of increasingly advanced technology, hydrometeorological events and climate change should be anticipated by improving Business Continuity Management, so that for an extreme event the bank has prepared itself to be able to operate immediately, especially for bank activities vital ones such as customer service. Other risk management must also receive serious attention so that bank business management runs well and sustainably.

Bank Risk Trends

Cyber Risk

The very rapid development of information technology, increasingly massive use of the internet and social media has an impact on increasing bank risk exposure with an increase in cyber attacks (POJK 11, 2022) and (Strategic Analysis Council-State Intelligence Agency, 2017). Cyber attacks infiltrate (break into) vulnerable banking systems and destroy specific targets. Forms of cyber attacks range from infiltration of spyware programs to sabotage (destruction) of banking infrastructure.

Here are some examples of cyber attacks that can occur in the banking sector:

a. *Phishing*is a form of fraud by sending fake emails or messages claiming to be a bank or other official organization to trick customers into providing personal or confidential information such as account numbers, birth mother's name, passwords, PIN codes, OTP codes, etc.
b. *Malware*: is software that has features or capabilities that can damage information systems. The disruption in question can cause losses to the information system owner, either directly or indirectly.
c. *Denial of Service*(DoS) and Distributed Denial of Service (DDoS) are attacks that attempt to disrupt or stop the continuous operation (availability) of an electronic system during the processing of transactions or authorized access, especially by making network capacity or computer power appear to have been exhausted due to the large number of access requests
d. *Web Defacement* is an attack carried out against a website by changing or modifying the website in such a way that the contents of the website change according to the attacker's wishes.

During the past pandemic, the threat of cyber attacks increased, data from the BSSN National Cyber Security Operations Center shows that in 2020, there were 495 million cyber attacks, a 5-fold increase compared to the previous year of 228 million

cases. Globally, the financial sector is the sector most frequently affected by cyber incidents (BSSN, 2021). The risk profile of cyber attacks on banks in Indonesia is still very high, as can be seen in Table 1.

Table 1. Banking Cyber Attack Risk Profile in 2020

Risk Level	Identified Risks
Very High	Social engineering, processing failure, hardware failure, internal fraud, hacker attacks
High	Bugs in applications, virus attacks, external fraud, data leaks due to malware/trojans, SQL injection, hampered IT operations due to lack of IT Human Resources, configuration weaknesses against malware attacks, phishing attacks
Medium	Skimming, IT system failure, system weaknesses when designing and establishing procedures, third party dependencies so that problem management has not been resolved optimally, network disruption at ATMs, misuse of system access, misuse of core banking access rights, misuse of access rights on network devices.

Source: BSSN, 2021.

A very high level of risk can have a significant impact on banking, especially in operational and financial terms. Factors causing this potential risk can come from internal or external parties to the Bank.

In order for banks to continue operating, banks must implement good governance and risk management by making good use of information technology while maintaining cyber resilience and security. Apart from that, banks must also establish strategies and procedures that are right on target and sustainable to deal with problems caused by cyber threats and incidents (POJK 11, 2022) and (POJK 29, 2022). Banks maintain cyber resilience by implementing at least the following processes:

(a) Identify assets, threats and vulnerabilities.

(b) Asset protection.

(c) Cyber incident detection.

(d) Cyber incident response and recovery.

The inherent risk assessment related to cyber security is carried out by taking into account at least 4 (four) assessment factors, namely technology, bank products, organizational characteristics and track record of cyber incidents.The implementation of risk management related to cyber security includes four aspects:

a. Cyber security risk governance, including the adequacy of appropriate active supervision by the board of directors and board of commissioners, and the development/formulation of the level of cyber security risk to be taken (risk appetite) and cyber security risk tolerance as well as cyber security risk culture and awareness.
b. Risk management framework related to cyber security. This includes the appropriateness of risk management strategies, organizational tools, and settings for cybersecurity-related policies, procedures, and risk limits.
c. Adequacy of risk management processes, human resources and risk management information systems related to cyber security.
d. Risk control system related to cyber security, which includes the adequacy of the internal control system and the adequacy of reviews.

Cyber risks must be properly mitigated, ways to mitigate cyber security risks include:

a. Always be careful when opening/downloading suspicious emails or messages and do not carelessly provide personal or confidential information to any party. Use the latest and most trusted antivirus and firewall to protect electronic devices from malware.
b. Increase password security, namely use safe and unique passwords and change them as often as possible.
c. Download the official bank application, avoid using public facilities and networks, and be careful when using social media.
d. Banks must improve their cyber security systems by updating their software regularly, conducting regular testing and audits, and having a dedicated team to monitor and respond to cyber threats.
e. Banks also need to educate their customers on how to use digital banking services safely.

According to Strategic Analysis Council-State Intelligence Agency (2017) a cyber threats are not only damages communication devices and information systems that are attacked by malicious programs such as viruses, worms, malware and the like, but also harms the psychology of users, and can even damage the culture and norms that exist in society, such as the emergence of many hate speeches, hoacks and the like. The threat of cyber risk will also increase reputational and legal risks.

Data Privacy Risk

Customer personal data is information that can be used to identify or trace the customer's identity, for example: name, address, telephone number, email, birth mother's name, identity card number, transaction history, preferences and so on. Customer personal information is an important asset for banks because it can be used to provide services that meet customer needs and desires. However, customer personal data can also be misused by unauthorized parties for purposes that are detrimental to customers, such as fraud, identity theft, extortion, stalking, and discrimination, etc. Breach or loss of customer personal data may occur due to cyber attacks, human error, procedural errors, or non-compliance with regulations. Banks are required to apply the principles of personal data protection in processing and updating personal data (POJK 6, 22) and (POJK 11, 2022).

Personal data protection risks must be appropriately mitigated. Ways to reduce personal data protection risks include:

a. Customers should choose a bank that has a good reputation and is committed to protecting its customers' personal information.
b. Customers are required to read and understand the bank's privacy policy before using digital banking services.
c. Customers also have the right to view, change or delete their personal data stored by the bank in accordance with applicable regulations.
d. Banks are required to have strict and transparent systems and procedures for collecting, storing, processing and deleting customer personal data.
e. Banks must have a good cyber security system.
f. Banks are also required to comply with applicable regulations regarding the protection of customers' personal data (Law Number 11 of 2008 dated 21 April 2008 concerning Information and Electronic Transactions).

Outsourcing Risk

Transferring part of the work implementation to another party (hereinafter referred to as outsourcing) is transferring part of the work implementation to a service provider company in the context of contracting a work/providing labor services based on a work agreement and/or work contract.Handing over part of the work implementation to other parties has the potential to increase risks for the bank, namely outsourcing risk. Outsourcing risk is the risk that arises if tasks are delegated to a third party. Risks that may arise can be strategic risk, operational risk, regulatory risk, compliance risk, reputation and concentration (CNBC, 2021).

In outsourcing, Banks are required to apply the principles of prudence and effective risk management according to the scale, characteristics and complexity of the work being outsourced (POJK 9, 2016) and (POJK 11, 2022). According to OJK, "Outsourcing risk management practices include at least the following: (a) Active supervision of the board of directors and board of commissioners. (b) Adequacy of policies and procedures. (c) Adequacy in the process of risk identification, measurement, monitoring and control and risk management information systems, and internal control systems."

Based on the POJK above, "Banks that use third party service providers are also required to have the ability to supervise the implementation of bank activities carried out by third party service providers. must have a work agreement that takes into account at least: (a)Qualifications and competencies of owned human resources; (b) Commitment of service providers to maintain the confidentiality of bank and bank customer data and/or information; (c) Commitment of the service provider to submit the results of regular information technology audits carried out by independent auditors regarding the provision of services to the bank; (d) Any partial transfer of activities or subcontracts by the Service Provider will be carried out with written approval from the bank; (e) Mechanism for service providers to report critical incidents to the bank; (f) Mechanism for terminating the cooperation agreement if the agreement is terminated before the contract period ends; (g) Compliance with legal regulations regarding the provision of services by service providers; (h) Willingness of the service provider to fulfill the obligations and/or requirements stated in the Collaboration agreement; and (i) Willingness of the Service Provider to provide access to the financial supervisory authority and/or other institutions authorized to exercise control over the service activities provided in accordance with the provisions of laws and regulations."

Climate Change Risk

Climate change risk is the potential negative impact on humans or ecological systems due to the impacts of climate change.The issue of climate change has received serious attention from monetary and fiscal authorities in many countries, including Indonesia, especially since the signing of the Paris Agreement on April 22 2016. Climate change not only causes natural disasters that claim lives and property, but also disrupts macroeconomic stability and finance. In addition, climate change can affect financial system stability through various channels. First, climate change increases the likelihood that bank debtors will

default. Second, climate change encourages banks to reduce their lending. Third, climate change causes an increase in insurance premiums. Fourth, climate change reduces the value of real estate or financial assets (Bisnis.Com, 2022).

The results of a survey by Illuminate Asia as a representative of the International Research Institutes (IRIS) show that concern about climate change and its impacts is quite high in Indonesia (52%), higher than the global average (44%). Indonesians are quite optimistic (54%) about the ability to reverse climate change in the next few years or a decade compared to the global average, where 26% believe this will happen in the next decade, 24% in the middle of this century, and 20% other not sure. However, Indonesian people's awareness and understanding of the prospects and solutions to climate change is still low (IRIS, 2021).

Climate and environmental risks have a significant impact on banking risk. Climate change has an impact on the emergence of climate-related prudential risks in banking. Climate risks refer to transition risks and physical risks. Apart from being vulnerable to physical risks, government policies towards a low-carbon economy also increase bank exposure to transition risks. Indonesia's journey towards a low carbon economy began with the ratification of the Paris Agreement through the ratification of Law Number 16 of 2016. Indonesia has targeted and moved towards a national contribution (NDC) in the form of reducing carbon emissions by 41% by 2030 and moving towards neutrality CO2 (2060). Furthermore, the government's decision to implement a carbon tax to harmonize tax regulations and increase the use of electric vehicles, solar panels and other new energy (technology), is implemented in accordance with Law Decree Number 7 of 2021 dated 29 October 2021. This is predicted to influence the direction banking industry business in the future. Risks arising from climate change are a challenge for banks, and banks are increasingly required to be able to adapt by incorporating climate risk considerations into strategic decision making, business processes, governance and risk management frameworks.

Therefore, banks are required to carry out stress tests on the impact of climate risk on potential climate change on banking risks: credit, operational, liquidity, market and reputation risks (OJK, 2023).

Indonesia's Finance Minister cited research published in 2021 by a Swiss research institute and said climate change could also cause major losses to the economy. Countries around the world could lose more than 10% of their total economic value or gross domestic product (GDP) if the 2050 Paris Agreement is not fulfilled. It is estimated that Indonesia will lose 40% of its gross domestic product (GDP) in 2050 due to climate change. This figure is much higher than the average global government loss of only 10-18%. Meanwhile, findings from the Ministry of National Development Planning (PPN)/National Development Planning Agency (Bappenas) in early 2022 showed that the impact of climate change could cause economic losses of up to IDR 544 trillion for the Indonesian state during the 2020-2024 period (Trenasia.Com, 2022).The impact of climate change will increase bank operational risks. For this reason, banks must strengthen their business continuity management systems.

Corporate governance

Bank are obliged to implement good governance in carrying out their business activities at all levels or levels of the organization in accordance with the provisions of statutory regulations (POJK 17, 2023).This is intended to increase the bank's competitiveness and resilience as well as encourage stable and sustainable performance growth. The implementation of good governance at least includes the principles of: transparency, accountability, responsibility, independence and fairness.

Good bank governance means the structure, processes and mechanisms of bank management that pay attention to, create and maintain the interests of all relevant stakeholders as well as carrying out banking operations in accordance with the provisions of laws and regulations, must also be based on standards, ethical values, principles and practices. generally accepted.

The implementation of bank governance supported by integrated risk management will improve the quality of healthy bank management, increase competitiveness and resilience and encourage sustainable growth.

Integrated Risk Management

Risk in the banking industry is the potential for future events, both expected and unexpected, to have a negative impact on a bank's income or capital due to uncertainty. This uncertainty occurs because there is no or insufficient information regarding what will happen regarding the event, how likely it is to occur (likelihood), and how big the impact will be on the target (impact). Meanwhile, risk management itself refers to a series of procedures and methods to identify, measure, monitor and control risks arising from banking activities and keep them within acceptable limits (bank risk appetite), controlled and profitable.

The implementation of the risk identification process is carried out at least through analysis of the bank's specific risk characteristics and the risks of other bank products and business activities. Risk measurement periodically assesses the suitability of assumptions, data sources and procedures used in risk measurement, as well as improving the risk measurement system if significant changes occur in the Bank's business activities, including products, transactions and other risk factors. Risk monitoring activities are carried out by assessing risk exposure and improving the reporting process if significant changes occur in the bank's business activities, products, transactions, risk factors, information technology and risk management information systems. Banks

are required to implement an integrated risk management process in all their business units to manage certain risks that could threaten the continuity of the bank's business.

Thus, integrated risk management is a structured approach with a certain methodology for managing uncertainty, assessing risks including developing strategies for managing and mitigating risks using existing resources. The strategies referred to in risk management that can be taken include:others are transferring risks to other parties (insurance), avoiding risks, reducing the negative effects of risks, reserving certain costs such as CKPN etc.

Integrated risk management is very important in banking because risk factors can arise from various sources. Risks are predictable and unforeseen events that can have a negative impact on bank income and capital. Therefore, at the beginning of implementing risk management, banks must be able to identify risks in detail, both existing risks and risks that may occur. After a thorough identification process, the next step for banks is to measure, monitor and manage risks. The purpose of this measurement is so that banks can estimate losses and their impact on bank capital, taking into account business risks. To monitor risk, banks assess risk exposures, especially those that are significant or could affect bank capital.

One of the things that banks must follow in managing risk management is a rule called Basel issued by The Basel Committee on Banking Supervision (BCBS) internationally, starting from Basel I (minimum capital provision), Basel II (minimum capital requirements, supervisory review process, market discipline) and Basel III (more detailed capital structure and liquidity arrangements).

Regarding risk governance/implementation, the international risk management standard ISO 31000: 2018 highlights several important points, namely:

a. The goal of risk management is to create and protect corporate value.
b. Risk management is an integral part of organizational leadership and governance.
c. Risk management must consider the context in which it is applied: the internal and external context of the organization.
d. Risk management must consider human behavior and cultural factors.

Considering that risk management is an integral part of all organizational activities, the implementation of risk management must be carried out in an integrated manner in order to obtain optimal results. Integrated risk management is defined as a comprehensive, systematic and coordinated approach to identifying, measuring, monitoring and managing risks arising from bank business operational activities, which can or may affect the company's vision, mission and strategic objectives by ensuring that all available resources has been used to create value, both short and long term for the interests of stake holders.

According to Susilo and Kaho (2018) that the integration of risk management is very dependent on understanding the organizational structure and context. We know that organizational structures differ from one bank to another which is adjusted to the size of the business, goals, objectives and complexity faced. Thus, risk must be managed in every part of the organizational structure related to business operations and everyone in the organization, from top management to lower level employees, has the responsibility to manage the risks they face. Integrating risk management into the organization requires understanding the organization's governance which also identifies potential risks contained in the structure and processes at each level.Governance controls the management of an organization, its external and internal relationships, rules, processes and organizational practices to achieve its goals.

Integrating risk management into an organization is a dynamic and iterative process that must be adapted to the company's needs and culture. Risk management is part of, and should be closely linked to, an organization's strategy and operations, as well as its purpose, governance, leadership and commitment.

Implementing integrated risk management in banking operations allows companies to manage all risks that arise in all activities, integrated into relevant business processes, with clear, responsive and timely risk manager responsibilities. It helps in prioritizing actions, selecting possible alternatives, and supports decision making. This data and information is used as a basis for measuring bank performance more accurately, assessing the risks of bank business activities, and creating a strong risk management infrastructure to increase bank competitiveness.

Thus, implementing integrated risk management can create and protect value (increase shareholder value), improve performance, encourage innovation and support target achievement. The highest value creation for a company is the achievement of its vision and mission as well as the values it adheres to. This can be achieved if risk management is integrated with the strategic planning process in order to achieve the company's vision, mission and values. This means that risk management must be integrated at every stage by looking at the company's current conditions (macro environment, micro environment and organizational environment) towards the desired future conditions (vision, mission and values), focusing on implementation or strategy execution (competitive strategy, initiative strategy and functional strategy), while not neglecting efforts to monitor targets, both short-term and long-term targets. The above process should be carried out dynamically, according to changes in the

business environment that need to be continuously anticipated well, especially in the era of VUCA (Volatility, Uncertainty, Complexity and Ambiguity), uncertainty and the development of artificial intelligence, where many disruptions occur very quickly.

5. CONCLUSIONS AND RECOMMENDATION

Conclusion

1. The development of technology, especially information technology, hydrometeorological events / climate change and the increasingly massive use of the internet and social media in various areas of our lives, has an impact on increasing and increasing the complexity of bank risks.
2. Bank risk trends include cyber risk, data privacy risk, climate change risk and outsourcing risk.
3. The implementation of good governance and supported by integrated risk management can encourage improvements in the quality of sound banking management, increase competitiveness, resilience and encourage sustainable growth.

Recommendation

1. Banks must implement governance and integrated risk management by utilizing technology, especially information technology.
2. Banks must always maintain cyber resilience and security. Apart from that, banks must also determine appropriate and sustainable strategies and actions to overcome problems caused by cyber threats and climate change.
3. Banks should strengthen business continuity management to anticipate extreme events so that banks can continue and/or immediately be able to operate to serve customers.

REFERENCES

1) An Nur (2023).https://an-nur.ac.id/blog/risiko-perbankan-digital-dan-cara-mitigation.html. An Nur Islamic University, Lampung.
2) BSSN (2021). https://www.bssn.go.id/bssn-terbitkan-profil-risiko-sektor-perbankan-as-acuan-pelaku-industri-perbankan-dan-community-memitigating-threats-dan-kerentanan-cyber/.
3) Bisnis.Com (2022). https:// Ekonomi.bisnis.com/read/20220729/9/1560622/opini-risiko-iklim-stabel-sistem-finansial.
4) CDP (2022).https://cdn.cdp.net/cdp-production/comfy/cms/files/files/000/006/114/original/Bahasa_CDP_Resourcepack.pdf.-AssessmentClimate Risks and Vulnerabilities-Training Guide for Cities.
5) CNBC (2021).https://www.cnbcindonesia.com/market/20211103113315-17-288645/hati-hati-ini-risiko-mengintai-bank-digital-di-masafront.
6) State Intelligence Agency Strategic Analysis Board (2017). Indonesian Cyber 2018 – 2030 Threats, Attacks and Mitigation. Jakarta.
7) EY and IIF (2021). Global Bank Risk Management Survey. 12th Annual.
8) Hanggraeni, D. (2016). Integrated Corporate Risk Management Based on ISO 31000: Theory and Research Results. Publishing Institution, Faculty of Economics, University of Indonesia. Jakarta.
9) Indonesian Bankers Association (2016). Bank Risk Management Strategy. PT. Gramedia Pustaka Utama. Central Jakarta.
10) IRIS (2021). Iris Global Climate Change Survey.
11) Lam, J. (2006). Enterprise Risk Management, Comprehensive Guide for Directors, Commissioners and Risk Professionals. BSMR Team Translation, PT. Ray Indonesia. Central Jakarta.
12) Leo J.S. and V.R. Kaho (2018). Risk Management Based on ISO 31000: 2018 Guide for Risk Leaders and Risk Practitioners. Publisher PT Gramedia Widiasarana Indonesia, Jakarta.
13) OJK (2023).https://www.ojk.go.id/id/berita-dan-kegiatan/publikasi/ Documents/ Pages/Panduan-Climate-Risk-Stress-Testing-(CRST)-Perbankan-2023/ Guide %20Climate%20Risk% 20Stress%20Testing%20(CRST)%20Banking%202023.pdf
14) POJK Number : 17/POJK.03/2014 dated 18 November 2014 concerning the Implementation of Integrated Risk Management for Financial Conglomerates.
15) POJK Number : 18 /POJK.03/2014 dated 18 November 2014 concerning the Implementation of Integrated Governance for Financial Conglomerates.
16) POJK Number : 9 /POJK.03/2016 dated 26 January 2016 concerning Prudential Principles for Commercial Banks Handing over Part of the Work Implementation to Other Parties.
17) POJK Number : 18/POJK.03/2016 dated 16 March 2016 concerning the Implementation of Risk Management for Commercial Banks.

18) POJK Number : 65/POJK.03/2016 dated 23 December 2016 concerning the Implementation of Risk Management for Sharia Banks and Sharia Units.
19) POJK Number : 6 /POJK.07/2022 dated 14 April 2022 concerning Consumer and Public Protection in the Financial Services sector.
20) POJK Number : Number 11 /POJK.03/2022 dated 6 July 2022 concerning the Implementation of Information Technology by Commercial Banks.
21) POJK No:29 /SEOJK.03/2022 dated 27 December 1922 concerning Cyber Resilience and Security for Commercial Banks.
22) POJK Number : 17 dated 14 September 2023 concerning Implementation of Commercial Bank Governance.
23) Steinberg, R.M. (2011). Governance, Risk Management, and Compliance. It Can't Happen to Us ---- Avoiding Corporate Disaster While Driving Success. John Wiley & Sons, Inc., Hoboken, New Jersey.
24) Trenasia (2022).https://www.trenasia.com/dampak-bahan-iklim-serial-1-menghitung-kerugian-negara-akibat-krisis-lingkungan.
25) Zed, M. (2014). Library Research Methods. Indonesian Obor Library Foundation. Jakarta.