Scientific Journal of Informatics
Vol. 12, No. 1, Feb 2025
p-ISSN 2407-7658 https://journal.unnes.ac.id/journals/sji/index e-ISSN 2460-0040

Evaluating ISO Standards for Indonesian PDP Law Compliance: A Regulatory Mapping and Literature Review

Egriano Aristianto[1*], Muhammad Hafizhuddin Hilman[2], Setiadi Yazid[3]
[1, 2, 3]Faculty of Computer Science, Universitas Indonesia, Indonesia

Abstract.
Purpose: This paper aims to demonstrate how ISO standards such as ISO/IEC 27001:2022, ISO/IEC 27002:2022, and ISO/IEC 27701:2019 can assist Indonesian organizations in facilitating compliance with the Personal Data Protection (PDP) Law. It highlights the challenge organizations face due to the lack of clear guidance in the law, then shows how these ISO standards can guide them to achieve the compliance. The study also maps the regulation's requirements and how that requirements can be fulfilled by certain approaches provided by the standards and offers a clearer path toward full compliance.
Methods: This research employs a qualitative approach, combining a literature review, document analysis, and comparative assessment. It provides systematic Indonesian PDP Law-ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27701 mapping, an analysis of their alignment, a gap analysis, and how these standards able to demonstrate compliance to Indonesian PDP Law.
Result: This study shows that from 14 mandatory requirement topics of Indonesian PDP Law that have been mapped, The ISO/IEC 27001:2022 only able to cover 1 topic, while ISO/IEC 27002:2022 able to provide controls to accommodating 8 topics and ISO/IEC 27701:2019 able to provide controls to accommodating 13 topics. But by combining these standards, then all of mandatory requirements of Indonesian PDP Law can be satisfied.
Novelty: This study shows how international standards like ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27701 would help organize compliance to the Indonesian PDP Law while also strengthening data protection practices in Indonesia.

Keywords: Indonesian personal data protection law, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27001, Regulatory compliance, Information security, Data privacy
Received February 2025 / **Revised** May 2025 / **Accepted** May 2025

INTRODUCTION

Cybersecurity is a very important aspect of every organization across the world today [1], [2]. When the General Data Protection Regulation (GDPR) went into effect in the European Union in 2018, it set a new standard for data privacy that includes stringent protections for how personal data is processed, stored, and secured [3], [4]. The organizations of various sectors are adopting their information security practices to comply with the GDPR requirements in this context, especially the organizations that deal with sensitive data [5], [6]. In Indonesia itself, similar regulations were enacted in 2022. The "Undang-Undang Nomor 27 Tahun 2022" concerns personal data protection (PDP Law). The regulation aims to safeguard personal data within the digital ecosystem that poses significant risks, including data breaches, cyber-attacks, and misuse of personal information. [7], [8], [9], [10]. On the contrary, as with the new regulations, organizations face some challenges in their attempt to comply with them [11], [12], similar to how the organization in the EU went through trying to comply with GDPR at its early release [5], [13], [14]. One of the main problems that typically arises when organizations initiate the process to achieve compliance with the regulation is not knowing the modalities of how they are going to comply with the regulation since no thorough documentation exists on how to comply [5], [6], [7], [13], [15].

The Indonesian PDP Law represents a significant transition towards regulating data in a manner that is globally compliant, such as with GDPR [16], [17], [18]. Despite these similarities in the legal objectives of the GDPR and in the Indonesian PDP Law, there are very notable differences in their implementations and enforcement, which will cause significant stumbling blocks to meet the local requirements based on

*Corresponding author.
Email addresses: egriano.aristianto@ui.ac.id (Aristianto)*, muhammad.hilman@ui.ac.id (Hilman), setiadi@cs.ui.ac.id (Yazid)
DOI: 10.15294/sji.v12i1.21538

international standards for Indonesian organizations [19], [20], [21]. Unlike the GDPR, the Indonesian PDP Law does not have detailed implementation guides [7], [19], [20].

There are notable standards such as ISO/IEC 27001, which outlines Information Security Management Systems (ISMS) [22], ISO/IEC 27002, which provides the information security controls [23], and ISO/IEC 27701 which covers Privacy Information management system (PIMS)[24]. Several studies show that implementing ISO standards such as ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27701 can help to comply with GDPR [6], [25], [26]. Hence, by adopting comprehensive information security and privacy framework from these standards that provide structured and risk-based approaches to managing information security and privacy, organization can enhance their information security and privacy practice to fulfil both the explicit and implicit requirements of the PDP Law [5], [6], [7], [25], [26].

But due the particular needs for the law, such as in Indonesian PDP Law, it needs to draw carefully the mapping of these ISO standards to the national regulations, to analyze potential gaps in compliance and correct them [6], [7], [25]. In this regard, it needs to defined on how extent these ISO standards able to accommodate the requirements of Indonesian PDP Law, to figure out whether these standards are fully satisfy the requirements or there are some gaps that need to be sorted out.

This study seeks to fill the gap by conducting qualitative research that follows these research questions:
1. To what extent do ISO Standards fulfill the requirements of the Indonesian Personal Data Protection Law?
2. How do ISO Standards help an organization to ensure compliance with the Indonesian PDP Law?

By comparing the framework with Indonesian PDP law, this research maps in detail specific controls of ISO/IEC 27001:2022, ISO/IEC 27002:2022, and ISO/IEC 27701:2022, and the requirements of Indonesian regulation. Overall, this research is aimed at giving practical insight and guidance for Indonesian organizations to implement as an adoption of the ISO/IEC 27001:2022, ISO/IEC 27002:2022, and ISO/IEC 27701:2022 measures to create an escalated organization data protection strategy and align them to create regulatory compliance.

RELATED WORKS

In the field of Information Systems, regulatory compliance refers to an organization's ability to design and operate technological and procedural systems in accordance with external laws, policies, and standards that govern data and system behavior [27]. This includes ensuring that information systems implement technical, administrative, and organizational controls to satisfy legal obligations related to data protection, security, and governance[27]. Regulatory compliance in Information System is not only a legal concern but also a socio-technical challenge involving system design, risk assessment, control implementation, and continuous auditability [27].

Several studies [6], [15], [28], [29] have taken some approach to examining the key provisions of the Data Protection Regulation to gain an understanding of the compliance requirements, and it shows that the practical manifestations of compliance measures can differ across sectors. For instance, by examining a detailed legal and security analysis to map key requirements to on-the-ground processes, facilitating the effective understanding and implementation of GDPR-compliant practices [6], [28], [29]. Similarly, Lakshmi et al. [15] employed the same techniques to evaluate the need for GDPR compliance in the mobile banking industry by conducting legal and security analysis, where they map and compare relevant mobile banking security practices with critical GDPR provisions, such as data subject rights, consent management, and encryption. However, these studies [6], [15], [28], [29] show that organizations must extend their strategy beyond just meeting regulatory requirements and implement appropriate security frameworks to become GDPR compliant by filling gaps and reducing inconsistencies.

ISO/IEC 27001 has become most widely regarded as a base ISF that helps organizations meet compliance requirements under different data protection regulations (e.g., GDPR and equivalent global standards) [6], [30], [31]. The popularity of ISO/IEC 27001 is in part due to its structured, risk-based approach to information security management that is aligned with regulatory compliance [30], [31], [32]. ISO 27001 assists organizations in understanding the requirements for establishing and maintaining an Information Security Management System (ISMS) and helps them meet relevant regulations [6], [33]. But, implementing that standard without any additional enhancements, may leave organizations vulnerable to

non-compliance [26], [30]. Similar with that, Nugraha et al. [7], in line with Indonesian PDP Law studied the combination of ISO/IEC 27001 with the country PDP Law, their research concluded that ISO 27001 has provided a general alignment with the data protection regime in Indonesia, but there are some significant areas that remain unclear and still require further effort to comply with the detail of legal obligations. Although ISO 27001 tends to lay down a solid baseline for security, it requires additional tailoring to be relevant to the regulation such as GDPR or Indonesian PDP Law, which highlights the need to adapt security frameworks in accordance with region tools and legal requirements [7], [26].

Next, ISO/IEC 27002 is a guide that complements the ISO/IEC 27001 standard by providing specific guidance on security controls that bind directly to the requirements defined in ISO/IEC 27001 [6], [34]. Through their study, Diamantopoulou et al. discussed how ISO 27002 extends ISO 27001 by took a two-phase approach to identify and map the security controls outlined in ISO 27002 to the proceedings described within GDPR that ISO 27001 does not completely capture, including those related to data subject rights, breach notification, and consent management, and they conclude that ISO 27002 can assist organizations with more directly addressing these regulatory needs by implementing the controls it describes [6]. Diamantopoulou et al. mentioned that ISO/IEC 27002 provides more granular breakdown of specific security controls that includes practical recommendations for managing access controls, encryption, and data integrity, which are critical for protecting personal data and can be applied during system design and development phases, making it easier for organizations to implement Privacy by Design principles, which it is a core requirement in GDPR and similar regulations [6]. Diamantopoulou et al. concluded that ISO 27002 supports ISO 27001 and significantly helps organizations to improve their ISMS framework, thus making it easier to fulfill the exact requirements of data protection regulations [6].

Lastly, the ISO/IEC 27701:2019 is a privacy-focused extension of ISO 27001 and ISO 27002 that helps organizations manage personal data responsibly by providing a framework called the Privacy Information Management System (PIMS), which supports organizations in protecting personal data and aligning with laws like the GDPR or similar regulations worldwide [25], [35]. The standard promotes a risk-based approach to managing privacy, focusing on protecting data confidentiality, availability, and integrity [25]. It also introduces practical processes for handling personal data, such as managing user requests, defining data retention limits, and ensuring privacy across international transfers [35]. ISO 27701 can be a useful tool to help organizations demonstrate compliance with privacy laws and gives businesses a structured and internationally recognized way to manage privacy [25].

RESEARCH METHODOLOGY

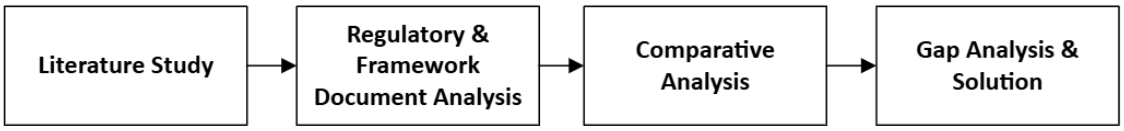

Figure 1. Research methodology flow diagram

This research employs a qualitative approach that includes a literature review, document analysis, and comparative analysis to determine how ISO/IEC 27001 and ISO/IEC 27002 align with the Indonesian Personal Data Protection (PDP) Law and to identify their comparison with the GDPR. This approach provides a comprehensive foundation for assessing how these frameworks can facilitate compliance with Indonesian regulations.

Literature study

The search strategy focuses on finding relevant literature that discusses how ISO Standards in relation to regulatory compliance of PDP regulation, including the GDPR, and how to do the comparative analysis between these standards with the regulation to find out how these standards able to assist organizations in achieving compliance with the PDP regulation.

Key search terms included in these steps are "ISO", "GDPR compliance," "personal data protection law," and "Indonesia PDP Law". Based on these keywords, the search is enhanced with Boolean Operators to refine the search results, ensuring relevance to the research questions [36]. In this research, the Boolean Operators that are being used are '("GDPR" OR "personal data protection" OR "Indonesian PDP") AND

("compliance" OR "regulatory" OR "law") AND ("support" OR "assist" OR "guidance") AND ("controls" OR "framework" OR "ISO")'

The search process was then filtered using the inclusion and exclusion criteria outlined in Table 1

Table 1. Inclusion & exclusion criteria

Inclusion Criteria	Exclusion Criteria
- Articles published since 2020	- Article published before 2020
- Articles in English Language	- Non-English Articles
- Articles that are relevant to the research questions	- Articles that are out of the scope of the research questions
- Articles that focus on the application of the ISFs in the context of data protection law	- The article is not focused on the application of the ISFs in the context of data protection law

The search included several research databases (Emerald Insight, IEEE Xplore, ScienceDirect, and SpringerLink) and indexer such as Google Scholar. The search results were first refined by inclusion-exclusion criteria and to the relevance of the articles to our research question. The literature identified from the initial review was analyzed in further detail to evaluate its relevance to the research focus. Then, the studies that addressed the alignment between data protection regulations and ISO Standards were prioritized to be referenced. After this analysis, the literatures that were gathered was then narrowed down to a final selection. This refined set of studies provides valuable insights into how ISO Standard can be leveraged to support organizations in compliance with data protection laws.

The collected literature was extracted and analyzed at this stage to gather relevant information, including data, methodology, and results, particularly concerning a regulatory framework such as GDPR and the Indonesian PDP Law. This was done by identifying the specific ISO Standards controls that were applied in each of the studies and comparing and assessing how these controls would align with the data protection requirements in regulations. The analysis focused on a thematic data classification, which was undertaken following extraction. This involved identifying themes that demonstrated how ISO standards aligned with the requirements of the Indonesian PDP Law and giving a fundamental understanding of how these two frameworks really do support compliance with local data protection regulation.

Regulatory & framework document analysis

In this step, a comprehensive document analysis was performed to systematically extract and map the key requirements of the Indonesian PDP Law and GDPR to understand the fundamental provisions. This analysis involved an in-depth examination of each regulation to pinpoint critical areas, including principles, data subject rights, data processing obligations, security and protection measures, and more. Furthermore, the study mapped the requirements of the Indonesian PDP Law against the specific controls and clauses within ISO/IEC 27001:2022, ISO/IEC 27002:2022, and ISO/IEC 27701:2019 frameworks. The mapping process was conducted using a clause-by-clause comparative technique, where each article of the Indonesian PDP Law was manually reviewed and interpreted to identify its underlying security or privacy principles. This approach draws from prior studies [6], [7], [15], [16], [28], [29] which demonstrates clause-by-clause comparative mapping between regulation and ISO standards. This mapping process enabled a structured outline of regulatory requirements in relation to the controls provided by the ISO standards.

Comparative analysis

This step is performed to assess the similarities and differences between the Indonesian PDP law and GDPR in order to analyze which provisions are covered in both of the laws and which elements are unique to each of them, with a final goal to assess both the common compliance needs determined by the two laws, as well as the distinct characteristics of Indonesian PDP law which may lead to the divergence in compliance strategies. The comparative construction of regulatory frameworks in information systems research draws from the tradition of legal-informatics and governance studies, where laws are analyzed in relation to technical frameworks to identify enforcement needs, structural gaps, or policy interoperability [5], [19]. This approach allows researchers to map abstract legal requirements into actionable security or privacy controls. By comparing the GDPR and Indonesia's PDP Law, this study seeks to understand regulatory convergence and divergence, and how these influence organizational compliance strategies [7], [19].

Subsequently, a thorough mapping of the PDP Law's provisions with regards to the ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27701 controls were conducted to identify which aspects of the law are

reflected by and supported through the given objectives and controls specified by the aforementioned standards and which provisions of the PDP Law lack coverage and controls [6], [7], [35]. This analysis highlighted where the ISO frameworks significantly align with PDP Law provisions as well as areas where further compliance steps or adjustments are needed. This comprehensive review provided insights into the strengths and weaknesses of the ISO frameworks as they relate to Indonesian PDP Law and has provided guidance to organizations as to where further controls may be required to achieve full compliance.

Gap analysis & solution

After mapping and comparing the Indonesian PDP Law with the ISO/IEC 27001:2022, ISO/IEC 27002:2022, and ISO/IEC 27701:2019 frameworks, this paper explores the gaps identified between the regulation and the frameworks. This review gives an overview of certain PDP Law requirements that are not fully fulfilled by controls of the ISO frameworks and therefore enables an in-depth assessment of the gaps. As a result, the steps described are actionable for your organization to reach full compliance with Indonesian regulations. These recommendations are based on former research [6], [26], including studies overlapping plans to close compliance gaps identified when comparing the ISO standards to GDPR's requirements. Through the utilization of these well-founded solutions, the work offers practical insights and organizational strategies that can help fill regulatory gaps, so organizations are successfully able to address the particular demands of the PDP Law and international security standards.

RESULTS AND DISCUSSIONS

Indonesia's PDP Law which was enacted with the Undang-Undang Nomor 27 Tahun 2022 on October 17, 2022, is intended to protect human rights in relation to personal data. This law safeguards personal data and protects the constitutional rights of data subjects. The law outlines the roles of parties managing personal data, data subjects' rights, the obligations of controllers and processors, regulations on the transfer of data, as well as sanctions for violations. Therefore, the presence of this regulation encourages organizations to comply with regulatory compliance.

Appendix A provided a detailed breakdown of PDP Law article topics and their classifications, it outlines explains the key aspects of the law for practical understanding with the law. It is classified by five categories which are:

1. Definitions that explain the basis for defining the provisions in the regulations
2. Mandatory Requirements is the requirements you need to comply with, such as having a DPO, conducting a DPIA, have an obligation to fulfill the rights of data subjects, and ensuring you have security measures to protect the data security and privacy.
3. Role of Government determines what the enforcement entities are there for.
4. Directions from the Government to explain what are the government's guidance & directions regarding this regulation.
5. Legal Consequences details the consequences, reinforcing the need for compliance. Which can be multiple kinds of penalties that may apply as a result when an organization does not comply with requirements.

The legal consequences that organizations will face make this compliance critical, alongside the risks regarding data security and privacy. The sanctions can be fines, lawsuits, and bans on data processing activities, depending on how serious the state of non-compliance is. Additionally, multiple or serious violations could lead to intensified scrutiny from regulatory agencies and even a decline in public confidence, which could threaten the organization's brand and its ability to do business [5], [7], [37].

1. Article 57: The PDP Law imposes administrative sanctions, starting from a written warning, suspension of the processing of personal data temporarily, deletion or destroying personal data, and/or fines in the form of 2% of revenue each year or acceptance of the annual variable violations.
2. Article 67:
   - Act 1: Anyone who intentionally and unlawfully obtains, collects, and uses personal data from others will be liable to a fine of Rp. 5 billion and/or a maximum prison sentence of 5 years.
   - Act 2: Intentional and unlawful disclosure of personal data of others will lead to a fine of Rp. 4 billion and/or a maximum prison.
   - Act 3: Anyone who intentionally and unlawfully falsifies personal data to harm oneself or another person, which may result in harm to the other person, will be liable to a fine of Rp. 5 billion and/or a maximum prison sentence of 5 years.

3. Article 68: Any organization that has interfered with the sanctity of the personal data collected to benefit itself or others will face a fine of up to Rp. 6 billion. The person most directly responsible for this will face a prison sentence of up to 6 years.
4. Article 69: The PDP Law also allows the confiscation of all profits and assets of an organization found guilty of the above-mentioned violations.

Furthermore, Appendix B describes the key differences and similarities between the GDPR and Indonesia's PDP Law, including but not limited to regulation about personal data definitions, rights of data subjects, obligations of controllers and processors, and notification of data breaches. Both the Indonesian PDP Law and the GDPR are created to protect personal data and people's privacy. They both cover key areas like how consent should be given, how to keep data safe, what rights individuals have, what to do when there's a data breach, and how data can be transferred across countries. So overall, they aim for the same thing: making sure people's personal data is treated fairly and responsibly.

But there are some clear differences in how the Indonesian PDP Law and the GDPR apply the rules and handle responsibilities. The Indonesian PDP Law includes several things that the GDPR doesn't directly mention, like what happens when a data controller organization changes (merges, splits, or shuts down), involving the public in policy-making, clearly listing actions that are strictly forbidden when using personal data, criminal penalties for serious violations, and a built-in two-year transition period for organizations to fully comply. GDPR doesn't cover those parts as directly in its main regulation. There are also some technical differences. For example, in the case of data subject rights, Indonesian law requires organizations to respond within 3 days, while GDPR gives up to one month. For administrative fines, Indonesia sets the maximum at 2% of annual income, while GDPR allows up to 4% of global turnover, which is much higher. And when it comes to special data processing rules, the Indonesian law gives extra attention to people with disabilities, while GDPR only explicitly mentions children. These differences showing that how each of the law is being shaped by its own local context, but both of it still working toward the same goal.

Then the analysis further the intersection of international standards ISO/IEC 27001:2022, ISO/IEC 27002:2022, and ISO/IEC 27701:2019 with the Indonesian PDP Law. These internationally recognized standards featuring robust information security and privacy frameworks were evaluated by comparing them with the PDP Law's mandatory requirements.

Table 2. Regulatory requirements and ISO framework comparison

Requirement	PDP Law Article Number	ISO/IEC 27001:2022	ISO/IEC 27002:2022	ISO/IEC 27701:2019
General Obligations of processing of Personal Data	Article 19-24	×	×	Clause 7.2.1, 7.2.2, 7.2.3, 7.2.4, 7.3.2, 7.3.3
Special Provisions for Data Processing	Article 25-26	×	×	Clause 7.2.2, 7.2.3, 7.3.3
Accountability and Record Keeping	Articles 27-33	×	×	Clause 7.2.1, 7.2.2, 7.2.8, 7.3.2, 7.3.3, 7.3.6, 7.3.8, 7.4.2
Conduct an impact assessment on personal data protection	Article 34	×	×	Clause 7.2.5
Security and Protection Measures	Articles 35-39	Clause 4-9	All clauses	Clause 5, 6 & 7.2.6
Rights of Data Subjects	Articles 40-45	×	Clause 8.10	Clause 7.3.4 & 7.3.6
Data Breach Notifications	Articles 46-47		Clause 5.5, 5.24, 5.25, 5.26	Clause 6.13
The Change of Data Controller Organization	Article 48	×	×	Clause 8.4.2 & 8.5.1
Obligatory to Comply with Regulatory Body	Article 49	×	Clause 5.31	Clause 6.15.1, 7.2.2, 8.2.1, 8.2.5, 8.3.1
Exceptions for Protection	Article 50	×	Clause 5.31	×
Obligations of Data Processors	Articles 51-52	×	×	Clause 7.2.6 & 8
Data Protection Officers	Articles 53-54	×	Clause 5.34	Clause 6.3.1.1
Transfer of Personal Data	Articles 55-56	×	Clause 5.14	Clause 7.2.7 & Clause 8.5
Prohibitions on the Use of Personal Data	Article 65-66	×	Clause 5.33, 5.34, 8.12	Clause 6.3.1, 7.2.1, 7.2.2, 7.4.1, 7.4.2, 8.5.5

Table 2 maps each Indonesian PDP Law requirement to ISO standards, noting alignments and identifying gaps, offering a clear view of how international practices support national legal directives. By that mapping, we can see that ISO/IEC 27701:2019 able to support most of mandatory requirements of Indonesian PDP Law, while ISO/IEC 27002:2022 able to just eight of fourteen mandatory requirements, and ISO/IEC

27001:2022 only covers one which it's about Security and Protection Measure. Section below explains further of how these ISO Standards able to support organization to satisfy the mandatory requirements of Indonesian PDP Law.

General obligations of processing of personal data

On article 19-24 Indonesian PDP Law it's requiring the organization to obtain an explicit consent in an agreement with the data subject to carry out the processing of personal data. This consent must match the actual purpose of collecting the data. The organization must explain the legal reason for collecting the data, what data is being collected, how long it will be kept, and what the person's rights are. The request must be written or recorded, easy to understand, and clearly explained. If the person doesn't agree, the organization isn't allowed to process the data. The organization must also keep proof that consent was given.

For these requirements, ISO/IEC 27701:2019 provides several guidance to help organizations create a proper system to handle consent the right way. Clauses 7.2.1 and 7.2.2 make sure the organization clearly defines why they are collecting personal data and that they have a legal reason to do it. Clauses 7.2.3 and 7.2.4 guide how to ask for permission and keep records of it. Then, Clauses 7.3.2 and 7.3.3 help the organization explain everything clearly to the person: what data is collected, for what purpose, how long it's stored, and what rights the person has. These steps make sure the person understands and provides consent to enable organization to process their data.

Special provisions for data processing

On article 25-26 Indonesian PDP Law it requires organization to give extra care when handling personal data of children and persons with disabilities. If they want to collect or use a child's personal data, they must get permission from the child's parent or legal guardian. For data subject with disabilities, consent should come directly from them if possible, or from their guardian if needed. Importantly, the way organizations ask for this permission must match the person's condition, by using a method that's respectful, understandable, and accessible.

To accommodate these requirements, ISO/IEC 27701:2019 provides some approach that organization can do that covered on Clause 7.2.2, 7.2.3, and 7.3.3. Clause 7.2.2 says that organizations must have a valid legal reason for processing personal data, which includes making sure consent is obtained properly. Then Clause 7.2.3 helps organizations figure out when and how they should ask for consent, so they can adjust their approach depending on the individual's condition, like using more accessible formats for data subject with disabilities. Lastly Clause 7.3.3 encourages organizations to clearly explain to the data subject (or their guardian) what the data is for, what their rights are, and what will happen to their data. This helps ensure that even those who need special protection, like children or people with disabilities, are informed and empowered before their data is processed.

Accountability and record keeping

On article 27-33 Indonesian PDP Law it underlining that organizations must only process personal data for clear and limited purposes, exactly what the person agreed to. The processing must be legal and transparent, and the data subject must be informed about what's being done with their data, in simple and understandable language. Organizations must also check that the data is accurate and complete, and if someone asks for corrections, they must update the data within three days and tell the person once it's done. Organizations are also required to keep a full record of all data processing activities. Finally, individuals have the right to access their data and see how it's been processed, unless access poses risks to others or national security.

ISO/IEC 27701:2019 controls making sure organizations only processing the personal data for valid reasons and based on what the subject data has agreed to. On Clause 7.2.1 and 7.2.2 ensuring organizations process personal data only for valid reasons that are clearly defined and communicated. Then on Clause 7.2.8 supports transparency by requiring records of data processing, which also makes it easier to show compliance. Then on Clause 7.3.2 and 7.3.3 help organizations explain in plain language what data is collected, how it's used, and what rights of data subject have, so communication is always clear and accessible. Next, Clause 7.3.6 ensures data subject can correct or erase their data and 7.3.8 guarantees they can access it, including its processing history. This action should be done within a reasonable timeframe. Lastly Clause 7.4.2 reinforces the idea that personal data must only be used for the original purpose and not

be misused. But for this requirement, organizations need to make sure that they comply with the SLA required by the regulation which is 72 hours to handling the subject data's request until it done.

Conduct an impact assessment on personal data protection
On article 34 Indonesian PDP Law, it requires the organization before they are processing the personal data, they must carry out a Personal Data Protection Impact Assessment (DPIA). This means they must look ahead and think about what risks could happen to data subject's personal data, like leaks, misuse, or errors, and then plan how to prevent or reduce those risks. The goal is to make sure the personal data is handled safely, and that data subject's rights are protected.

ISO/IEC 27701:2019 on Clause 7.2.5 highlighting the same. That clause guides organizations to perform a privacy impact assessment before collecting or using personal data. It helps them identify possible privacy risks and decide what steps are needed to reduce those risks. This aligns directly with what the law expects: understanding the impact of data processing and taking action to protect individuals. By following this clause, organizations can make sure they've thought things through, planned for any potential issues, and acted responsibly to protect data subject's personal data.

Security and protection measures
On article 35-39 Indonesian PDP Law it mandates clearly hat organizations must keep personal data safe and secure. This means they must build systems and take practical steps, like using strong security measures to prevent unauthorized access, misuse, or leaks of the data. They have to make sure the data stays private, and only authorized person can access it. Also, everyone involved in processing the data must be properly supervised, and the systems used must be trustworthy, secure, and able to show accountability.

To satisfy the requirement, organizations may utilize the guidance provided from ISO/IEC 27001:2022, ISO/IEC 27002:2022, and ISO/IEC 27701:2019. The ISO/IEC 27001:2022 on Clause 4–9 helps organizations build a solid Information Security Management System to control how information security is handled, from understanding risks to setting goals, assigning responsibilities, and checking system performance. Then, ISO/IEC 27002:2022 supports the directions from ISO/IEC 27001:2022 by providing practical, detailed controls like access control, encryption, system monitoring, and physical security that directly protect data from being exposed or accessed without permission. In addition, ISO/IEC 27701:2019 on Clause 5, 6, and 7.2.6 extends these protections to cover privacy. It ensures that data processing is not only secure, but also privacy-respecting, and it applies to every process that runs within the organization that has personal data in it.

Rights of data subjects
Article 40-45 Indonesian PDP Law is for protecting the rights of individuals to stop or limit how their personal data is used. If someone withdraws their consent, the organization must stop processing their data within 3 days. Data subject can also ask for their data to be paused or limited, and the organization must inform them of the action taken. If the purpose of collecting the data is done, or if the person asks for it, the data must be deleted or destroyed, especially if it was collected illegally or is no longer needed. And importantly, the organization must let the person know when their data has been deleted or destroyed.

ISO/IEC 27002:2022 and ISO/IEC 27701:2019 provide the guidance that organization can follow to make sure they fulfil subject data's right regarding their data, especially in case of request to stop, limit, or removing their data. Clause 8.10 of ISO/IEC 27002:2022 talks about secure deletion of information. It helps organizations make sure that when personal data is no longer needed, it can be safely erased or destroyed so that no one can retrieve it again. Then, ISO/IEC 27701:2019 Clause 7.3.4 supports the right of individuals to withdraw their consent and request the deletion of their data, while Clause 7.3.6 ensures that data subject can access, correct, or erase their data when appropriate. But, for this requirement organization need to make sure that they including the 72 hours SLA on their procedure when handling these requests.

Data breach notifications
In article 46-47 Indonesian PDP Law it regulated the organization on the situation where there's an event of failure to protect the data, like data breach where someone's personal information is leaked or exposed, then the organization must send a written notice within 3 days to the person whose data was affected and to the government agency that responsible for data protection. In some cases, they also need to inform the public. The notice must explain what happened, when, how the data was exposed, and what the organization

is doing to fix it. The organization is fully responsible for following privacy protection rules, even after an incident has occurred.

ISO/IEC 27002:2022 provides detailed guidance for handling security incidents. Clause 5.24 helps organizations prepare for incidents, while Clauses 5.25 and 5.26 cover how to respond and learn from them, including communication and accountability. These clauses ensure that when something goes wrong, the organization acts quickly, tracks what happened, and communicates clearly. Then, ISO/IEC 27701:2019 Clause 6.13 supports this by requiring organizations to have clear procedures for managing privacy incidents, including when and how to notify affected individuals. Organization needs to make sure that they have included 72 hours SLA on their procedure when handling the event of failure to protect the data to inform the data subject and to the government agency responsible for data protection.

The change of data controller organization

Article 48 Indonesian PDP Law regulates the situation where there's a restructuration is happen to the organization such as merger, split, acquisition, or closure, and mandates that the organization should tell the data subject what will happen to their personal data, both before and after the change. This can be done directly or through public announcements. If the company is shut down, it must explain how it will handle the data, such as whether it will be stored, transferred, deleted, or destroyed, and this must follow the law and be clearly communicated to the data subjects.

In this case, ISO/IEC 27701:2019 Clause 8.4.2 ensuring that when an organization stops handling data subject's personal data, it has to properly return, transfer, or securely delete that data. This supports the requirement for responsible handling of personal data during a company's closure. Then Clause 8.5 focuses on managing data transfers including if it's across jurisdictions, which includes making sure transfers are lawful and that people are informed, while also aligning with the need to notify data subjects during mergers or other corporate changes. These clauses can help organizations stay transparent and responsible when their structure changes.

Obligatory to comply with regulatory body

On article 49 Indonesian PDP Law it emphasizes that the organizations that control or process personal data must follow the instructions given by government agency responsible for data protection. That agency has the authority to issue rules, investigate, and enforce the law. So, when they give an order, whether it's to correct something, stop certain processing, or take extra protective steps, the organization must comply. Aligning with this requirement, Clause 5.31 of ISO/IEC 27002:2022 help organization to ensure they able to identify and comply with all legal, regulatory, and contractual obligations, which includes following government orders related to data protection. Then, ISO/IEC 27701:2019 Clause 6.15.1 reinforces compliance with such legal requirements, while Clause 7.2.2 helps organizations confirm the legal basis for data processing, ensuring their practices align with regulations. Then Clauses 8.2.1 and 8.2.5 guide data processors to respect agreements and instructions from controllers, which includes complying with any legal requirements they're told to follow. Finally, Clause 8.3.1 ensures that even third-party processors respect the rights of data subjects, especially when responding to regulatory requests.

Exceptions for protection

While organizations must generally follow strict rules to protect personal data, article 50 Indonesian PDP Law explains that some obligations can be waived in special situations. These include cases involving national security, law enforcement, public administration, or financial sector oversight. So, under these specific conditions, certain rights, like giving access, updating, or deleting data that might legally be put on hold.

To satisfy this requirement, Clause 5.31 of ISO/IEC 27002:2022 tells organizations to always identify and comply with legal and regulatory requirements, including recognizing when exceptions apply. This means organizations are guided to understand not only their regular obligations but also the situations where exceptions are allowed by law. By following this clause, they can ensure that when these special cases arise, like a government investigation, they act lawfully while still respecting the broader principles of data protection.

Obligations of data processors
On article 51-52 Indonesian PDP Law it highlights that a Personal Data Processor (someone handling data on behalf of another party) must only process data based on clear instructions from the Personal Data Controller. If they go beyond those instructions, they take full responsibility for any issues. If they want to involve another processor, they need written approval. Also, data processors must follow the same rules as controllers: keeping data accurate, recording all processing activities, protecting it from leaks, and making sure only authorized people can access it.

As organizations that have a role as Personal Data Processor or organizations that have Personal Data Processors that work under them to handle some processing of personal data, ISO/IEC 27701:2019 provide the guidance for organizations about how to taking care of it on Clause 7.2.6 & Clause 8. Clause 7.2.6 ensures that data processors clearly document their roles and follow the agreed purposes when handling personal data. It reinforces that processors should not act on their own but stick to what the data controller has instructed. Then, Clause 8 and all its sub-clauses give a full set of guidelines for Personal Data Processors, including ensuring security, protecting confidentiality, keeping processing records, and involving subcontractors only with permission. These ISO requirements help organizations behave responsibly, stay within their role, and meet all the legal expectations for processing personal data.

Data protection officers
On article 51-52 Indonesian PDP Law it regulates for organizations that process personal data, especially for public services, sensitive data, or large-scale tracking, must appoint officers responsible for Personal Data Protection. These officers (commonly called Data Protection Officers or DPOs) must be professionals who understand the law, know how data protection works, and are capable of doing the job properly. Their duties include giving advice, monitoring compliance, overseeing risk assessments, and acting as the go-to person for any data protection issues. They must also consider the specific risks that come with different types of data processing.

Align with this requirement, in Clause 5.34 of ISO/IEC 27002:2022 it recommends that organizations assign someone to perform independent reviews of information security, this includes evaluating how well data protection measures are working, which aligns with the DPO's monitoring function. Then, Clause 6.3.1.1 of ISO/IEC 27701:2019 specifically addresses the need to assign roles and responsibilities for privacy, including the appointment of someone with clear responsibility for privacy-related tasks. These ISO clauses ensure that the right person is in place to guide, oversee, and act as the organization's trusted point of contact for all matters related to data protection.

Transfer of personal data
Indonesian PDP Law on article 55 & 56 regulates the provision for transferring personal data. When personal data is shared, whether within Indonesia or sent abroad, both the sender and the recipient must protect the data according to the law. If the data is sent to another country, the organization must first check if that country has data protection rules equal to or stronger than Indonesia's. If not, the organization must make sure the recipient has binding protection in place. And if there's still no guarantee, the data can only be sent if the person explicitly agrees to the transfer.

To support organizations to satisfy this requirement, ISO/IEC 27002:2022 & ISO/IEC 27701:2019 providing several clauses to help guide organizations regarding this. On the Clause 5.14 of ISO/IEC 27002:2022 ensures that organizations handle information transfers securely, especially when sharing it with other parties. It emphasizes setting up rules and protections for both sides of the transfer. Meanwhile, Clause 7.2.7 of ISO/IEC 27701:2019 supports cross-border transfers by requiring organizations to confirm legal grounds and ensure adequate protection is in place before sending data. Clause 8.5 adds further controls for processors, especially around international transfers, making sure consent is collected when needed and that protection standards are upheld. These ISO clauses help organizations manage data transfers responsibly and lawfully, both locally and internationally.

Prohibitions on the use of personal data
Indonesian PDP Law strictly prohibits the misuse of personal data which is stated in the article 65 & 66. No one, whether an organization, individual, or third party, can collect, use, or share someone else's personal data without a proper reason. It's also forbidden to create or manipulate fake data to benefit oneself

or others, especially if it could harm the person whose data is involved. In short, personal data must be respected, not exploited or falsified.

Then, ISO/IEC 27002:2022 and ISO/IEC 27701:2019 provides some control for helping organizations to ensure that their internal process are comply with that requirement. On ISO/IEC 27002:2022 Clause 5.33 and 5.34 help organizations protect records and prevent unauthorized access or misuse, while Clause 8.12 focuses on preventing data leaks through controls that detect and block unauthorized disclosures. On the privacy side, ISO/IEC 27701:2019 Clause 6.3.1 ensures that people working with personal data understand and follow the rules. Clauses 7.2.1 and 7.2.2 help define lawful purposes and conditions for data use, ensuring no unauthorized or harmful processing takes place. Additionally, Clauses 7.4.1 and 7.4.2 support privacy by design, encouraging minimal data use and preventing misuse. Then on Clause 8.5.5 it emphasizes the importance of disclosing data only under lawful and justified circumstances.

CONCLUSION

While ISO/IEC 27001:2022 provides comprehensive framework for ISMS, it does not fully satisfy the requirements of Indonesian PDP Law since it lack clear instruction about how to fulfil specific aspect of Indonesian PDP Law requirement, especially on privacy aspect, but it does support on the Data Security & Protection Measure aspect which covered on article 35-39. Then ISO/IEC 27002:2022 able to providing several controls that can be utilized by organization to help them comply with the Indonesian PDP Law, even though it does not satisfy all mandatory requirements, but it able to covers on the Data Security & Protection Measure, Rights of Data Subjects, Data Breach Notifications, Obligatory to Comply with Regulatory Body, Exceptions for Protection, Data Protection Officers, Transfer of Personal Data, Prohibitions on the Use of Personal Data. And lastly ISO/IEC 27701:2019 able to covers almost all Indonesian PDP Law mandatory requirements, since that standard is mainly focused on Data Privacy aspect which on the Indonesian PDP Law itself also concern. Only one requirement that is not covered by ISO/IEC 27701:2019 which is Exceptions for Protection since it does not able to explicitly mention about how to handling such condition.

Similar like previous researches where it mentioned that companies that has implemented ISO/IEC 27001 and ISO/IEC 27002, despite they already are in a strong position to comply with GDPR requirements because it provides a solid foundation and can significantly aid organizations in achieving GDPR compliance, the organizations still required to implement additional GDPR-specific controls and measures to fully meet the regulation's requirements [6]. Both Indonesian PDP Law and GDPR shared many similarities in the aspect of data protection and data privacy, and made the previous research about how these ISO standard able to help organization to comply with the regulation is still on the same page. In this research, it come to the surface the fact that the same condition applies to the case of compliance to Indonesian PDP Law. Although organization has implementing some specific or one of the ISO standards, that does not mean that the organization already comply with the Indonesian PDP Law, as found by Nugraha et al., that even though the organization already implement the ISO/IEC 27001, there are still many gaps between the applied standard and the regulation’s requirement [7]. Implementing standard partially like ISO/IEC 27001 standard, with or without ISO/IEC 27002, it’s still not enough to make the organization fully complied with the Indonesian PDP Law because ISO/IEC 27001 and ISO/IEC 27002 only covers on Information Security Management System and Security Controls aspect, while the Indonesian PDP Law also having many requirements on privacy aspect, hence they still need to do the extra effort to cover the privacy aspect and it can be helped by the controls provided by ISO/IEC 27701.

Then, as to the research questions, this study finds:

1. To what extent do ISO Standards fulfill the requirements of the Indonesian Personal Data Protection Law?
   The analysis based on Table 2 shows that from 14 mandatory requirement topics of Indonesian PDP Law, The ISO/IEC 27001:2022 only able to cover 1 topic, while ISO/IEC 27002:2022 able to provide controls to accommodating 8 topics and ISO/IEC 27701:2019 able to provide controls to accommodating 13 topics. But by combining these standards, then full compliance of the mandatory requirements can be achieved.
2. How do ISO Standards help an organization to ensure compliance with the Indonesian PDP Law?
   Applying all of these standards combined can support compliance mainly because of their end-to-end risk management processes, security and privacy controls that may be customizable to underlying Indonesian PDP Law requirements. But if the organization only apply these frameworks partially,

then there will be several measures needed to push the organization to be able comply with the Indonesian PDP Law.

The study highlights the practical implications of ISO/IEC 27001:2022. ISO/IEC 27002:2022, and ISO/IEC 27701:2019 for organizations in Indonesia that manage large volumes of personal or sensitive data, particularly those operating in highly regulated sectors that want to develop an organized and effective implementation of Indonesian PDP Law compliance. These standards provides comprehensive, yet having specific roles that can support and guide organizations to achieve compliance with the Indonesian PDP Law. ISO/IEC 27001:2022 provides the ISMS framework which help organization to having a globally standard framework to protecting information that is being processed, and then being complemented by ISO/IEC 27002:2022 that provides the technical controls to achieve a secure information system environment on the organization, lastly on the privacy aspect is being supported by controls from ISO/IEC 27701:2019. Which, by implementing all of these standards organization can achieve compliance to Indonesian PDP law. However, some specific adjustments still need to be implemented within the organization to comply with those regulatory requirements such as handling the Data Subject's request and providing notification timeframe to be limited as 3 x 24 hours since that timeframe is explicitly mentioned on these ISO standards.

Future research should formulate an integrated compliance framework that merges the rigor of ISO standards with specific adaptations to fully address the nuances of the Indonesian PDP Law. This comprehensive approach would streamline compliance efforts and bolster the overall data protection posture of organizations within Indonesia.

Research Limitations

Although this paper specifically addresses ISO/IEC 27001:2022, ISO/IEC 27002:2022, and ISO/IEC 27701:2019, it is crucial to note that additional information security and privacy frameworks may also provide useful information relevant to compliance with the Indonesian PDP Law. Such alternative frameworks may help reinforce data protection and data privacy either through additional considerations or additional safeguards. Additionally, the study's reliance on secondary data and document analysis may limit the generalizability of its findings across all Indonesian organizations. Future research could address this limitation by exploring the applicability of other frameworks and conducting empirical studies directly within Indonesian organizations with a specific scope of industry. Such studies would offer a practical view of PDP Law compliance, potentially validating and expanding upon the insights gained from this research.

REFERENCES

[1] J. S. Rana, P. Siwatch, and S. Sharma, "Introduction to Cyber Security," *International Journal of Advanced Research in Science, Communication and Technology*, pp. 246–250, 2024, doi: 10.48175/ijarsct-17639.

[2] N. Jevtić and I. Alhudaidi, "The importance of information security for organizations," *Serbian Journal of Engineering Management*, vol. 8, no. 2, pp. 48–53, 2023, doi: 10.5937/SJEM2302048J.

[3] L. Bertolaccini *et al.*, "The significance of general data protection regulation in the compliant data contribution to the European Society of Thoracic Surgeons database," *European Journal of Cardio-Thoracic Surgery*, vol. 64, no. 3, Sep. 2023, doi: 10.1093/ejcts/ezad289.

[4] A. Wodi, "The EU General Data Protection Regulation (GDPR): Five Years After and the Future of Data Privacy Protection in Review," *SSRN Electronic Journal*, 2023, doi: 10.2139/ssrn.4601142.

[5] Y. Smirnova and V. Travieso-Morales, "Understanding challenges of GDPR implementation in business enterprises: a systematic literature review," *International Journal of Law and Management*, vol. ahead-of-print, no. ahead-of-print, Jan. 2024, doi: 10.1108/IJLMA-08-2023-0170.

[6] V. Diamantopoulou, A. Tsohou, and M. Karyda, "From ISO/IEC27001:2013 and ISO/IEC27002:2013 to GDPR compliance controls," *Information & Computer Security*, vol. 28, no. 4, pp. 645–662, Jun. 2020, doi: 10.1108/ICS-01-2020-0004.

[7] A. A. Nugraha and A. H. Nasyuha, "Integrating ISO 27001 and Indonesia's Personal Data Protection Law for Data Protection Requirement Model," *Journal of Information Systems and Informatics*, vol. 6, no. 2, pp. 1052–1069, Jun. 2024, doi: 10.51519/journalisi.v6i2.754.

[8] F. Fitriyanti, S. Devty, S. Putri, and R. E. Thora, "SECURING PERSONAL DATA IN E-KYC: VITAL FOR DIGITAL ECONOMY GROWTH," *Diponegoro Law Review*, vol. 9, no. 1, pp. 104–120, Apr. 2024, doi: 10.14710/dilrev.9.1.2024.104-120.

[9] Z. S. Zuwanda, L. Judijanto, H. Khuan, and A. Triyantoro, "Normative Study of Law No. 27 of 2022 on the Protection of Personal Data and its Impact on the Fintech Industry in Indonesia," *West Science Law and Human Rights*, vol. 2, no. 04, pp. 421–428, Oct. 2024, doi: 10.58812/wslhr.v2i04.1367.

[10] G. Faza and D. Wiyanti, "Tanggung Jawab Bank Syariah Indonesia (BSI) terhadap Nasabah yang Diretas Data Pribadinya Berdasarkan Undang-Undang No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik Jo. Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi," *Bandung Conference Series Law Studies*, vol. 4, no. 2, pp. 867–873, 2024, doi: 10.29313/bcsls.v4i2.12630.

[11] A. A. Nugraha and A. H. Nasyuha, "Integrating ISO 27001 and Indonesia's Personal Data Protection Law for Data Protection Requirement Model," *Journal of Information Systems and Informatics*, vol. 6, no. 2, pp. 1052–1069, Jun. 2024, doi: 10.51519/journalisi.v6i2.754.

[12] G. Gumilar, E. Budiarto, M. Galinium, and C. Lim, "Personal Data Protection Framework for Web Developers and API Providers under UU PDP," in *2023 International Conference on Informatics, Multimedia, Cyber and Informations System (ICIMCIS)*, IEEE, Nov. 2023, pp. 189–194. doi: 10.1109/ICIMCIS60089.2023.10349040.

[13] P. Machado, J. Vilela, M. Peixoto, and C. Silva, "A systematic study on the impact of GDPR compliance on Organizations," in *Proceedings of the XIX Brazilian Symposium on Information Systems*, New York, NY, USA: ACM, May 2023, pp. 435–442. doi: 10.1145/3592813.3592935.

[14] S. Ngobeni *et al.*, "Towards a GDPR Compliance Assessment Toolkit," *European Conference on Cyber Warfare and Security*, vol. 23, no. 1, pp. 313–321, Jun. 2024, doi: 10.34190/eccws.23.1.2278.

[15] K. K. Lakshmi, H. Gupta, and J. Ranjan, "Analysis of General Data Protection Regulation Compliance Requirements and Mobile Banking Application Security Challenges," in *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 2020, pp. 1028–1032. doi: 10.1109/ICRITO48877.2020.9197954.

[16] F. Razi, H. Tuasikal, and D. P. Markus, "Implementation and Challenges of the Personal Data Protection Law in Indonesia," *Jurnal Indonesia Sosial Teknologi*, vol. 5, no. 12, pp. 6015–6021, 2024, doi: 10.59141/jist.v5i12.1285.

[17] J. E. Widodo, A. Suganda, and Tubagus Achmad Darodjat, "DATA PRIVACY AND CONSTITUTIONAL RIGHTS IN INDONESIA," *PENA LAW: International Journal of Law*, vol. 2, no. 2, Sep. 2024, doi: 10.56107/penalaw.v2i2.187.

[18] I. G. N. P. Widiatedja and N. Mishra, "Establishing an independent data protection authority in Indonesia: a future–forward perspective," *International Review of Law, Computers & Technology*, vol. 37, no. 3, pp. 252–273, Sep. 2023, doi: 10.1080/13600869.2022.2155793.

[19] V. A. Simbolon and V. Juwono, "Comparative Review of Personal Data Protection Policy in Indonesia and The European Union General Data Protection Regulation," *Publik*, vol. 11, no. 2, p. 178, 2022, doi: 10.31314/pjia.11.2.178-190.2022.

[20] Hendro and M. Deckri Algamar, "Navigating the Personal Data Protection Law in Indonesia: A Practical Guide to Establishing a Data Protection Function," Jun. 2024, *Indonesia*.

[21] A. A. Tisnadisastra and P. Mokoginta, *Data Protection 2024: Indonesia*. Jakarta, Indonesia: White & Case LLP, 2024.

[22] International Organization for Standardization, "ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements," 2022. [Online]. Available: https://www.iso.org/standard/27001

[23] International Organization for Standardization, "ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls," 2022. [Online]. Available: https://www.iso.org/standard/75652.html

[24] International Organization for Standarization, "ISO/IEC 27701:2019. Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines," 2019.

[25] E. Lachaud, "ISO/IEC 27701 Standard: Threats and Opportunities for GDPR Certification," *European Data Protection Law Review*, vol. 6, no. 2, pp. 194–210, 2020, doi: 10.21552/EDPL/2020/2/7.

[26] J. Serrado, R. F. Pereira, M. Mira da Silva, and I. Scalabrin Bianchi, "Information security frameworks for assisting GDPR compliance in banking industry," *Digital Policy, Regulation and Governance*, vol. 22, no. 3, pp. 227–244, Aug. 2020, doi: 10.1108/DPRG-02-2020-0019.

[27] M. J. Haber and D. Rolls, “Regulatory Compliance,” Apress, 2024, pp. 243–251. doi: 10.1007/979-8-8688-0233-1_21.
[28] A. Marotta and S. Madnick, “A Framework for Investigating GDPR Compliance Through the Lens of Security,” 2021, pp. 16–31. doi: 10.1007/978-3-030-83164-6_2.
[29] M. Rhahla, S. Allegue, and T. Abdellatif, “Guidelines for GDPR compliance in Big Data systems,” *Journal of Information Security and Applications*, vol. 61, p. 102896, Sep. 2021, doi: 10.1016/j.jisa.2021.102896.
[30] A. Folorunso, V. Mohammed, I. Wada, and B. J. Samuel, “The impact of ISO security standards on enhancing cybersecurity posture in organizations,” *World Journal Of Advanced Research and Reviews*, vol. 24, no. 1, pp. 2582–2595, 2024, doi: 10.30574/wjarr.2024.24.1.3169.
[31] D. S. K. Putra, S. Tistiyani, and S. U. Sunaringtyas, “The Use of ISO/IEC 27001 Family of Standards in Regulatory Requirements in Some Countries,” in *2021 2nd International Conference on ICT for Rural Development (IC-ICTRuDev)*, IEEE, Oct. 2021, pp. 1–6. doi: 10.1109/IC-ICTRuDev50538.2021.9656529.
[32] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, “The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda,” *The Tqm Journal*, vol. 33, no. 7, pp. 76–105, 2021, doi: 10.1108/TQM-09-2020-0202.
[33] F. Mera-Amores and H. N. Roa, “Enhancing Information Security Management in Small and Medium Enterprises (SMEs) Through ISO 27001 Compliance,” Springer International Publishing, 2024, pp. 197–207. doi: 10.1007/978-3-031-53963-3_14.
[34] I. Bashofi and M. Salman, “Cybersecurity Maturity Assessment Design Using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002,” in *2022 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom)*, IEEE, Jun. 2022, pp. 58–62. doi: 10.1109/CyberneticsCom55287.2022.9865640.
[35] S. A. Grishaeva, “Development and Implementation of Privacy Information Management for Compliance with International Standard ISO 27701:2019,” pp. 198–200, 2021, doi: 10.1109/itqmis53292.2021.9642925.
[36] S. Rao and K. Moon, “Literature Search for Systematic Reviews,” in *Principles and Practice of Systematic Reviews and Meta-Analysis*, Cham: Springer International Publishing, 2021, pp. 11–31. doi: 10.1007/978-3-030-71921-0_2.
[37] *UU Nomor 27 Tahun 2022*. 2022.