Equivalent: Jurnal Ilmiah Sosial Teknik
Volume 8, Issue 2, 713-730
e_ISSN: 2775-0833
https://jurnalequivalent.id/index.php/jequi/index
DOI: doi.org/10.59261/jequi.v8i2.313

Information Technology Risk Management Analysis in the Implementation of Law Number 27 of 2022 Concerning Personal Data Protection at PT XYZ

Ervin Hermawan*
Universitas Bina Nusantara, Indonesia

Nilo Legowo
Universitas Bina Nusantara, Indonesia

***Corresponding author:**
Ervin Hermawan, Universitas Bina Nusantara, Indonesia. ✉ervin.hermawan@binus.ac.id

Article Info:

Article history:
Received: April 8, 2026
Revised: May 20, 2026
Accepted: June 04, 2026

Keywords:
Risk Management; Personal Data Protection; ISO 31000:2018; Mitigation Strategies; IT Security; Compliance.

Abstract

Background: Along with the rapid development of information technology and digitalization, organizations increasingly rely on personal data to support business operations. This reliance also increases the potential risk of data leakage, misuse, and cyberattacks, prompting the Indonesian government to enact Law No. 27 of 2022 on Personal Data Protection (PDP Law).
Objective: This research aims to develop internal policies related to personal data management in accordance with the data protection principles of the PDP Law, as well as to identify and analyze information technology security risks in order to formulate mitigation strategies using the ISO 31000:2018 approach.
Methods: The methodology used is descriptive qualitative, with data collection techniques including document studies, employee surveys from various divisions, and direct observation of the current information technology security infrastructure and procedures.
Results: The results showed that the company lacked a systematic risk management system; the security infrastructure contained critical gaps, including the absence of multi-factor authentication and end-to-end encryption. Quantitative survey data indicated that approximately 67% of employees (114 out of 169 respondents) lacked foundational knowledge of PDP Law principles, and an assessment of cybersecurity controls revealed that 25 out of 153 prescribed controls had not yet been implemented.
Conclusion: Based on these findings, a mitigation strategy was developed in the form of internal policies governing personal data management, strengthening IT security systems through encryption technologies and role-based access control, and conducting regular training to increase employee awareness.

To cite this article: Hermawan, E., & Legowo, N. (2026). Information Technology Risk Management Analysis in the Implementation of Law Number 27 of 2022 Concerning Personal Data Protection at PT XYZ. *Equivalent: Jurnal Ilmiah Sosial Teknik*, 8(2), 713-730. https://doi.org/10.59261/jequi.v8i2.313

INTRODUCTION

Information technology and digitalization have had a significant impact on various aspects of life, including personal data management. Personal data is now an asset for organizations, especially companies operating in the consulting sector such as PT XYZ, a subsidiary of PT Holding XYZ. As a company engaged in engineering consulting, the company manages various types of personal data to support its business and operational processes. According to Mandru (2024), data has become a strategic asset that has a significant impact on operational efficiency and decision-making in business. Proper data management allows companies to increase competitiveness and avoid the risk of information leakage that can be detrimental to the

organization.

One of the main challenges in managing personal data is the risk of data leakage, which can have serious consequences for the sustainability of the organization. Ho et al. (2023) state that, "The two key problems facing an organization after a data breach are (1) financial losses, and (2) customer misgiving (such as brand equity loss, customer turnover)" (p. 2). This confirms that the impact of data leaks is not only technical but also strategic, including economic losses and loss of customer trust that are difficult to recover. In many cases, companies are required to pay the cost of forensic audits and compensation to customers and also suffer reputational losses that may lead to suspension of service usage by those customers. For example, in Indonesia, Law Number 27 of 2022 related to Personal Data Protection requires that data controllers must notify data subjects in case of a breach of personal data (Article 39). Organizational preparedness in responding to incidents is critical, and this provision highlights that fact.

The rapid development of digital technology has profoundly transformed the information management ecosystem. While digitalization brings substantial operational benefits, it has simultaneously generated significant threats to personal data security, particularly through cyberattacks such as data theft, ransomware deployment, and privacy breaches. These growing threats underscore the imperative for robust legal frameworks to safeguard personal data at both the organizational and national levels.

Data and Information Security in the Digital Age is not just a technical product but an ongoing, multidimensional process. As Schneier (Bronk, 2026; Ho et al., 2023; Schneier, 2015) argues, security must be understood as a continuous process rather than a static product, and the protection of data and information systems must therefore be approached in an integrated manner, encompassing technological safeguards, organizational policy, and human resource preparedness.

While cybersecurity protection technologies and software have grown increasingly sophisticated, the human element continues to represent the most critical and challenging vulnerability to manage. As Zwilling et al. (2022) demonstrate, human error remains the weakest link in the cybersecurity chain (Alrusaini, 2026). This principle highlights a fundamental security paradox: regardless of the level of technical investment, if user awareness and behavioral compliance do not improve commensurately, the overall system remains susceptible to data breaches and unauthorized access. Common manifestations of human error include the use of weak or reused passwords, susceptibility to phishing and social engineering attacks, inadvertent clicking of malicious links, and failure to apply timely security updates.

The Personal Data Protection Law (PDP Law) in Indonesia is present in response to this challenge (Alrusaini, 2026). The PDP Law aims to provide legal protection for individuals over their personal data, while also establishing an obligation for organizations or data controllers to maintain data security against leakage and misuse of personal data. Article 35 Paragraph (1): "The Personal Data Controller is obliged to protect the Personal Data it manages from unauthorized processing of personal data." These interconnected pressures encompassing rapid digital transformation, escalating cyber threats, and stringent regulatory enforcement collectively underscore the critical need for a systematic and integrated risk management approach. Organizations that fail to align their IT security infrastructure and governance policies with PDP Law requirements are exposed not only to legal sanctions but also to significant reputational and operational consequences.

Based on the 2024 RKAP Draft, PT XYZ reported a projected revenue of IDR 1,636.6 billion. Under Article 57 of the PDP Law, non-compliant organizations may face administrative sanctions of up to 2% of annual revenue, equating to a potential maximum fine of IDR 32.7 billion. This financial exposure, when contextualized alongside global data breach costs averaging USD 4.35 million (IBM Security, 2023) and the added burden of forensic investigation, incident recovery, and reputational remediation, renders PDP Law compliance a critical strategic and risk management priority, not merely a legal obligation.

In complying with these regulations, the company faces a number of problems, here are no internal rules related to the control of personal data, including policies governing responsibility and mechanisms for the protection of personal data within the company. Information technology security system vulnerabilities that need further improvement. As part of

a State-Owned Enterprise (SOE) that has public responsibility, the company has the potential to face challenges in ensuring compliance with the PDP Law. These challenges include managing personal data in accordance with legal principles and provisions, mitigating the risk of data breaches, and adjusting internal policies and procedures.

As a regulation that aims to protect personal data, the PDP Law (Personal Data Protection Law) requires companies to maintain the security of managed data. However, attempted cyberattacks can threaten the company's compliance with the PDP Law. The resulting risks of cyberattacks on PDP Law compliance include:

Administrative and financial sanctions. Companies that fail to protect personal data in accordance with the PDP Law can be subject to significant administrative fines. Administrative fines are a maximum of 2% of revenue. Companies must also bear the cost of system recovery due to cyberattacks. According to the IBM Security report (2023), "The average cost of a data breach globally has risen to $4.35 million," indicating that the financial impact of a data breach is significant and cannot be ignored.

Reputational loss. Personal data leaks can reduce customer trust in the company, damaging its image in the eyes of the public and stakeholders. According to Ramkumar Janakiraman, Joon Ho Lim and Rishika Rishika (2018), "The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Field Experiment," data breach announcements can affect customer behavior, including a decrease in trust and loyalty to the company (Leszkiewicz et al., 2026; Luo et al., 2026).

Potential legal lawsuits. Individuals whose data is leaked have the right to file lawsuits against the company, in accordance with the provisions of the PDP Law. The novelty of this study lies in the integrative approach between the ISO 31000:2018-based risk management framework and the context of the implementation of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), which is a new and strategic regulation in the Indonesian legal system. This study adopts a systematic approach from ISO 31000:2018 to identify, analyze, evaluate, and respond to information technology risks that have the potential to cause violations of the PDP Law. In contrast to prior studies such as Mamuaja and Cahyono (2024), who applied ISO 31000 for general IT risk analysis, and Nasution (2025), who focused on a comparative analysis of GDPR and PDP Law principles, the present study uniquely integrates a comprehensive ISO 31000:2018 risk management cycle with the specific compliance obligations of the Indonesian PDP Law within an actual organizational context. Furthermore, existing literature has not sufficiently addressed the development of empirically grounded, actionable mitigation frameworks tailored to consulting firms operating under Indonesian SOE governance structures. This is a novelty because, until now, there have not been many studies that specifically combine risk management frameworks with the in-depth implementation of the PDP Law in the Indonesian corporate environment.

The objectives of this study are to develop internal policies related to personal data management that regulate operational procedures in accordance with the personal data protection principles stipulated in the Personal Data Protection (PDP) Law. In addition, this study aims to conduct information technology security risk management by identifying key information security risks that have the potential to result in violations of the PDP Law, analyzing the vulnerability level of technological infrastructure that may be exploited by cyber threat actors to gain unauthorized access to personal data, and implementing risk mitigation measures based on the ISO 31000:2018 framework. These mitigation efforts are intended to reduce the likelihood and impact of personal data leakage, unauthorized access, or misuse resulting from cyberattacks, thereby enhancing the overall effectiveness of personal data protection within the organization.

METHOD

Frame of Thought

This framework was used to answer the research objectives, which were: the determination of major risks in the implementation of the PDP Law, the evaluation of the effectiveness of the implemented mitigation measures, and the formulation of relevant strategic solutions. Consequently, it was anticipated that the research could provide not only practical guidance for companies but also contribute theoretically to the development of information technology risk management focused on the protection of personal data.

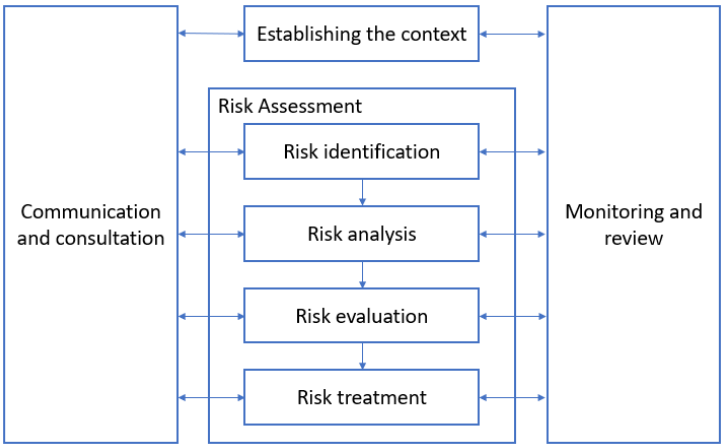

Figure 1. *ISO 31000:2018* Framework
source: research data

A risk management framework based on ISO 31000:2018 involved several core steps:

a. Contextualization: It referred to identifying the scope, objectives, and risk management criteria related to the protection of personal data.
b. Risk identification was conducted through document review and field observation, covering all major IT assets and data processing activities within PT XYZ.
c. Risk analysis evaluated the likelihood and consequences of identified risks.
d. The severity of the risk was determined, and risks were prioritized accordingly.
e. Risk management involved creating strategies to avoid, mitigate, transfer, or accept risks.
f. Monitoring and evaluation of progress: Effective mitigation measures needed to be continuously monitored and evaluated.
g. Communication and consultation were conducted throughout the risk management process.

The current state of IT risk management at PT XYZ reflected considerable challenges in data security governance and compliance with the Personal Data Protection Law (PDP Law). Moreover, awareness and preparedness of human resources (HR) in addressing cyber threats remained critically low, and this organizational unpreparedness significantly increased the risk of data leakage incidents and the erosion of customer trust.

As demonstrated in the preceding subsection, the existing risk management practices in the organization were primarily reactive rather than proactive prior to the implementation of the information technology audit. IT risks had not been fully identified and systematically assessed, nor was there continuous risk monitoring to detect emerging threats. Existing risk management policies lacked sufficient mitigation mechanisms for protecting customers' personal data. These policies required substantial strengthening to more effectively integrate structured risk management frameworks with regulatory compliance requirements.

Data Collection Techniques

This study employed data collection techniques designed to obtain comprehensive and relevant information regarding the implementation of the Personal Data Protection Law at PT XYZ. Data were collected through surveys, document studies, and observations. The survey was conducted to obtain primary data from internal employees directly or indirectly involved in the management of personal data and the use of the company's information technology systems. The questionnaire contained questions related to personal data security, company data security, and basic understanding of the Personal Data Protection Law. The survey objectives were (1) to measure employee awareness and understanding of the company's personal data protection policy, (2) to assess compliance with data protection procedures and employee attitudes, and (3) to identify gaps in the understanding, implementation, and internal control of personal data.

The data collection process was conducted systematically and efficiently through several stages. First, the survey unit and target respondents were determined, namely approximately 100 PT XYZ employees from various divisions such as the Project Management Office, Human

Resources, Finance, Accounting, Business, Power Plant, Network, Corporate Secretariat, and the Internal Supervisory Unit. Second, the questionnaire was prepared, which included respondent demographic data (division, age, gender) and respondent statements on a nominal scale of "Yes," "No," and "Don't Know." Third, the questionnaire was validated and piloted on more than 169 respondents to assess the consistency of answers and the relevance of the questions. Finally, the questionnaire was distributed and completed through WhatsApp Groups and other data collection mechanisms, ensuring valid and representative data.

Data Analysis Techniques

The research used a qualitative descriptive approach to analyze information technology risk management strategies in the context of the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) at PT XYZ. This approach was chosen because it allowed for in-depth data collection to understand risks and mitigation strategies relevant to the implementation of the PDP Law.

The risk analysis showed the existence of technical challenges such as IT security vulnerabilities, operational risks related to the integration of business processes with regulations, and compliance risks due to employees' lack of awareness of the PDP Law. The study also assessed the effectiveness of risk management strategies implemented using frameworks such as ISO 31000:2018 to identify risk patterns and measure the success of the mitigations carried out.

RESULTS AND DISCUSSION

Results

The Risk Identification

In the ISO 31000:2018-based risk management process, the risk identification stage serves to uncover all potential events that can have an impact on the achievement of organizational goals, in this case related to the company's compliance with Law No. 27 of 2022 concerning Personal Data Protection (PDP Law). Identification is carried out systematically on all work units that have direct or indirect involvement in the collection, storage, processing, and control of personal data.

The following is an explanation of the coding used in risk identification in risk studies:

1) KR (Risk code)
2) Demonstrate the unique identity of the overall risk, which is marked with labels such as R1, R2, ... R12
3) KP (Risk causation code)
4) Demonstrate the unique identity of the overall risk cause, which is marked with labels such as P1, P2, ... P12
5) KD (Risk Impact Code)
6) Demonstrate the unique identity of the overall risk impact marked with labels such as D1, D2, ... D12

The risks identified include the causes and impacts of risks from information security threats from technical/non-technical aspects, internal/external factors and risk factors based on the results of field observations, employee surveys, document studies. Table 1 is an identification mapping of the risk of a personal data breach:

Table 1. Identification of Personal Data Management at PT XYZ

ID	Risk	Impact	Category	Risk Owner
	Internal Non-Technical Factors			
R1	High potential for violations of the Personal Data Protection (PDP) Law due to a lack of enforceable rules.	Potential regulatory fines, reputational damage, and loss of customer trust.	Governance	MMR & MHK
R2	Human error in managing critical data and access to IT systems.	Configuration errors, data leaks, and operational losses.	Governance	MSDM & MTI
R3	Low level of accountability in personal data management.	Difficulty in conducting forensic audits and	Governance	MSPI

ID	Risk	Impact	Category	Risk Owner
		recovery during incidents, reducing third-party trust.		
	External Non-Technical Factors			
R4	Ambiguity in interpreting certain articles of the PDP Law (external).	Incorrect regulatory implementation and potential legal violations.	Governance	MMR & MHK
	Internal Technical Factors			
R5	Sensitive data is easily accessed or stolen by unauthorized parties.	Risk of personal data leaks, legal claims, and loss of stakeholder trust.	IT Security Operations	MTI
R6	Weak access control creates loopholes for illegal access to the organization's critical documents and data.	Unauthorized access to strategic information, threatening business continuity.	IT Security Operations	MTI
R7	Lack of an early detection system means data leaks cannot be responded to quickly and in a timely manner.	Increased damage due to delayed security incident handling.	IT Security Operations	MTI
R8	Misuse of corporate accounts, potentially becoming a pathway for phishing attacks.	Potential loss of critical data and exposure to malware.	IT Security Operations	MTI & MHK
R9	Lack of security configuration on public cloud services creates loopholes for data leaks and unauthorized access.	Company data is vulnerable to illegal access and misuse.	IT Security Operations	MTI
R10	The absence of a "never trust, always verify" approach makes the system vulnerable to lateral movement in the event of a compromise.	Cyber attacks can spread quickly to various internal systems.	IT Security Operations	MTI
R11	The system is infected by malware, ransomware, or other viruses that can damage or steal data.	Operational disruption, financial loss, and loss of critical data.	IT Security Operations	MTI
	External Technical Factors			
R12	External threats in the form of cyber attacks from professional hackers or cybercriminal groups that can compromise system integrity, confidentiality, and availability (external).	Reputational damage, service disruption, and potential legal claims.	IT Security Operations	MTI

Source: Research Data

Based on table 1, it was found that internal technical factors are the most dominant source of risk in the context of the implementation of personal data protection and information technology security in organizations. Seven of the twelve risks identified fall into this category, most of which are related to weaknesses in security systems, access control, lack of early detection systems, and security configurations of IT services, including in cloud infrastructure and network architecture. All internal technical risks are under the responsibility of the Information Technology Division, which demonstrates the importance of this unit's role in maintaining the integrity, confidentiality, and availability of company data.

In addition, non-technical risks, especially those related to governance and compliance, also have a significant contribution to the risk profile of the organization. These risks include the absence of internal policies governing the protection of personal data, low accountability in data management, and ambiguity in the interpretation of regulations from outside the organization. Handling these risks cannot be done sectoral but must involve cross-functional synergy between

the Compliance, Legal, Human Resources, and Internal Auditor units, to ensure that the application of the principle of personal data protection is not only focused on technical aspects, but also in harmony with policies, laws, and organizational culture.

After mapping the types of risks and those responsible, the next step in the risk management process is to identify the *root cause* and impact analysis of each risk that has been registered. Identifying the causes of risk is important to describe the root of the underlying problems, whether systemic, procedural, technical, or behavioral. By understanding the causes deeply, organizations can design mitigation actions that are preventive, not just reactive.

As a follow-up to the risk identification process, the next stage is to outline the causes and impacts of each of the risks that have been mapped. This step aims to understand the root of the problem and the consequences that may arise, so that the right mitigation strategy can be developed. The explanation of the causes and impacts of the risks above is grouped into 2 main risk sources, namely:

1) The causes and impacts of the risk are that there is no internal policy governing the Protection of Personal Data.

   The first risk is related to non-technical mitigation recommendations for internal policy needs related to Personal Data Protection within PT XYZ. This risk is owned by MMR as the party directly responsible (*Responsible*), with BOD as the fully responsible party (*Accountable*), as well as the Secretary, KS, VP of Field, Manager, and as a supporting party (*Support*). BOD is involved as a consulted and informed party. Table 2 lists the causes of risk in the absence of an internal policy governing Personal Data Protection.

Table 2. Identify The Cause of The Risk in The Absence of an Internal Policy Governing The Protection of Personal Data.

Factors	KR	CD	Risk Causes	Description of Risk Causes
Internal	R1	P1	No internal policy regarding Personal Data Protection	The absence of internal policies in line with the PDP Law causes organizations to not have personal data protection guidelines.
	R2	P2	Lack of understanding of human resources towards cyber threats	Accidental or omission of HR leads to mishandling of data and access settings.
	R3	P3	There is no internal *audit control* related to compliance with PDP Law regulations	Unavailability of audit control mechanisms in supervision of personal data management
External	R4	P4	Government regulations related to the PDP Law are not clear	The unclear meaning of certain articles causes doubts in the implementation of policies.

Source: Research Data

The impact of non-technical risks arises due to weak internal policies and suboptimal understanding and supervision of personal data protection within the organization. This impact not only affects operational aspects but also increases potential regulatory breaches and loss of control over personal data. Impacts can be classified into two sources, namely internal and external.

Internal impact factors come from within the organization, such as employees' ignorance of correct procedures, negligence that causes incidents, and the absence of an adequate evaluation system. Meanwhile, external impacts lead to uncertainty in the implementation of policies due to the influence of factors outside the organization, including unclear directives or standards from the government regarding the implementation of the PDP Law. Table 3 summarizes the impact on the risk of the absence of an internal policy governing the Protection of Personal Data.

Table 3. Impact of Risk in the Absence of an Internal Policy Governing the Protection of Personal Data

Categories	KR	KD	Risk Impact	Risk Impact Description
Internal	R1	D1	Potential regulatory fines,	It can result in legal investigations,

Categories	KR	KD	Risk Impact	Risk Impact Description
			reputational damage, and loss of customer trust.	administrative penalties, and lower public trust in the company.
	R2	D2	Misconfiguration, data leaks, and operational losses occur.	A small mistake can result in a major disruption to the system and the potential for loss of important data.
	R3	D3	It is difficult to conduct forensic audits and recovery during incidents, reducing the trust of third parties.	Complicating the post-incident investigation process and creating legal uncertainty.
External	R4	D4	Errors in the implementation of regulations and potential violations of the law.	Companies can be considered non-compliant even though they have tried to follow the rules.

Source: Research Data

Table 3 provides a comprehensive overview of the consequences of non-technical risks in the context of personal data protection. Understanding this impact is very important so that management can take proactive steps in developing clear internal policies, educating human resources, and building *a* sustainable audit and supervision system. Through this comprehensive risk identification, companies can more easily determine mitigation priorities, establish control plans, and strategize to improve information security governance and compliance with the PDP Law on an ongoing basis.

2) Causes and impacts of security system vulnerability risk Information technology infrastructure

The second risk related to technical mitigation recommendations on the causes and impacts of risks is divided into internal and external categories. Internal factors reflect weaknesses or shortcomings in the system. Meanwhile, external factors come from outside the organization that are generally difficult to control directly, such as attacks from third parties. Table 4 presents a list of the risk causes that have been identified, along with a description describing the potential consequences of each risk cause:

Table 4. Identifying the Causes of the Vulnerability of Information Technology Infrastructure Security Systems

Factors	KR	Code	Risk Causes	Risk Description
Internal	R5	P5	Unencrypted system	Data stored or transmitted in the system is not protected by encryption mechanisms, so it can be easily accessed by unauthorized parties in the event of a leak incident.
	R6	P6	Unauthorized access to shared systems/folders	The lack of access control causes sensitive data to be accessed by unauthorized employees, opening up opportunities for data misuse or manipulation.
	R7	P7	Delay in detection of leak incidents	The absence of an adequate early detection or monitoring system results in data leak incidents not being immediately identified, thus causing a wider impact.
	R8	P8	Corporate email is used for external purposes (marketplace, social media)	The use of official email for external services increases the risk of exposing a corporate account to credential theft, spam, and cyberattacks.
	R9	P9	Use *of public cloud* without security controls	Storing corporate data on public *cloud* services without security and encryption policies can lead to data exposure to third parties.
	R10	P10	IT infrastructure has not yet implemented *Zero*	The absence of a *Zero Trust approach* makes the system trust devices/applications by default without multi-layered verification, making it

Factors	KR	Code	Risk Causes	Risk Description
			Trust	easier to access unauthorized ones.
	R11	P11	There is no anti-malware protection system	System unpreparedness for malware such as viruses, spyware, or ransomware, allows for service interruptions, data loss, and system corruption.
External	R12	P12	Attacks from third parties (hackers)	Attacks from outside the company such as phishing, brute-force attacks, or exploiting security vulnerabilities, which are carried out with the motive of data theft, extortion, or sabotage.

Source: Research Data

Once the cause of the risk has been identified, the next step is to determine the impact that may arise if the cause is not adequately controlled. The impacts of these risks are classified into two main sources, namely internal and external. Internal impacts are direct consequences that occur within the organizational environment, such as operational losses and data breaches by internal parties. Meanwhile, external impacts involve reactions from outside parties, such as legal sanctions, loss of public trust, or reputational damage due to the company's failure to protect personal data. In accordance with ISO 31000:2018, following risk identification, a semi-quantitative risk assessment was applied. Each risk was evaluated on two dimensions: Likelihood (scale 1–5: Rare to Almost Certain) and Impact (scale 1–5: Insignificant to Catastrophic). The resulting Risk Priority Score (RPS = Likelihood × Impact) classifies risks as Low (1–4), Moderate (5–9), High (10–19), or Very High (20–25). This matrix-based approach enables systematic prioritization of mitigation efforts. Table 5 presents a list of the identified impacts, along with a description of the potential consequences of each risk impact.

Table 5. Identify The Risk Impact Of Information Technology Infrastructure Security System Vulnerabilities

Impact Source Categories	Risk Code	Code	Risk Impact	Description
Internal	R5	D5	Personal data is vulnerable to being stolen or modified (violating Article 58 of the PDP Law)	Data theft can have a direct impact on relationships with clients and business partners.
	R6	D6	Misuse of personal data by internal (breach of confidentiality)	Potential sabotage or use of information by irresponsible parties.
	R7	D7	Increased damage due to delays in handling security incidents.	The impact of incidents becomes wider because they are not immediately detected and controlled.
	R8	D8	Potential loss of important data and exposure to malware.	Attackers can access data and other systems using compromised credentials.
	R9	D9	Company data is vulnerable to illegal access and misuse.	Sensitive company information can be spread to uninterested parties.
	R10	D10	Cyberattacks can spread quickly to various internal systems.	Once one point is compromised, the attacker can move freely to another system.
	R11	D1	Operational disruptions, financial losses, and loss of critical data.	Operational activities have been halted, and the potential cost of recovery is enormous.
External	R12	D12	Reputational damage, service interruptions, and	It can destroy customer trust, resulting in loss of market share

Impact Source Categories	Risk Code	Code	Risk Impact	Description
			potential lawsuits.	and financial losses.

Source: Research Data

Table 5 clarifies how risks in IT security management impact not only the system, but also on legal compliance and business continuity. This impact analysis is the main basis for the next stage, namely *risk* analysis and determination of the right mitigation strategy.

Discussion

Risk Mitigation Recommendations for Causes There is no internal policy governing the Protection of Personal Data

In the process of implementing Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), the existence of an internal policy framework and organizational awareness are the main pillars in maintaining compliance with regulations. From a governance perspective, the absence of formal internal policies constitutes a critical gap in accountability structures, as organizations cannot operationalize regulatory compliance without clearly delineated procedural standards (Ayundyahrini et al., 2026; Barafort et al., 2019). The ISO 31000:2018 framework identifies governance as an integral component of risk context setting, whereby the absence of internal policies amplifies the organization's inherent risk exposure and reduces its capacity to establish an effective control environment (Ayundyahrini et al., 2026). Based on the results of risk identification, there are a number of non-technical challenges that originate from the internal and external environment of the organization, including the absence of internal policies related to personal data protection, a lack of human resource understanding of cyber threats, the absence of internal audit controls over regulatory compliance, and a lack of clarity regarding technical regulations issued by the government.

These non-technical risk mitigation efforts focus on strengthening governance structures, policies, and human resource capabilities as a form of organizational commitment to the principles of transparency, accountability, and prudence in personal data management.

Table 6. Risk of the absence of an internal policy governing the protection of personal data

Risk Source Category	Risk Code	Risk Causes	Risk Description	Person in Charge
Internal Internal Internal	P1	No internal policy regarding Personal Data Protection	Policy formulation is the normative basis so that all personal data processing is in accordance with the PDP Law. Socialization is needed so that employees understand and apply it.	IT Sub
	P2	Lack of understanding of human resources towards cyber threats	Regular training establishes an information security culture and raises awareness of the risk of data breaches.	IT and HR sub
	P3	There is no internal *audit control* related to regulatory compliance with the PDP Law	*Internal audits* that incorporate the compliance elements of the PDP Law help detect violations early and encourage continuous improvement.	Internal Supervisory Unit
External	P4	Government regulations related to the PDP Law are not clear	Proactive steps by drafting internal policies show the good faith of the organization even though there are no detailed technical instructions from the government.	Legal Sub

Source: Research Data

As part of efforts to strengthen personal data protection governance, non-technical risk identification plays an important role in uncovering internal organizational weaknesses that are not systemic but have a significant impact on regulatory compliance. Based on the results of the study, there are a number of non-technical risk causes that need to be mitigated immediately. To reduce potential violations of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), a series of mitigation measures that are non-technical but strategic are needed. The following is a description of the mitigation proposed to address the causes of these risks:

1. No internal policy related to Personal Data Protection (P1)
   a. Mitigation is carried out through the preparation and implementation of internal policies that explicitly govern the management of personal data, including classification, authorization of access, processing and storage of data and consent of personal data subjects. Where personal data is contained in the management of customer data, partner data, employee data.
   b. This policy is prepared with reference to the principles in the PDP Law and is the basis of reference for all work units.
   c. Once prepared, the policy must be thoroughly socialized so that it is understood and implemented by all employees.

The following are the obligations that must be fulfilled by companies in implementing compliance with the PDP Law in companies to minimize potential violations of the PDP Law.

Table 7. Companies' Obligations Related to the Regulation of the PDP Law

No	Obligations	Fulfillment Criteria
1	Maintaining DP confidentiality	a. Availability of internal rules/SOPs b. Appointment of Officers/Officers who carry out the DP protection function c. There is a DP processor statement that it will use DP according to the designation
2	Protecting DP from unauthorized processing	
3	Prevent DPs from being accessed illegally	
4	Protect and ensure the safety of the DP it processes	Appointment of Officials or Officers who carry out the function of DP Protection
5	Supervise each party involved in the processing of DP under the control of the DP Controller	
6	Updating and/or correcting DP errors and/or inaccuracies	DP Verification by DP Processor (BPO)
7	Ensure the accuracy, completeness and consistency of the DP by verifying	
8	Have a DP processing basis	Amendment of agreement (existing), Amendment of contract, Statement of officer & Pensioner
9	Show proof of consent that has been given by the DP Subject	
10	Granting and refusing to grant DP access to DP Subjects	a. Availability of internal rules/SOPs b. Appointment of Officers/Officers who carry out the DP Protection function
11	Perform DP processing based on the DP Controller's orders	Available assignment in writing from the Controller to the Processor
12	Obtain written approval from the DP Controller before engaging other DP Processors	Written assignment is available for the involvement of other DP Processors
13	Convey information on the legality, purpose, type, relevance, details, retention, duration of DP processing and DP subject rights	Socialization/ FGD/ Meeting with DP Subjects

source: research data

2. Lack of understanding of human resources towards cyber threats (P2)

a. The mitigation strategy is carried out by organizing periodic training and socialization to all employees related to cybersecurity and personal data protection.
b. The training covers topics such as phishing, password management, as well as everyone's responsibility for the data they manage.
c. This increased literacy is expected to form a strong and risk-aware information security culture.
d. There is no internal audit control related to regulatory compliance with the PDP Law (P3)
e. Mitigation is carried out by integrating the compliance aspects of the PDP Law in the company's IT internal audit program.
f. The audit will evaluate the extent to which the implementation of data security policies and procedures is in accordance with regulations.
g. The results of the *audit* are used as the basis for continuous improvement and adjustment.

3. Government regulations related to the PDP Law are unclear (P4)
   a. Although technical regulations from the government are not complete, organizations can take anticipatory steps through the preparation of internal policies based on the basic principles of the PDP Law.
   b. This internal policy shows the organization's commitment to compliance with personal data protection and is proof of good faith if an external *audit is* conducted.
   c. Organizations also need to set up a regulatory monitoring team to immediately adjust policies when formal technical rules are issued.

The implementation of non-technical mitigation is planned in stages, starting in Semester 1 of 2025, by adjusting the readiness of resources, the urgency of risks, and the operational needs of the organization. This approach is expected to provide a normative foundation, form a risk-aware culture in the work environment, and provide a sustainable evaluative mechanism in ensuring compliance with the PDP Law. The following roadmap describes a plan for implementing non-technical mitigations based on previously identified risk causes:

Table 8. Non-Technical Mitigation of Risk Causes of the Absence of an Internal Policy Governing the Protection of Personal Data

Kd	Mitigating Risk Causes	Implementation Phase	Implementation Time (Estimated)	Remarks
P1, P4	Preparation and socialization of internal policies on personal data protection	Early Phase	Semester 1 2025	The normative basis for the management of personal data applies even though technical regulations are not complete
P2	Regular socialization and training on data security and cybersecurity practices to all employees	Sustainable	Semester 1 2025 (recurring every 3 Months)	Increase employee awareness and shape the organization's information security culture
P3	Integration of PDP Law compliance into the *Information Technology internal* audit program	Sustainable	FY4 2025	Periodic evaluation as a control over policy implementation and continuous adjustment

Source: Research Data

Based on the non-technical mitigation roadmap table above, it can be concluded that the risk control strategy for personal data protection breaches is not only dependent on the application of technology but is also heavily influenced by the existence of clear policies, increased information security literacy, and effective internal oversight mechanisms. With structured and sustainable implementation, this non-technical mitigation is expected to form a strong foundation

for personal data governance and to be in line with the principles stipulated in Law Number 27 of 2022 concerning Personal Data Protection.

Risk Mitigation Recommendations for Risk Causes of Information Technology Infrastructure Security System Vulnerabilities

Vulnerabilities in the information technology infrastructure security system are one of the sources of strategic risks identified in the implementation of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) within PT XYZ. An evaluation of the existing conditions shows that some important aspects of personal data protection have not been fully protected technically or at the policy level.

Table 9. Vulnerability Risks of Information Technology Infrastructure Security Systems

Risk Source Category	Code	Risk Causes	Risk Description	Person in Charge
Internal	P1	Unencrypted system	Data stored or transmitted in the system is not protected by encryption mechanisms, so it can be easily accessed by unauthorized parties in the event of a leak incident.	IT Sub
	P2	Unauthorized access to shared systems/folders	The lack of access control causes sensitive data to be accessed by unauthorized employees, opening up opportunities for data misuse or manipulation.	IT Sub
	P3	Delay in detection of leak incidents	The absence of an adequate early detection or monitoring system results in data leak incidents not being immediately identified, thus causing a wider impact.	IT Sub
	P4	Corporate email is used for external purposes	The use of official email for external services increases the risk of exposing a corporate account to credential theft, spam, and cyberattacks.	Communication and Legal Sub
	P5	Use *of public cloud* without security controls	Storing corporate data on public *cloud* services without security and encryption policies can lead to data exposure to third parties.	IT Sub
	P6	IT infrastructure has not yet implemented *Zero Trust*	The absence of a *Zero Trust approach* makes the system trust devices/applications by default without multi-layered verification, making it easier to access unauthorized ones.	IT Sub
	P7	Absence of anti-malware protection system	System unpreparedness for malware such as viruses, spyware, or ransomware, allows for service interruptions, data loss, and system corruption.	IT Sub
External	P8	Attacks from third parties (hackers)	Attacks from outside the company such as phishing, brute-force attacks, or exploiting security vulnerabilities, which are carried out with the motive of data theft, extortion, or sabotage.	IT Sub and Risk Management

Source: Research Data

Based on table 9, it is possible to identify several risk causes arising from significant weaknesses in the information technology security system. These security gaps have the potential to be exploited by unauthorized parties, thereby resulting in data breaches, service interruptions, as well as legal losses and reputational damage to the company. In the context of compliance with Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), these risks must be mitigated comprehensively, considering that the PDP Law requires every controller and data processor to ensure the security of personal data through adequate technical and organizational measures (Article 39 and Article 40). Therefore, the implementation of targeted technical mitigations aligned with best practices in information security is required. These mitigation measures are designed to strengthen IT infrastructure, reduce the attack surface, and improve the detection and response capabilities for security incidents. The technical mitigation recommendations that can be implemented include the following.

a) End-to-end encryption implementation for all data storage and communications.
b) Implement role-based access control (RBAC) and conduct regular directory access audits.
c) Implementation of SIEM systems for early monitoring and detection of data breach incidents.
d) Issuing a policy prohibiting the use of corporate email for external service access.
e) Enforcement of cloud security policies, including encryption, layered authorization, and storage audits.
f) Adoption of a Zero Trust architecture for all internal systems and networks.
g) Implement EDR and enterprise antivirus solutions with automatic updates and isolation of infected devices.
h) Improving perimeter defense, firewalls, penetration testing (pentests), and regular employee security awareness training.

To ensure that information security risk mitigation runs in a structured and effective manner, it is necessary to prepare an implementation roadmap that takes into account urgency, technical complexity, and resource availability. This roadmap aims to guide the implementation of technical mitigation in stages, starting from fundamental steps that have a direct impact on data protection, to more complex system architecture transformation. The preparation of this roadmap also considers the suitability of data protection obligations based on Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), especially in terms of implementing adequate technical and procedural measures (Articles 39 and 40 of the PDP Law). The following is a technical mitigation roadmap that can be used as a reference for implementation:

Table 10. Mitigating The Vulnerability of Information Technology Infrastructure Security Systems

Kd	Technical Mitigation	Implement-ation Phase	Implementation Time (Estimated)	Remarks
P1	End-to-end encryption implementation for all data storage and communications.	Short Term	Semester 1 2025	Top priority to protect sensitive data, supporting Article 39 of the PDP Law
P2	Implement role-based access control (RBAC) and *folder access audits on a regular basis.*	Short Term	Semester 1 2025	Restricting unauthorized access; requires *regular* audits
P3	Issuing a policy prohibiting the use of corporate email for external services.	Short Term	Semester 1 2025	Can be done immediately through internal policies
P4	Implement EDR and corporate antivirus with automatic updates and isolation of infected devices.	Short Term	Semester 1 2025	Securing endpoints from malware and exploits
P5	Implementation of SIEM	Medium	Semester 1 2025	Log integration &

Kd	Technical Mitigation	Implement-ation Phase	Implementation Time (Estimated)	Remarks
	systems for early monitoring and detection of leak incidents.	Term		SIEM system configuration
P6	Enforcement *of cloud security policies* includes encryption, layered authorization, and *storage audits*.	Medium Term	Semester 1 2025	Need coordination with cloud vendors & SOPs
P7	Adoption of *a Zero Trust* architecture for all internal systems and networks.	Long-Term	Semester 1 2025	Total transformation in access management
P8	Improving perimeter defense, firewalls, attack simulations (pentests), and regular employee awareness socialization	Long-Term	Semester 1 2025 – Semester 1 2026	It needs to be done periodically and continuously

Source: Research Data

This risk mitigation roadmap recommendation can be implemented gradually starting from Semester 1 2025 to Semester 2 2026. The timing of the selection considers the readiness of infrastructure, budget allocation, and the urgency of strengthening the information security system in accordance with the provisions of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). By starting implementation in the middle of the year, organizations have sufficient time to conduct technical planning, resource procurement, and internal policy socialization before entering the strategic phases of the following year. This roadmap is expected to serve as the basis for implementing measurable and sustainable mitigation to strengthen the company's information security resilience.

The budget value required for each mitigation activity is not discussed in detail in this document. This is because the focus of this study is on the preparation of technical strategies for mitigating information security risks, not on financial planning or project financing. Estimated implementation costs can be further adjusted by the relevant unit based on actual needs, the complexity of the systems owned, and the organization's internal procurement policies. A separate budget evaluation is recommended to be conducted by the project management and finance teams as part of further implementation planning.

Risk Treatment

Monitoring and Review

Monitoring and review are an important stage in the risk management process according to ISO 31000:2018, which aims to ensure that all designed and implemented risk management measures continue to operate effectively and in accordance with the dynamics of the organizational environment. In the context of PT XYZ, monitoring and review play a strategic role in ensuring that mitigation of information technology security risks related to personal data protection is consistent, sustainable, and well documented.

Monitoring is carried out across various aspects of mitigation implementation, both technical and non-technical. Monitoring activities include:

a) The development process of risk mitigation treatments
b) Risk treatment status
c) Mitigation activities that have been carried out
d) Risk treatments requiring follow-up
e) Descriptions of risk treatment follow-up actions

To support accountability and traceability of mitigation implementation, the entire monitoring process is integrated into the company's action tracker system. This action tracker is a management tool that records and monitors the status of all mitigation action plans, including assigned responsibilities, implementation deadlines, progress status, and evidence of completion.

By incorporating mitigation measures into the action tracker, the implementation of risk controls becomes easier to monitor across functions and over time.

Furthermore, the existence of the action tracker also serves to increase management's awareness of the importance of risk mitigation follow-up. Each responsible work unit can transparently view the progress of mitigation implementation, while being encouraged to maintain collective commitment to resolving risk findings on schedule. This encourages risk management to be not only the technical responsibility of the IT unit, but also part of the company's overall risk management culture.

The review process is carried out periodically to assess whether the implemented strategies and controls remain relevant, adequate, and aligned with regulatory developments (including derivative policies of the PDP Law), technological changes, and the latest threat landscape. The results of the review are used to refine policies, adjust existing controls, or formulate new strategies if new gaps or risks are identified.

With a structured monitoring and review system integrated into the company's mechanisms, organizations can actively evaluate the effectiveness of risk handling, increase management accountability for data security, and maintain sustainability in building strong, regulatory-compliant personal data protection governance.

Communication and Consultation

Communication and consultation are fundamental elements of risk management based on ISO 31000:2018, ensuring that all stakeholders understand and participate in risk management (Songa et al., 2026; Weinstein, 2026;Tirrell et al., 2026). In the context of PT XYZ, communication and consultation play an important role in increasing awareness of personal data security, strengthening compliance with Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), and optimizing coordination among internal departments, regulators, business partners, and third parties. Without effective communication and consultation, the implementation of risk mitigation strategies may be hindered, and the company may face risks of data breaches, administrative sanctions, and declining customer trust.

To ensure that risk management implementation runs effectively and involves all stakeholders, the company implements a structured and sustainable communication and consultation strategy. Communication is carried out to convey important information related to policies, procedures, and risk status, while consultations are conducted to ensure that each mitigation decision considers cross-functional perspectives and strengthens synergy across functions. This communication and consultation strategy is designed to build shared awareness, improve coordination, and accelerate responses to the dynamics of information security risks and regulatory changes. The following is the concept of communication and consultation strategies in risk management within the company, presented in the following table:

Table 11. Concept Of Communication and Consulting Strategy in Risk Management at PT XYZ

Aspects	Description
Purpose	Building understanding, engagement, and support from all stakeholders on IT security risk management and implementation of the PDP Law.
Forms of Communication	Socialization of personal data protection policies Audit and action tracker information- Cybersecurity education through regular training
Consultation Form	Cross-functional coordination in policy formulation and risk mitigation Consulting with external parties such as cloud vendors and compliance consultants
Media/Channels	Company intranet Official circular/email Inter-sectoral coordination forum and cross-sectoral FGD
Stakeholders	Management
Expected Results	Increased *awareness* of all employees- Alignment between policies, technical processes, and regulations Responsive to changing risks and regulations

Source: Research Data

With a structured communication and consulting strategy in place, the company not only ensures that all stakeholders understand their roles and responsibilities in risk management, but also creates a collaborative culture that supports the effective implementation of personal data protection policies. Through an open communication process and participatory consultation, companies can respond to risk dynamics adaptively and maintain compliance with applicable regulations, especially Law Number 27 of 2022 concerning Personal Data Protection.

CONCLUSION

The result of this series of studies, several conclusions were formulated that reflect the actual conditions and challenges faced by companies in implementing information technology risk management to support compliance with Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This conclusion is based on the results of observations, internal survey analysis, and risk evaluation based on the ISO 31000:2018 framework. There are two main problems both technical and non-technical faced by companies in the implementation of Law Number 27 of 2022 concerning Personal Data Protection.

The application of the ISO 31000:2018 framework, with a systematic approach to determining IT security risk management strategies, has an impact on compliance with the PDP Law. Steps ranging from establishing the context, identifying, analyzing, evaluating, and treating risks, as well as monitoring and communication, have been carried out in a structured manner. This allows PT XYZ to classify risks based on priority levels as well as design more effective mitigation strategies. The ISO 31000:2018 approach can help map inherent, residual, and target risks in a structured manner. The implementation of a risk management system oriented toward the protection of personal data is not only a legal obligation but also a strategic necessity for long-term business sustainability.

Through an ISO 31000:2018-based risk management approach, this study produced several conclusions as follows. It is important to acknowledge several limitations of this study. First, the research was conducted within a single organization (PT XYZ), which may limit the generalizability of the findings to other companies or sectors. Second, the use of a nominal-scale survey instrument (Yes/No/Do Not Know) limits the granularity of quantitative analysis. Third, the absence of formally issued technical regulations from the Indonesian government at the time of data collection constrained the operationalization of certain PDP Law compliance criteria. Future research is recommended to: (1) replicate this framework across multiple organizations in different sectors to test generalizability; (2) adopt a Likert-scale or mixed-scale instrument to capture more nuanced levels of employee awareness; (3) conduct longitudinal studies to track the effectiveness of implemented mitigation strategies over time; and (4) explore the integration of ISO 27001:2022 with ISO 31000:2018 as a complementary framework for comprehensive personal data security governance.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to PT XYZ for providing the necessary data and support for this study on Information Technology Risk Management Strategy in the Implementation of Law Number 27 of 2022 Concerning Personal Data Protection. Special thanks are extended to all employees who participated in the surveys and provided valuable insights, as well as to the management team for facilitating access to company documents and resources.

AUTHOR CONTRIBUTION STATEMENT

Ervin Hermawan responsible for conceptualization, methodology, writing - original draft, writing, review & editing, supervision. Nilo Legowo as an advisor of the Master of Information Systems Management Binus University Graduate Program Master Program

REFERENCES

Alrusaini, O. A. (2026). A Hybrid Structural Equation Modeling–Artificial Intelligence Model for Enhancing Cybersecurity of Personal Information in Mobile Applications. *International*

Journal of Human–Computer Interaction, *42*(1), 525–540. https://doi.org/10.1080/10447318.2025.2508314

Ayundyahrini, M., Widianti, T., Firdaus, H., Azzumar, M., Ega, A. V., Rakhmawati, T., Damayanti, S., Sumaedi, S., Dinaseviani, A., & Syahlani, N. (2026). A novel risk assessment framework: integrating fuzzy failure mode and effect analysis with ISO 31000 and ISO 9001 standards. *International Journal of Quality & Reliability Management*, *43*(4), 1217–1247.

Barafort, B., Mesquida, A., & Mas, A. (2019). ISO 31000-based integrated risk management process assessment model for IT organizations. *Journal of Software: Evolution and Process*, *31*(1), e1984.

Bronk, C. (2026). Things Get Cybernetic: How Artificial Intelligence May Impact Cybersecurity. In *Cyber Security: Policy and Technology* (pp. 155–169). Springer.

Febriansyah, J. P. E., & Kurnia, I. (2026). The Construction of the Consent Principle in the Protection of Medical Personnel's Personal Data and Its Legal Consequences in Healthcare Practice. *JIHK*, *7*(2), 1181–1196.

Ho, F. N., Ho-Dac, N., & Huang, J. S. (2023). The Effects of Privacy and Data Breaches on Consumers' Online Self-Disclosure, Protection Behavior, and Message Valence. *Sage Open*, *13*(3). https://doi.org/10.1177/21582440231181395

IBM Security, M. (2023). Cost of a data breach report 2023. *Ibm. Com*.

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing*, *82*(2), 85–105.

Leszkiewicz, A., Sunder, S., Kumar, V., & Dev, C. S. (2026). Customer Acquisition Through Intermediaries (vs. Brand) Shapes Lifetime Value: Evidence From the Hotel Industry. *Production and Operations Management*, 10591478261437884.

Lund-Tønnesen, J. (2026). Digital surveillance governance: understanding developments in the use of personal data in public sector reform. *Public Management Review*, 1–28.

Luo, Y., Chen, S., & Zhang, P. (2026). A Review of Research on Data Security Risk: Consequences, Mechanisms, and Response. *Journal of Economic Surveys*.

Mamuaja, H. B. M., & Cahyono, A. D. (2024). SIOLGA information technology risk management analysis using ISO 31000. *Journal of Information Systems and Informatics*, *6*(1), 57–67.

Mandru, S. kanth. (2024). Privileged Access Management and Regulatory Compliance. *Journal of Artificial Intelligence, Machine Learning and Data Science*, *2*(2), 727–732. https://doi.org/10.51219/JAIMLD/Srikanth-mandru/182

Nasution, E. R., & Harmika, Z. (2025). Perlindungan Hukum Terhadap Nasabah Bank Yang Mengalami Kebocoran Data Pribadi Ditinjau Dari Undang-Undang Nomor 27 Tahun 2022. *Innovative: Journal Of Social Science Research*, *5*(4), 11373–11384.

Schneier, B. (2015). *Secrets and lies: digital security in a networked world*. John Wiley & Sons.

Songa, A., Rajagukguk, W., & Tewu, D. (2026). An Analysis of Operational Risk Management in the Appointment Process of School Principals at Foundation X Based on ISO 31000: 2018. *Indonesian Interdisciplinary Journal of Sharia Economics (IIJSE)*, *9*(1), 8036–8046.

Syrmoudis, E., Luzsa, R., Ehrlich, Y., Agidigbi, D., Kirsch, K., Rudolf, D., Schlaeger, D., Weber, J., & Grossklags, J. (2026). Unlocking personal data from online services: user studies on data export experiences and data transfer scenarios. *Human–Computer Interaction*, *41*(2), 101–125.

Tirrell, Z., Lybrand, S., Soderlund, N., & Parkinson, B. (2026). Accessing the risks: A mixed methods study of risk management in Australian pharmaceutical market access. *Health Policy*, 105608.

Weinstein, S. (2026). An evaluation of the utility of ISO 31022: 2020 [risk management–guidelines for the management of legal risk] for use by micro-entities. *International Review of Law, Computers & Technology*, *40*(1), 98–119.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269