International Journal of Safety and Security Engineering
Vol. 15, No. 1, January, 2025, pp. 113-126
Journal homepage: http://iieta.org/journals/ijsse

Identifying and Validating Critical Factors in Designing a Comprehensive Data Protection Impact Assessment (DPIA) Framework for Indonesia

Sidik Prabowo[1*], Maman Abdurohman[1], Hilal Hudan Nuha[1], Sarwono Sutikno[2]

[1] School of Computing, Telkom University, Telekomunikasi Street 1st, Bandung, West Java 40257, Indonesia
[2] Institut Teknologi Sumatera, Jl. Terusan Ryacudu, Way Huwi, South Lampung, Lampung 35365, Indonesia

Corresponding Author Email: pakwowo@telkomuniversity.ac.id

https://doi.org/10.18280/ijsse.150113

Received: 21 October 2024
Revised: 5 December 2024
Accepted: 22 January 2025
Available online: 31 January 2025

Keywords:
data protection impact assessment, Indonesia, critical factor, regulation

ABSTRACT

As Indonesia undergoes rapid digital transformation, robust data protection frameworks have become critical, particularly in enforcing the Personal Data Protection Act (UU PDP). This study develops a localized Data Protection Impact Assessment (DPIA) framework to align with international standards and Indonesia's unique economic and cultural conditions. Through stakeholder engagement, risk management strategies, and technological solutions, the proposed framework addresses the challenges diverse sectors face, from large corporations to small and medium-sized enterprises (SMEs). The research recommends practical tools like automation and cloud-based systems to enhance compliance and foster responsible data practices. This work provides a roadmap for improving privacy management, ensuring regulatory compliance, and promoting data security across Indonesia's dynamic digital landscape.

1. INTRODUCTION

As digital transformation accelerates globally, the importance of robust data protection frameworks has become increasingly evident. The European Union’s General Data Protection Regulation (GDPR), which introduced Data Protection Impact Assessments (DPIAs) in 2018, set a benchmark for identifying and mitigating risks associated with personal data processing activities [1]. This global standard has influenced the development of similar regulations worldwide, including Indonesia’s Personal Data Protection Act (Undang-Undang Pelindungan Data Pribadi, UU PDP), enacted in 2022. The UU PDP mandates DPIAs for high-risk data processing activities [2], aligning with GDPR principles.

As one of Southeast Asia’s largest digital markets, Indonesia faces unique challenges in implementing effective DPIAs due to its diverse demographic, cultural, and technological landscape. The rapid growth of e-commerce, financial services, and healthcare industries necessitates a tailored approach to data protection that addresses these complexities. However, existing literature on DPIA practices has predominantly focused on developed economies, leaving a significant research gap in understanding how to adapt these frameworks for developing contexts like Indonesia.

Moreover, previous research highlights that the successful deployment of DPIA frameworks in different jurisdictions depends heavily on contextual factors, such as regulatory alignment, organizational culture, stakeholder involvement, and risk management practices [3, 4]. These studies underscore the importance of a localized approach to DPIA design, which ensures legal compliance and addresses the specific needs and challenges of the operating environment.

This study aims to bridge this gap by identifying and validating the critical factors necessary for designing a comprehensive DPIA framework that complies with the UU PDP while catering to Indonesia’s specific needs. By integrating international best practices with local requirements, this research provides practical insights to support organizations in enhancing data protection practices and achieving regulatory compliance. Key objectives include defining essential DPIA components, validating their relevance in the Indonesian context, and proposing scalable solutions for diverse organizational capacities.

This study, which conducts empirical research involving stakeholder surveys, expert interviews, and statistical analysis, seeks to provide practical insights and guidelines for Indonesian organizations to enhance their data protection practices and ensure compliance with legal requirements.

To achieve the research objectives, the study is guided by the following key research questions:

1) What critical factors must be considered when designing a DPIA framework tailored to the Indonesian context?

2) How do these factors align with the requirements of Indonesia's Personal Data Protection Act (UU PDP)?

3) What methodologies can be employed to validate the relevance and effectiveness of these factors in implementing a DPIA framework?

4) How can organizations in Indonesia practically implement the validated DPIA framework to enhance data protection and ensure compliance with regulatory standards?

These research questions are central to the study, as they focus on uncovering the essential elements required for a DPIA framework that meets the legal requirements of the UU PDP and addresses the specific challenges and needs of

Indonesian organizations. The findings from this research are expected to contribute significantly to developing a DPIA framework that supports responsible data management practices in Indonesia's rapidly evolving digital economy.

2. LITERATURE REVIEW

We have undertaken a comprehensive review of several relevant studies published previously. Table 1 presents the findings from these searches, along with key insights that can serve as valuable contributions to our current research.

Table 1. Related research review

Author(s)	Year	Title/Source	Key Findings/Contribution	Relevance to DPIA Framework in Indonesia
Clarke	2011	An evaluation of privacy impact assessment guidance documents	Evaluates various PIA guidance documents, highlighting strengths and weaknesses in their approaches to assessing privacy risks.	Provides a foundational understanding of the effectiveness of existing PIA guidance, which can inform the creation of tailored DPIA guidelines in Indonesia.
Wright et al.	2013	A comparative analysis of privacy impact assessment in six countries	Compares PIA practices in six countries, identifying commonalities and differences in implementation. Emphasizes the importance of contextual adaptation of PIAs.	Offers insights into how different countries have adapted PIA practices, which can be used to identify best practices and potential challenges for DPIA in Indonesia.
Wadhwa et al.	2013	Evaluating privacy impact assessments	Discusses the effectiveness of PIAs and suggests improvements for their implementation, focusing on stakeholder engagement and transparency.	Suggests critical elements for effective DPIA implementation, such as stakeholder involvement and transparency, which are crucial for the Indonesian context.
Wright	2013	Making privacy impact assessment more effective	Proposes strategies to enhance the effectiveness of PIAs, including integrating them early in project planning and improving accessibility of PIA results.	Provides strategies for improving DPIA effectiveness in Indonesia by ensuring early integration and making the results accessible to all stakeholders.
Notario et al.	2015	PRIPARE: Integrating privacy best practices into a privacy engineering methodology	Introduces the PRIPARE framework, which integrates privacy best practices into engineering methodologies, emphasizing the role of privacy by design.	Offers a methodology for incorporating privacy best practices into DPIA, which could be adapted to suit Indonesia's regulatory and technological environment.
Vemou et al.	2018	An evaluation framework for privacy impact assessment methods	Develops an evaluation framework for assessing different PIA methods, focusing on their comprehensiveness, adaptability, and stakeholder engagement.	Provides a framework that can be used to assess and refine DPIA methods in Indonesia, ensuring they are comprehensive and adaptable to local needs.

2.1 Global data protection impact assessment (DPIA) standards

Data Protection Impact Assessment (DPIA) is a process designed to help organizations identify and mitigate risks associated with the processing of personal data. The concept gained prominence with the introduction of the GDPR in 2018, which made DPIAs mandatory for processing activities that pose high risks to individuals' rights and freedoms (European Commission, 2018). DPIAs are intended to ensure that data processing activities comply with privacy regulations and do not infringe upon individuals' privacy rights. Studies have shown that DPIAs are critical in enhancing transparency, accountability, and trust in data-processing activities [3].

Globally, the implementation of DPIA varies significantly depending on the regulatory environment and the maturity of data protection frameworks in different countries. In the European Union, DPIA is a well-established practice under the GDPR, with specific guidelines provided by the European Data Protection Board (EDPB) on when and how to conduct a DPIA [5]. Research by van Dijk et al. has highlighted the effectiveness of DPIAs in the European Union (EU), particularly in sectors such as healthcare and finance, where data processing risks are high [4].

Outside the EU, countries like Canada and Australia have also adopted DPIA-like processes, though often under different names, such as Privacy Impact Assessments (PIAs). In Canada, PIAs are required under the Privacy Act for federal government institutions, while in Australia, the Office of the Australian Information Commissioner (OAIC) and provide guidelines for conducting PIAs, especially when handling sensitive information [6]. These international examples show that while DPIA is globally recognized, its implementation is often tailored to each country's legal and cultural context.

In developing economies, the adoption of DPIAs and similar frameworks face unique challenges due to varying levels of regulatory enforcement, technological infrastructure, and awareness of data protection issues. Studies have indicated that in regions like Africa and Southeast Asia, the implementation of DPIAs is still in its nascent stages, often hindered by limited resources and expertise [7]. Despite these challenges, there is growing recognition of the need for robust data protection frameworks to support digital transformation in these regions.

2.2 Relevance to Indonesia

Indonesia's 2022 enactment of the UU PDP marks a significant step toward aligning with international data protection standards. For instance, regions with low internet penetration and limited technological literacy encounter challenges that are not adequately addressed by GDPR-inspired practices.

While the principles of GDPR provide a solid foundation, their direct application in Indonesia may be limited. Studies like those conducted by Dashti and Ranise [8] highlight the need for tailored Data Protection Impact Assessment (DPIA) methodologies that factor in local risks and stakeholder dynamics. This is particularly crucial in Indonesia's diverse economic landscape, where small and medium-sized enterprises (SMEs) play a dominant role yet often lack the resources for comprehensive compliance.

Additionally, research on DPIA implementations in other developing countries, such as India and Brazil, underscores the significance of government support and public-private partnerships in addressing resource constraints. By incorporating such innovative methodologies, Indonesia could enhance its data protection framework, effectively addressing its unique infrastructural and cultural challenges.

More recent research, such as Dashti and Ranise [8] proposes tool-assisted methodologies for conducting DPIAs, which can significantly reduce the complexity of risk assessments for resource-constrained organizations. Similarly, Hart et al. [9] advocate for a fuzzy-based approach to prioritizing privacy risks, offering practical solutions that align with the challenges developing economies face.

Recent case studies from Africa and Southeast Asia highlight the significance of tailored regulatory frameworks for regional differences. For instance, hybrid manual and automated DPIA tools effectively address resource limitations while ensuring compliance. Indonesia can use these insights to create a framework that blends global best practices with local adaptations, promoting wider adoption and sustainability in various organizations contexts.

Despite the growing body of literature on DPIAs, there remains a lack of critical analysis on their implementation in developing regions. This study aims to address this gap by evaluating the relevance and limitations of existing practices and proposing a localized approach tailored to Indonesia's regulatory, cultural, and technological context.

These factors must be adapted to Indonesia's local needs and conditions. For example, stakeholder engagement may need to consider the diverse levels of data protection awareness and expertise across different sectors. Similarly, risk assessment methodologies should be aligned with the specific regulatory requirements set forth by the UU PDP.

While substantial research exists on DPIA in developed regions, more literature should be on its implementation in Indonesia and similar developing economies. This gap presents an opportunity for further research, particularly in understanding how DPIA frameworks can be effectively designed and implemented in these contexts. This study aims to fill this gap by providing empirical insights into the critical factors for DPIA in Indonesia, contributing to the broader discourse on global data protection practices.

3. RESEARCH METHODOLOGY

This study employs a qualitative research design to identify and validate critical factors for a comprehensive DPIA framework in Indonesia. The research draws upon a literature review, expert consultations, and a comparative analysis of international best practices.

3.1 Data collection methods

Literature Review:

A systematic review of global DPIA frameworks and academic articles was conducted to identify factors relevant to data protection. The review included documents such as the GDPR, ISO/IEC 27001 standards, NIST Risk Management Framework, and scholarly research on privacy impact assessments in various jurisdictions.

Expert Consultations:

Semi-structured interviews were conducted with data protection officers, legal experts, IT professionals, and policymakers in Indonesia. These consultations provided insights into the practical challenges and requirements for implementing DPIAs within the local context.

Comparative Analysis:

The study compared 17 factors from seven best practice frameworks and 33 from six academic articles to identify commonalities and contextual differences. Criteria for selection included relevance to data privacy regulations, adaptability to diverse organizational sizes, and practical applicability in resource-constrained settings.

3.2 Analysis techniques

The identified factors were subjected to a two-stage validation process:

Factor Consolidation:

Duplicate and overlapping factors were eliminated, and similar factors were merged to create a streamlined list. This process ensured that the final set of factors was comprehensive without redundancy.

Contextual Validation:

Each factor was evaluated for relevance and applicability to Indonesia's regulatory and technological landscape. Expert feedback and case studies from similar developing economies informed this validation.

The methodology was developed to emphasize transparency and replicability. By outlining each step and documenting techniques and data sources, we enable the validation of findings, which encourages future research to build on this foundation and enhances cumulative knowledge in the field.

Creating a comprehensive Data Protection Impact Assessment (DPIA) framework demands careful consideration of several key factors, particularly within Indonesia's evolving data protection landscape. As illustrated in Figure 1, the following critical factors are essential for designing an effective DPIA framework based on international best practices and Indonesia's unique characteristics. These factors are outlined below, each accompanied by a concise explanation and relevant references to existing literature:

3.2.1 Stakeholder involvement

One of the most important factors in the success of any DPIA framework is the involvement of key stakeholders. Wright et al. [3] emphasize that a successful DPIA process requires the participation of diverse stakeholders, including Data Protection Officers (DPOs), legal experts, IT professionals, and senior management.

Involving a wide range of stakeholders ensures that the assessment is comprehensive and addresses technical and legal aspects of data protection.

In the Indonesian context, stakeholder involvement must be broadened to include government regulators, industry representatives, and civil society organizations [10]. This is particularly important given the varying levels of data protection awareness and resources available across different sectors.

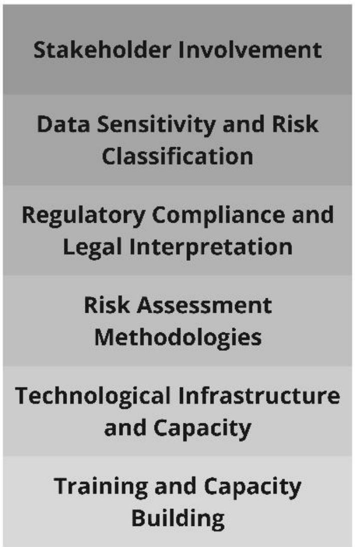

Stakeholder Involvement
Data Sensitivity and Risk Classification
Regulatory Compliance and Legal Interpretation
Risk Assessment Methodologies
Technological Infrastructure and Capacity
Training and Capacity Building

Figure 1. Identified Indonesian DPIAs critical factors

Some industries, such as finance and healthcare, are more advanced regarding data security practices. In contrast, others, such as Small and Medium-Sized Enterprises (SMEs), may need more infrastructure and expertise to comply fully with DPIA requirements. Ensuring that all stakeholders are represented in the DPIA process is essential for identifying the risks unique to each sector and providing a practical and scalable framework across the board.

3.2.2 Data sensitivity and risk classification

A robust DPIA framework must include a clear method for classifying data sensitivity and assessing risk levels. Under the UU PDP, particular attention must be paid to the processing of specific personal data, which may include data related to health information, genetics, criminal records, or personal financial information [2]. Identifying and categorizing data sensitivity is critical for determining the level of protection and controls that need to be applied.

For Indonesia, context-specific risk assessment methodologies should be implemented where regulatory requirements and enforcement may differ between regions and industries. These methodologies must account for both the legal risks outlined by the UU PDP and the practical realities of Indonesia's technological infrastructure. In less digitized regions, the DPIA framework should consider non-digital data processing risks, such as those associated with paper records, which still play a significant role in many organizations.

3.2.3 Regulatory compliance and legal interpretation

Compliance with the UU PDP is fundamental to implementing a DPIA framework. The law mandates that DPIAs be conducted for high-risk processing activities, but clarity around legal interpretation is still emerging. Indonesian organizations must understand when and how to conduct DPIAs. Many businesses struggle with interpreting these requirements due to their complexity and the evolving nature of Indonesia's data protection regulations.

Therefore, an effective DPIA framework should include compliance mechanisms that assist organizations in determining when a DPIA is necessary. These mechanisms can be supported by checklists, automated tools, or templates designed specifically for Indonesian legal and regulatory contexts. Training and education are also essential to improving organizations' understanding of the law and how to apply it effectively.

3.2.4 Risk assessment methodologies

A robust DPIA framework requires well-defined risk assessment methodologies to evaluate data sensitivity and prioritize privacy risks effectively. According to Hart *et al.*, a fuzzy-based approach can systematically assess and prioritize privacy risks by reducing the subjectivity inherent in risk evaluations [9]. This method involves well-defined criteria for measuring the likelihood and impact of privacy risks, offering a more structured approach to identifying critical threats to data security. Similarly, Dashti *et al.*, propose a tool-assisted risk analysis methodology for DPIAs that aids data controllers in identifying risks to individuals' rights and freedoms, providing automated assistance in data processing specification and risk analysis [8]. Furthermore, Gellert emphasizes that understanding the concept of risk within the GDPR is essential, as the regulation defines risks in compliance and the potential impact on data subjects' rights [11]. This approach underscores the need to carefully assess risks' likelihood and severity, ensuring that DPIAs are a data protection compliance tool [11]. In alignment with international standards such as ISO/IEC 27001, which provides a systematic approach to managing sensitive information and assessing security risks, these methodologies ensure that organizations can address technical and organizational risks in a globally recognized framework. Finally, *Dashti et al.*, further highlight the role of pragmatic, tool-assisted methodologies for DPIAs, particularly in public administration sectors where risk assessments can guide decision-making and ensure adherence to data protection regulations [8].

3.2.5 Technological infrastructure and capacity

The effectiveness of any Data Protection Impact Assessment (DPIA) framework depends on an organization's technological capability to manage and safeguard personal data. In Indonesia, where technological infrastructure varies significantly across sectors and regions, the DPIA framework must be scalable and adaptable to organizations of different sizes and with various technical capabilities. Larger organizations, particularly in industries like finance and telecommunications, often have access to advanced data protection tools and dedicated personnel, allowing them to implement robust privacy protection measures. For instance, implementing Advanced Metering Infrastructure (AMI) in Indonesia's energy sector illustrates how larger enterprises can leverage sophisticated technologies to support secure and efficient data management systems [12].

In contrast, small and medium-sized enterprises (SMEs) and public sector institutions often need more resources and a lack of technological expertise. Research indicates that SMEs in Indonesia, while increasingly adopting digital technologies, usually struggle with the digital transformation process, and their capacity to handle complex data protection requirements remains limited [13]. The DPIA framework should, therefore, include scalable solutions that allow for basic data protection measures to be implemented in resource-constrained environments while also providing more advanced tools and systems for larger organizations with sophisticated needs. For example, digital technology has been shown to enhance the resilience of SMEs in Indonesia, particularly when responding to external shocks such as natural disasters [14].

To address these disparities in technological readiness, policymakers, and technology developers must provide supportive policies and cost-effective solutions tailored to the needs of smaller organizations. This includes access to cloud computing, data analytics tools, and automated systems that can simplify compliance with data protection regulations [14]. By enabling scalability and flexibility in deploying these tools, Indonesia can create a more inclusive DPIA framework that accommodates the diversity of its organizational landscape.

3.2.6 Training and capacity building

Effective implementation of a DPIA framework requires substantial training and capacity-building efforts. Many Indonesian organizations, particularly SMEs and public sector institutions, need more expertise to fully understand and conduct DPIAs. A comprehensive capacity-building strategy is necessary to bridge this knowledge gap, focusing on educating key personnel about data protection, risk management, and compliance with the UU PDP.

To ensure a successful DPIA implementation, organizations must invest in training programs to improve technical knowledge on data protection issues. These programs should be tailored to suit the varying levels of expertise across sectors. Large organizations may require advanced training on technical solutions, while SMEs may need basic training on data privacy principles and the legal requirements under the UU PDP. Research highlights the effectiveness of targeted training in building capacity for organizations dealing with sensitive data, such as in the health sector, where tailored training programs have been shown to enhance personnel's capacity to manage data responsibly significantly [15].

Training programs should be scalable and incorporate various formats, including online learning platforms, to make them accessible to a wider audience. For example, digital learning platforms have successfully addressed capacity challenges in sectors with resource limitations, such as Indonesia's health information system, which benefited from introducing a national digital learning platform [16].

In the context of SMEs, capacity building can also include peer learning and mentorship programs, where smaller organizations can learn from more established ones. Studies show that capacity-building initiatives, including periodic training and ongoing mentorship, can significantly improve organizational readiness to implement digital tools and comply with regulatory frameworks. Similarly, government-backed support programs for SMEs can help overcome resource constraints by providing access to training materials and technical support at low cost.

For long-term success, capacity building must be continuous and evolving to keep pace with technological advancements and changes in the regulatory landscape. This requires the development of institutional training frameworks that are regularly updated and aligned with international best practices. Government initiatives to support capacity building across industries, such as Indonesia's focus on strengthening human resources for data protection in key sectors, can serve as a model for scaling up efforts across all industries [17].

4. VALIDATING CRITICAL FACTORS

Identifying critical factors in designing a DPIA framework for Indonesia must be validated to ensure they meet international standards, accurately assess risks, and align with regulatory requirements. Validation is key to ensuring that the framework complies with national laws, follows global best practices, and can be effectively implemented across various sectors. This section focuses on three major aspects of validation:

4.1 International best practices

Validating the critical factors in Indonesia's DPIA framework requires benchmarking against international best practices in data protection and privacy management. These best practices provide a solid foundation for managing privacy risks, conducting thorough assessments, and implementing security controls that protect personal data. Two major frameworks—GDPR and ISO/IEC 27001—are globally recognized standards that help organizations develop robust data protection strategies. The NIST Information Security Risk Management Framework (RMF) offers comprehensive guidance on assessing and managing information security risks, particularly in sensitive data environments.

GDPR and DPIA

The GDPR requires Data Protection Impact Assessments (DPIAs) for processing activities posing a high risk to individuals' privacy. The regulation outlines a risk-based approach that organizations can adopt to ensure compliance and mitigate potential threats to data subjects. Under the GDPR, DPIAs are required when introducing new data processing technologies, engaging in large-scale processing of sensitive data, or conducting profiling activities that could impact individuals [1]. GDPR emphasizes a thorough risk assessment process that evaluates the severity and likelihood of risks, requiring organizations to implement risk mitigation strategies to protect data.

Applying GDPR's risk-based approach to the Indonesian context provides a strong foundation for developing a DPIA framework tailored to local regulatory requirements under the UU PDP. By adopting GDPR-aligned practices, Indonesian organizations can better understand how to structure their data protection strategies and ensure compliance with regional and global data protection laws [11].

ISO/IEC 27001

Another critical international standard is ISO/IEC 27001, which focuses on establishing an information security management system (ISMS) that addresses information confidentiality, integrity, and availability. ISO/IEC 27001 provides a comprehensive set of security controls and risk management processes that can be applied to protect personal data. For DPIA validation, this framework offers guidance on continuously assessing risks, implementing security measures, and monitoring the effectiveness of these controls.

In Indonesia, aligning DPIA frameworks with ISO/IEC 27001 ensures that data security risks are managed effectively, particularly in the highly sensitive healthcare and finance sectors. Using the Annex, A controls from ISO/IEC 27001, organizations can adopt encryption, access control, and regular audits, which are essential for safeguarding sensitive information [8].

NIST Information Security Risk Management Framework (RMF)

The National Institute of Standards and Technology (NIST) provides a highly regarded Risk Management Framework (RMF) that organizations can leverage to validate their DPIA frameworks. NIST's RMF emphasizes a structured process for managing information security risks across six steps, as depicted in Figure 2. These steps are designed to ensure that organizations can identify the appropriate risk mitigation strategies based on the data's sensitivity and the risk level associated with specific data processing activities.

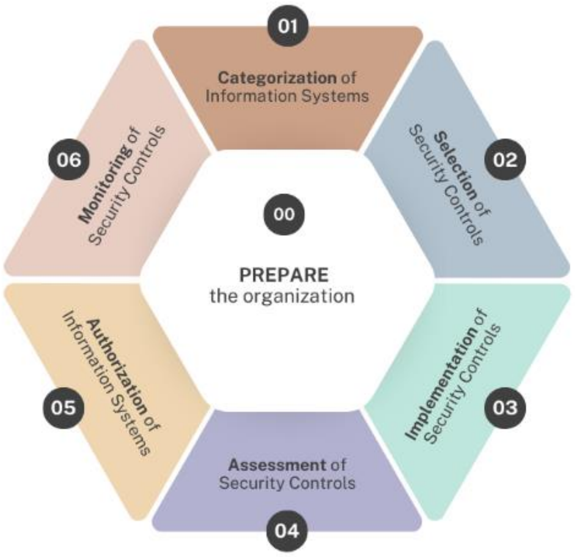

01
Categorization of Information Systems
02
Selection of Security Controls
03
Implementation of Security Controls
04
Assessment of Security Controls
05
Authorization of Information Systems
06
Monitoring of Security Controls
00
PREPARE the organization

Figure 2. NIST risk management framework

For instance, in the categorization phase, organizations determine the impact levels of data processing on *confidentiality*, *integrity*, and *availability*. This aligns with the DPIA process, where organizations assess the risks associated with different types of data, particularly sensitive personal information like health records or financial data. Following the categorization, organizations use the selection phase to identify appropriate security controls, similar to selecting technical and organizational measures in a DPIA framework.

NIST's RMF is particularly relevant for Indonesian sectors that deal with critical infrastructure or highly sensitive information. By integrating NIST's risk management principles, Indonesian organizations can ensure that their DPIA frameworks comply with local regulations and follow a globally recognized standard for managing information security risks. The RMF's continuous monitoring and assessment process also aligns well with the need for ongoing DPIA updates, especially as new risks and data processing technologies emerge [18].

While international best practices offer a robust framework, their successful application in Indonesia requires customization to local regulatory, cultural, and technological contexts. For example, the Indonesian UU PDP has specific requirements around high-risk processing activities, such as profiling or the large-scale processing of sensitive data. Additionally, sectors such as telecommunications and public administration may have unique risk factors that still need to be fully addressed by international frameworks.

SMEs and resource-constrained organizations in Indonesia may face challenges in adopting full-scale GDPR or ISO/IEC 27001 models. Therefore, the DPIA framework should include scalable and simplified versions of these best practices, enabling organizations with limited capacity to comply with local and international standards.

Validating Indonesia's DPIA framework through alignment with international best practices, such as GDPR, ISO/IEC 27001, and NIST's RMF, ensures it meets the highest data protection and risk management standards. By incorporating these globally recognized frameworks and adapting them to Indonesia's unique regulatory and technological landscape, the DPIA framework can be comprehensive and flexible, ensuring it applies to organizations of all sizes and sectors.

4.2 Risk assessment tools

Risk assessment tools play a critical role in validating a DPIA framework by enabling organizations to systematically evaluate potential risks to personal data during data processing activities. These tools provide a structured approach to identifying, assessing, and mitigating risks, essential for ensuring compliance with data protection regulations, such as Indonesia's Personal Data Protection Act (UU PDP).

Key Risk Assessment Tools

Several internationally recognized risk assessment tools and frameworks can be adapted to the Indonesian context, helping organizations quantify and manage privacy-related risks effectively:

1) Privacy Impact Assessment (PIA) assesses the privacy risks associated with data processing activities, particularly in high-risk operations such as large-scale data processing or profiling [3]. These tools help organizations ensure that appropriate data protection measures are in place to mitigate risks to individuals' privacy. For example, automated PIA tools offer pre-configured templates that guide users through assessing privacy risks based on the types of data processed and the potential for harm [8].

2) ISO/IEC 27005 focuses on information security risk management and can be integrated into the DPIA framework to identify personal data risks. This standard provides detailed guidance on the risk management process, including risk identification, analysis, evaluation, and treatment, as depicted in Figure 3. Using ISO/IEC 27005, organizations can map out the likelihood and impact of risks associated with specific data processing activities, allowing them to implement targeted controls to reduce these risks [19].

3) The OCTAVE Allegro framework is a structured methodology designed to identify, assess, and mitigate operational risks related to critical information assets. As shown in Figure 4, it involves eight key steps, from establishing risk measurement criteria to formulating mitigation strategies. By focusing on the operational risk environment, OCTAVE Allegro helps organizations prioritize and address vulnerabilities effectively, ensuring that critical assets are protected through a systematic and repeatable process [20, 21].

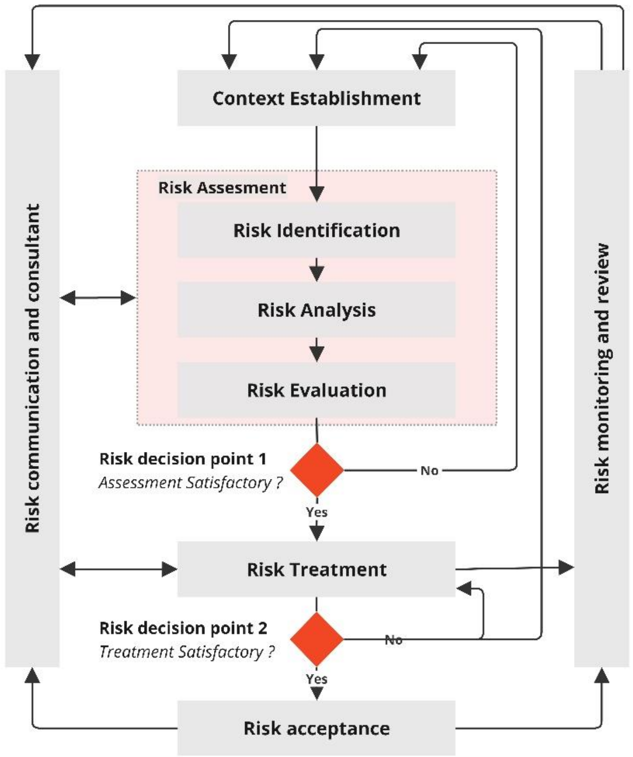


Figure 3. ISO/IEC 27005 information security risk management process

It provides a detailed framework for identifying and analyzing risks related to data processing, helping organizations prioritize risk mitigation actions based on the business impact of potential data breaches [20].

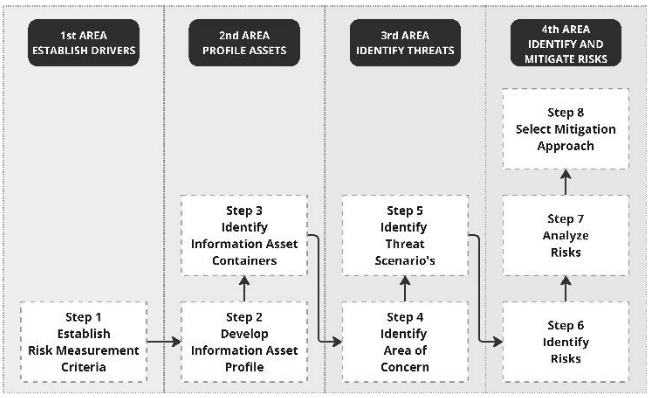

1st AREA
ESTABLISH DRIVERS
2nd AREA
PROFILE ASSETS
3rd AREA
IDENTIFY THREATS
4th AREA
IDENTIFY AND MITIGATE RISKS
Step 8
Select Mitigation Approach
Step 3
Identify Information Asset Containers
Step 5
Identify Threat Scenario's
Step 7
Analyze Risks
Step 1
Establish Risk Measurement Criteria
Step 2
Develop Information Asset Profile
Step 4
Identify Area of Concern
Step 6
Identify Risks

Figure 4. OCTAVE Allegro area and step

Adapting Risk Assessment Tools to Indonesia's Context

While these risk assessment tools provide a strong foundation for managing risks, they must be adapted to suit Indonesia's technological, regulatory, and sector-specific challenges. For example, large organizations in sectors such as finance and telecommunications can benefit from comprehensive tools like ISO/IEC 27005 or the NIST RMF, as they often have the technical capacity and resources to implement detailed, resource-intensive assessments.

In contrast, small and medium-sized enterprises (SMEs) and public sector institutions may require more scalable and simplified risk assessment tools that allow them to comply with regulations without incurring significant costs. Tools such as automated PIA templates can provide a cost-effective solution for smaller organizations by offering pre-configured assessments that streamline the DPIA process [22]. Additionally, integrating these tools with existing cloud-based platforms can help organizations manage data protection without advanced technical expertise.

Sector-Specific Risk Assessment Modules

Given the diverse sectors within Indonesia's economy, the DPIA framework should incorporate sector-specific risk assessment modules that address the unique risks associated with different industries. For instance, in the healthcare sector, risk assessment tools should focus on protecting sensitive health data and the potential consequences of data breaches, such as patient identity theft or unauthorized access to medical records. On the other hand, the finance sector may need tools that assess the risks associated with financial fraud and cyber-attacks on sensitive transactional data.

By customizing risk assessment tools to fit the needs of various industries, organizations can better manage the specific risks they face, ensuring that their DPIA frameworks are compliant with regulations and tailored to their operational realities.

Continuous Risk Monitoring and Updates

A critical aspect of risk assessment tools is their ability to support continuous monitoring and updates. Organizations must regularly review and update their risk assessments as data processing technologies evolve and new risks emerge. Tools that offer real-time tracking and automatic updates ensure that risk assessments remain current, helping organizations mitigate new threats proactively.

Moreover, risk scoring systems integrated into these tools can help organizations understand the magnitude of their risks, allowing them to prioritize their risk mitigation efforts based on data-driven insights. This is particularly useful in dynamic sectors such as telecommunications, where data processing practices change frequently and require constant vigilance.

4.3 Regulatory feedback

Another critical component in validating the effectiveness of a DPIA framework is incorporating regulatory feedback from government bodies and data protection authorities. In Indonesia, article 35 of UU PDP outlines the legal obligations for conducting DPIAs, particularly for high-risk processing activities. Engaging with regulators such as the Indonesian Ministry of Communication and Digital of the Republic of Indonesia (KOMDIGI) and the Indonesian National Cyber and Crypto Agency (BSSN) ensures that the DPIA framework aligns with national laws and regulatory expectations, providing organizations with the guidance they need to achieve compliance.

Ensuring Compliance with National Laws

The UU PDP requires that Data Protection Impact Assessments (DPIAs) be conducted for data processing activities that pose a high risk to individuals' privacy. This is especially important for sensitive personal data or large-scale data processing. The Data Protection Authority (DPA) regulatory bodies are expected to provide guidelines and oversight to ensure that organizations meet these requirements. By incorporating regulatory feedback into the DPIA framework, organizations can ensure that their assessments are aligned with the legal thresholds set by the law.

For instance, regulatory feedback can clarify grey areas in the law, such as what constitutes high-risk data processing or how to handle cross-border data transfers. Regular engagement with regulators allows organizations to stay informed about the latest regulatory updates and interpretations of the law. Studies indicate that continuous collaboration with regulators helps ensure that data protection frameworks remain adaptive to evolving regulatory requirements, which is essential in fast-developing regulatory environments like Indonesia [17].

Collaborative Development of Guidelines

Regulatory authorities often develop guidelines and best practices for conducting DPIAs. These guidelines provide practical steps for organizations to follow, ensuring that DPIA processes are compliant with regulations and streamlined and useful for implementation. By working closely with regulators, organizations can provide feedback on the feasibility and practicality of these guidelines, ensuring that they are adaptable to the unique challenges faced by different sectors.

For example, the GDPR has shown the benefits of regulator-led consultations, where data controllers can seek clarification on DPIA requirements. Similarly, ongoing consultations between regulatory bodies and organizations in Indonesia can lead to sector-specific guidance, particularly important in healthcare and financial services industries, where data protection requirements are more stringent.

Workshops and Public Consultations

Engaging with regulators through workshops and public consultations is an effective way to gather feedback on the DPIA framework. These platforms allow organizations to raise concerns about the practical challenges of implementing DPIAs, such as resource constraints, technological limitations, or the complexities of assessing risks in cross-border data processing.

In Indonesia, public consultations led by KOMDIGI allow regulators and organizations to collaborate on refining DPIA guidelines. Through these consultations, organizations can voice their concerns, and regulators can offer insights into navigating the challenges of implementing DPIAs under the UU PDP. Research suggests that such collaborative efforts help foster transparency and compliance, improving the overall effectiveness of data protection frameworks.

Adapting to Regulatory Changes

Organizations must continuously update their DPIA documents to remain compliant as data protection laws evolve. Incorporating regulatory feedback ensures organizations can respond effectively to regulatory changes, such as UU PDP updates or new data protection guidelines. Continuous engagement with regulators helps organizations avoid emerging data privacy issues and ensures that their DPIA frameworks remain dynamic and adaptable.

For instance, regulators may introduce new requirements around data localization, cross-border data transfers, or the handling of biometric data. By incorporating ongoing feedback from regulators, organizations can update their DPIA in real time, ensuring that their assessments reflect the latest legal and regulatory developments.

Feedback Mechanisms within the Framework

Organizations should establish internal feedback mechanisms to incorporate regulatory feedback into their DPIA processes and ensure continuous improvement. This includes setting up regular reviews of DPIA procedures, integrating updates from regulators, and conducting internal audits to assess compliance with the latest regulatory requirements. Additionally, by maintaining open communication channels with regulatory authorities, organizations can seek guidance and support when facing complex data protection challenges.

5. CHALLENGES IN IMPLEMENTING A DPIA FRAMEWORK IN INDONESIA

Given Indonesia's unique cultural, technological, and regulatory landscape, implementing a DPIA framework presents several challenges, as depicted in Figure 5. These challenges must be addressed to ensure the DPIA framework is effective, scalable, and adaptable across diverse sectors. This section explores the key obstacles that Indonesian organizations face in implementing DPIA, including cultural and social considerations, technological readiness, and regulatory enforcement.

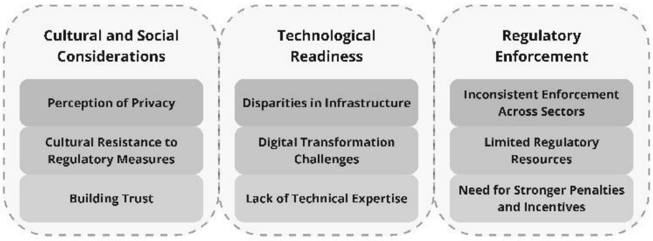

Cultural and Social Considerations
Perception of Privacy
Cultural Resistance to Regulatory Measures
Building Trust
Technological Readiness
Disparities in Infrastructure
Digital Transformation Challenges
Lack of Technical Expertise
Regulatory Enforcement
Inconsistent Enforcement Across Sectors
Limited Regulatory Resources
Need for Stronger Penalties and Incentives

Figure 5. Challenges in implementing DPIA in Indonesia

5.1 Cultural and social considerations

One significant challenge in implementing a DPIA framework in Indonesia is the country's diverse cultural and social landscape. Indonesia is home to various ethnic groups and languages, and cultural norms influence how individuals and organizations perceive privacy and data protection.

Perception of Privacy

In some regions of Indonesia, there is limited awareness of data privacy issues, which can hinder the implementation of DPIA frameworks. Cultural attitudes toward privacy may differ significantly from Western norms, where personal data protection is often seen as a fundamental right. Studies suggest that in many developing regions, including parts of Indonesia, individuals may prioritize economic benefits or convenience over data privacy, leading to lower levels of engagement with privacy regulation [13]. This challenges organizations aiming to implement DPIAs, as the broader societal understanding of personal data risks is often underdeveloped.

Cultural Resistance to Regulatory Measures

In certain sectors or communities, there may be resistance to regulatory measures perceived as imposing external controls on how organizations manage their data. Cultural norms that value informal business practices or communal decision-making may conflict with the structured and formal requirements of a DPIA framework. For instance, small and medium-sized enterprises (SMEs) in rural areas may resist implementing DPIAs due to a lack of understanding of the benefits and necessity of these assessments, especially when viewed as time-consuming and resource-intensive.

Building Trust

Building trust between regulators, organizations, and the public is essential for successfully adopting DPIA frameworks. In Indonesia, where skepticism toward government regulations can sometimes be high, efforts to build trust and promote the benefits of data protection through awareness campaigns and community engagement will be critical. Studies have shown that targeted education initiatives can improve public perception of privacy and data protection [17].

5.2 Technological readiness

The varying levels of technological readiness across sectors and regions in Indonesia present another challenge to implementing DPIA frameworks. Technological infrastructure is unevenly developed, with advanced capabilities in urban and industrial sectors but significant gaps in rural areas and smaller organizations.

Disparities in Infrastructure

Indonesia's digital infrastructure is highly developed in major urban centers like Jakarta and Surabaya, where large organizations in sectors such as finance and telecommunications have access to advanced data protection tools and resources. However, in rural and remote areas, many organizations face significant limitations regarding internet connectivity, digital literacy, and access to modern technologies. For example, SMEs and public sector institutions in these regions may lack the technical infrastructure to conduct DPIAs effectively, relying instead on paper-based systems or outdated technology [13].

Digital Transformation Challenges

While Indonesia is undergoing a rapid digital transformation, many organizations are still in the early stages of adopting data protection technologies. Implementing DPIAs relies heavily on an organization's capacity to integrate technology into its operations, conduct risk assessments, and ensure data security. This requires a significant investment in IT infrastructure and training for personnel, which can be a challenge for smaller organizations with limited budgets.

Lack of Technical Expertise

In addition to infrastructure challenges, Indonesia has a significant skills gap in data protection and privacy management. Many organizations lack the technical expertise required to conduct DPIAs, including the ability to assess data risks, implement technical safeguards, and comply with data protection laws. This lack of knowledge makes it difficult for organizations to adopt and maintain a DPIA framework without substantial external support or government-provided resources [14].

5.3 Regulatory enforcement

The success of a DPIA framework depends on effective regulatory enforcement, but challenges in enforcing data protection laws pose significant obstacles to its widespread adoption in Indonesia.

Inconsistent Enforcement Across Sectors

One key challenge in Indonesia is the inconsistent enforcement of data protection laws across sectors. Larger organizations, particularly those in highly regulated sectors like banking and telecommunications, are more likely to comply with data protection regulations, as they have the resources to implement comprehensive compliance programs. However, in other sectors—particularly those with fewer regulatory oversight mechanisms, such as retail or hospitality—there is less compliance with data protection laws, leading to gaps in enforcing DPIA requirements.

Limited Regulatory Resources

Indonesia's regulators, including KOMDIGI, face significant challenges regarding resource constraints and the capacity to monitor and enforce data protection laws throughout the country. The limited availability of resources makes it difficult for regulators to audit organizations, conduct compliance checks, and ensure that DPIAs are being implemented effectively. This creates a compliance gap in which many organizations may not fully understand or adhere to DPIA requirements.

Need for Stronger Penalties and Incentives

To encourage greater compliance with DPIA requirements, regulators may need to introduce stronger penalties for non-compliance and incentives for organizations adopting best data protection practices. Penalties for data breaches or failure to conduct DPIAs should be clearly outlined and enforced to deter negligence. On the other hand, offering incentives such as compliance certifications or tax benefits for organizations that demonstrate a commitment to data protection could help drive broader adoption of DPIA frameworks.

The successful implementation of a DPIA framework in Indonesia requires addressing several key challenges, including cultural and social considerations, technological readiness, and regulatory enforcement. By recognizing and addressing these challenges, organizations and regulators can work together to develop a robust, scalable, and compliant DPIA framework that meets the diverse needs of Indonesia's economic sectors and regions.

6. PROPOSED DPIA FRAMEWORK FOR INDONESIA

This study follows a comprehensive methodology that integrates best practices from various frameworks and academic sources to identify and validate critical factors for designing a data protection impact assessment (DPIA) framework suitable for Indonesia. The process depicted in Figure 6 involved three primary stages: reviewing best practice frameworks, analyzing academic literature, and synthesizing these insights to develop a set of key factors relevant to Indonesia's DPIA context.

The first step in the methodology involved reviewing 17 factors from 7 best practice frameworks related to Privacy Impact Assessments (PIA), 33 factors from 6 academic articles, and 26 factors from 4 best practice frameworks specific to *Information Technology Risk Management* (ITRM). These sources were selected based on their relevance to risk assessment and privacy protection, especially in sectors that closely align with the challenges faced by Indonesian organizations.

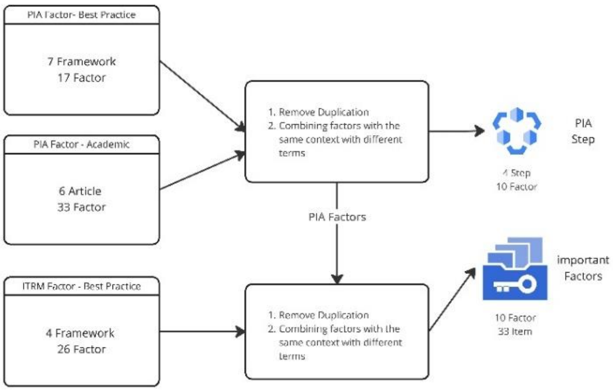


Figure 6. DPIA important factors harmonization methodology

A consolidation process was conducted after compiling the factors from the above sources. This involved eliminating duplicates—instances where different frameworks or studies listed the same factor under different terminology—and merging similar factors with the same contextual meaning but different labels. This step was critical to ensure the final set of factors was comprehensive yet streamlined, avoiding redundancy while capturing all relevant aspects of DPIA implementation.

The consolidated factors were then grouped into a structured framework based on their thematic similarities. This resulted in two main outputs:

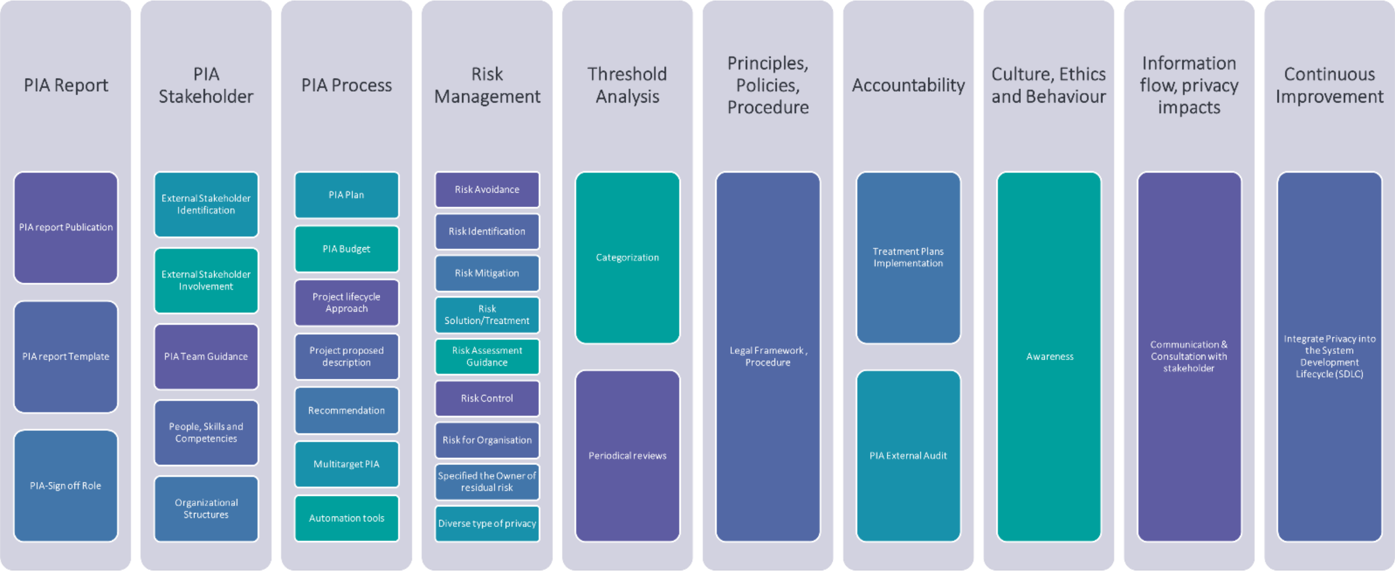
• A 4-stage process with 10 categories of DPIA factors that provide a structured approach for organizations to follow when implementing DPIA frameworks.

• A 10 factors comprising 33 specific items further breaks down the critical components necessary for conducting a comprehensive DPIA tailored specifically to Indonesia's regulatory and operational context.

This methodology's outcome is a refined and validated set of factors for conducting DPIAs, which balance global best practices with localized adaptations. By synthesizing these factors, the proposed DPIA framework for Indonesia becomes both scalable and practical, offering guidelines for organizations of different sizes and sectors to implement DPIAs effectively.

6.1 Important factors

The proposed DPIA framework for Indonesia, developed from extensive research and analysis of existing best practices and academic literature, is structured around several key components that address different stages of the DPIA process. These critical factors, as depicted in Figure 7, ensure that the framework is comprehensive and adaptable to the diverse needs of Indonesian organizations. Below is a breakdown of the identified factors, categorized into various themes crucial for implementing a successful DPIA.



PIA Report
PIA report Publication
PIA report Template
PIA-Sign off Role
PIA Stakeholder
External Stakeholder Identification
External Stakeholder Involvement
PIA Team Guidance
People, Skills and Competencies
Organizational Structures
PIA Process
PIA Plan
PIA Budget
Project lifecycle Approach
Project proposed description
Recommendation
Multitarget PIA
Automation tools
Risk Management
Risk Avoidance
Risk Identification
Risk Mitigation
Risk Solution/Treatment
Risk Assessment Guidance
Risk Control
Risk for Organisation
Specified the Owner of residual risk
Diverse type of privacy
Threshold Analysis
Categorization
Periodical reviews
Principles, Policies, Procedure
Legal Framework , Procedure
Accountability
Treatment Plans Implementation
PIA External Audit
Culture, Ethics and Behaviour
Awareness
Information flow, privacy impacts
Communication & Consultation with stakeholder
Continuous Improvement
Integrate Privacy into the System Development Lifecycle (SDLC)

Figure 7. DPIAs important factors

6.1.1 PIA report

The PIA report serves as the central document that outlines the findings of the DPIA. It includes:

• PIA Report Publication: Ensures transparency and accountability by making the DPIA report available for stakeholders to review.

• PIA Report Template: This template provides a standardized format for organizations, ensuring consistency in DPIA reporting across sectors.

• PIA Sign-Off Role: This role designates specific individuals or teams responsible for approving and finalizing the DPIA, ensuring the process is overseen by accountable parties.

6.1.2 PIA stakeholders

Effective stakeholder involvement is critical for a successful DPIA. This category includes:

• External Stakeholder Identification and Involvement: Identifying and engaging external stakeholders, such as regulatory bodies, customers, or partners, ensure that diverse perspectives are considered in the DPIA process.

• PIA Team Guidance: Ensures that the internal DPIA team receives appropriate guidance on how to conduct assessments effectively.

• People, Skills, and Competencies: This section highlights the need for trained professionals with expertise in data protection, privacy risks, and regulatory compliance.

• Organizational Structures: These refer to the internal structures that support the DPIA process and ensure that roles and responsibilities are clearly defined.

6.1.3 PIA process

The PIA process covers the detailed steps involved in conducting a DPIA:

• PIA Plan and Budget: Outlines the resources and financial considerations required for a DPIA.

• Project Lifecycle Approach: Ensures that the DPIA is integrated into the organization's project management process, from planning to completion.

• Project Proposal Description and Recommendations: Describes the project scope and provides actionable recommendations based on the DPIA findings.

• Multi-Target PIA and Automation Tools: This approach focuses on assessing multiple aspects of data processing and utilizing automated tools to streamline the DPIA process.

6.1.4 Risk management

A thorough risk management strategy is essential for mitigating data protection risks. This category includes:

• Risk Avoidance, Identification, Mitigation, and Treatment: Involves identifying potential privacy risks and taking steps to avoid or mitigate them.

• Risk Assessment Guidance: Provides structured guidance on assessing the severity and likelihood of risks.

• Risk Control and Ownership: Clarifies who manages residual risks after completing the DPIA.

• Diverse Types of Privacy: This recognizes the different forms of privacy (e.g., informational, bodily, and communication) that must be protected.

6.1.5 Threshold analysis

The threshold analysis determines whether a DPIA is required for a particular data processing activity:

• Categorization: Categorizes the types of data processing activities based on their risk levels.

• Periodic Reviews: Ensures that DPIAs are reviewed and updated regularly to reflect changes in the data processing environment.

6.1.6 Principles, policies, and procedures

• This category addresses the legal and procedural framework that supports the DPIA:

• Legal Framework and Procedures: This ensures that the DPIA complies with national and international data protection laws, such as the Indonesian Personal Data Protection Act (UU PDP) and the General Data Protection Regulation (GDPR).

6.1.7 Accountability

Accountability is a key factor in ensuring that data protection measures are effectively implemented:

• Treatment Plans Implementation: Focuses on applying measures identified during the DPIA to mitigate privacy risks.

• PIA External Audit: This policy encourages external audits to ensure that regulatory requirements and best practices have conducted the DPIA process.

6.1.8 Culture, ethics, and behavior

The organizational culture plays a significant role in the success of the DPIA:

• Awareness: Raises awareness about the importance of privacy protection across the organization, ensuring that all employees understand their role in maintaining data security

6.1.9 Information flow and privacy impacts

This factor focuses on the flow of information and how it impacts privacy:

• Communication and Consultation with Stakeholders: Ensure stakeholders are kept informed throughout the DPIA process, particularly regarding privacy and data security decisions.

6.1.10 Continuous improvement

The DPIA process should not be a one-time activity but part of an ongoing effort to improve data protection:

• Integrating Privacy into the System Development Lifecycle (SDLC): This approach incorporates privacy considerations into every stage of system development, ensuring that data protection is built into the organization's processes from the ground up.

Figure 7 breaks down the critical components of a DPIA into ten key dimensions, covering the end-to-end process from planning and execution to reporting and continuous improvement. It highlights the importance of:

• Stakeholder engagement for collaboration and transparency,

• Risk management for effective privacy protection,

• Compliance with regulatory frameworks, and

• Sustainability through continuous improvement and integration into development lifecycles.

This holistic approach ensures that the DPIA framework aligns with international best practices while being adaptable to Indonesia's regulatory and organizational context.

6.2 Implications for policy and practice

This subsection highlights key factors necessary for the successful implementation of a Data Protection Impact Assessment (DPIA) framework in Indonesia. These factors, along with their descriptions and implications for policy and practice, are systematically outlined in Table 2.

Table 2. Factors description and implications

Factor	Description	Relevance to Indonesia
Stakeholder Involvement	Engagement of DPOs, legal experts, IT professionals, and management to ensure a holistic assessment.	Essential for bridging knowledge gaps and ensuring a comprehensive evaluation, particularly in sectors like healthcare and finance.
Data Sensitivity and Risk Classification	Clear methods for identifying and classifying data sensitivity and risks.	Critical for prioritizing resources in regions with limited technological infrastructure.
Regulatory Compliance	Alignment with the UU PDP and interpretation of its requirements.	Provides clarity for SMEs and larger organizations on compliance obligations.
Risk Assessment Methodologies	Adoption of structured frameworks like ISO/IEC 27005 for systematic evaluation.	Enables scalability and practical application for organizations of varying capacities.
Technological Infrastructure	Leveraging automation and digital tools for DPIA processes.	Helps resource-constrained organizations improve efficiency and compliance.
Training and Capacity Building	Development of training programs tailored to varying expertise levels across sectors.	Addresses the skills gap in SMEs and promotes knowledge-sharing initiatives.

6.2.1 Informing training programs

The identified factors underscore the need for tailored training programs that address the varying levels of expertise across Indonesian organizations. For SMEs, simplified modules focusing on basic compliance and risk management can be developed, while larger organizations may benefit from advanced technical training.

6.2.2 Policy design

Policymakers can use these findings to design regulations that provide clearer guidance on DPIA implementation, especially for high-risk sectors like healthcare and finance. This includes offering incentives for compliance and penalties for negligence.

6.2.3 Technology integration

Promoting cloud-based solutions and automated DPIA tools can reduce barriers to implementation for organizations in less digitized regions. Government-supported initiatives to provide affordable access to these technologies can foster broader adoption.

6.2.4 Stakeholder collaboration

The involvement of industry representatives, regulators, and civil society organizations ensures that the framework is practical and aligned with the realities of Indonesia's socio-economic landscape.

This section systematically outlines these factors and emphasizes their significance, linking the study's findings to practical steps that can enhance data protection practices in Indonesia.

6.3 DPIA framework

To address Indonesia's unique challenges, the Data Protection Impact Assessment (DPIA) framework must be tailored to align with the country's regulatory, socio-cultural, and technological landscape. The proposed framework ensures that organizations across various sectors and sizes can effectively implement DPIAs by considering risk factors, stakeholder engagement, and regulatory enforcement.

Customized DPIA Approach

The proposed DPIA framework for Indonesia is designed to be flexible and adaptive, allowing organizations to align their DPIA implementation with their specific risks, resources, and technical capacity. Below are the key aspects of the customized approach:

a) Flexibility and Scalability

The framework must be scalable to accommodate both large organizations and SMEs (Small and Medium-sized Enterprises):

- Large organizations in sectors like finance and telecommunications can integrate automated DPIA tools with granular risk analysis, leveraging advanced technologies and dedicated experts.
- SMEs and public institutions with limited resources can streamline the DPIA process using automated PIA templates and pre-configured tools. This ensures compliance without requiring deep technical expertise [22].

b) Sector-Specific Integration

Each sector has different risk profiles, so the DPIA framework should offer sector-specific modules to address their unique challenges:

- In healthcare, the focus should be on safeguarding patient data and ensuring compliance with standards such as Health Insurance Portability and Accountability (HIPAA).
- In finance, the framework must prioritize fraud prevention and cybersecurity measures to protect sensitive financial data and ensure compliance with the Payment Card Industry Data Security Standard (PCI DSS) standards.
- This sector-specific approach ensures that organizations focus on relevant risks while complying with the Indonesian UU PDP.

c) Use of Automation and Cloud-Based Platforms

To enhance efficiency, the proposed DPIA framework encourages the use of automated tools and cloud platforms:

- Cloud-based platforms provide accessible solutions, especially for organizations in remote areas with limited resources.
- Automated tools can offer real-time risk assessments and pre-configured templates, helping organizations conduct DPIAs quickly and effectively.

d) Regulatory Support and Collaboration

The DPIA framework should emphasize collaboration with regulators such as Kominfo to ensure the implementation of guidelines and best practices. This collaboration should involve regular audits, feedback loops, and incentives for organizations that successfully implement the framework.

7. CONCLUSIONS

This study comprehensively analyzes the critical factors for designing a Data Protection Impact Assessment (DPIA) framework tailored to Indonesia's unique regulatory, cultural, and technological landscape. By synthesizing international best practices with localized adaptations, the proposed framework offers scalable and practical solutions for diverse organizational contexts, including small and medium-sized enterprises (SMEs) and larger enterprises in regulated industries.

Key findings highlight the importance of stakeholder involvement, scalable risk assessment methodologies, and technological readiness in implementing effective DPIAs. The study underscores the relevance of capacity-building initiatives and automated tools to bridge knowledge and resource gaps, particularly in less digitized regions. Additionally, alignment with international standards such as GDPR, ISO/IEC 27001, and NIST's Risk Management Framework ensures that the framework meets global benchmarks while addressing local challenges.

The implications of this research extend beyond Indonesia, providing a model for adapting DPIA practices in other developing economies undergoing digital transformation. However, the study has limitations, including the lack of empirical validation through pilot implementations and a focus on theoretical frameworks. Future research should address these gaps by conducting case studies and exploring the impact of the proposed DPIA framework on organizational compliance and data protection outcomes.

This study contributes to the broader field of privacy management by advancing the discourse on localized data protection strategies. It also supports Indonesia's efforts to foster trust and accountability in its rapidly evolving digital economy.

ACKNOWLEDGMENT

We thank Telkom University's Research and Community Service (PPM) Department for fully funding this project through the Internal grant Scheme. We hope this research will strengthen the Indonesian landscape of Personally Identifiable Information.

REFERENCES

[1] General Data Protection (GDPR), EU GDPR (General Data Protection Regulation). 2016. Available: https://gdpr-info.eu/.

[2] Dewan Perwakilan Rakyat-indonesia, Undang Undang No 27 Tahun 2022 Tentang Pelindungan Data Pribadi. 2022. Available: https://peraturan.bpk.go.id/Download/224884/UU%20Nomor%2027%20Tahun%202022.pdf.

[3] Wright, D., De Hert, P. (2012). Privacy Impact Assessment (Vol. 6). Dordrecht: Springer. http://doi.org/10.1007/978-94-007-2543-0

[4] Van Dijk, N., Gellert, R., Rommetveit, K. (2016). A risk to a right? Beyond data protection risk assessments. Computer Law & Security Review, 32(2): 286-306. http://doi.org/10.1016/j.clsr.2015.12.017

[5] European Data Protection Board (EPDB). (2017). Guidelines on Data Protection Impact Assessment (DPIA). https://ec.europa.eu/newsroom/article29/items/611236/en.

[6] Office of the Australian Information Commissioner. https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/privacy-impact-assessments/guide-to-undertaking-privacy-impact-assessments.

[7] Prinsloo, P., Kaliisa, R. (2022). Data privacy on the African continent: Opportunities, challenges and implications for learning analytics. British Journal of Educational Technology, 53(4): 894-913. http://doi.org/10.1111/bjet.13226

[8] Dashti, S., Ranise, S. (2019). A tool-assisted methodology for the data protection impact assessment. In Proceedings of the 16th International Joint Conference on e-Business and Telecommunications (ICETE 2019), pp. 276-283. https://www.scitepress.org/Link.aspx?doi=10.5220/0007932202760283.

[9] Hart, S., Ferrara, A.L., Paci, F. (2020). Fuzzy-based approach to assess and prioritize privacy risks. Soft Computing, 24: 1553-1563. http://doi.org/10.1007/s00500-019-03986-5

[10] Aprilianti, I., Dina, S. A. (2021). Co-regulating the indonesian digital economy (No. 30). Policy Paper. https://repository.cips-indonesia.org/media/publications/332998-co-regulating-the-indonesian-digital-eco-30376717.pdf.

[11] Gellert, R. (2018). Understanding the notion of risk in the general data protection regulation. Computer Law & Security Review, 34(2): 279-288. http://doi.org/10.1016/j.clsr.2017.12.003

[12] Prakoso, M.H., Irawan, F., Sufianto, A.M., Rediansyah, D. (2023). Comprehensive assessment of small batch advanced metering infrastructure utilization on java region to support Indonesian smart grid systems. In 2023 4th International Conference on High Voltage Engineering and Power Systems (ICHVEPS), Denpasar Bali, Indonesia, pp. 103-108. https://doi.org/10.1109/ICHVEPS58902.2023.10257557

[13] Trinugroho, I., Pamungkas, P., Wiwoho, J., Damayanti, S.M., Pramono, T. (2022). Adoption of digital technologies for micro and small business in Indonesia. Finance Research Letters, 45: 102156. http://doi.org/10.1016/j.frl.2021.102156

[14] Chan, S., Jalaluddin, J., Asni, K. (2023). Digital technology as a resilience-enhancing tool for SMES in earthquake-prone developing countries. In E3S Web of Conferences, 447: 03002. http://doi.org/10.1051/e3sconf/202344703002

[15] Hosseinpoor, A.R., Nambiar, D., Tawilah, J., Schlotheuber, A., Briot, B., Bateman, M., Davey, T., Kusumawardani, N., Myint, T., Nuryetty, M.T., Prasetyo, S., Suparmi, Floranita, R. (2018). Capacity building for health inequality monitoring in Indonesia: Enhancing the equity orientation of country health information systems. Global Health Action, 11(sup1): 7-12. http://doi.org/10.1080/16549716.2017.1419739

[16] Chrysantina, A., Sanjaya, G., Pinard, M. (2019). Improving health information management capacity with digital learning platform: The case of DHIS2 online academy. Procedia Computer Science, 161: 195-203. http://doi.org/10.1016/j.procs.2019.11.115

[17] Nurdin, M., Baharuddin, T. (2023). Capacity building challenges and strategies in the development of new capital city of Indonesia. Jurnal Bina Praja, 15(2): 221-232. http://doi.org/10.21787/jbp.15.2023.221-232

[18] Enterprise, I.P.T. (2020). NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.01162020

[19] ISO/IEC 27005:2018. ISO, 2020. https://www.iso.org/standard/75281.html, accessed on Mar. 24, 2022.

[20] Kurt, E.S., Yaşar, A., Terzioğlu, K., Demirkıran, S. (2022). A new generation method for assessing information security risks: OCTAVE Allegro. In International Conference on Eurasian Economies 2022, Baku - AZERBAIJAN, 2022. http://doi.org/10.21236/ada470450

[21] Caralli, R.A., Stevens, J.F., Young, L.R., Wilson, W.R. (2007). Introducing octave allegro: Improving the information security risk assessment process. Hansom AFB, MA. https://www.semanticscholar.org/paper/Introducing-OCTAVE-Allegro%3A-Improving-the-Security-Caralli-Stevens/490fb4c8fad85a2ea6975504b4984d713cfb0361.

[22] Zibuschka, J. (2020). Analysis of automation potentials in privacy impact assessment processes. In Computer Security: ESORICS 2019 International Workshops, CyberICPS, SECPRE, SPOSE, and ADIoT, Luxembourg City, Luxembourg, pp. 279-286. https://doi.org/10.1007/978-3-030-42048-2_18

NOMENCLATURE

Term	Definition
AMI	Advanced Metering Infrastructure
BSSN	Badan Siber Dan Sandi Negara
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officers
EPDB	European Data Protection Board
EU	European Union
GDPR	General Data Protection Regulation
HIPAA	Health Information Privacy
ISMS	Information Security Management System
ISO/IEC	International Organization for Standardization
ITRM	Information Technology Risk Management
KOMDIGI	Indonesian Ministry of Communication and Digital of the Republic of Indonesia (Kementerian Komunikasi dan Digital)
NIST	National Institute of Standards and Technology
OAIC	Office of the Australian Information Commissioner
PIA	Privacy Impact Assessment
RMF	Nist Risk Management Framework
SDLC	System Development Lifecycle
SMEs	Small And Medium-Sized Enterprises
UU PDP	Undang-Undang Pelindungan Data Pribadi