International Conference on Sustainable Economics, Management, and Accounting (ICSEMA 2025) Proceedings
Vol. 01 No. 01 Year 2025, Page 4203-4213

ANALYSIS OF OPERATIONAL RISK MANAGEMENT AT BANK SYARIAH INDONESIA CIREBON BRANCH OFFICE

Nining Wahyuningsih[1]*, Diana Djuwita[2]*, and Vira Maghfirah[3]*

[1-3] FEBI, Universitas Islam Negeri Siber Syekh Nurjati Cirebon, Indonesia
*Email corresponding autor: niningwningsih@syekhnurjati.ac.id

Abstract

The purpose of this study was to analyze the factors that cause operational risk at Bank Syariah Indonesia Cirebon Branch Office and analyze the implementation of operational risk management at Bank Syariah Indonesia Cirebon Branch Office. This research method uses a qualitative approach and the type of research is a case study. The data sources used are primary data through interviews and secondary data through library research. The data collection techniques used were interviews and documentation. The data analysis techniques used were data reduction, data presentation and conclusion drawing. The results showed that there were four factors that caused operational risk at Bank Syariah Indonesia Cirebon Branch, namely Human Resources (HR) factors such as deliberate actions, acts of fraud and opportunities to trick the system, other factors, internal process factors, namely failures in internal processes such as fraud and ineffectiveness of subsequent procedures, IT system factors occurred due to cyber attacks such as ransomware, then external event factors that endangered the operations of Bank Syariah Indonesia Cirebon Branch Office mainly came from cyber attacks such as ATM break-ins, and ransomware attacks. natural disasters such as earthquakes. Implementation of operational risk management analysis at Bank Syariah Indonesia Cirebon Branch, specifically by identifying, measuring risk, monitoring risk and controlling risk. The application of operational risk management analysis at Bank Syariah Indonesia Cirebon Branch, specifically by identifying, measuring risk, monitoring risk and controlling risk. In general, this research enriches the understanding of operational risk dynamics to support the improvement of risk management practices in Islamic banking.

Keywords: *Risk management Operations, Islamic Banking, and Human Resources, Cybersecurity, Risk Factors*

INTRODUCTION

Financial institutions have developed various methods to reduce risks and improve their overall performance. Risk management is one of the methods used by financial institutions to mitigate various types of risks. Risk management is an essential element whose implementation must be carefully considered, especially in banks as one of the financial institutions (Nelly et al., 2022).

Operational risk is an important component of management. Operational risk is a risk that is influenced by a number of variables, including systems, processes, procedures, human factors, and external events. Operational risk is not only influenced by certain people, but also by how well the company's directors and managers handle it. In Islamic banking, operational risk is the most important risk for managers to control, compared to other risks.

Research by (Sapiri, 2025) highlights the complex interconnections between different types of risks and underlines the importance of adopting an integrated risk management framework. The analysis shows that events related to one type of risk can have far-reaching implications for others, amplifying overall risk exposure and vulnerability. emphasizes the need for a holistic approach to risk management that takes into account the interdependencies between credit, market, and operational risks. Implications for risk management practices, regulatory frameworks, and systemic stability are discussed, highlighting the importance of enhancing operational resilience and promoting collaboration between academia, industry, and regulatory bodies.

Risk is related to the possibility of an event or condition that has an impact and threatens the target goals and objectives. Therefore, the risk needs to be anticipated and minimized in order to avoid something unexpected happening. Efforts that can be applied to avoid the possibility of risks that will occur are by; measuring, analyzing, and controlling risk. Management is so important to the sustainability of a financial institution, it needs to be processed as well as possible. The increasing complexity of risk is caused by innovation in Islamic banking products such as the emergence of increasingly complex Islamic banking products, for example sukuk, futures murabahah and so on, which has an impact on new challenges in identifying and managing risks, in addition to the increasingly widespread use of information technology, which increases new risks such as cyber risk and system failure risk (Suhaimi, 2021)

Operational Risk Management aims to minimize the potential negative impacts of internal process failures, human error, system failures, or external events. To achieve its operational objectives, Islamic banks must consider operational risks that could affect its operational performance, including the risk of losses resulting from inadequate or failed internal processes, human resources, and systems from external events

In managing a financial institution, operational risk management is crucial. Islamic financial institutions must consider ways to control and reduce risks that are expected to arise in the future. The most important aspect of operational risk management is implementing processes that comply with relevant SOPs, managing risks, and limiting risks so that all business operations can run smoothly and as desired. The information collected can be used as a standard for Islamic bank performance, allowing them to make accurate assessments of potential losses that may occur in the future. Therefore, it is very important and beneficial for Islamic banks to carry out operational risk management (Anam, 2023)

One of the recent risk cases is service disruption and ransomware cyber attacks that threaten customer data leaks. Ransomware is a type of malware or dangerous virus that attacks computer systems. The mode of this cybercrime is to lock the victim's access and then demand a ransom. Bank Syariah Indonesia (BSI) is suspected of being the victim of a Lockbit 3.0 ransomware attack in May 2023. This attack disrupted BSI's banking services, such as ATMs and mobile banking, for several days. Here are some facts related to the ransomware attack on BSI: This attack is suspected of occurring before May 8, 2023, when the BSI Mobile application and ATMs experienced errors and could not be accessed, Lockbit 3.0 is suspected of stealing 1.5 terabytes (TB) of BSI customer data, Lockbit asked BSI for a ransom of US$ 20 million or around Rp 296 billion so as not to leak BSI customer data, BSI increased customer service hours during the mobile banking recovery period, BSI stated that all banking services had gradually returned to normal and recovered since Thursday, May 11, 2023 and BSI assured customers that their funds were guaranteed safe (Prakarsa, 2024)

In general, there are four factors that cause operational risk, namely human factors, IT system factors, internal process failure factors, and external event factors. One opinion states that human factors are related to bank employees, where operational risks can occur either intentionally or unintentionally, and are not limited to certain units. Although the Islamic financial industry is growing rapidly, this is not balanced by the availability of human resources (HR) who have competence in the sharia field. Based on data from several economic experts, around 25-30 percent of HR in Islamic financial institutions have a background in sharia competence. According to the Association of Islamic Economists (IAEI), the number of HR who have competence in the field of Islamic economics is still very limited, so most of them come from conventional study programs (Ardian, 2022)

The causes of this risk can be divided into several factors. First, the human factor, namely the risk arising from violations committed by employees, such as negligence or carelessness, for example a signature forged by employees. Second, the risk caused by process errors such as data input errors by employees. Third, the risk that occurs due to system disruptions, such as computers that are damaged or hang. Finally, external factors that can cause losses to the company, such as natural disasters such as floods or earthquakes. Non-compliance with operational risk management can have a negative impact on employees, customers, and the company itself (Nengsih & Meidani, 2021)

In an effort to reduce operational risk, the Bank has improved the quality of its human resources through ongoing education and training programs, with the aim of improving employees' ability to carry out their duties more effectively. In addition, the Bank has also evaluated and revised existing policies and procedures, checked access levels and transaction limits according to the duties and responsibilities of each employee, developed information technology, and implemented an internal control system. To maintain business continuity in the face of undesired events, the Bank has a Business Continuity Management (BCM) system and an off-site backup location used during BCM testing. In terms of disaster management, the Bank has a data center and disaster recovery center located in two different locations in the country that allow critical systems including core systems, payments, and regulatory reporting to continue running even in the event of a disaster (Bank, 2019)

The importance of managing risk management in the operational activities of Islamic banking because Islamic banking activities are more complex so they need to be analyzed. This study aims to analyze risk management, namely what are the factors causing operational risk and how is the analysis of the implementation of operational risk management at Bank Syariah Indonesia Cirebon Branch Office

LITERATURE REVIEW AND HYPOTHESIS FORMULATION

Risk Management.

Management is the process of planning, organizing, implementing and controlling tasks in using the resources owned by the organization to achieve company goals. In addition, management is a scientific discipline that oversees the process of cooperation between people or groups, which involves managing human resources or other resources effectively and efficiently to achieve certain goals. Organizations as a container for management activities to achieve the expected goals, in essence every organization needs to regulate or manage existing resources (Mulyani & Jamilah, 2022).

Risk in the context of banking is a potential event, either predictable or unpredictable, that has a negative impact on the bank's income and capital. In order to establish a risk management process, at the initial stage the bank must accurately identify risks by recognizing and understanding all existing and potential risks arising from a new bank business, including risks originating from other affiliated companies (Ilyas, 2019).

Rational risk management is an indispensable component of effective corporate management in a credit organization. In International Convergence of Capital Measurement and Capital Standards, the Basel Committee on Banking Supervision defines operational risk as a risk of losses as a result of inadequate or ineffective internal processes, the actions of people or technical systems, or external events (Chumakova et al, 2025).

Risk in the view of Islam, in the effort to earn a living a Muslim is faced with uncertainty about what will happen. Humans can plan business activities or investments, but cannot be sure of the results, whether they will make a profit or actually experience a loss. As explained in the Qur'an, letter Luqman verse 34 Meaning: *"Indeed, Allah alone has knowledge about the Day of Judgment; and it is He who sends down rain, and know what is in the womb. And no one is can know (with certainty) what he will try tomorrow. And no one can know where on earth he will be dead. Indeed, Allah is All-Knowing, All-Knowing*" (QS. Lukman (31):34).

Risk is an element of life in this world. Most people are worried that uncertainty will result in losses because they believe that the future is unpredictable. However, uncertainty about future events can also have a positive impact if the results are beneficial. On the other hand, only Allah SWT knows the future of humans, therefore every Muslim is required to try hard to face these conditions.

Every job done by humans will be held accountable to Allah SWT, where each individual will be returned to him. In addition, humans must not act carelessly and must carry out their duties with full ihsan, namely by carrying out work optimally and maximally (Ardian, 2022)

In the Islamic perspective, risk management is an effort to maintain the trust of Allah SWT over wealth for the benefit of humanity. This activity is carried out by trying to manage the trust of Allah SWT over wealth for the good of the company. Various verses in the Qur'an emphasize the importance of managing this risk. The success of a company in managing risk can have a positive effect on improving the company's performance. Thus, improving the performance of a company that is well managed through risk management can be understood as a form of the company's success in maintaining the trust of Allah SWT (Agustin & Hasan, 2022).

The implementation of risk management can increase shareholder value, provide a better picture to bank managers regarding the possibility of future losses, improve systematic decision-making techniques and procedures based on the availability of information, which is the basis for more accurate performance measurement, and build a strong risk management infrastructure to increase bank competitiveness (Suhaimi, 2021).

Operational Risk.

Operational risk is the risk that arises due to inadequacy or failure in internal processes, human error, system failure, or external events that affect the bank's operations. In other words, operational risk can prevent the bank from carrying out normal operational activities, such as those caused by natural disasters, fires, or other factors, such as attacks from hackers who successfully access and damage data in the bank's data center. There are three main factors that can cause operational risk, namely infrastructure (including technology, policies, environment, security, disputes, and so on), processes, and resources (Syafii & Siregar, 2020).

Operational risk management refers to the risk of loss caused by inadequate internal processes, human error process failures, system failures, and external events that affect bank operations. Therefore, risk control must provide sufficient and effective assurance of smooth operations and produce reliable reporting. These sources of risk can cause events that have a negative impact on bank operations, so that the emergence of various types of operational risk events is an indicator of success or failure in operational risk management. These types of operational risks can be grouped into several categories, namely: internal fraud, external fraud, employment issues, work environment safety, customers, products, and business practices, damage to physical assets, disruptions in business activities, system failures, and errors in processes or operational activities (Jarir, 2017)

Operational risk is the risk that arises due to inadequacy or failure in internal processes, human error, system failure, or external events that affect the bank's operations. In other words, operational risk can prevent the bank from carrying out normal operational activities, such as those caused by natural disasters, fires, or other factors, such as attacks by hackers who successfully access and damage data in the bank's data center. There are three main factors that can cause operational risk, namely infrastructure (including technology, policies, environment, security, disputes, and so on), processes, and resources. (Syafii & Siregar, 2020)

The main objective of operational risk management is to reduce the potential negative impacts of internal process failures, human errors, system failures, and external events. External events that can affect bank operations include cooperation with other parties. Banks are obliged to apply the principle of prudence in carrying out their operations, so that there are no losses due to negligence. This principle of prudence is applied because the function of banks as intermediary institutions, which collect and distribute funds, involves various risks that can threaten the continuity of the bank's business. Therefore, risk management is needed as a step to apply the principle of prudence in bank operations (Murwadji, 2018).

Operational risk can cause direct or indirect financial losses, as well as potential losses. Direct financial losses occur when Islamic banks lose money, such as due to theft by employees, either systematically or physically. Indirect losses can occur if Islamic banks make mistakes in bookkeeping or claim costs due to information technology errors. Meanwhile, potential losses are losses that arise due to the loss of opportunities to make a profit. In addition, operational risks can also cause losses that cannot be measured in money, such as due to operational failures that lead to a decline or loss of the reputation of Islamic banks. (Sarwoto, et.al.,2020).

Every bank is required to carry out the process of identification, measurement, monitoring, and control of all material risk factors. Risk factors refer to various parameters that affect risk exposure, while material risk factors have a significant impact on the bank's financial condition. The process of identification, measurement, monitoring, and control of risk must be supported by a timely risk management information system, as well as accurate and informative reports on the bank's financial condition, functional activity performance, and risk exposure. Risk measurement needs to be adjusted to the characteristics and complexity of the bank's business activities. To ensure accuracy, banks must have an independent unit that monitors the results of risk measurements carried out by the party implementing the transaction, monitors the level and trend of risk, and analyzes the direction of risk development. Effective implementation of risk management requires risk control that takes into account the results of risk measurement and monitoring that have been carried out. (Rustam, 2024).

Operational risk of Islamic banks is inherent in every activity of Islamic banks such as financing, funding and other transactions, both investment, buying and selling and services. Operational risk is caused by: 1) Human Resources; This risk arises when employees are less aware of the existence of risks that can occur. 2) Internal Process Failure; This risk arises due to ineffectiveness and inefficiency in operations. Ineffectiveness means that there are factors that can thwart the achievement of goals, while inefficiency refers to achieving goals that require more costs than they should. 3) IT Systems; Technology systems make a big contribution to an organization, but on the other hand, these systems can also create new risks. The company's dependence on computer systems, for example, increases the risk of computer damage. 4) External events; Operational risks caused by external factors cannot be controlled by Islamic banks, because the frequency of occurrence is difficult to predict and the possibility of the occurrence of the event cannot be ascertained, especially if triggered by natural factors.

RESEARCH METHODS

This study uses a qualitative method approach. This type of research uses field research which is considered the broadest approach to be used as a method in order to collect qualitative data. In this study, the researcher will conduct field research at Bank Syariah Indonesia Cirebon Dr. Cipto Branch Office, where the researcher will conduct direct research in the field which will then be concluded from the results of the study. The purpose of this qualitative research using field research is to provide a systematic, factual and accurate description of the Operational Risk Management Analysis at Bank Syariah Indonesia Cirebon.

The data sources that will be used in this study are primary data sources and secondary data sources. The data sources that will be used in this study are primary data sources and secondary data sources. The primary data source in this study is data obtained from direct interviews with related parties concerned at the research location. Secondary data sources are obtained from data related to the study including operational risk management data, books related to operational risk management, journals, and other data that can help researchers to obtain relevant data

Data collection techniques in this study conducted interviews with informants in the risk management unit at Bank Syariah Indonesia Kc. Cirebon is Micro-Financing Risk Office and Risk Officer Financing Consume. Micro-Financing Risk Office Has the task of identifying, assessing and managing risks related to the provision of financing to micro customers. Risk Officer Financing Consume. Has the task of identifying, assessing and managing risks related to the provision of credit to individuals and has a very crucial role in ensuring the sustainability and health of the consumer credit portfolio in a financial institution

Its main task is to ensure that the financing portfolio remains healthy. The data analysis process in this study uses three simultaneous activity flows, namely Data Reduction, Data Presentation, Decision Making and Verification. Data validity techniques used are Credibility Test, Dependability Test, Confirmability Test. Research location at Bank Syariah Indonesia Cirebon branch office Dr Cipto.

RESULTS AND DISCUSSION

Factors Causing Operational Risk at Bank Syariah Indonesia Cirebon Branch Office.

The risks that occur in Islamic banking consist of several risks, namely operational risk, reputation risk, legal risk and financial risk. Operational risk is generally caused by human factors, internal processes, IT systems, and external events. Internal and external factors can be related to humans and other factors, namely natural disasters, such as earthquakes, volcanic eruptions, tsunamis and others that cause bank activities not to run properly.

There are four factors that cause operational risk, namely Human Resources (HR) factors, IT system factors, internal process failure factors, and external event factors.

a. Human Resources (HR) Factors;

Operational risks caused by Human Resources (HR) can occur due to deliberate elements motivated by fraudulent actions or the opportunity to trick the system. The opportunity to cheat is driven by urgent life needs and ultimately justifies any means. Mitigation of operational risks caused by Human Resources (HR) is controlling, dual control in the sense of direct supervision of two levels above, for example customer service to the branch operation service manager, all operational activities must be strictly supervised by the branch manager, such as customer fund withdrawals must come in person. If authorized to someone else, cash withdrawals at the teller must be verified with the customer concerned. Other risk mitigation is routine coaching once a month with the branch operation service manager and attended by the branch office internal audit, there is also BCM (Business Continuity Management) which is a procedure created by Bank Syariah Indonesia to ensure that bank operations continue to run every month, by visiting the branch. This is intended to improve the operational risks that arise, violations if they violate the provisions are immediately prevented. At the time of prevention, there must be an exit meeting to find a solution so that it does not happen again.

other operational risks caused by human error, for example, errors in bookkeeping reporting. This operational risk will affect banking operations. If there are errors in bookkeeping or reporting, revisions are made through monthly audits to check and correct errors. Other mitigation efforts include training, one of which is excellent service training and improving employee skills related to the principles of Islamic banking, which is carried out periodically.

Operational risks caused by Human Resources at Bank Syariah Indonesia Cirebon Branch mainly originate from technical errors and deliberate actions. The mitigation implemented emphasizes supervision, coaching, training, and implementation of strict procedures to prevent and correct emerging risks. Management of these risks is very important to maintain smooth operations and customer trust in the bank.

This is in line with previous research conducted by (Anita et al., 2023) showing that Human Resource Risk, or often referred to as People Risk, is usually related to employees. This risk arises when employees lack awareness of the existence of risks that can occur. Unhealthy competition in the workplace becomes a problem if employees do not have adequate skills and knowledge to carry out their duties properly. Other problems include lack of honesty, unauthorized taking of company assets, and organizational culture that can unknowingly trigger negative behavior from employees.

b. Internal Process Factors;

Operational risks caused by internal processes include fraud such as unauthorized withdrawal of customer funds, transactions carried out without the presence of customers, accepting bribes in marketing activities, and processing fictitious financing. This operational risk can occur due to internal processes that involve various transactions in banking, such as teller transactions, customer service, and financing, where internal actors have full access to the process. Mitigation of operational risks caused by internal processes routinely reminds all employees of the potential risk of fraud that occurs not only in Cirebon, but also globally in the banking industry. Every morning briefing, information sharing is carried out regarding fraud cases that have occurred, as well as inspections with the audit team which are carried out every month at branch offices. In addition, it is important to monitor employee lifestyles to identify potential risks that arise. The steps to improve operational risks caused by internal processes are changes from within the employees themselves, although coaching, direction, and strict internal and external supervision have been carried out, significant changes can only be achieved if employees have personal awareness. If an employee cannot control his/her consumer behavior even though he/she has received guidance and supervision, then the changes will not occur optimally.

Operational risks caused by internal processes at Bank Syariah Indonesia Cirebon Branch involve fraud, system problems, and lack of understanding of regulations. Mitigation efforts are focused on improving supervision through audits and briefings, developing regulatory understanding, and monitoring employee lifestyles. However, the main factor that determines the success of mitigation is the personal awareness of employees to comply with procedures and avoid fraudulent actions. Infrastructure improvements and soft skills development are also important parts of preventing operational risks. That this risk arises due to ineffectiveness and inefficiency in operations. Ineffectiveness means that there are factors that can thwart the achievement of goals, while inefficiency refers to achieving goals that require more costs than they should. In general, process risks are closely related to transaction activities, including sales, pricing, documentation, confirmation, and fulfillment of obligations. This type of risk can potentially cause losses in financial aspects, customer satisfaction, and company reputation (Anita et al., 2023)

c. IT System Factors;

IT system factors are frequent computer downtime or errors that can result in input errors that can hinder the process of inputting customer data into the system. The rapid growth and breadth of bank operational activities with various innovative products have been supported by advances in technology and systems. Often this support has actually caused banks to become dependent on technology and information systems (Baroroh & Faizin, 2023).

Operational risks caused by IT systems can arise due to lack of system and device updates, such as PCs that have not been updated or devices that do not meet standards. This can increase the potential vulnerability to threats or disruptions that can ultimately pose a risk to bank operations. These risks are often caused by IT systems that are not updated regularly and devices that do not support or do not meet security standards. Efforts to reduce the potential for operational risks, mitigation carried out by Bank Syariah Indonesia Cirebon Branch Office include securing the system by strengthening network security and routinely updating software. As a remedial measure, Bank Syariah Indonesia Cirebon Branch continues to periodically update its IT system and strengthen its internal network to increase resilience to security threats and ensure that bank operations run smoothly and safely.

Operational risks caused by IT systems at Bank Syariah Indonesia Cirebon Branch Office are mainly caused by technical weaknesses in system security, lack of device updates, and cyber attacks. Risk mitigation focuses on improving network security, routine system and antivirus updates, and monitoring connected devices. These steps are designed to improve the resilience of IT systems, ensure smooth bank operations, and protect customer data and the integrity of the banking system.

This is in line with the theoretical basis that technology systems provide a great contribution to an organization, but on the other hand, these systems can also create new risks. A company's dependence on computer systems, for example, increases the risk of computer damage. Examples of such risks include data corruption, programming errors, weaknesses in security systems, the use of untested technology, and excessive reliance on certain models in business decision making (Sudarmanto et al., 2021).

d. External Event Factors;

External event factors are events or conditions beyond the direct control of an organization that can negatively impact its operational activities. These events are often unpredictable and can cause significant disruption to the business. (Baroroh & Faizin, 2023).

Operational risks caused by external events include those related to ATM hacking, which is generally done through external techniques such as card phishing. This incident involves actions by external parties who take customer funds without consent and can cause losses for the bank and customers. In addition, operational risks caused by external events can occur due to other factors such as demonstrations or riots that can disrupt the smooth running of banking activities and endanger employee safety. Natural disasters such as earthquakes, tsunamis, floods, and fires can also be threats that disrupt operations and safety.

Mitigation measures against external event risks at Bank Syariah Indonesia Cirebon Branch Office through several preventive measures, such as each ATM machine is equipped with CCTV which must be active at all times, ATM officers routinely check the ATM machines to ensure that there are no suspicious additional devices installed by irresponsible parties. On the other hand, to increase customer awareness, Bank Syariah Indonesia also actively conveys information about potential security threats through social media. In an effort to improve and reduce operational risks due to external events, Bank Syariah Indonesia Cirebon Branch Office focuses on strengthening the security system, both in terms of technology and operational procedures so that potential external risks can be minimized and banking activities continue to run safely and smoothly

Implementation of Operational Risk Management at Bank Syariah Indonesia Cirebon Branch Office;

The implementation of operational risk management analysis at Bank Syariah Indonesia Cirebon Branch, especially by identifying detailed analysis of the strengths, weaknesses, opportunities, and threats faced by a branch can help identify risk-prone areas and areas that are potentially missed in the initial analysis to help identify potential risks. Risk measurement regularly monitors changes in risk and simulates various scenarios to determine key indicators to measure the potential impact of various risk events. Risk monitoring regularly monitors identified results and produces periodic risk reports for management. These reports contain information about identified risks, their severity, and actions taken. Finally, risk control provides regular training to employees to improve risk awareness and risk management capabilities, uses reliable information systems to support business processes and risk management, and develops a robust system to prevent and detect errors.

Risk analysis at Bank Syariah Indonesia Cirebon Branch Office is carried out by considering the existing risks and the level of control applied. The identified risks are divided into medium and high risk categories. High risks that can harm the bank's finances must be addressed immediately with a primary focus on preventing fictitious financing. Risk assessment at Bank Syariah Indonesia Cirebon Branch Office shows positive results with a relatively low level of fraud incidents each year. It is hoped that this situation will continue to be maintained. The solutions implemented to manage risk at Bank Syariah Indonesia Cirebon Branch Office include improving employee capabilities, periodic supervision, and complete and accurate verification and monitoring. Document verification is also carried out strictly to ensure that the documents received are in accordance with the originals. Risk monitoring at Bank Syariah Indonesia Cirebon Branch Office is carried out routinely by the RBC (Risk Business Control) unit which is carried out every month. This monitoring not only covers operational aspects, but also financing where all documents will be thoroughly checked by internal audit.

The implementation of operational risk management analysis at Bank Syariah Indonesia Cirebon Branch is quite good by carrying out four main steps, namely risk identification, risk measurement, risk monitoring, and risk control.

Bank Syariah Indonesia Cirebon Branch has a fairly good risk management system, especially in terms of risk identification, analysis, assessment, resolution and monitoring.

1. Bank Syariah Indonesia Cirebon Branch has identified various types of risks, both external risks (e.g. fraud) and internal risks (e.g. procedural errors). The focus is on risks that can cause financial losses, especially those related to financing.
2. Risk analysis is carried out carefully and takes into account the frequency of risk occurrence and its potential impact. Things that are considered high risk must be handled based on priority.
3. Risk assessments are conducted periodically to ensure that risks are managed. This assessment is based on the urgency of the risk and its potential impact on the company.
4. Bank Syariah Indonesia Cirebon Branch has implemented various risk management solutions including: Improving employee competency, stricter supervision and more detailed document review.
5. Risk monitoring is carried out continuously by the Risk Business Control (RBC) department which covers various levels of the organization from branch offices to head office.

Bank Syariah Indonesia Cirebon Branch takes a comprehensive risk management approach. Starting from identification to monitoring, prevention efforts are a top priority including risks and business areas that have clear risk mechanisms so that risks that cannot be handled at the branch level are immediately handled at a higher level. Bank Syariah Indonesia Cirebon Branch shows a strong commitment to operational risk management. However, there is still room for improvement, especially in terms of risk measurement and the use of technology. Through continuous improvement and innovation, Bank Syariah Indonesia Cirebon Branch is able to strengthen business resilience.

CONCLUSION

There are four factors that cause operational risk, namely Human Resources (HR) factors such as deliberate actions, fraudulent actions and opportunities to trick the system. Other factors are internal process factors, namely failures in internal processes such as fraud and ineffective procedures in operational risk management, internal weaknesses, lack of supervision, and incompatibility between infrastructure and operational needs. Furthermore, IT system factors occur due to cyber attacks such as ransomware and lack of system updates. Finally, external incident factors that endanger operations mainly come from cyber attacks, ATM hacking, phishing, and ransomware attacks. Natural disasters such as earthquakes, tsunamis, floods, and fires

Implementation of operational risk management analysis at Bank Syariah Indonesia Cirebon Branch by in-depth identification of the strengths, weaknesses, opportunities and threats faced by the branch. Risks are measured routinely to monitor changes that occur, and simulations of various scenarios are carried out to determine the main indicators of various risk events. Risk monitoring is carried out periodically to monitor the results of identification, prepare risk reports that include the level of severity, and actions that have been taken. In addition, risk control is realized through routine training for employees, which aims to increase awareness of risk and the ability to manage risk. Bank Syariah Indonesia Cirebon Branch communicates the importance of operational risk management to all employees by conducting socialization to unify understanding.

BIBLIOGRAPHY

Anam, H. (2023). Manajemen Risiko Operasional Bank Syariah; Teori dan Manfaat. Jurnal At-Tamwil: Kajian Ekonomi Syariah, 5(1), 16–31

Anita, S. Y., Kustina, K. T., Wiratikusuma, Y., Sudirjo, F., Sari, D., Rupiwardani, I., Nugroho, L., Rakhmawati, I., Harahap, A. K., & Anwar, S. (2023). Manajemen Risiko. Jakarta: Global Eksekutif Teknologi.

Aprilia, Y., Khilmia, A., & Ahmad, Z. I. (2022). Manajemen Risiko Operasional Pada Perbankan Syariah: Bibliometrik. IQTISHADIA Jurnal Ekonomi & Perbankan Syariah, 9(2), 192–203.

Agustin, H., & Hasan, H. (2022). Teori Manajemen Resiko Bank Syariah. *Jurnal Tabarru': Islamic Banking and Finance*, *5*(2), 551–564

Ardian, M. F. (2022). Manajemen Risiko Operasional Pada PT. Bank Syariah Indonesia Area Aceh.

Bank, P. M. R. (2019). Manajemen Risiko.

Baroroh, Z. R., & Faizin, M. (2023). Manajemen Risiko Operasional Produk Pembiayaan KPR dalam Upaya Meminimalisir Kerugian di Bank Syariah. Falahiya: Journal of Islamic Banking and Finance, 2(1), 14–25.

Chumakova, E., Korneev, D., Gasparian, M., Titov, V., & Makhov, I. (2024). Innovative Neural Network Approaches to Operational Risk Management in Financial Institutions. *Journal of Lifestyle and SDGs Review*, *5*(1), e04195. https://doi.org/10.47172/2965-730X.SDGsReview.v5.n01.pe04195

Daya, S., Fau, S., & Damanik, T. P. (2019). Analisis Risiko Operasional Dengan Pendekatan Metode Erm Pada JNE Telukdalam. Program Studi Manajemen Sekolah Tinggi Ilmu Ekonomi Nias Selatan Telukdalam.

Murwadji, T. (2018). Penerapan Manajemen Risiko Operasional Perbankan Di Koperasi Guna Meningkatkan Citra Koperasi di Masyarakat. Jurnal Hukum Positum, 3(1), 19–36

Nelly, R., Siregar, S., & Sugianto, S. (2022). Analisis Manajemen Risiko Pada Bank Syariah: Tinjauan Literatur. Reslaj: Religion Education Social Laa Roiba Journal, 4(4), 918–930.

Nengsih, I., & Meidani, D. (2021). Strategi Manajemen Menghadapi Risiko Operasional Pada Pt Bank Pembiayaan Rakyat Syariah (Bprs) Haji Miskin Pandai Sikek. Jurnal Manajemen Dan Profesional, 2(1), 12–31.

Prakarsa, Z. E. (2024). MANAJEMEN RISIKO OPERASIONAL PADA BANK SYARIAH INDONESIA (BSI) KC BENGKULU S PARMAN I.

Sapiri, M. (2025). Understanding Financial Risk Dynamics: A Qualitative Inquiry into Credit, Market, and Operational Risks in Banking, Investment, and Corporate Sectors. *Golden Ratio of Data in Summary*, *5*(2), 182–192. https://doi.org/10.52970/grdis.v5i2.719

Sarwoto, S., Siregar, S., & Sugianto, S. (2020). Studi Literatur Analisis Risiko Operasional Pada Perbankan Syariah. 1(1), 558–560.

Sudarmanto, E., Astuti, A., Kato, I., Basmar, E., Simarmata, H. M. P., Yuniningsih, Y., Irdawati, I., Wisnujati, N. S., & Siagian, V. (2021). Manajemen Risiko Perbankan.

Suhaimi, A. (2021). Studi Manajeman risiko Pada Bank Syariah Indonesia (BSI). Jurnal Manajemen Risiko, 2(1), 73–78.