Journal of Information Systems and Informatics
Vol. 6, No. 2, June 2024 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v6i2.754 Published By DRPM-UBD

Integrating ISO 27001 and Indonesia's Personal Data Protection Law for Data Protection Requirement Model

Arya Adhi Nugraha[1], Asyahri Hadi Nasyuha[2]

[1]Fakultas Teknologi Informasi, Magister Teknologi Informasi, Universitas Teknologi Digital Indonesia, Yogyakarta, Indonesia
[2]Fakultas Teknologi Informasi, Sistem Informasi, Universitas Teknologi Digital Indonesia, Yogyakarta, Indonesia
Email: [1]student.aryaadhi23@mti.utdi.ac.id, [2]asyahrihadi@gmail.com

Abstract

This research explores the integration of ISO/IEC 27001:2022 with Indonesia's Personal Data Protection (PDP) Law to establish a robust framework for data protection and information security within organizations operating in Indonesia. The research addresses the challenges of aligning the comprehensive information security management systems (ISMS) standard of ISO/IEC 27001:2022 with the specific legal requirements of the PDP Law, which governs personal data collection, processing, and protection. Employing the Action Design Research (ADR) methodology, the study involves a thorough review of existing literature, consultations with domain experts, and the development of a structured framework for integration. Key findings highlight the complementary nature of ISO/IEC 27001:2022's risk-based approach and the PDP Law's emphasis on data subject rights, consent management, and breach notification. The integration framework provides organizations with a unified approach to meet both international standards and local regulatory requirements, enhancing overall data protection. The research concludes with insights and recommendations for organizations seeking to navigate the complex landscape of data protection compliance, emphasizing the importance of harmonizing security measures with legal mandates to build a comprehensive and effective data protection strategy.

Keywords: ISO 27001:2022; Personal Data Protection Law; Data Security Compliance; Information Security Management Systems (ISMS).

1. INTRODUCTION

In today's digital landscape, the importance of data protection cannot be overstated. Organizations worldwide are increasingly held accountable for safeguarding personal data, driven by both international standards and local regulations. Emerging technologies, platform-based business models, and the spread of smart working practices are multiplying the number of entry points in computer networks and thus their vulnerability [1]. Information systems are

This work is licensed under a Creative Commons Attribution 4.0 International License.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

essential for the corporate sector in the current era of development, acting as a foundation for the expansion of businesses or organizations [2]. A system that includes gathering, processing, storing, analyzing, and disseminating data for predetermined goals is known as an information system [3]. This is particularly crucial in Indonesia, where the digital economy is rapidly expanding. Indonesia's digital economy is projected to reach USD 130 billion by 2025, driven by the growth of e-commerce, fintech, and digital services. With over 200 million internet users, Indonesia ranks among the largest online markets globally. This surge in digital activity has brought significant benefits but also heightened the risks associated with data breaches and cyber threats.

The record number of cybersecurity breaches exposed had risen by a staggering 36 billion in 2020, marking the worst year on record for information technology security [4]. The proliferation of cyber threats and the increasing sophistication of cyberattacks underscore the urgent need for robust data protection measures. The Indonesian government has responded to these threats by enacting the Personal Data Protection Law (PDP Law) to regulate how personal data is collected, stored, processed, and shared. This law aims to enhance the protection of personal data and build public trust in the digital ecosystem.

Alongside local regulations, numerous organizations implement management systems integrated with quality, environmental, occupational health and safety, and information security based on international standard clusters such as ISO 9001, ISO 14001, OHSAS 18001, and ISO/IEC 27001 to manage risks and improve their general viabilities [5]. International standards such as ISO/IEC 27001:2022 provide a robust framework for information security management [6]. ISO/IEC 27001:2022 helps organizations manage their information security risks effectively through a systematic approach that encompasses people, processes, and IT systems.

Data protection requirements are becoming increasingly stringent worldwide. In Indonesia, the PDP Law mandates clear guidelines for obtaining consent, ensuring data subject rights, and promptly notifying authorities in case of data breaches. These requirements aim to enhance the protection of personal data and build public trust in the digital ecosystem. ISO/IEC 27001:2022, on the other hand, provides a comprehensive set of controls and processes for managing information security risks. Key elements include risk assessment, policy development, incident management, and continuous improvement [7]. These controls help organizations protect all types of information, not just personal data, ensuring a broad security posture.

Integrating the requirements of ISO/IEC 27001:2022 with the specific mandates of Indonesia's PDP Law can create a robust data protection framework. This integration ensures that organizations not only comply with local regulations but

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

also adhere to international best practices in information security management. By aligning these frameworks, organizations can achieve comprehensive compliance and enhanced security, effectively safeguarding personal data in Indonesia's burgeoning digital economy [8].

A closer look at ISO/IEC 27001:2022 reveals its emphasis on a systematic approach to managing information security risks [9]. The standard outlines a structured process for risk assessment and treatment, which includes identifying potential threats, assessing their impact and likelihood, and implementing appropriate controls to mitigate them [10]. This risk-based approach ensures that organizations prioritize their resources and efforts on the most significant risks, thereby enhancing their overall security posture [11].

The PDP Law complements this by providing specific legal requirements for data protection, such as obtaining explicit consent from data subjects before processing their personal data (Article 6), ensuring that data subjects have the right to access, correct, and delete their data (Article 25), and notifying authorities and affected individuals in the event of a data breach (Article 32). These provisions are designed to protect individuals' privacy and personal data, thereby building trust in the digital economy [12].

Despite the robust frameworks provided by ISO/IEC 27001:2022 and Indonesia's Personal Data Protection Law (PDP Law), significant gaps exist between these standards. These gaps can pose substantial challenges for organizations striving to achieve comprehensive data protection and compliance. ISO/IEC 27001:2022 focuses broadly on information security management systems, offering a wide array of controls and processes to manage various security risks. However, it may not fully address specific legal requirements unique to the PDP Law, such as explicit consent management and detailed data subject rights. Conversely, the PDP Law, while stringent in its mandates for personal data protection, may lack the comprehensive risk management approach embedded in ISO/IEC 27001:2022. This dichotomy creates a critical problem for organizations that must adhere to both standards, potentially leading to compliance issues and security vulnerabilities if only one framework is implemented. The primary purpose of this research is to bridge these gaps by developing an integrated framework that aligns the requirements of ISO/IEC 27001:2022 with the mandates of the PDP Law. This integration aims to ensure that organizations not only comply with local regulations but also follow international best practices in information security management, thereby achieving a holistic and robust data protection strategy.

Moreover, the PDP Law's requirements for data subject rights and breach notification can be incorporated into the incident management and continuous improvement processes defined by ISO/IEC 27001:2022. This ensures that organizations not only respond effectively to data breaches but also continuously

improve their data protection measures based on lessons learned from past incidents.

This paper is structured as follows. Firstly, it discusses the research background and problem. Secondly, it discusses the action design research method. Thirdly, it discusses the mapping of ISO/IEC 27001:2022 and the PDP Law using the integrated requirement engineering model. Finally, it discusses results before concluding with options for further research.

By integrating the requirements of ISO/IEC 27001:2022 with the mandates of Indonesia's PDP Law, organizations can create a comprehensive and effective data protection framework that enhances their security posture, ensures legal compliance, and builds trust in the digital economy. This integrated approach not only helps organizations protect personal data but also supports their overall information security objectives, thereby contributing to the growth and sustainability of Indonesia's digital economy.

2. METHODS

2.1. Research Methods

The primary focus of this research is to address the challenges associated with integrating ISO/IEC 27001:2022 with the Personal Data Protection (PDP) Law in the context of organizations operating in Indonesia. The main problem lies in aligning the requirements and processes of ISO/IEC 27001:2022, which is a comprehensive standard for information security management systems, with the specific provisions of the PDP Law, which regulates the collection, processing, and protection of personal data. In line with Action Design Research (ADR) methodology, this study adopts a structured approach to designing and implementing a solution to the identified problem [13]. The action phase involves several key steps [14].

First, an integrated approach to literature review is conducted to understand the requirements and principles of both ISO/IEC 27001:2022 and the PDP Law. This includes exploring academic research, industry publications, and regulatory guidelines to gain insights into best practices and challenges related to data protection compliance. Second, Qualitative Observations Study and Comparative Analysis to understand the practical challenges and integration points between ISO/IEC 27001:2022 and Indonesia's Personal Data Protection (PDP) Law. Third, Translation into Design based on the findings from the literature review and expert consultation, a structured framework or methodology is developed for integrating ISO/IEC 27001:2022 with the PDP Law. This framework outlines the steps, processes, and controls necessary to achieve compliance with both frameworks while addressing any potential conflicts or overlaps.

The evaluation phase focuses on assessing the effectiveness of the developed solution in addressing the integration challenges. Key activities include analyzing real-world case studies of organizations operating in Indonesia to apply the developed framework/methodology, collecting data throughout the implementation process, and analyzing the collected data to assess the effectiveness of the integrated approach in ensuring compliance with both ISO/IEC 27001:2022 and the PDP Law. In the reflection phase, the insights gained from the evaluation phase are reflected upon to refine the developed solution and provide recommendations for future research and practice. This includes reflecting on the successes and challenges encountered during the implementation process, using insights from the evaluation phase to refine the integrated framework/methodology, and providing recommendations for organizations looking to integrate ISO/IEC 27001:2022 with the PDP Law based on the lessons learned and refined solution.

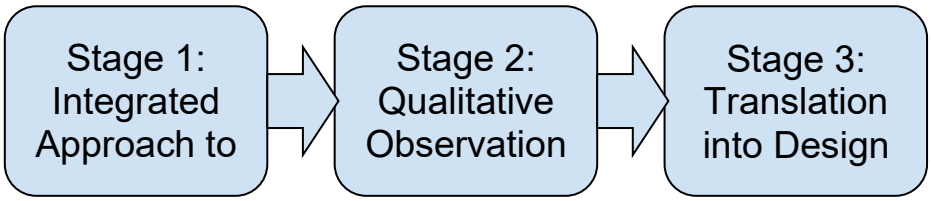

Figure 1. The Research Direction

2.2. Stage 1: Integrated Approach to Literature Review

The first stage of this research adopts an Integrated Approach to Literature Review (IALR) to comprehensively understand the existing frameworks and standards related to data protection and information security. The IALR method combines systematic literature review techniques with thematic analysis to ensure a thorough examination of relevant academic research, industry publications, and regulatory guidelines.

Once the relevant literature was collected, a thematic analysis was performed to identify common themes and gaps within the existing research. This analysis involved coding the literature to extract significant themes related to the integration of ISO/IEC 27001:2022 and the PDP Law. Key themes included risk management, data classification and handling, data subject rights, consent management, breach notification, and documentation and reporting. The thematic analysis helped in understanding how these themes are addressed in each framework and where overlaps or gaps exist.

The integrated literature review provided a robust foundation for the subsequent stages of the research [18]. It highlighted the need for a harmonized approach that bridges the gaps between ISO/IEC 27001:2022 and the PDP Law, ensuring that organizations can achieve comprehensive compliance and robust data protection. This stage also identified best practices and potential challenges that could inform the design of the integrated framework. By synthesizing insights from diverse sources, the IALR method ensured a well-rounded understanding of the subject matter, setting the stage for the development and implementation phases of the research.

2.3. Stage 2: Qualitative Observations Study and Comparative Analysis

The second stage of this research involves an in-depth Qualitative Observations Study and Comparative Analysis to understand the practical challenges and integration points between ISO/IEC 27001:2022 and Indonesia's Personal Data Protection (PDP) Law. A systematic comparative analysis maps the requirements and controls of ISO/IEC 27001:2022 against the PDP Law to identify overlaps, and gaps. Key areas of comparison include risk management, data classification and handling, consent management, data subject rights, breach notification, and documentation and reporting. The findings from this stage highlight specific integration challenges and inform the development of a harmonized framework that ensures comprehensive compliance and robust data protection.

2.4 Stage 3: Translation into Design

The final stage of this research is Translation into Design, where insights from the literature review and comparative analysis are synthesized into a cohesive, integrated framework. This framework is designed to bridge the gaps identified between ISO/IEC 27001:2022 and Indonesia's PDP Law, ensuring that organizations can comply with both local regulations and international standards effectively. The design process involves developing detailed guidelines and controls that align with both frameworks, addressing specific requirements such as risk management, data classification, consent management, data subject rights, breach notification, and documentation. By integrating these elements into a unified model, the framework provides a comprehensive approach to data protection and information security. This stage also includes iterative feedback from stakeholders to refine the design, ensuring practical applicability and addressing any emerging challenges. The resulting integrated framework aims to enhance organizational compliance, mitigate risks, and protect personal data within Indonesia’s rapidly growing digital economy.

3. RESULTS AND DISCUSSION

3.1. Overview of Indonesia's Personal Data Protection Law

Indonesia's Personal Data Protection (PDP) Law, enacted to safeguard individuals' personal data, marks a significant milestone in the country's efforts to regulate data privacy and security. The law, officially known as Law No. 11 of 2020 concerning Information and Electronic Transactions (UU ITE), introduces comprehensive provisions governing the collection, processing, storage, and transfer of personal data by both public and private entities [16]. At its core, the PDP Law aims to protect individuals' rights to privacy and data protection while fostering trust in digital transactions and promoting innovation in the digital economy. It establishes clear guidelines for the handling of personal data, ensuring transparency, accountability, and fairness in data processing activities.

Key provisions of the PDP Law include requirements for obtaining consent from data subjects prior to collecting and processing their personal data, as well as obligations to inform data subjects of the purposes and methods of data processing. The law also grants data subjects rights to access, rectify, and erase their personal data, empowering individuals to exercise control over their personal information. One of the notable aspects of the PDP Law is its extraterritorial application, which extends its jurisdiction to foreign entities that process personal data of individuals located in Indonesia. This provision reflects Indonesia's commitment to aligning its data protection standards with international norms and ensuring consistency with global privacy regulations.

Enforcement mechanisms outlined in the PDP Law include sanctions for non-compliance, such as fines, temporary suspension of operations, and criminal penalties for egregious violations. The law also establishes the Indonesian Personal Data Protection Authority (Badan Perlindungan Data Pribadi or "BPDP") tasked with overseeing compliance, handling complaints, and promoting awareness of data protection issues [15]. While the PDP Law represents a significant step forward in protecting individuals' privacy rights, its implementation poses various challenges for organizations operating in Indonesia. Compliance with the law requires comprehensive data governance frameworks, robust security measures, and ongoing monitoring and assessment of data processing activities.

Overall, the PDP Law reflects Indonesia's commitment to modernizing its legal framework to address the evolving challenges of data privacy and security in the digital age. By adhering to its provisions and adopting best practices in data protection, organizations can foster trust, mitigate risks, and unlock the full potential of Indonesia's digital economy.

3.2. Overview of ISO/IEC 27001:2022

ISO/IEC 27001 is referred to as the leading international standard for information security management [16]. ISO/IEC 27001:2022, the latest version of the International Organization for Standardization's (ISO) Information Security Management System (ISMS) standard, provides a globally recognized framework for organizations to establish, implement, maintain, and continually improve their information security management systems. In Indonesia, ISO/IEC 27001:2022 holds significant relevance as organizations seek to strengthen their cybersecurity posture and ensure compliance with regulatory requirements. The adoption of ISO/IEC 27001:2022 in Indonesia is driven by various factors, including the growing threat landscape, increasing digitization, and the need to protect sensitive information from cyber threats and data breaches. With the country's expanding digital economy and the proliferation of online transactions, organizations face heightened risks associated with unauthorized access, data theft, and malicious activities.

ISO/IEC 27001:2022 provides a systematic approach to managing information security risks, encompassing people, processes, and technology. Its principles-based approach enables organizations to tailor security controls and measures to their specific needs and risk profiles, fostering flexibility and scalability in implementation. By adopting ISO/IEC 27001:2022, organizations in Indonesia can demonstrate their commitment to protecting sensitive information, enhancing customer trust, and mitigating the impact of security incidents. The implementation of ISO/IEC 27001:2022 in Indonesia requires careful planning, resource allocation, and commitment from organizational leadership. It involves various stages, including risk assessment, policy development, implementation of security controls, and ongoing monitoring and review. Organizations must also ensure compliance with local regulations, industry standards, and contractual obligations while aligning their ISMS with ISO/IEC 27001:2022 requirements. ISO/IEC 27001:2022 certification offers tangible benefits for organizations operating in Indonesia, including improved cybersecurity resilience, enhanced competitiveness, and expanded market opportunities. Certified organizations gain a competitive edge in the marketplace, as ISO/IEC 27001:2022 certification serves as a testament to their commitment to information security best practices and compliance with international standards.

In Indonesia, government agencies, financial institutions, healthcare providers, and other critical infrastructure sectors are increasingly recognizing the importance of ISO/IEC 27001:2022 certification in safeguarding sensitive information and ensuring business continuity. Regulatory bodies may also reference ISO/IEC 27001:2022 requirements in their guidelines and directives, further incentivizing organizations to pursue certification. As organizations in Indonesia navigate the complexities of information security management and regulatory compliance,

ISO/IEC 27001:2022 serves as a valuable tool for addressing emerging threats, enhancing cybersecurity resilience, and fostering a culture of continuous improvement. By embracing ISO/IEC 27001:2022, organizations can proactively manage information security risks and safeguard their digital assets in an increasingly interconnected and data-driven world.

3.3. ISO/IEC 27001:2022 - PDP Law Mapping

The mapping of ISO/IEC 27001:2022 and PDP law was done to highlight the gaps and overlaps between the two as follows:

3.3.1 ISO/IEC 27001:2022 -PDP Law Gaps

As organizations strive to bolster their data protection measures in an increasingly digitized world, the integration of global standards such as ISO/IEC 27001:2022 with local regulations like Indonesia's Personal Data Protection (PDP) laws presents a formidable challenge. While ISO/IEC 27001:2022 provides a comprehensive framework for information security management systems (ISMS), PDP laws impose specific requirements for the protection of personal data, necessitating alignment between these two regulatory regimes. In this context, a critical examination of the gaps between ISO/IEC 27001:2022 and PDP laws is essential to identify discrepancies, inconsistencies, and areas of divergence that may hinder organizations' efforts to achieve comprehensive data protection compliance.

Tabel 1. ISO/IEC 27001:2022 -PDP Law Gaps

Point Gap	ISO/IEC 27001:2022	PDP Law
Scope and Focus	Clause 4.3 delineates the boundaries and objectives of the Information Security Management System (ISMS) within an organization, encompassing organizational units, information assets, business processes, and external parties. This scope directs attention to critical areas for protection and management. In tandem, ISO/IEC 27001:2022 emphasizes a risk-based	Article 4 typically defines key terms and concepts used throughout the legislation. These definitions help provide clarity and consistency in interpreting and applying the provisions of the law. While the specific contents of Article 4 may vary depending on the jurisdiction and the specific data protection law in question, it commonly includes definitions for terms such as "personal

Point Gap	ISO/IEC 27001:2022	PDP Law
	approach to security (Clause 6.1), comprehensive control implementation from Annex A (Clause 6.1.3), compliance with legal and regulatory requirements (Clause 6.1.3), and continuous improvement (Clause 10)	data," "data controller," "data processor," "processing," "consent," "data subject," "sensitive personal data," and other relevant terms.
Data Classification and Handling	Not clearly define, but state about information classification (annex 5.12 and 5.34)	Article 17 outlines the obligations of Personal Data Controllers in the processing of personal data, which inherently includes aspects of data classification and handling. While it does not explicitly mention "data classification," the article mandates that controllers process personal data fairly and transparently, ensuring it is used for legitimate, specific, and explicit purposes. Controllers must ensure the accuracy of the data, taking steps to rectify or delete incorrect information, and implement appropriate technical and organizational measures to secure data against unauthorized or unlawful processing, accidental loss, destruction, or damage.
Consent Management	Does not have a specific clause dedicated to consent management for personal data processing, organizations typically	Article 6 focuses on the principles surrounding the consent of data subjects for the processing of their personal data. This article

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Point Gap	ISO/IEC 27001:2022	PDP Law
	address consent management within the broader context of risk assessment (Clause 6.1.1), control implementation (Clause 6.1.3), and compliance with legal and regulatory requirements (Clause 6.1.3).	stipulates that personal data can only be processed with the explicit consent of the data subject, ensuring that the consent is given freely, specifically, and informed. It emphasizes that the consent must be obtained prior to the processing and must be documented as proof.
Data Subject Rights	does not provide specific guidance on fulfilling data subject rights	Article 25 outlines the rights of data subjects regarding their personal data. This article grants data subjects several key rights, including the right to access their personal data, the right to correct inaccurate or incomplete data, and the right to request the deletion or destruction of their data under certain conditions. Additionally, data subjects have the right to withdraw their consent for data processing and to object to or restrict the processing of their personal data. Article 25 also provides data subjects with the right to data portability, allowing them to obtain and reuse their personal data across different services.
Breach Notification	does not provide detailed guidance on breach notification procedures, it emphasizes the importance of incident management and	Article 32 addresses the obligations of Personal Data Controllers regarding breach notification. This article mandates that in the event

Point Gap	ISO/IEC 27001:2022	PDP Law
	reporting. Clause 10.2 requires organizations to establish, implement, maintain, and continually improve a process for incident management, including incident detection, reporting, assessment, and response.	of a personal data breach, the data controller must notify the affected data subjects and the relevant authorities without undue delay. The notification must include detailed information about the nature of the breach, the personal data affected, the potential consequences, and the measures taken or proposed to address the breach and mitigate its adverse effects. Article 32 aims to ensure transparency and prompt communication, enabling affected individuals to take necessary precautions to protect themselves and allowing authorities to take appropriate actions to oversee compliance and enforce data protection regulations. This requirement helps to maintain trust and accountability in the management and protection of personal data.
Documentation and Reporting	Clause 7.5 of ISO 27001:2022 requires organizations to establish, implement, maintain, and continually improve documented information to support the operation of the ISMS.	Article 15 pertains to the obligations of Personal Data Controllers regarding documentation and reporting. This article requires that Personal Data Controllers maintain comprehensive records of all data processing activities under their responsibility.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Point Gap	ISO/IEC 27001:2022	PDP Law
		The documentation must include details such as the purposes of data processing, descriptions of the categories of personal data and data subjects, the recipients to whom personal data have been or will be disclosed, and the period for which the personal data will be stored.

The integration of ISO/IEC 27001:2022 and Indonesia's Personal Data Protection Law (PDP Law) highlights several gaps and complementary strengths that organizations must address to ensure comprehensive data protection and information security. ISO/IEC 27001:2022 provides a robust framework for managing information security through a risk-based approach, emphasizing the need for continuous improvement and compliance with regulatory requirements. Its scope includes defining the boundaries and objectives of the Information Security Management System (ISMS) and implementing extensive controls to manage risks effectively. However, the ISO standard does not explicitly address some critical areas covered by the PDP Law. For instance, while ISO/IEC 27001:2022 implicitly involves consent management within its broader risk assessment and compliance framework, it lacks detailed guidelines for obtaining and managing consent from data subjects. The PDP Law fills this gap with Article 6, which mandates explicit, informed consent for personal data processing, ensuring that data subjects have control over their information.

Similarly, ISO/IEC 27001:2022 's emphasis on incident management and reporting (Clause 10.2) does not provide detailed breach notification procedures. In contrast, Article 32 of the PDP Law requires prompt notification of data breaches to affected individuals and relevant authorities, ensuring transparency and enabling protective measures. This specificity is crucial for maintaining trust and accountability in data handling practices. Moreover, while ISO/IEC 27001:2022 mandates the maintenance of documented information to support the ISMS (Clause 7.5), it does not detail the comprehensive record-keeping required by Article 15 of the PDP Law. The PDP Law necessitates detailed records of all data processing activities, including purposes, data categories, recipients, and retention periods. This extensive documentation supports transparency, regulatory compliance, and the protection of data subject rights, as outlined in Article 25.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

3.3.2 ISO/IEC 27001:2022 -PDP Law Overlaps

While ISO/IEC 27001:2022 and Indonesia's Personal Data Protection Law (PDP Law) each have their distinct focuses, there are several areas where they overlap, providing complementary guidance for organizations seeking to ensure comprehensive information security and data protection.

Both ISO/IEC 27001:2022 and the PDP Law emphasize the importance of implementing security controls to protect personal data. ISO/IEC 27001:2022 requires organizations to conduct risk assessments (Clause 6.1) and apply appropriate controls from Annex A to mitigate identified risks. Similarly, the PDP Law requires Personal Data Controllers to implement technical and organizational measures to secure personal data against unauthorized or unlawful processing, accidental loss, destruction, or damage (Article 17). This overlap ensures that organizations adopt a thorough approach to managing risks and protecting data.
ISO/IEC 27001:2022 mandates compliance with applicable legal and regulatory requirements related to information security (Clause 6.1.3). The PDP Law, as a specific regulatory requirement in Indonesia, provides detailed provisions for protecting personal data, such as obtaining consent (Article 6), ensuring data accuracy (Article 17), and notifying authorities in case of a breach (Article 32). Organizations operating in Indonesia must comply with both ISO/IEC 27001:2022 and the PDP Law, making this overlap crucial for ensuring legal compliance.

Both standards emphasize the importance of maintaining detailed documentation. ISO/IEC 27001:2022 requires organizations to establish, implement, maintain, and continually improve documented information to support the ISMS (Clause 7.5). The PDP Law complements this by requiring comprehensive records of all data processing activities (Article 15), including the purposes of processing, categories of personal data, and retention periods. This alignment ensures that organizations have thorough and accessible records to demonstrate compliance and support accountability.

ISO/IEC 27001:2022 encourages a culture of continuous improvement through its requirement for regular review and updates of the ISMS (Clause 10). This involves monitoring, measuring, analyzing, and evaluating the effectiveness of security controls and practices. Similarly, the PDP Law requires organizations to keep their data protection measures up to date and responsive to new risks and regulatory changes. This overlap reinforces the need for organizations to remain vigilant and proactive in their data protection efforts.

The overlaps between ISO/IEC 27001:2022 and Indonesia's PDP Law provide a solid foundation for organizations to build a comprehensive information security and data protection framework. By leveraging the complementary aspects of both

standards, organizations can ensure they meet high standards of security and compliance, ultimately protecting personal data and maintaining the trust of stakeholders. Recognizing and addressing these overlaps allows organizations to streamline their efforts, avoid duplication, and create a cohesive strategy for managing information security and data protection effectively.

3.3.3 ISO/IEC 27001:2022 -PDP Requirements Integration

Integrating the requirements of ISO/IEC 27001:2022 with Indonesia's Personal Data Protection Law (PDP Law) presents a comprehensive approach to ensuring robust data protection and information security within organizations. This integration involves harmonizing the risk-based methodologies and controls of ISO 27001 with the specific legal requirements and data protection principles outlined in the PDP Law.

The cornerstone of ISO/IEC 27001:2022 is its risk-based approach to managing information security. Organizations are required to conduct thorough risk assessments (Clause 6.1) to identify potential threats and vulnerabilities to their information assets. This process involves evaluating the likelihood and impact of various risks and implementing appropriate controls from Annex A to mitigate them. Integrating PDP Law into this framework enhances the risk management process by incorporating specific data protection risks. For example, compliance with PDP Law requires organizations to consider risks associated with personal data processing, such as unauthorized access, data breaches, and non-compliance with consent requirements (Article 6). By aligning these risk assessments, organizations can develop a more holistic understanding of their security landscape and implement more targeted and effective controls.

ISO/IEC 27001:2022 provides a comprehensive set of controls in Annex A that cover various aspects of information security, including access control, cryptography, and incident management. When integrating PDP Law requirements, organizations must pay particular attention to controls that address data protection directly. For instance, PDP Law mandates specific measures for ensuring data accuracy, protecting sensitive personal data, and providing data subjects with rights to access, correct, and delete their data (Articles 17 and 25). Organizations can enhance their ISMS by incorporating these legal requirements into their control environment, ensuring that both security and data protection needs are met. This integration ensures that personal data is processed in compliance with legal standards while maintaining the integrity and confidentiality of all information assets.

Documentation and reporting are critical components of both ISO/IEC 27001:2022 and PDP Law. ISO/IEC 27001:2022 requires organizations to maintain documented information to support the operation of the ISMS (Clause

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

7.5), including policies, procedures, and records of security incidents. PDP Law extends these requirements by mandating comprehensive records of data processing activities (Article 15). This includes details on the purposes of processing, categories of data, data subjects, recipients, and retention periods. By integrating these documentation requirements, organizations can create a unified and comprehensive record-keeping system that meets both security and data protection obligations. This consistency not only aids in demonstrating compliance during audits but also enhances transparency and accountability in data handling practices.

Effective incident response is crucial for both ISO/IEC 27001:2022 and PDP Law compliance. Clause 10.2 of ISO/IEC 27001:2022 requires organizations to establish, implement, and continually improve an incident management process, including incident detection, reporting, assessment, and response. PDP Law complements this by stipulating specific breach notification requirements (Article 32). In the event of a personal data breach, organizations must promptly notify affected data subjects and relevant authorities, providing detailed information about the breach and measures taken to mitigate its impact. Integrating these requirements ensures that organizations can respond swiftly and effectively to security incidents, minimizing potential harm to individuals and maintaining regulatory compliance.

Both ISO/IEC 27001:2022 and PDP Law emphasize the importance of continuous improvement. ISO/IEC 27001:2022 requires organizations to regularly review and update their ISMS to address new threats and vulnerabilities (Clause 10). Similarly, PDP Law mandates that data protection measures be regularly reviewed and updated to reflect changes in the legal and regulatory landscape. By integrating these continuous improvement processes, organizations can ensure that their information security and data protection practices remain current and effective. This proactive approach helps organizations stay ahead of evolving threats and regulatory requirements, thereby enhancing their overall resilience and compliance posture.

Integrating the requirements of ISO/IEC 27001:2022 with Indonesia's PDP Law provides a comprehensive framework for managing information security and data protection. By harmonizing risk management methodologies, enhancing data protection controls, maintaining consistent documentation, and establishing robust incident response procedures, organizations can achieve a high standard of security and compliance. This integrated approach not only safeguards personal data but also builds trust with stakeholders, ensuring that information assets are protected in accordance with both international standards and local legal requirements.

4. CONCLUSION

The integration of ISO/IEC 27001:2022 with Indonesia's Personal Data Protection (PDP) Law represents a significant step towards establishing a robust data protection framework that aligns international standards with local regulatory requirements. This comprehensive approach ensures that organizations operating in Indonesia can achieve both compliance with local laws and adherence to global best practices in information security management.

ISO/IEC 27001:2022 provides a systematic framework for managing information security risks through its detailed requirements for risk assessment, incident management, and continuous improvement. However, the standard does not cover specific areas such as explicit consent management, detailed breach notification procedures, and extensive record-keeping, which are crucial components of the PDP Law. The PDP Law complements ISO 27001:2022 by providing explicit guidelines for these areas, ensuring a more holistic approach to data protection.

By mapping the requirements of ISO/IEC 27001:2022 with the PDP Law, organizations can address potential overlaps and gaps. For instance, while ISO/IEC 27001:2022 emphasizes risk management and regulatory compliance, the PDP Law mandates specific actions such as obtaining explicit consent (Article 6), notifying authorities and data subjects in case of a breach (Article 32), and maintaining detailed records of data processing activities (Article 15). This alignment helps organizations ensure that they are not only secure but also legally compliant, fostering trust and accountability in their data handling practices.

In conclusion, the integration of ISO/IEC 27001:2022 and Indonesia's PDP Law is essential for organizations aiming to protect personal data effectively. This combined framework not only enhances security and compliance but also supports the growth of Indonesia's digital economy by ensuring that data protection measures meet both international and local standards. Future research and continuous improvement efforts are necessary to adapt to evolving data protection challenges and maintain high standards of information security and privacy.

REFERENCES

[1] V. Hooper and J. McKissack, "The emerging role of the CISO," *Business Horizons*, vol. 59, no. 6, pp. 585-591, 2016.
[2] M. Monica, D. Kurniawan, and R. Prabowo, "Analisis Manajemen Risiko Sistem Informasi Pengelolaan Data English Proficiency Test (EPT) dan Portal Informasi di UPT Bahasa Universitas Lampung Menggunakan

Metode ISO 31000," *J. Komputasi*, vol. 8, no. 1, pp. 83–90, 2020, doi: 10.23960/komputasi.v8i1.2351.

[3] D. Anjeli, S. T. Faulina, and A. Fakih, "Sistem Informasi Perpustakaan Sekolah Dasar Negeri 49 OKU Menggunakan Embarcadero XE2 Berbasis Client Server," *J. Inform. dan Komput.*, vol. 13, no. 2, pp. 57–66, 2022.

[4] C. A. Makridis, "Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018," *Journal of Cybersecurity*, vol. 7, no. 1, p. tyab021, 2021.

[5] S. N. V. Schweizerische, "Information technology-Security techniques-Information security management systems-Requirements," *ISO/IEC International Standards Organization*, 2013.

[6] E. Lachaud, "ISO/IEC 27701 standard: Threats and opportunities for GDPR certification," *Eur. Data Prot. L. Rev.*, vol. 6, p. 194, 2020.

[7] Y. I. Alzoubi, A. Q. Gill, and A. Al-Ani, "Distributed Agile Development Communication: An Agile Architecture Driven Framework," *J. Softw.*, vol. 10, no. 6, pp. 681-694, 2015.

[8] M. J. Anwar, A. Q. Gill, and G. Beydoun, "A review of information privacy laws and standards for secure digital ecosystems," *in ACIS 2018-29th Australasian Conference on Information Systems*, 2018, pp. 1-10.

[9] G. Bou Ghantous and A. Gill, "DevOps: Concepts, practices, tools, benefits and challenges," *PACIS2017*, 2017, pp. 1-12.

[10] A. M. Algarni and Y. K. Malaiya, "A consolidated approach for estimation of data security breach costs," *in 2016 2nd International Conference on Information Management (ICIM)*, 2016, pp. 26-39.

[11] A. S. Sudarwanto and D. B. B. Kharisma, "Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia," *Journal of Financial Crime*, vol. 29, no. 4, pp. 1443-1457, 2022.

[12] Republic of Indonesia, "Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi," *Indonesian Government*, 2022.

[13] City of New York, Active Design Guidelines, 2010.

[14] City of North Vancouver, Active Design Guidelines, 2015.

[15] A. Aptika, "Teguh: Amanat UU, Presiden Tetapkan lembaga OTORITAS PDP," *Ditjen Aptika*, 24-Oct-2022.

[16] H. Susanto, M. N. Almunawar, and Y. C. Tuan, "Information security management system standards: A comparative study of the big five," *International Journal of Electrical Computer Sciences IJECSIJENS*, vol. 11, no. 5, pp. 23-29, 2011.

[17] Republic of Indonesia, "Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," 2022.

[18] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Computers & Security*, vol. 38, pp. 97-102, 2013.