Business Review and Case Studies, Vol. 6 No. 3, December 2025
Permalink/DOI: http://dx.doi.org/10.17358/brcs.6.3.459
Available online at http://journal.ipb.ac.id/index.php/brcs
EISSN: 2721-6926

IDENTIFICATION OF OPERATIONAL RISKS IN PARTNER DATA PROCESSING AT PT BANK SYARIAH XYZ

Dwi Okta Priandi[1], Siti Jahroh, Nur Hasanah

School of Business, IPB University
Jl. Raya Padjajaran, 16151, Bogor, Indonesia

Article history:

Received
26 August 2025

Revised
29 November 2025

Accepted
17 December 2025

Available online
31 December 2025

ABSTRACT

Background: PT Bank Syariah XYZ has experienced a data breach incident in 2023. In response to the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), which came into effect in 2024, the bank sought to implement these provisions in its operations. The implementation of risk management is crucial for minimizing potential financial losses and ensuring business continuity during the implementation process.
Purpose: This study aimed to identify risk factors and sources, analyze their potential impacts, and propose control measures using the Failure Mode and Effect Analysis (FMEA) method.
Design/methodology/approach: The research was conducted from March to June 2025 and involved eight respondents directly responsible for third-party data management. The approach used was descriptive, qualitative, and quantitative, with data collection through interviews, questionnaire surveys, and group discussions. A quantitative analysis was performed using the FMEA method, focusing on three main stages of data management: collection, processing, and storage. The scope of this study covered operational aspects such as internal processes, human resources, technology, external events, and governance.
Findings/Result: Of the 18 risks identified, seven were classified as priority risks. In the data collection stage, the partner has not yet appointed a Person in Charge of Data Protection (PIC PDP) nor implemented the provisions stipulated in the PDP Law (RR07). Risks included the use of a single email account (RR05) and a low understanding of the PDP Law by third parties (RR08). In the processing stage, the main risks were related to the length of the analysis time (RR11) and the inaccuracy of the partner data (RR09). Meanwhile, in the storage stage, the dominant risks included cyberattacks on devices (RR17) and data decentralization (RR16). Most priority risks originate from technological aspects (43%), followed by external events (29%).
Conclusion: The results of the study show that PT Bank Syariah XYZ faces significant challenges in managing the risks of implementing the PDP Law, particularly in relation to partner data processing.
Originality/value (State of the art): This study makes an original contribution by integrating the FMEA framework in the context of the implementation of the PDP Law in the Indonesian Islamic banking industry, and provides a basis for strengthening risk management and personal data security in the financial services sector.

Keywords: FMEA, risk management, Personal Data Protection Law (PDP Law), priority risks, financial services

How to Cite:
Priandi, D. O., Jahroh, S., & Hasanah, N. (2025). Identification of operational risks in partner data processing at PT Bank Syariah XYZ. Business Review and Case Studies, 6(3), 459. https://doi.org/10.17358/brcs.6.3.459

[1] Corresponding author:
Email: dokta13798@gmail.com

INTRODUCTION

The rapid development of information technology (IT) has become a double-edged sword. On the one hand, it provides significant convenience and efficiency in human activities, but on the other hand, it opens new avenues for crime and unlawful acts (Saly & Sulthanah, 2023). According to Ardiansyah (2023), this technological advancement introduces emerging challenges and risks, particularly in cyber security. In Indonesia, cyber security has become a critical issue, as cyber threats often lead to violations and the misuse of personal data (Saly & Sulthanah, 2023). One of the most severe consequences of these threats is data breach.

Data breaches pose a serious risk to organizations, arising from both internal and external sources, whether intentional or unintentional (Cheng et al. 2017). The McAfee Report (2015) revealed that 57% of data leaks originate from external factors, while 43% are caused by internal factors, based on studies conducted across organizations in the Asia-Pacific region, the United Kingdom, and North America. Similar incidents have occurred in Indonesia's banking sector. For instance, Putri et al. (2023) reported that PT Bank Syariah XYZ experienced a customer data leak in 2023, which has the potential to result in identity theft, fraud, and financial exploitation, ultimately damaging the institution's reputation. The cyberattack of May 2023 further disrupted digital banking services, eroded customer trust, and threatened long-term operational stability (Cheng et al. 2017). This highlights the urgent need for comprehensive personal data protection policies.

As part of mitigation efforts, the Indonesian government enacted Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). Prior to its enactment, the regulatory framework governing personal data protection in Indonesia was fragmented and lacked a comprehensive integration. This law represents a significant milestone in establishing a unified and systematic legal foundation for data governance. According to Cahyani & Marianata (2024), the primary objective of the PDP Law is to provide legal protection for individuals in the management of their personal data by both public and private entities. Furthermore, the law emphasizes accountability, transparency, and compliance as key principles for strengthening trust and safeguarding digital ecosystem integrity in Indonesia.

Nevertheless, the implementation of the PDP Law at the organizational level presents several challenges, particularly in operational practice. Data leaks may stem from internal process failures, human negligence, weak technological safeguards, or inadequate supervision (Cheng et al. 2017). In the banking industry, where operational systems are inherently complex, such risks may emerge from human resources, internal processes, technology, external events, or governance factors (Cooper et al. 2010; Nurapiah, 2019). As defined by Nurapiah (2019), operational risk refers to the potential for loss arising from internal process failures, human errors, technological disruptions, or external events that may threaten a bank's operational stability.

Currently, PT Bank Syariah XYZ's risk management is guided by Financial Services Authority Regulation Number 65/POJK.03/2016 concerning the Implementation of Risk Management for Sharia Commercial Banks and Sharia Business Units. Risk measurements are generally performed by considering the frequency and impact of events. In this study, the Failure Mode and Effect Analysis (FMEA) method was used to assess risk based on three main indicators, namely severity, occurrence, and detection. Although the FMEA method is widely used in the manufacturing sector (Huang et al. 2020), it has also been adapted to various other fields such as health (Kumru & Kumru, 2013), mining (Dinmohammadi & Shafiee, 2013; Balaraju et al. 2019), logistics (Rosih et al. 2015), food (Wahyuni et al. 2025), and services (Mahacintya et al. 2025; Rahmah et al. 2025).

Robust personal data protection regulations are important in the context of personal data protection research, and several countries have issued such regulations. For example, in the European Union, the General Data Protection Regulation (GDPR) requires all entities handling the data of European citizens to comply with the protection principles within a clear legal framework (Gashi & Peci, 2020). The urgency of personal data protection is to safeguard consumer data and market conditions, which requires effective risk management (Dewi, 2017; Shetty, 2023; Azmi et al. 2024). However, research using FMEA to assess personal data protection risks is still limited, especially in the service sector, which accounts for only approximately 4% of total FMEA studies (Huang et al. 2020).

Although FMEA has been extensively applied in manufacturing and industrial settings (Huang et al. 2020), its utilization in the service sector, especially for assessing the risks of personal data protection, is still very limited. Previous studies have generally focused on the analysis of physical process failures in the fields of health, mining, and logistics, whereas this study adapts FMEA to analyze digital and procedural risks related to personal data management. The novelty of this study lies in the FMEA method for assessing operational risks in the context of personal data protection in the Islamic banking sector.

This study used an exploratory qualitative approach with observations and interviews. The problem-solving approach in this study begins by identifying sources of operational risk in partner data processing at PT Bank Syariah XYZ. Each process involving partner data is analyzed to identify potential failures that could lead to violations of the PDP Law principles. Furthermore, the Failure Mode and Effect Analysis (FMEA) method was used to systematically assess each risk based on three main indicators: severity, occurrence, and detection. The assessment results were used to calculate the Risk Priority Number (RPN) of each identified failure, so that high-priority risks could be identified and controlled.

Therefore, this study aims to fill this gap by analyzing the implementation of the Personal Data Protection Law within the framework of operational risk management in the financial services sector, particularly at PT Bank Syariah XYZ. The objectives of this study were to identify risk factors, analyze risk levels, and determine priority risks in the implementation of the PDP Law, with a focus on third-party data management. This study used an exploratory qualitative approach through observation and interviews, with a scope covering three main stages of data management: collection, processing, and storage. Operational risks are examined from various perspectives, including internal process failures, human resource limitations, technology issues, external events, and governance.

METHODS

This research was conducted at the Head Office of PT Bank Syariah XYZ, located at The Tower Building, Jalan Gatot Subroto No. 27, Karet Semanggi Village, Setiabudi District, South Jakarta. Data collection was conducted from March to June 2025. The primary and secondary data were used in this study. The primary data were obtained through interviews and questionnaires. Secondary data were obtained from company documents and various other sources. The respondents were determined based on an expert assessment within the company.

This study employed a descriptive qualitative and quantitative approach, with data collection conducted through interviews, questionnaire surveys, and discussions with pre-selected respondents. Quantitative calculations were performed using the FMEA (Failure Mode and Effect Analysis) method. The stage of determining the scope, context, and criteria for risk management was carried out through in-depth interviews with internal parties at PT Bank Syariah XYZ, followed by a descriptive analysis. This was done to identify the various operational risks faced by the company and related to the PDP Law. The data generated will be analyzed and reinforced with feedback from internal parties obtained from the interviews. The results explain the identified operational risks. The use of in-depth interviews and descriptive analysis refers to the research on operational risk management conducted by Nurapiah (2019) and Firmansyah (2024).

The sample in this study was determined using a non-probability sampling method with purposive sampling. This technique was chosen because it allows the researcher to involve participants with specific knowledge and experience relevant to the research topic. This approach ensures that the data and information collected are accurate, focused, and contextually meaningful (Palinkas et al. 2015). The respondents were identified based on their understanding of operational activities and risk management practices in partner data processing at PT Bank, Syariah XYZ.

In the risk assessment process, the FMEA method can be used to identify and evaluate potential failures and determine their risk levels (Desy et al. 2014). Rosih et al. (2015) and Bahrami et al. (2012) used the FMEA method in their research to assess and determine priority risk. In the risk assessment stage, the FMEA method was used as follows (McDermott et al. 2008; Mollah, 2005; Subriadi & Najwa, 2020):

1. Determine the severity level by assessing the severity of the impact of a risk on a scale of to 1-5, with criteria ranging from insignificant to fatal.

2. Determine the occurrence level by assessing how likely the cause of failure is to occur on a scale of 1-5, with criteria ranging from very rare to very frequent.
3. The detection level is determined by measuring how well the failures can be controlled or managed. This detection level indicates the ability to detect risks before their impact arises, using a rating scale of 1-5 with criteria ranging from very easy to very difficult.
4. The risk priority level is calculated by multiplying the severity, occurrence, and detection levels (McDermott et al. 2008; Mollah 2005).

   RPN = (Severity rate) × (Occurrence rate) × (Detection rate)

5. The risks are ranked by calculating the critical RPN value, which is the total RPN divided by the number of risks. Risks with an RPN value above the critical value are considered priority and require further risk control. Mahacintya (2024) used this approach to rank the risks. Here's the equation.

   Critical value RPN = (RPN' s Total)/ (Amount of Risks)

This study began by establishing a risk context as the foundation for understanding the operational environment. The next stage involves identifying risk sources within the scope of operational risks, including internal processes, human resources, technology, and governance. This identification process was carried out through in-depth interviews and descriptive analysis to obtain a comprehensive understanding of potential risks. The identified risks were then analyzed using the Failure Mode and Effect Analysis (FMEA) method to determine the priority level of operational risks. Using this method, a Risk Priority Number (RPN) is generated, which serves as the basis for identifying risks that require further control actions, as shown in Figure 1.

RESULTS

Determination of scope, context, and criteria

At this stage, researchers conducted interviews with parties involved in the implementation of the PDP Law at PT Bank Syariah XYZ. This was done to understand the flow of the PDP Law implementation, the scope of risks to be analyzed, and to establish the context and criteria for risk assessment. Operational risks are analyzed based on five factors: internal processes, human resources, technology, external events, and governance. Risk assessment focuses on potential failures that could affect the implementation of the PDP Law, particularly during the collection, processing, and storage of partner data. Risks are measured based on the probability, impact, and extent to which such failures can be detected.

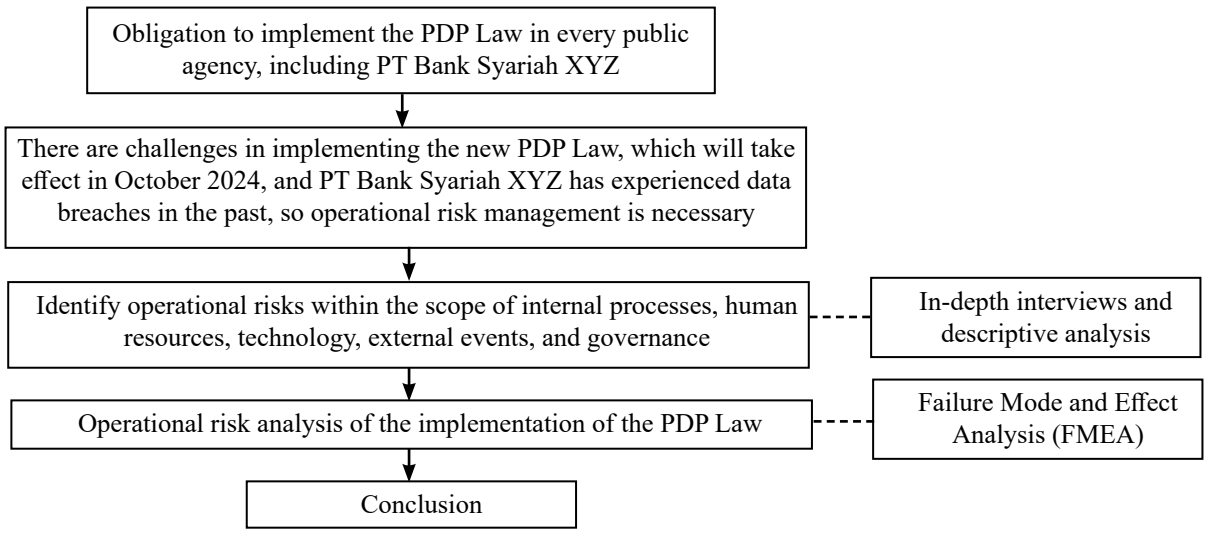

Figure 1. Framework for operational risk analysis of PDP law implementation

Risk Identification Result

Based on the results of the risk identification, impact, causes, and detection controls, 18 risks in partner data processing were identified. During the partner data collection stage, eight potential risks were identified, with codes RR01–RR08. These risks include the risk of partner data being sent to the wrong company email address, physical partner documents being lost or scattered, incomplete partner data, partner data collected exceeding the list of required documents, the collection device still using a single email account, the email device being infected with a virus or cyberattack, partners not yet having a PDP person in charge, not yet implementing the provisions of the PDP Law, and a lack of understanding of the PDP Law regulations, as shown in Table 1.

At the data processing stage, four potential risks were identified and coded as RR09 to RR12. These risks include inaccurate partner data, accreditation proposals that do not comply with the provisions of the Personal Data Protection (PDP) Law, lengthy analysis processes, and the absence of a monitoring mechanism for partner data analysis. Each of these risks has the potential to disrupt data integrity and delay decision-making within an organization. The lack of adequate monitoring mechanisms also increased the likelihood of undetected errors during the evaluation process. A detailed summary of the identified risks is provided in Table 2.

At the partner data storage stage, six potential risks were identified and coded as RR13 to RR18. These risks include improper storage of physical data or documents, difficulties in accessing stored partner data, failures in data storage systems, and lack of centralized data management. In addition, there is a risk of cyberattacks targeting the devices used for data storage as well as non-compliance with internal regulations regarding data classification. Such risks may compromise data security, accessibility, and organizational efficiency, if not properly managed. A detailed overview of the risks is presented in Table 3.

Table 1. Results of risk identification in the data collection stage of partner data processing

Operational scope	Code	Risk
Internal process	RR01	Partner data sent to the wrong company email address
	RR02	Physical documents of partners lost or scattered
People	RR03	Incomplete partner data
	RR04	The partner data collected exceeds the list of required documents
Technology	RR05	The collection device still uses a single email account
External events	RR06	Email device infected with a virus or cyber attack
	RR07	The partner does not yet have a PDP representative and has not yet implemented the provisions of the PDP Law
Governance	RR08	Lack of understanding regarding the provisions of the PDP Law

Table 2. Results of risk identification in the data processing stage of partner data processing

Operational scope	Code	Risk
Internal process	RR09	Partner data is inaccurate
People	RR10	Partner accreditation proposals do not comply with PDP Law provisions
Technology	RR11	The analysis process takes a long time
Governance	RR12	There is no mechanism for monitoring the partner data analysis process

Table 3. Results of risk identification in the data storage stage of partner data processing

Operational scope	Code	Risk
Internal process	RR13	Physical data or documents of partners are not stored properly
People	RR14	Difficulty retrieving stored partner data
Technology	RR15	Data failed to be saved
	RR16	Data is not centralized
External events	RR17	Cyber attacks on devices used
Governance	RR18	Classification of data storage distribution does not comply with internal regulations

The overall results of identification at various stages of partner data collection, processing, and storage indicate that most potential failures originate from the scope of internal processes, human resources, and technology. This suggests that the potential risks in partner data processing come not only from individual or technological weaknesses but also from inefficiencies in the internal processes implemented**.**

Assessment Risk

After obtaining the risk identification results, the next stage is risk assessment using FMEA. This aims to measure the RPN value by multiplying the severity (S), occurrence (O), and detection (D). Through this calculation, each potential risk can be ranked based on its level of criticality and the urgency of the required mitigation efforts. The FMEA approach allows researchers to prioritize risks systematically and focus on the most significant ones that could impact operational stability. A detailed summary of the risk assessment results for the data collection, processing, and storage stages of partner data is presented in Table 4.

Referring to Table 4, the RPN calculation results from each stage were considered to determine the priority risks. Priority risks were determined by comparing the RPN and critical RPN values with the established critical RPN threshold. Risks with RPN values exceeding the critical threshold were categorized as high-priority and demand prompt control measures. This approach ensures that risk management efforts focus on the most significant threats to operational effectiveness and data protection.

Critical RPN Value

After calculating the RPN value for each potential failure in the data collection, processing, and storage processes, the critical RPN value was determined. This value was obtained by dividing the total RPN value by the number of potential failures. The critical RPN value is then used as a risk priority criterion. If the RPN value is above the critical RPN value, it is considered a priority. The following are the RPN values for each stage of partner data processing:

Table 4. Results of risk assessment for the collection, processing, and storage of partner data

Phase	Code		S	O	D	RPN
Data collection	RR01	Partner data sent to the wrong company email address	4.2	1	2	8.4
	RR02	Physical documents of partners lost or scattered	4.2	1.4	2.4	14.11
	RR03	Incomplete partner data	2.6	2.6	1.8	12.17
	RR04	The partner data collected exceeds the list of required documents	2.8	1.2	1.8	6.05
	RR05	The collection device still uses a single email account	3.4	3.4	2.2	25.43
	RR06	Email device infected with a virus or cyber attack	3.8	1.6	2.6	15.81
	RR07	The partner does not yet have a PDP representative and has not yet implemented the provisions of the PDP Law	4.2	2.8	3	35.28
	RR08	Lack of understanding regarding the provisions of the PDP Law	3.8	2.6	2.2	21.74
Data processing	RR09	Partner data is inaccurate	4.0	1.4	2.2	12.32
	RR10	Partner accreditation proposals do not comply with PDP Law provisions	3.6	1.2	1.8	7.78
	RR11	The analysis process takes a long time	2.6	2.2	2.2	12.58
	RR12	There is no mechanism for monitoring the partner data analysis process	2.8	1.8	1.8	9.07
Data storage	RR13	Physical data or documents of partners are not stored properly	3.8	1.8	2	13.68
	RR14	Difficulty retrieving stored partner data	2.6	2	2	10.4
	RR15	Data failed to be saved	3.2	1.8	2	11.52
	RR16	Data is not centralized	3.6	2.4	2	17.28
	RR17	Cyber attacks on devices used	4.2	2	2.8	23.52
	RR18	Classification of data storage distribution does not comply with internal regulations	3.4	2	2.2	14.96

Based on Table 5, the identified potential failures that have been assigned RPN values are grouped according to their respective priority levels. The grouping process focuses on risks with RPN values that exceed a predetermined critical RPN threshold. These high-priority risks represent failure modes that have the greatest potential to affect operational continuity and data protection compliance. By categorizing them, an organization can allocate resources more effectively to mitigate the most critical vulnerabilities. This analytical approach also supports the development of targeted and systematic risk control strategies.

Based on Figure 2, there were three potential failures that exceeded the critical RPN value, namely RR07 with an RPN value of 35.28. This potential failure originates from the scope of external events and ranks highest, indicating that the partner does not yet have a PIC PDP and has not implemented the provisions of the PDP Law (RR07). This risk has a moderate probability of occurrence and detection, but has a significant impact. The second and third positions are RR05 with an RPN of 25.43 and RR08 with an RPN of 21.74. RR05 indicates that the use of a single email account in the data collection stage is a priority risk originating from the technological scope. Meanwhile, RR08 originates from the scope of governance, where there is a potential failure to understand PDP provisions. All three potential failures were largely related to compliance with personal data protection regulations. This has an impact on a company's reputation. This is in line with previous research showing that a failure to comply with regulations can cause financial losses and reduce market confidence in the long term (Sreenivasamurthy, 2017).

During data processing, two risks exceeding the critical RPN value were identified: RR11 with an RPN value of 12.58 and RR09 with an RPN value of 12.32, as shown in Figure 3. Both risks are related to the potential for the inaccurate processing of partner data, which requires a long time for data analysis. These potential failures can directly impact the quality and accuracy of decision making. This aligns with the research by Kozioł-Nadolna & Beyer (2021), which highlights that one of the common issues in decision-making is the limitation of information and data.

Furthermore, at the data storage stage (Figure 4), two risks were identified as exceeding the critical RPN value, namely RR17 with an RPN score of 23.53 and RR16 with an RPN score of 17.28. RR17 represents the potential risk of cyberattacks targeting devices used for data storage, whereas RR16 reflects the issue of non-centralized data management. Both risks are critical because they can compromise the confidentiality, integrity, and availability of the stored data. In the banking sector, such vulnerabilities are of particular concern, as cyberattacks, data breaches, and server failures can disrupt operations and erode customer trust (Ali et al. 2022). Therefore, it is essential for organizations to strengthen their cybersecurity infrastructure and implement centralized, well-monitored data storage systems.

Table 5. Critical value of RPN for partner data processing

Processing stage	Critical RPN Values
Data collection	17.37
Data processing	10.44
Data storage	15.23

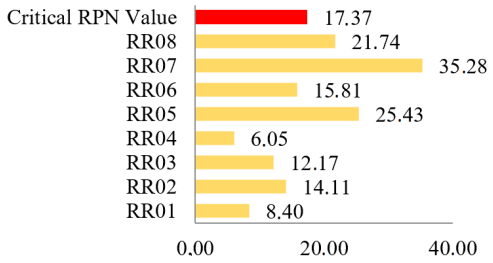

Figure 2. RPN and critical RPN values for the data collection stage in partner data processing

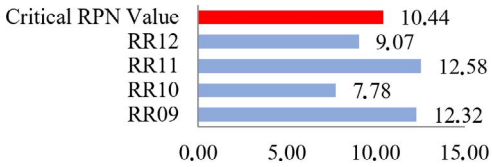

Figure 3. RPN and critical RPN values for the data processing stage in partner data processing

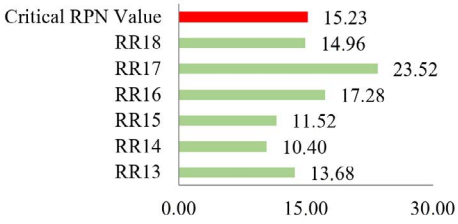

Figure 4. RPN and critical RPN values for the data storage stage in partner data processing

Referring to Table 6, it can be seen that the priority risks identified at each stage require further risk control measures. These risks have the potential to cause significant disruptions in partner data processing activities. Without proper mitigation, such risks may lead to data inaccuracies, process delays, or even violations of data-protection regulations. Therefore, it is essential to implement effective control strategies to minimize the likelihood and impact of these failures. Strengthening internal procedures and monitoring mechanisms will help ensure that data processing remains secure, efficient, and compliant with the applicable regulations.

Based on Figure 5, priority risks mostly come from the scope of technological operations (43%) and external events (29%). This indicates that the use of technology plays an important role in partner data processing. The use of technology is not only a challenge faced by the banking sector, but can also add value to banking practices, both in service delivery and repetitive business processes (Tambunan & Nasution, 2023). Third-party compliance and cyberattack prevention are also important because non-compliance with regulations and cyberattacks can result in financial losses and damage to a company's reputation in the long term (Sreenivasamurthy, 2017; Ali et al. 2022).

Managerial Implication

Based on the results of the risk analysis in the implementation of the Personal Data Protection Law at PT Bank Syariah XYZ, several important implications were identified that require serious management attention. These implications highlight the need for a more integrated and proactive approach to managing the operational risks related to personal data. The analysis shows that risks originating from external events and technology remain the dominant factors affecting data protection compliance.

First, during the partner data collection stage, the company must develop special tools that can accommodate the process of collecting partner data in a secure and comprehensive manner. In addition, this tool is expected to minimize the use of a single email account and avoid potential cyber threats that could target email systems. Furthermore, during the data processing stage, management is encouraged to integrate technological tools that support the automation of the data analysis processes. This effort will not only support the analysis process, but also enhance the accuracy of the data and information generated. Furthermore, decision making can be performed more effectively and efficiently based on accurate data.

During the data-storage phase, management can use a centralized storage system with high security levels. The use of this system can facilitate the company to process partner data in a controlled manner and minimize the risk of data leakage. This system must also be equipped with reliable security protection such as encryption and threat detection. Finally, the human resources aspect also needs to be considered by management. Continuous efforts should be made to conduct training and awareness programs regarding the principles of the Personal Data Protection Law for internal and external business partners. A comprehensive understanding of the rights and obligations related to personal data processing can strengthen compliance and foster a more responsible work culture.

In addition, management can apply the FMEA method as an alternative for assessing banking operational risks. The application of this method enables the early identification of potential failures, determination of the severity and likelihood of risks, and establishment of more effective control strategies. FMEA not only serves as a risk evaluation tool but also as a basis for management in making data-driven decisions to improve the efficiency, compliance, and sustainability of bank operations.

Tabel 6. Priority risk in partner data processing

Phase	Operational scope	Code	RPN
Data collection	External events	RR07	35.28
	Technology	RR05	25.43
	Governance	RR08	21.74
Data processing	Technology	RR11	12.58
	Internal process	RR09	12.32
Data storage	External events	RR17	23.52
	Technology	RR16	17.28

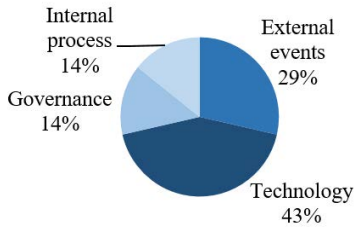

Figure 5. Percentage of priority risk based on operational scope

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

The implementation of the Personal Data Protection Law (PDP Law) at PT Bank Syariah XYZ encounters various risk-related challenges, particularly in the processing of partner data. Based on the results of this study, 18 potential sources of operational failure were identified across the stages of data collection, processing, and storage. Specifically, seven risks are associated with the data collection stage, four risks are identified in the data processing stage, and six risks occur during the data storage stage. These findings indicate that vulnerabilities are distributed throughout all phases of data management, highlighting the complexity of ensuring compliance with PDP Law. Therefore, a structured and continuous risk management approach is essential to minimize potential failures and strengthen data protection practices within the organization.

Additionally, seven priority potential failures that required further control and mitigation measures were identified. From the data collection stage, there were three priority risks: RR07 with an RPN value of 35.28, RR05 with an RPN value of 25.43, and RR08 with an RPN value of 21.74. In the data processing stage, two priority risks were identified: RR11 with an RPN value of 12.58 and RR09 with an RPN value of 12.32. Furthermore, two priority risks were found in the data storage stage, specifically RR17 with an RPN value of 23.52 and RR16 with an RPN value of 17.28. These results indicate that the most critical risks are spread across all data management stages, thus emphasizing the need for comprehensive and stage-specific control strategies.

These results highlight that the use of advanced technology for data security, establishment of robust data governance policies, and adherence to regulatory compliance are critical factors in ensuring the effective implementation of the Personal Data Protection (PDP) Law. A well-structured technological framework not only enhances data protection, but also supports transparency and accountability within organizational processes. Furthermore, the findings confirm that the Failure Mode and Effect Analysis (FMEA) method is both relevant and practically applicable in the financial services sector, particularly in banking institutions. This method provides a systematic approach for identifying, evaluating, and prioritizing operational risks associated with data management. Therefore, integrating FMEA into a bank's risk management framework can strengthen preventive measures and improve the overall resilience of data protection systems.

Recommedations

The implementation of the Personal Data Protection (PDP) Law at PT Bank Syariah XYZ requires a comprehensive and integrated risk-management approach. Appropriate risk control measures should be developed collaboratively through consultations with the risk management unit to ensure alignment with organizational policies and regulatory standards. In this study, risk management analysis was conducted from the perspective of internal company management, focusing on the stages of data collection, processing, and storage. However, this internal scope provides only a partial view of the broader data-protection landscape. Therefore, future research should expand the analysis to include external stakeholders and explore the wider context of PDP Law implementation across the financial services ecosystem.

FUNDING STATEMENT: This research did not receive any specific grants from funding agencies in the public, commercial, or not-for-profit sectors.

CONFLICTS OF INTEREST: The author declares no conflict of interest

DECLARATION OF GENERATIVE AI STATEMENT: During the preparation of this work, the authors used ChatGPT to check grammar and polish the text. After using this tool/service, the authors reviewed and edited the content as required and took (s) full responsibility for the content of the publication.

REFERENCES

Ali S. M., Hoq S. M. N., Bari A. B. M. M., Kabir G., & Paul S. K. (2022). Evaluating factors contributing to the failure of information system in the banking industry. PLOS ONE, 17(3), e0265674. https://doi.org/10.1371/journal.pone.0265674

Ardiansyah W. M. (2023). Peran teknologi dalam transformasi ekonomi dan bisnis di era digital. JMEB Jurnal Manajemen Ekonomi & Bisnis, 1(1), 12. https://doi.org/10.59561/jmeb.v1i01.89

Azmi M. N. A., Saifudin H., Purba C. T., Suryaningtyas

A., & Situmorang U. S. (2024). Analisa kasus kebocoran data pada Bank Indonesia dalam sistem perbankan. Jurnal Multidisiplin Ilmu Akademik, 1(6), 448–458. https://doi.org/10.61722/jmia.v1i6.3267

Bahrami M., Bazzaz D. H., & Sajjadi S. M. (2012). Innovation and improvements in project implementation and management using FMEA technique. Procedia - Social and Behavioral Sciences, 41, 418–425. https://doi.org/10.1016/j.sbspro.2012.04.050

Balaraju J., Raj M. G., & Murthy C. S. (2019). Fuzzy-FMEA risk evaluation approach for LHD machine – A case study. Journal of Sustainable Mining, 18(4), 257–268. https://doi.org/10.1016/j.jsm.2019.07.003

Bank Syariah Indonesia. (2024). Lampiran dokumen standar prosedur pengendalian pelindungan data pribadi. Jakarta: BSI.

Cahyani W. D., & Marianata A. (2024). Analisis kebijakan perlindungan data pribadi di Kota Bengkulu: Studi implementasi UU PDP dalam era digital. Jurnal Kajian Hukum dan Kebijakan Publik, 2(1), 623. https://jurnal.kopusindo.com/index.php/jkhkp

Cheng L., Liu F., & Yao D. (2017). Enterprise data breach: Causes, challenges, prevention, and future directions. WIREs Data Mining and Knowledge Discovery, 7(5), e1211. https://doi.org/10.1002/widm.1211

Cooper T., Faseruk A., & Johnson L. D. (2010). Impact of privacy and confidentiality on valuation: An international perspective. Journal of Financial Management and Analysis, 23(2), 1–10. https://www.proquest.com/scholarly-journals/impact-privacy-confidentiality-on-valuation/docview/861734709/se-2

Desy I., Hidayanto B. C., & Astuti H. M. (2014). Penilaian risiko keamanan informasi menggunakan metode failure mode and effects analysis di divisi TI PT Bank XYZ Surabaya. Seminar Nasional Sistem Informasi Indonesia, 467–472.

Dewi S. (2017). Model regulation for data privacy in the application of biometric smart card. Brawijaya Law Journal, 4(1). https://doi.org/10.21776/ub.blj.2017.004.01.06

Dinmohammadi F., & Shafiee M. (2013). A Fuzzy-FMEA risk assessment approach for offshore wind turbines. International Journal of Prognostics and Health Management, 4(1), 1–10. https://kar.kent.ac.uk/80276/

Firmansyah R. (2024). Penilaian risiko mitra penggilingan padi di PT Agrobisnis Banten Mandiri (PERSERODA) [Tesis]. Institut Pertanian Bogor.

Gashi F., & Peci B. (2020). Protection of personal data and privacy in banking sector in Kosovo and its impact in consumer protection. Perspectives of Law and Public Administration, 9(1). https://oaji.net/articles/2021/7107-1617120478.pdf

Huang J., You J.-X., Liu H.-C., & Song M.-S. (2020). Failure mode and effect analysis improvement: A systematic literature review and future research agenda. Reliability Engineering & System Safety, 199, 106885. https://doi.org/10.1016/j.ress.2020.106885

Kozioł-Nadolna K., & Beyer, K. (2021). Determinants of the decision-making process in organizations. Procedia Computer Science, 192, 2375–2384. https://doi.org/10.1016/j.procs.2021.09.006

Kumru M., & Kumru P. Y. (2013). Fuzzy FMEA application to improve purchasing process in a public hospital. Applied Soft Computing, 13(1), 721–733. https://doi.org/10.1016/j.asoc.2012.08.007

Mahacintya, C. V. (2024). Perancangan manajemen risiko operasional pada administrasi fakultatif reasuransi umum PT XYZ (Master's thesis). Bogor: Graduate School, Bogor Agricultural University.

Mahacintya C. V., Hasanah N., & Ramadyanto W. (2025). Operational risk management design of general reinsurance facultative administration PT. XYZ. Jurnal Aplikasi Bisnis dan Manajemen, 11(1), 265–278. https://doi.org/10.17358/jabm.11.1.265

McAfee LLC. (2015). McAfee report grand theft data: Data exfiltration study: Actors, tactics, and detection. https://www.trellix.com/enterprise/en-us/assets/reports/rp-data-exfiltration.pdf

McDermott R. E., Mikulak R. J., & Beauregard M. R. (2008). The basics of FMEA (2nd ed.). Productivity Press.

Mollah A. H. (2005). Application of failure mode and effect analysis (FMEA) for process risk assessment. BioProcess International. https://www.bioprocessintl.com/process-monitoring-and-controls/application-of-failure-mode-and-effect-analysis-fmea-for-process-risk-assessment

Nurapiah D. (2019). Manajemen risiko operasional

pada perbankan syariah di Indonesia. Ekonomi Syariah dan Bisnis Perbankan, 3(1), 66–73. https://doi.org/10.37726/ee.v3i1.14

Otoritas Jasa Keuangan. (2016). Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 65/ POJK.03/2016 tentang Penerapan Manajemen Risiko Bagi Bank Umum Syariah dan Unit Usaha Syariah. https://jdih.ojk.go.id/

Palinkas L.A., Horwitz S.M., Green C.A., Wisdom J.P., Duan N., & Hoagwood K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. Administration and Policy in Mental Health and Mental Health Services Research 42(5): 533-544. https://doi.org/10.1007/ s10488-013-0528-y

Putri D. F., Andriani S., Sari W. R., & Nabbila F. L. (2023). Analisis perlindungan nasabah BSI terhadap kebocoran data dalam menggunakan digital banking. Jurnal Ilmiah Ekonomi dan Manajemen, 1(4), 173–181. https://doi. org/10.61722/jiem.v1i4.331

Rahmah T. L., Novianti T., & Mulyati H. (2025). International analysis of operational risk management in logistic companies: A case study of PT Sugiarto Jaya Mandiri Transport Bogor. International Journal of Research and Review, 12(1), 140–147. https://doi.org/10.52403/ ijrr.20250117

Rosih A. R., Choiri M., & Yuniarti R. (2015). Analisis risiko operasional pada departemen logistik dengan menggunakan FMEA. Jurnal Rekayasa dan Manajemen Sistem Industri, 3(3), 580–591.

Saly J. N., & Sulthanah L. T. (2023). Pelindungan data pribadi dalam tindakan doxing berdasarkan Undang-Undang Nomor 27 Tahun 2022. Jurnal Kewarganegaraan, 7(2), 1708–1713. https://journal.upy.ac.id/index.php/pkn/article/ download/5413/3214

Sreenivasamurthy G. V. (2017). Corporate ethics and compliance: Building trust and reputation in the market. International Journal of Research and Analytical Reviews, 4(4), 170–175. http://www. ijrar.org/IJRAR19D5067.pdf

Shetty P. (2023). Data privacy and risk management: Collaboration is key on tackling privacy risks/ issues. Journal of Artificial Intelligence & Cloud Computing, 2(4), 1–4. https://doi.org/10.47363/ JAICC/2023(2)224

Subriadi A. P., & Najwa N. F. (2020). The consistency analysis of failure mode and effect analysis (FMEA) in information technology risk assessment. Heliyon, 6(1), e03161. https://doi. org/10.1016/j.heliyon.2020.e03161

Tambunan R., & Nasution M. I. (2022). Tantangan dan strategi perbankan dalam menghadapi perkembangan transformasi digitalisasi di era 4.0. Sci-Tech Journal, 2(2), 148–156. https://doi. org/10.56709/stj.v2i2.75

Wahyuni H. C., Rosid M. A., Azara R., & Voak A. (2025). Blockchain technology design based on food safety and halal risk analysis in the beef supply chain with FMEA–FTA. Journal of Engineering Research, 13, 590–595. https://doi. org/10.1016/j.jer.2024.02.003