Vol. 8, No. 3, June 2026

ISI Journal of Information Systems and Informatics

Published By Asosiasi Doktor Sistem Informasi Indonesia

Integrating ISO, CIPP and CMMI Frameworks for Data Privacy Compliance: A System-Level Maturity Assessment with PDCA-Based Architecture in a KBMI Group IV Bank

Delfindra Faiz Noorhadi[1], Mukhammad Andri Setiawan [2]

[1,2] Informatics Department, Postgraduate Program, Faculty of Industrial Technology, Islamic University of Indonesia

Received:
October 28, 2025
Revised:
May 10, 2026
Accepted:
May 30, 2026
Published:
June 22, 2026

Corresponding Author:
Author Name*:
Delfindra Faiz Noorhadi
Email*:
delfindra.noorhadi@students.uii.ac.id

DOI:
10.63158/journalisi.v8i3.1623

Abstract. This study examines the organizational and technical readiness of a systemically important Indonesian bank (KBMI Group IV) in responding to the enactment of the Personal Data Protection (PDP) Law, which necessitates robust privacy engineering and system architecture adaptation. This maturity assessment is conducted as a single-case study based on empirical data collected from two primary respondents: a Business Branch Manager and a Department Head Application Developer. To comprehensively evaluate the system, this study integrates a multi-model framework. First, the Context, Input, Process and Product (CIPP) model qualitatively measures the organization's governance, resources, workflows and policy impacts. These qualitative findings are then translated into CMMI-based process maturity scores. The observed empirical findings reveal an overall maturity score of 3.69, positioning the organization at Level 3 (Defined) as an institutional baseline rather than a sector-wide indicator. The observed findings also expose a regulatory conflict between the PDP Law's 'Right to be Forgotten' and mandatory financial data retention regulations. To address these observed gaps, the study proposes two framework outputs: a comprehensive mapping matrix that aligns regulatory requirements with ISO 27001 and ISO 27701 standards and a conceptual PDCA-based system architecture utilizing data masking and pseudonymization. Although the proposed framework is developed within the context of a single institution, it offers a valuable preliminary foundation for evaluating technical privacy compliance in the banking sector, subject to further validation across a broader range of financial institutions.

Keywords: CIPP, CMMI Maturity Assessment, PDP Law Compliance, Privacy Engineering, Banking Information Systems

1. INTRODUCTION

Currently, data security issues particularly data breaches are becoming an increasingly important concern for both public and private organizations [1]. Data from the Ministry of Communication and Information Technology indicates that 47.8% of organizations still lack an adequate understanding of Personal Data Protection (PDP) regulations and their provisions [2]. This vulnerability is further reflected in the National Cyber and Encryption Agency (BSSN) report, which recorded 330 million traffic anomalies and 241 suspected data breaches throughout 2024 [2]. To address these challenges, the government enacted Law No. 27 of 2022 on Personal Data Protection, which came into effect in October 2024 [3].

The PDP Law is designed to protect personal data from misuse, illegal access and data leaks, dividing personal data into two categories: general personal data and specific personal data [4], [5]. In practice, the implementation of the PDP Law faces various obstacles, including low organizational awareness, uneven technical readiness and the need for more structured governance guidelines [2]. As regulatory compliance with data protection laws requires significant financial and organizational investment [6], a systematic and structured approach is essential to ensure effective adherence.

Sectors with high risk of data breaches, particularly in the finance industry, are highly relevant in the context of personal data protection [6], [7], [8]. Banking is considered especially vulnerable, facing two primary risks: consumer data security and errors in transaction processing [5]. The sector operates under strict standards for personal data management, given its dependence on the collection, storage and processing of large volumes of customer data, including financial, transactional, identity and biometric records [9].

In May 2023, Bank BSI experienced a ransomware attack known as LockBit 3.0, resulting in the leakage of sensitive customer data [4], [10]. The BSI incident served as a stark warning to the national banking ecosystem. The research focuses specifically on one KBMI Group IV bank, which are groups of banks with medium to large core capital that manage assets between more than IDR 14 trillion and above IDR 70 trillion [11]. Classified as a Systemic Bank in accordance with POJK No. 2/POJK.03/2018, where failure in banks

with these characteristics has the potential to cause a domino effect on other financial institutions, triggering the risk of massive withdrawals (bank runs) and disrupting the stability of the national financial system [12], [13]. This condition underscores the urgency of implementing globally proven information security standards.

The International Organization for Standardization (ISO) plays an important role by providing technical specifications that regulate how systems, products and processes should operate [14]. In the context of data security, ISO 27001 is one of the most widely adopted standards, designed to establish, implement and continuously improve an Information Security Management System (ISMS) [15]. The implementation helps organizations reduce losses from information security incidents while increasing consumer confidence and competitive advantage [16]. However, ISO 27001 does not comprehensively cover privacy aspects. ISO 27701 was therefore introduced as an extension of ISO 27001, focusing specifically on Personal Information Management Systems (PIMS) [14], helping organizations meet increasing privacy demands as technology and regulations evolve [17]. Although the PDP Law clearly stipulates legal obligations, it does not yet provide technical implementation guidelines [4]. ISO 27001 and ISO 27701 are crucial in bridging the gap between technical requirements and regulatory mandates, as the use of ISO-based standards in isolation has been identified as a key implementation challenge for privacy compliance [18].

The effectiveness of this implementation cannot be assessed solely based on the final results but must be evaluated through a systematic and comprehensive process. The CIPP Model and CMMI Model were selected for the evaluation. The CIPP Model provides a framework for guiding formative and summative evaluations of projects, programs, personnel, products, institutions and systems [19]. Research by Kaivanpanah and Zarrin demonstrates that the CIPP Model can effectively identify critical obstacles in evaluation processes [20]. The CMMI Model complements this by helping organizations measure process maturity and capability, identify improvement priorities and guide implementation [21], [22], [23]. Together, both models are applied to assess the effectiveness of personal data protection policy implementation within the specific institutional context of this study.

While existing literature extensively discusses the legal implications of data protection laws, a significant research gap remains in formal semantic mapping that translates these legal mandates into operational system architectures for specific institutions [18]. To address this gap, this single-case study examines data privacy compliance and operational readiness within a systemic Indonesian bank (KBMI Group IV). The study's novelty lies in the integration of the CIPP model and CMMI framework within a PDCA-based compliance architecture operationalized through ISO 27001 and ISO 27701 control mapping. This approach enables a structured assessment of governance effectiveness, maturity capability and regulatory alignment in addressing conflicts between emerging privacy obligations and legacy data retention requirements. Consequently, the study establishes an institutional baseline for technical privacy compliance, subject to broader multi-institutional validation.

2. METHODS

2.1 Research Design and Workflow

This study uses qualitative and quantitative methods to integrate the ISO, CMMI and CIPP models for data privacy compliance in Indonesia. The research workflow consists of three sequential stages: (1) problem analysis and formalization, (2) data collection and validation and (3) computational analysis and maturity assessment, as shown in Figure 1.

Figure 1. Research Process

The three stages are connected in sequence as follows. In Stage 1, the Context, Input, Process and Product (CIPP) model is applied to qualitatively assess the organization's governance structure, resource allocation, operational workflows and policy outcomes. In Stage 2, the qualitative findings from the CIPP evaluation are translated into the Capability Maturity Model Integration (CMMI) framework to quantitatively determine the maturity level of established processes across six compliance domains. In Stage 3, the empirically identified gaps are systematically aligned with the control requirements of

ISO 27001 and ISO 27701, establishing the foundation for a conceptual Plan-Do-Check-Act (PDCA) compliance architecture as a proposed design output.

2.2 Data Source

Data collection was conducted through structured interviews using preprepared questions supported by systematic recording techniques [24]. To establish a focused single-case study, the empirical scope was deliberately restricted to one KBMI Group IV bank. Interviews were conducted with two primary respondents who hold direct authority and responsibility for managing customer personal data: the Business Branch Manager, providing a strategic governance perspective and the Department Head Application Developer, providing a technical and operational perspective. These two respondents were selected purposively based on their institutional roles as the most directly accountable personnel for data privacy compliance within the assessed organization.

2.3 Data Triangulation

To address potential respondent bias arising from the limited sample size, a source-based data triangulation technique was employed. Operationally, interview responses were systematically cross-referenced against three categories of internal documentation: (1) standard operating procedures (SOPs) for data handling, (2) system architecture logs and (3) internal security policy documents. This triangulation served a confirmatory function, verifying that the privacy practices stated by respondents were consistent with official corporate documentation, rather than relying solely on subjective self-reporting. It should be noted, however, that this triangulation process was used for verification and confirmation purposes only, the documents were reviewed qualitatively by the researchers and were not subjected to formal coding or systematic content analysis. This distinction is acknowledged as a methodological boundary of the study.

2.4 Modification CMMI

The integration of CIPP and CMMI enables a more comprehensive evaluation approach. The qualitative findings derived from the CIPP assessment are transformed into a structured CMMI-based measurement scale, enabling the quantitative evaluation of processes across six established compliance domains: (1) Data Subject Rights, (2) Controller Obligations, (3) Data Processing Principles, (4) Security and Risk Management, (5) Incident Response and Breach Notification and (6) Cross-Border Data Transfers. The

Overall Maturity Score (M_{Total}) is determined using the unweighted arithmetic mean of all assessed compliance areas. This relationship can be formally represented as shown in Equation 1.

$$M_{Total} = \frac{1}{n}\sum_{i=1}^{n} C_i \quad (1)$$

where C_i represents the score of each of the n=6 compliance areas.

To tailor the evaluation structure to the specific organizational context being studied, the CMMI model was strategically modified by restricting the measurement scale to range only from Level 1 (Initial) to Level 4 (Quantitatively Managed). This modification was applied to increase the relevance of the evaluation structure to the specific organizational context under study [21]. Maturity Level 5 (Optimizing) is not used because this level requires continuous improvement supported by long term historical data analysis, which is often not available in the early stages of standard adoption [22]. Furthermore, because this study design only collected data at a single point in time, measuring trends in sustainable innovation was not valid due to the lack of time-series data required in the maturity model design principle [22]. The following is an explanation of each level used in this study:

1) Level 1: Initial (Processes or controls are completely absent, undocumented and unrecognized)
2) Level 2: Managed (There is awareness of the need for processes or controls. Some basic practices have begun to be implemented but are not yet standardized are inconsistent across departments and are not yet formally documented)
3) Level 3: Defined (Processes or controls have been defined, formally documented and communicated to all relevant units/divisions)
4) Level 4: Quantitatively Managed (Defined processes are not only implemented but also monitored, measured for effectiveness and evaluated periodically)

2.4.1 Scoring Procedure

To ensure transparency and reproducibility, the scoring procedure for each compliance domain is described as follows. For each compliance requirement listed in Table 1, a maturity level score was assigned on a scale of 1 to 4 based on the convergent evidence

from two sources: (1) the structured interview responses of the two primary respondents and (2) the triangulated internal documentation. Scores were assigned by the lead researcher and subsequently reviewed by the co-researcher to minimize individual scoring bias. A score of 4 (Quantitatively Managed) was assigned when both interview evidence and documentary evidence confirmed that the practice was fully implemented, monitored and periodically evaluated. A score of 3 (Defined) was assigned when practices were documented and communicated but lacked systematic measurement. A score of 2 (Managed) was assigned when basic practices existed but were inconsistent or not formally documented. A score of 1 (Initial) was assigned when no recognizable process existed. The domain-level score for each of the six compliance areas was then calculated as the arithmetic mean of all requirement-level scores within that domain.

Table 1. Six Compliance Domain Scores

No.	Compliance Domain	No of Requirements
1	Data Processing	3
2	Data Subject Rights	4
3	Obligations of Controllers and Processors	4
4	Security and Risk Management	3
5	Transfer of Personal Data	1
6	Governance and Accountability	3
	Total	18

This table presents the six compliance domains and their requirement counts. Full item-level scores, domain averages and the overall maturity score calculation are presented in Table 3 in the Results section.

2.4.2 ISO–PDP Mapping Matrix Construction

To operationalize the ISO–PDP compliance framework, a formal mapping matrix was constructed by the research team through formal semantic matching, aligning the functional requirements of each PDP Law article with the corresponding technical controls of ISO 27001 and ISO 27701. The mapping was reviewed and discussed between the two researchers to ensure consistency and logical alignment of each mapped control. It should be explicitly noted, however, that formal expert validation by external compliance officers or independent institutional personnel was not conducted in this

study. The mapping matrix presented in Table 2 should therefore be treated as a theoretically grounded and internally reviewed proposal rather than a formally externally validated framework. This constitutes a methodological limitation of the study and future research should subject this mapping matrix to independent expert validation, involving compliance officers, legal practitioners and IT security personnel to establish its broader technical and legal soundness before institutional adoption.

2.5 Methodological Limitations

This study acknowledges several methodological limitations. First, the empirical data relies on a highly restricted sample consisting of a single KBMI Group IV institution and two respondents, which raises potential threats to external validity and limits broad cross sector generalization. The limited respondent diversity means that scoring decisions ultimately reflect the perceptions and disclosures of two individuals, which may not fully represent the institution's actual compliance posture. Second, in computing the overall maturity score, equal weighting was applied to all compliance areas C_i under the baseline assumption that all security vectors uniformly contribute to PDP compliance. The justification and algorithmic optimization of weighted compliance vectors are reserved for future computational studies. Third, the ISO–PDP mapping matrix was constructed and internally reviewed by the research team but was not subjected to formal external expert validation, which limits the ability to claim its definitive technical and legal accuracy beyond the researchers' own assessment.

3. RESULTS AND DISCUSSION

3.1. RQ1: What is the level of awareness and readiness of organizations in Indonesia regarding the implementation of this personal data protection law, especially in the finance sector, particularly banking?

To assess the level of organizational awareness and readiness, data were collected through structured interviews. The two respondents, a Business Branch Manager and a Department Head Application Developer from one KBMI Group IV bank, who represented strategic, operational and technical perspectives in the implementation of the PDP Law. The interview data were analyzed using the CIPP Model (Context, Input, Process, Product) to evaluate organizational readiness across four dimensions: governance, resources,

processes and policy outcomes. It should be noted that all findings presented in this section reflect the perceptions and institutional disclosures of these two respondents, triangulated against internal documentation and should be interpreted accordingly. There are four components in this discussion:

1) Context

The Context evaluation aims to identify target needs, understand problems and assess whether the objectives set are in line with actual conditions [20]. The interview results on the Context aspect show that data protection awareness in the banking sector existed prior to the PDP Law, mainly based on the principle of bank secrecy. However, the PDP Law serves as a regulatory reinforcement that standardizes data protection practices in a more systematic manner. Compliance with the PDP Law is mainly driven by regulatory factors and reputation risk mitigation with top-down pressure from the OJK and Bank Indonesia. The previous implementation of ISO 27001 has been expanded through the adoption of ISO 27701 to form an integrated data security and privacy framework. For application developers, the PDP Law serves as a unifying framework that harmonizes awareness levels and ensures that data protection is implemented consistently throughout the system development cycle.

2) Input

Input components are used to assess an organization's readiness in terms of strategy, policy, resources, budget and infrastructure needed to support implementation [20]. The results of interviews on the Input aspect show that KBMI banks in groups IV have made structural adjustments in response to the PDP Law. The provision of a special budget and the establishment of a Data Protection Officer (DPO) function under the Compliance division reflect governance readiness, not merely administrative compliance. This readiness is reinforced through business process adjustments such as account opening procedures that indicate the application of the privacy-by-design principle at the operational level through the appointment of a PIC in each work unit. From a technical perspective, the findings show strong integration between corporate policy and system implementation. The translation of corporate guidelines into technical requirements for application developers indicates that compliance has been internalized in the system architecture. The implementation of encryption, periodic security testing and regular human resource awareness programs reflect an approach

that combines strengthening technical controls and human readiness to mitigate the risk of data leaks.

3) Process

Process is the stage where inputs are effectively utilized to achieve the expected goals, objectives and outcomes [20]. This stage focuses on monitoring policy implementation in the field to ensure that implementation is going according to plan, while also identifying obstacles, deviations and areas that need improvement during the process. The interview results on the Process aspect show that the implementation of the PDP Law has been carried out operationally through a multi-layered risk control mechanism, not merely administrative compliance. The compliance process is integrated into the data life cycle, starting from data mapping, the implementation of Data Protection Impact Assessment (DPIA) as a preventive measure and incident response procedures within a 72-hour time limit. The sustainability and validity of this process are maintained through periodic audits based on COBIT 2019 and ISO 27001, which serve as a dual oversight mechanism for the effectiveness of internal controls. However, implementation faces structural and technical challenges. There is a potential conflict between fulfilling the rights of data subjects, particularly the Right to be Forgotten and the obligation to retain banking data in accordance with OJK/BI regulations. To bridge this conflict, the organization does not perform hard deletion but adopts a data masking & data anonymization approach so that the organization tends to apply selective deletion and access restrictions. On the other hand, the existence of legacy systems and data fragmentation still hinders interoperability, although the adoption of data exchange standards such as JSON/XML has begun as a mitigation effort.

4) Product

The product aims to assess the effectiveness and impact of policies on the achievement of objectives formulated at the beginning of the program [20]. The results of interviews on the Product aspect show that the integration of ISO 27001 and ISO 27701 has shifted compliance from a mere regulatory checklist to a strategic asset for the organization. Respondents reported that no data breach incidents had occurred since implementation and that customers security perceptions and trust had increased, though it should be noted that these outcomes were self-reported by institutional representatives rather than independently measured. ISO 27701 acts as a compliance enabler that clarifies the

implementation of technical mandates of the PDP Law, such as ROPA, DPIA and the fulfillment of data subject rights that are not fully accommodated by general security standards. In the long term, the impact of implementation goes beyond technical aspects to strengthen business sustainability. Data protection is internalized as a privacy culture integrated into the customer experience, becoming a factor of competitive differentiation. Thus, the output of this system is not only legal compliance but also strengthened market trust and reputation resilience, which are essential for financial institutions in this high-risk digital era.

While the Context and Input evaluations demonstrated high awareness and adequate resource allocation, such as the formation of dedicated privacy teams and targeted budgets. The Process and Product evaluations revealed critical technical challenges. Rather than merely summarizing the procedural steps, direct statements from the stakeholders reveal significant operational friction. For example, regarding the conflict between data retention and deletion, the technical evaluation revealed that hard data deletion cannot be performed completely due to Bank Indonesia (BI) and Financial Services Authority (OJK) regulations, which require 7 to 10 years of data retention years [4], [25].

To navigate this, the Application Developer noted that the bank is forced to adopt data masking and data anonymization approaches to restrict access to data that is no longer needed. This highlights a critical technical bottleneck: the legal "Right to be Forgotten" directly collides with legacy financial compliance. Consequently, cryptographic pseudonymization and masking serve as necessary technical controls rather than optional security enhancements. Furthermore, the existence of legacy systems and data fragmentation continues to hinder seamless interoperability, although the adoption of data exchange standards such as JSON/XML has been initiated as a technical mitigation effort.

Following the qualitative CIPP measurements, the study proceeds to quantitatively assess organizational readiness using the modified CMMI framework. This model was selected for its ability to represent organizational capability in managing, controlling and improving processes on a continuous basis. The maturity assessment was conducted using the compliance requirement matrix presented in Table 2.

Table 2. Organizational Maturity Level

Compliance Area	Requirements	Related Articles	Measurement Matrix	Scale
Data Processing	Have a legal basis for each activity involving the processing of personal data	Article 20	• There is mapping for each data processing • There is legal documentation for each processing activity (e.g., consent forms, contract clauses, etc.)	4
	Processing is carried out in a limited, specific, legitimate and transparent manner	Article 16 paragraph (2), Article 27	• Data collection is limited to data relevant to the specified purpose • The privacy policy specifies the purpose of collecting each type of data	4
	Ensuring data accuracy, completeness and consistency	Article 29	• There is a data verification process at the time of data collection • There is a procedure for updating data periodically or upon request	4
Data Subject Rights	Provide clear information to the Subject of Personal Data	Article 5, Article 21	• A Privacy Notice is available, easily accessible and understandable, containing information in	4

Compliance Area	Requirements	Related Articles	Measurement Matrix	Scale
			accordance with Article 21	
	Provide access rights and copies of data to the Subject of Data	Article 7, Article 32	• There is a procedure for verifying the identity of the applicant • Data and processing records can be provided within 3x24 hours of receiving the request	4
	Facilitate the right to correct and update data	Article 6, Article 30	• There is a procedure for receiving and processing requests for data correction • Corrections or updates can be made within 3x24 hours of receiving the request	3
	Facilitate the right to delete and destroy data	Article 8, Article 43, Article 44	• There is a procedure for deleting/destroying data if the purpose has been achieved, consent has been withdrawn, or there is a request • There is evidence that the data has been deleted/destroyed	4

Compliance Area	Requirements	Related Articles	Measurement Matrix	Scale
Obligations of Controllers and Processors	Obtaining valid and explicit consent	Article 20 paragraph (2) letter a, Articles 21-24	• There is a written or recorded consent form that is easy to understand, using simple and clear language • There is a system for recording and managing proof of consent	4
	Processing data on children and persons with disabilities in a specific manner	Article 25, Article 26	• There is an age verification mechanism • There is a procedure for obtaining consent from the child's parent/guardian or the person with a disability / their guardian	3
	Recording all data processing activities	Article 31	• Create and maintain a Record of Processing Activities (RoPA)	4
	Supervising parties involved in data processing	Article 37, Article 51	• There is a data processing agreement with the Data Processor (Data Processing Agreement)	4

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Compliance Area	Requirements	Related Articles	Measurement Matrix	Scale
Security and Risk Management	Protecting and ensuring the security of personal data	Article 35, Article 39	• Implement encryption protocols and access controls for data security • Conduct security assessments based on the nature and risk of the data	4
	Maintaining the confidentiality of personal data	Article 36	• There is a Non-Disclosure Agreement for parties who can access the data	4
	Notifying data breaches	Article 46	• There are Standard Operating Procedures (SOP) for handling data breach incidents, which include the obligation to report in writing to the Data Subject and the Agency within 3x24 hours	3
Transfer of Personal Data	Ensuring data protection in cross-border transfers	Article 56	• There is a list of countries to which data is transferred and an assessment of the level of data protection in those countries	3

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Compliance Area	Requirements	Related Articles	Measurement Matrix	Scale
Governance and Accountability	Appointing an Officer/Official for Personal Data Protection (DPO)	Article 53, Article 54	• Assess whether the organization is required to appoint a DPO based on the criteria in Article 53	4
	Demonstrating accountability	Article 47	• Document all policies, procedures and compliance measures that have been taken	4
	Handling data transfers resulting from corporate actions (mergers, acquisitions, etc.)	Article 48	• Establish procedures for notifying data subjects of data transfers before and after corporate actions	4

Table 2 reveals a generally high level of compliance maturity across most assessed areas, with the majority of requirements scoring at Level 4 (Quantitatively Managed). However, two notable exceptions emerge. First, the facilitation of the right to correct and update data scores Level 3, reflecting that correction procedures exist and are documented but are not yet systematically monitored for timeliness or effectiveness. Second, the processing of data belonging to children and persons with disabilities also scores Level 3, indicating that while basic consent mechanisms are in place, procedures for obtaining guardian consent remain inconsistently applied across operational units. These variances suggest that while the assessed institution has achieved strong foundational compliance, targeted improvements in data subject rights handling and vulnerable group protections would be necessary to progress toward Level 4 maturity. Given that these scores derive from the assessments of two respondents triangulated against internal documentation, they should be treated as indicative rather than definitive measurements of institutional compliance.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

To synthesize these detailed requirement scores into a system-level evaluation, a modified Capability Maturity Model Integration (CMMI) framework was applied across the six core compliance areas. The Overall Maturity Score (M_{Total}) is calculated as the unweighted arithmetic mean of these compliance areas, expressed formally as shown in Equation 2.

$$M_{Total} = \frac{1}{n}\sum_{i=1}^{n} C_i \quad (2)$$

Table 3. Six Domain Scores Summary

No.	Compliance Domain	No of Requirements	Sum of Scores	Domain Scores
1	Data Processing	3	12	4
2	Data Subject Rights	4	15	3.75
3	Obligations of Controllers and Processors	4	15	3.75
4	Security and Risk Management	3	11	3.66
5	Transfer of Personal Data	1	3	3
6	Governance and Accountability	3	12	4
	Overall Maturity Score	18	68	3.69

Based on the assessment detailed in Table 2 and Table 3, the calculation yielded a total sum of 22.16 across the six compliance domains. The domain-level derivations are as follows: (1) Data Processing: 4.00 (sum of 12 across 3 requirements); (2) Data Subject Rights: 3.75 (sum of 15 across 4 requirements); (3) Obligations of Controllers and Processors: 3.75 (sum of 15 across 4 requirements); (4) Security and Risk Management: 3.66 (sum of 11 across 3 requirements); (5) Transfer of Personal Data: 3.00 (sum of 3 across 1 requirement); and (6) Governance and Accountability: 4.00 (sum of 12 across 3 requirements). Dividing the total by the number of domains $(M_{Total} = 22.16 / 6)$ produces an Overall Maturity Score of 3.69, placing the institution at Level 3 (Defined)

within the assessed case. This result indicates that processes related to personal data compliance are well documented, standardized and consistently implemented across divisions within the studied institution, though this finding should not be generalized beyond the single-case context without further multi-institutional validation.

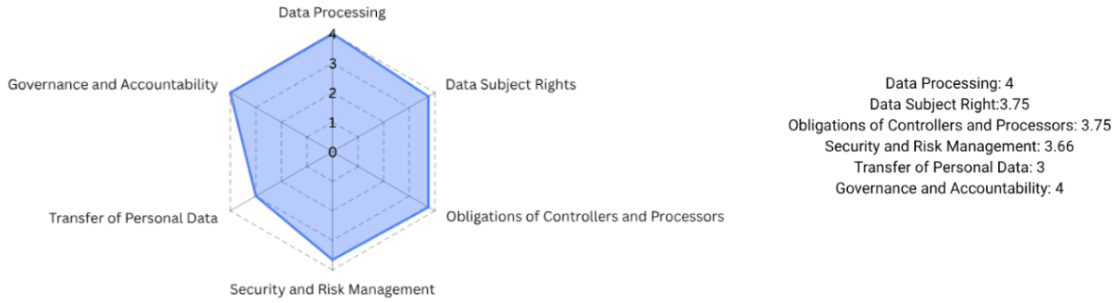

Figure 2. Overall Maturity Score

The radar chart (Figure 2) illustrates the distribution of maturity scores across the six compliance domains within the assessed case. Transfer of Personal Data recorded the lowest domain score (3.00), while Data Processing and Governance and Accountability achieved the highest (4.00). These variances should be interpreted cautiously, as the scores are derived from the assessments of two respondents triangulated against internal documentation rather than from a statistically representative sample. Equal weighting was applied to all domains under the baseline assumption that each compliance area contributes uniformly to foundational PDP Law adherence. However, this assumption may not reflect the actual regulatory risk weighting of each domain and future algorithmic maturity models should explore weighted compliance vectors, potentially prioritizing technical security controls over administrative governance measures to produce more risk-sensitive institutional assessments.

3.2. RQ2: How can ISO 27001 and ISO 27701 be implemented as an integrated framework model to bridge the gap in PDP Law compliance for the finance sector, particularly banking?

The integration of ISO 27001 and ISO 27701 as a framework model represents a strategic approach to bridging the compliance gap with the PDP Law in the financial sector, particularly banking [26], [27]. The integration of these two standards enables organizations to align information security management through the Information

Security Management System with data privacy management through the Privacy Information Management System within a single integrated governance framework.

To operationalize this integration, a formal mapping matrix was developed to bridge the clauses of ISO 27001 and ISO 27701 with the articles of the PDP Law [27]. The mapping methodology was constructed utilizing formal semantic matching, aligning the functional requirements of the national legal articles (e.g., Data Subject Rights, Controller Obligations) directly to the technical controls of the ISO standards. The mapping was reviewed and discussed between the two researchers to ensure consistency and logical alignment. It should be explicitly noted that formal expert validation by external compliance officers was not conducted. The mapping matrix should therefore be treated as a theoretically grounded and internally reviewed proposal rather than a formally externally validated framework. The resulting matrix (Table 4) identifies the similarities, gaps and overlaps between international standards and national regulations.

To maintain a clear evidential chain, a strict distinction must be made between the empirical observations and the conceptual architectural proposals. The preceding qualitative CIPP diagnosis and quantitative CMMI maturity assessment reflect the empirical data gathered directly from the assessed bank. In contrast, the subsequent formal mapping matrix (Table 4) and Plan-Do-Check-Act (PDCA) framework (Table 5) serve as proposed design outputs. These architectural models are constructed theoretically to resolve the specific operational and compliance gaps identified during the empirical evaluation.

Table 4. ISO-PDP Mapping Matrix of Functional and Technical Controls

Compliance Area	Focus on ISO 27001	Focus on ISO 27701	Justification
Data Subject Rights (Articles 5-13)	• A.18.1.4 (Privacy and protection of personally identifiable information)	• A.7.3.3 (Providing information to PII principals) • A.7.3.4 (Providing mechanism to modify or	This integration creates a balance between availability and privacy rights. ISO 27001 provides a security foundation to ensure that data can only be accessed by

Compliance Area	Focus on ISO 27001	Focus on ISO 27701	Justification
	• A.16.1.1 (Responsibilities and procedures) • A.13.2.1 (Information transfer policies and procedures) • A.9.4.1 (Information access restriction) • A.9.2.5 (Review of user access rights) • A.8.3.2 (Disposal of media)	withdraw consent) • A.7.3.5 (Providing mechanism to object to PII processing) • A.7.3.6 (Access, correction and/or erasure) • A.7.4.8 (Disposal) • A.7.5 (PII sharing, transfer and disclosure) • Clause 6.13.1.1 (Responsibilities and procedures)	authorized parties, thereby preventing leaks when data subjects request access. On the other hand, ISO 27701 provides specific procedural mechanisms to facilitate the exercise of these rights, such as the "consent withdrawal" mechanism and the right to be forgotten, which are mandated by Articles 5-13 of the PDP Law.
Data Processing (Articles 16-18)	• A.8 (Asset management) • A.11 (Physical and environmental security) • A.15 (Supplier relationships) • A.15.1.2 (Addressing security within supplier agreements) • A.18.1.4 (Privacy and protection of personally	• A.7.3.3 (Providing information to PII principals) • A.7.2.7 (Joint PII controller) • Clause 7.2 (Conditions for collection and processing) • Clause 7.4 (Privacy-by-design and privacy-by-default)	Legitimate data processing requires a secure environment and strict privacy principles. ISO 27001 focuses on securing physical assets and infrastructure where processing takes place to prevent sabotage or damage. Meanwhile, ISO 27701 implements the principles of Data Minimization and Limitation of Collection, ensuring that organizations only

Compliance Area	Focus on ISO 27001	Focus on ISO 27701	Justification
	identifiable information) • Clause 4 (Context of the organization)		process data for specific purposes and within the retention limits set out in Articles 16-18, so that processing does not become excessive.
Obligations of Controllers and Processors (Articles 20-54)	• A.6.1.1 (Information security roles and responsibilities) • A.8.1.3 (Acceptable use of assets) • A.8.2.2 (Labelling of information) • A.8.3.2 (Disposal of media) • A.9.2.5 (Review of user access rights) • A.9.4.1 (Information access restriction) • A.10 (Cryptography) • A.11.2.7 (Secure disposal or reuse of equipment) • A.12.1.2 (Change management) • A.12.4.1 (Event logging)	• A.7.2.2 (Identify lawful basis) • A.7.2.3 (Determine when and how consent is to be obtained) • A.7.2.4 (Obtain and record consent) • A.7.2.5 (Privacy impact assessment) • A.7.2.6 (Contracts with PII processors) • A.7.3.2 (Determining information for PII principals) • A.7.3.3 (Providing information to PII principals) • A.7.3.4 (Providing mechanism to modify or withdraw consent)	The PDP Law requires technical security measures. ISO 27001 addresses these technical requirements to maintain confidentiality and audit trails. ISO 27701 addresses organizational requirements by mandating Privacy Impact Assessments and the concept of Privacy-by-Design, which ensures that Controllers and Processors have measurable privacy risk management in place before data processing begins.

Compliance Area	Focus on ISO 27001	Focus on ISO 27701	Justification
	• A.12.4.3 (Administrator and operator logs) • A.13.2.4 (Confidentiality or non-disclosure agreements) • A.14 (System acquisition, development and maintenance) • A.15.2.1 (Monitoring and review of supplier services) • A.16.1.5 (Response to information security incidents) • A.16.1.7 (Collection of evidence) • A.18.1.3 (Protection of records) • A.18.1.4 (Privacy and protection of personally identifiable information) • Clause 6.1.2 (Information security risk assessment)	• A.7.3.5 (Providing mechanism to object to PII processing) • A.7.3.6 (Access, correction and/or erasure) • A.7.3.9 (Handling PII requests) • A.7.4.2 (Accuracy and quality) • A.7.4.3 (Limit PII collection) • A.7.4.4 (PII minimization objectives) • A.7.4.5 (PII de-identification and deletion at the end of processing) • A.7.4.7 (Retention) • A.7.4.8 (Disposal) • Clause 6.3.1.2 (Segregation of duties) • Clause 6.10.2.4 (Confidentiality or non-disclosure agreements)	

Compliance Area	Focus on ISO 27001	Focus on ISO 27701	Justification
	• Clause 5 (Leadership) • Clause 9 (Performance evaluation)	• Clause 6.13.1.1 (Responsibilities and procedures) • Clause 6.13.1.5 (Response to information security incidents) • Clause 7.2.8 (Records related to processing PII) • Clause 7.4 (Privacy-by-design and privacy-by-default) • Clause 5.3 (Leadership) • Clause 6.2 (Information security policies)	
Data Transfer and Sanctions (Articles 55-73)	• A.5.1.1 (Policies for information security) • A.9.1.1 (Access control policy) • A.13.2 (Information transfer) • A.13.2.1 (Information transfer policies and procedures)	• A.7.2.1 (Identify and document purpose) • A.7.2.2 (Identify lawful basis) • A.7.2.5 (Privacy impact assessment) • A.7.5.1 (Identify basis for PII transfer between jurisdictions)	To mitigate the risk of sanctions due to illegal data transfers, contract controls and transmission security are required. ISO 27001 ensures that data transfer channels are technically secure and bound by confidentiality agreements. ISO 27701 complements this with jurisdiction verification,

Compliance Area	Focus on ISO 27001	Focus on ISO 27701	Justification
	• A.13.2.2 (Agreements on information transfer) • A.16.1.5 (Response to information security incidents) • A.16.1.7 (Collection of evidence) • A.18.1 (Compliance with legal and contractual requirements) • A.18.1.1 (Identification of applicable legislation and contractual requirements)	• A.7.5.2 (Countries and international organizations to which PII can be transferred) • Clause 6.13.1.1 (Responsibilities and procedures) • Clause 6.15.1.1 (Identification of applicable legislation and contractual requirements) • Clause 7.5 (PII sharing, transfer and disclosure)	which ensures that the recipient country has an equivalent level of data protection or recognized standards, in accordance with the strict requirements for cross-border transfers in the PDP Law.

Table 4 functions as a conceptual architectural proposal rather than an empirical observation. It demonstrates theoretically how high-level regulatory mandates must be translated into granular, ISO-mapped technical controls to be computationally feasible within the bank's existing infrastructure.

Based on the empirically identified compliance gaps, particularly the regulatory conflict between the Right to Erasure and mandatory financial data retention and the lower maturity score in cross-border data transfers, the following PDCA-based compliance architecture is proposed as a conceptual design output. The PDCA (Plan-Do-Check-Act) cycle provides organizations with a systematic mechanism to plan, execute, evaluate and continuously refine their information security management and personal data protection practices [28]. Each phase within this cycle is defined by specific objectives and

operational activities that collectively form a closed feedback loop for sustained compliance improvement [29]. Table 5 presents the proposed framework by mapping concrete technical activities, relevant ISO 27001 and ISO 27701 control references and empirical justifications derived from the preceding CIPP diagnosis and CMMI maturity assessment to each corresponding phase of the cycle.

Table 5. PDCA Framework

Stage	Activity	Justification	Focus on ISO 27001 & ISO 27701
Plan	• Regulatory Conflict Alignment Designing technical policies for anonymization or data masking to mediate conflicts between the "Right to Erasure" (PDP Law) and the "10-Year Retention Requirement" (OJK). • Strengthening Cross-Border Transfer Mechanisms Developing Standard Contractual Clauses and assessing the eligibility of destination countries to improve weaknesses in data transfer	• CIPP Model: Technical obstacles were encountered in implementing the Right to be Forgotten due to conflicting regulations. • CMMI Model: Data Transfer is still at level 3.	• ISO 27001: A.7.4.8 (Disposal) & A.7.4.7 (Retention), A.13.2 (Information transfer) & A.18.1 (Compliance with legal requirements) • ISO 27701: A.7.5 (PII sharing, transfer and disclosure), A.7.5.1 (Identify basis for PII transfer between jurisdictions) & A.7.5.2 (Countries and international organizations to which PII can be transferred)
Do	• DPIA & ROPA Implementation Conducting Data Protection Impact Assessments for new	• CIPP Model: Respondents reported that data security practices	• ISO 27001: A.10 (Cryptography) & A.9 (Access

Stage	Activity	Justification	Focus on ISO 27001 & ISO 27701
	products and maintaining a real-time Record of Processing Activities. • Encryption & Access Control Implementation Implementing end-to-end encryption and strict access management on legacy systems • Privacy Culture Providing training to all staff to instill the mindset that privacy is part of the Customer Experience	contributed to increased customer trust and competitive advantage.	Control - A.9.1.1, A.9.2.5, A.9.4.1) • ISO 27701: A.7.2.5 (Privacy impact assessment) & Clause 7.2.8 (Records related to processing PII)
Check	• Data Subject Rights Response Audit Measuring whether the SLA response to customer requests (access/delete/correction) is consistently less than 3x24 hours • Third Party Review (Vendor) Audit vendor compliance with the Data Processing Agreement (DPA) clauses	• CMMI Model: Data Subject Rights area is still not optimal. • ISO Mapping: Clause A.15 (Supplier relationships) which requires monitoring of supplier services.	• ISO 27001: A.15 (Supplier relationships), A.15.2.1 (Monitoring and review of supplier services) & A.15.1.2 (Addressing security within supplier agreements) • ISO 27701: A.7.3.6 (Access, correction and/or erasure), A.7.3.9 (Handling PII requests) & A.7.3.3 (Providing

Stage	Activity	Justification	Focus on ISO 27001 & ISO 27701
			information to PII principals)
Act	• Vendor Sanctions & Termination Impose sanctions or terminate contracts with vendors who fail to comply with data protection standards • Legacy System Feature Enhancement Patch or upgrade legacy systems that are causing bottlenecks	• CIPP Model: Challenges such as legacy systems and vendor compliance monitoring remain serious challenges. • ISO Mapping: Clause A.15 (Supplier relationships) requires monitoring of supplier services.	• ISO 27001: A.15 (Supplier relationships), A.14 (System acquisition, development and maintenance) & A.12.1.2 (Change management) • ISO 27701: A.7.2.6 (Contracts with PII processors)

Table 5 outlines the proposed continuous privacy engineering workflow. Analytically, this PDCA framework addresses the operational friction observed during the empirical CIPP diagnosis by prescribing specific technical actions, such as data masking and pseudonymization, as necessary controls in the Plan and Do phases, derived from the identified compliance gaps rather than from tested implementation.

From this framework, the Plan phase includes a number of key activities to align regulations with ISO 27001 and ISO 27701. Pseudonymization is used as a data protection technique explicitly recognized in the GDPR to reduce risks to data subjects without hindering legitimate data processing and analysis, as pseudonymized data is still categorized as personal data [30]. In addition, strengthening cross border data transfer mechanisms is a strategic element to ensure that international data flows are in line with the principles of data subject rights protection, through a layered approach such as adequacy decisions, appropriate safeguards and derogations [31]. In this context, Standard Contractual Clauses (SCCs) serve as organization-based accountability instruments that compensate for the limitations of legal protection in the destination country through

contractual obligations reinforced by technical and organizational controls, rather than as a comprehensive assessment of the country's legal system [32].

In the Do phase of the PDCA cycle, organizations implement operational controls to ensure consistent personal data protection, including through the implementation of Data Protection Impact Assessments (DPIAs) in product development and the ongoing maintenance of Records of Processing Activities (ROPAs) to ensure accountability and transparency in data processing [26], [33], [34]. These efforts are reinforced by the implementation of end-to-end encryption and risk-based access controls, including on legacy systems, as key technical measures to prevent unauthorized access and data leaks [35]. This is supported by the strengthening of a privacy culture through regular training for all employees.

In the Check phase, organizations conduct audits of data subject rights compliance to ensure service consistency in accordance with service level agreements (SLAs), particularly with regard to data access, correction and deletion rights in line with the principles of timeliness and transparency emphasized in data protection regulations [36]. This oversight is complemented by an evaluation of vendor compliance with the Data Processing Agreement (DPA) to ensure that third party involvement does not weaken data protection controls [37].

Furthermore, in the Act phase, noncompliance is followed up with corrective actions such as imposing sanctions or terminating cooperation with vendors, as an effort to maintain accountability and minimize legal and reputational risks [38]. At the same time, continuous improvement is carried out through upgrades or patching of legacy systems that still pose technical obstacles so that the effectiveness of data protection controls and audits can continue to be improved [39].

3.3. Discussion

The integration of ISO 27001 and ISO 27701 necessitates significant structural adjustments to the bank's Information systems architecture. As noted during the CIPP evaluation, existing legacy systems hinder seamless interoperability. To address this, the adoption of standardized APIs (e.g., JSON/XML) must be coupled with secure software development practices, including rigorous input validation to prevent vulnerabilities such

as cross-site scripting or injection attacks [7]. Furthermore, the application of Advanced Encryption Standard (AES) algorithms for encrypted database storage is technically advisable. This allows the institution to maintain data portability and ensure privacy during routine system operations, fulfilling the dual requirements of confidentiality and operational availability without exposing plaintext customer data to internal threat actors [39].

While the assessed institution utilizes COBIT 2019 alongside ISO 27001 as a dual oversight mechanism, a critical comparison of these standards reveals distinct functional boundaries. COBIT primarily serves as an overarching IT governance framework focusing on bridging the gap between control requirements and business risks, while frameworks such as ITIL focus on IT service management and operations [28]. By extending ISO 27001 with ISO 27701, the bank can incorporate specific Personal Information Management System controls that neither COBIT nor ITIL provides. As the literature indicates, ISO 27001 functions as a globally recognized security benchmark that can be integrated with the broader governance strategies of COBIT and ITIL.

However, this approach carries risks and scalability limitations. Should the proposed PDCA framework fail to sustain ongoing compliance, the institution would face consequences extending beyond administrative sanctions. From a micro perspective, an information security incident poses severe reputational consequences that can permanently damage customer trust, employee morale and future business growth [14], [15]. From a macro perspective, due to the institution's status as a Systemic Bank (KBMI Group IV), a major data breach could trigger systemic financial risk. Financial institutions are highly interconnected; vulnerabilities or shocks in one node can easily amplify and cascade, causing spillover effects and potential defaults across the entire financial network [13].

These risks, however, are not solely driven by technical or operational failures but are further compounded by the complexity of navigating overlapping and, in some cases, conflicting regulatory requirements. In this context, ensuring continuous compliance becomes not only a matter of system reliability but also of aligning system design with divergent legal obligations that govern data management practices.

A particularly critical challenge arises from the tension between emerging privacy regulations and established financial compliance frameworks. The "Right to Erasure" (Right to be Forgotten) under the Personal Data Protection (PDP) Law introduces requirements that stand in direct contrast to data retention obligations mandated by Bank Indonesia (BI) and the Financial Services Authority (OJK), which require financial institutions to retain customer data for 7 to 10 years [4], [25]. This creates a structural constraint within the system, where fulfilling one regulatory requirement may inherently limit the ability to satisfy another.

From an ISO 27701 perspective, this tension reflects the interaction between data subject rights (Clause 7.3.6 - Access, correction and/or erasure) and (Clause 7.4 – privacy-by-design) [40], [41]. Importantly, ISO 27701 frames the right to erasure as conditional, requiring organizations to consider overriding legal obligations. As a result, deletion requests must be assessed within the broader regulatory landscape, including sector-specific mandates imposed by BI and OJK.

As permanent data deletion cannot be legally executed within the mandated retention period, organizations must implement alternative technical and organizational measures. Within the proposed PDCA framework, this necessitates positioning cryptographic pseudonymization, encryption and data masking as essential controls rather than optional enhancements [30], [42]. These mechanisms allow institutions to retain data in compliance with financial regulations while ensuring that personal data is effectively de-identified and access is tightly controlled.

By integrating these controls into the continuous improvement cycle of PDCA, the framework enables organizations to systematically manage regulatory conflicts while maintaining compliance, security and privacy objectives. This approach ultimately supports a balanced alignment between data subject rights, legal retention requirements and institutional resilience within the financial sector.

While the proposed PDCA architecture theoretically resolves these tensions, the internal validity risk of the empirical findings must be critically acknowledged. The baseline maturity score of 3.69 relies on a highly limited empirical base of only two primary respondents from a single KBMI Group IV institution. Although this limitation was partially

mitigated through strict document triangulation against internal technical documentation, system architectures and security policies, it is important to note that triangulation with a small sample does not eliminate self-reporting bias. It only partially reduces it. The maturity scores ultimately reflect the perceptions and disclosures of two individuals, which may not fully represent the institution's actual compliance posture. Consequently, while the proposed framework itself is structurally sound and replicable, the resulting quantitative maturity findings cannot be statistically generalized across the wider banking sector and must be interpreted strictly as an internal institutional baseline within the assessed case, pending broader multi-institutional validation.

4. CONCLUSION

This study contributes to a structured bank-level privacy compliance framework informed by CIPP-CMMI evaluation and ISO-based control mapping. When applied to a single KBMI Group IV bank, the framework identified within the assessed case an institutional maturity baseline of 3.69 (Level 3 - Defined) and highlighted a critical regulatory conflict between data privacy mandates and mandatory financial data retention regulations. To address these identified gaps, the study proposes a conceptual PDCA-based system architecture leveraging data masking and pseudonymization as proposed compliance outputs, this architecture has not been implemented or operationally tested and should not be interpreted as a validated compliance solution. Because the empirical base is limited to a single institution with two respondents, the specific maturity findings serve as an institutional baseline rather than a generalized sector-wide metric and broader claims regarding applicability across the wider banking sector should therefore be restrained. Nevertheless, the proposed framework remains potentially useful as an internal assessment tool and provides a replicable foundation for future validation. Future research should validate this framework across multiple financial institutions to establish its reproducibility and broader generalizability before sectoral inference can be drawn and should further explore the development of automated compliance checking algorithms utilizing Natural Language Processing (NLP) to audit Data Processing Agreements.

REFERENCES

[1] A. Chukwudi Tabitha, E. Patience, O. Tawo, and A. Oluwatoyin, "Data security strategies to avoid data breaches in modern information systems," *World Journal of Advanced Research and Reviews*, vol. 20, no. 3, pp. 2122–2144, Dec. 2023, doi: 10.30574/wjarr.2023.20.3.2515.

[2] Direktorat Operasi Keamanan Siber, *Lanskap Keamanan Siber Indonesia 2024*. Jakarta: Badan Siber dan Sandi Negara (BSSN), 2024.

[3] M. R. Syailendra, G. Lie, and A. Sudiro, "Personal data protection law in Indonesia: Challenges and opportunities," *Indonesia Law Review*, vol. 14, no. 2, pp. 56–72, Aug. 2024, doi: 10.15742/ilrev.v14n2.4.

[4] M. D. Algamar, A. B. Munir, and Hendro, "Managing Indonesian data breach notification in the financial services sector: A case for one-stop notification model," *Journal of Central Banking Law and Institutions*, vol. 3, no. 3, pp. 547–584, Sep. 2024, doi: 10.21098/jcli.v3i3.271.

[5] A. Wibowo, W. Alawiyah, and Azriadi, "The importance of personal data protection in Indonesia's economic development," *Cogent Soc. Sci.*, vol. 10, no. 1, pp. 1–13, Jan. 2024, doi: 10.1080/23311886.2024.2306751.

[6] C. Liu and M. A. Babar, "Corporate cybersecurity risk and data breaches: A systematic review of empirical research," *Australian Journal of Management*, vol. 51, no. 1, pp. 62–92, Nov. 2024, doi: 10.1177/03128962241293658.

[7] V. Komandla, "Safeguarding Digital Finance: Advanced Cybersecurity Strategies for Protecting Customer Data in Fintech," *ISAR Journal of Multidisciplinary Research and Studies*, vol. 1, no. 2, pp. 62–70, Aug. 2023.

[8] E. O. Paul *et al*, "Cybersecurity Strategies for Safeguarding Customer's Data and Preventing Financial Fraud in the United States Financial Sectors," *International Journal on Soft Computing*, vol. 14, no. 3, pp. 01–16, Aug. 2023, doi: 10.5121/ijsc.2023.14301.

[9] Otoritas Jasa Keuangan, *Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan*. Jakarta: OJK, Dec. 2023.

[10] R. A. Antoine, N. S. Farizqa, A. H. Hasna, and M. Pasaribu, "Penyalahgunaan Data Pribadi dalam Teknologi Transaksi Digital di Industri Perbankan Digital (Studi Kasus PT. Bank Syariah Indonesia)," *Jurnal Multidisiplin Ilmu Akademik*, vol. 2, no. 1, pp. 316–327, Mar. 2025, doi: 10.61722/jmia.v2i1.3147.

[11] Otoritas Jasa Keuangan, *Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2021 tentang Bank Umum*. Jakarta: OJK, Jul. 2021.

[12] Otoritas Jasa Keuangan, *Peraturan Otoritas Jasa Keuangan Nomor 2/POJK.03/2018 tentang Penerapan Bank Sistemik dan Capital Surcharge*. Jakarta: OJK, Mar. 2018.

[13] S. Ellis, S. Sharma, and J. Brzeszczyński, "Systemic risk measures and regulatory challenges," *Journal of Financial Stability*, vol. 61, pp. 1–47, Aug. 2022, doi: 10.1016/j.jfs.2021.100960.

[14] E. Sarah Kuzankah, E. Zainab Efe, O. Adedolapo, and A. Abimbola Oluwatoyin, "ISO 27001 in banking: An evaluation of its implementation and effectiveness in enhancing information security," *Finance & Accounting Research Journal*, vol. 5, no. 12, pp. 405–425, Dec. 2023, doi: 10.51594/farj.v5i12.684.

[15] K. Ryanto and V. Tundjungsari, "Standardization of Information Security Management in the Banking Sector using the ISO 27001:2022 Framework," *Journal La Multiapp*, vol. 5, no. 4, pp. 361–379, Jul. 2024, doi: 10.37899/journallamultiapp.v5i4.1399.

[16] W. Wu, K. Shi, C. H. Wu, and J. Liu, "Research on the Impact of Information Security Certification and Concealment on Financial Performance: Impact of ISO 27001 and Concealment on Performance," *Journal of Global Information Management*, vol. 30, no. 3, pp. 1–16, 2022, doi: 10.4018/JGIM.20220701.oa2.

[17] U. Nuruddeen, G. I. O. Aimufua, B. Maijamaa, and S. Bassey, "Assessment of data protection and privacy implementation in financial institutions in Nigeria," *International Journal of Innovative Information Systems & Technology Research*, vol. 13, no. 4, pp. 125–134, Dec. 2025, doi: 10.5281/zenodo.17490504.

[18] N. A. Zaguir, G. H. Magalhães, and M. M. Spinola, "Challenges and enablers for GDPR compliance: systematic literature review and future research directions," IEEE, May 2024, pp. 81608–81630. doi: .1109/ACCESS.2024.3406724.

[19] N. Bilan, R. Negahdari, H. Hazrati, and S. F. Moghaddam, "Examining the quality of the competency-based evaluation program for dentistry based on the CIPP model: A mixed-method study," *J. Dent. Res. Dent. Clin. Dent. Prospects*, vol. 15, no. 3, pp. 203–210, May 2021, doi: 10.34172/JODDD.2021.034.

[20] S. Kaivanpanah and M. Zarrin, "Evaluation of English for Banking Purposes (EBP) Courses Using Stufflebeam's Context, Input, Process and Product (CIPP) Model," *Journal of Modern Research in English Language Studies*, vol. 12, no. 3, pp. 1–26, 2025, doi: 10.30479/jmrels.2024.20762.2419.

[21] J. Gomes and M. Romão, "Evaluating Maturity Models in Healthcare Information Systems: A Comprehensive Review," *Healthcare*, vol. 13, no. 15, pp. 1–48, Jul. 2025, doi: 10.3390/HEALTHCARE13151847.

[22] E. Yassien, "The challenges of capability maturity model integration application in the dynamic environment," *Int. J. Inf. Syst. Change Manag.*, vol. 12, no. 1, pp. 17–34, 2020, doi: 10.1504/IJISCM.2020.112045.

[23] A. Brezavšček and A. Baggia, "Recent Trends in Information and Cyber Security Maturity Assessment: A Systematic Literature Review," *Systems*, vol. 13, no. 1, pp. 1–42, Jan. 2025, doi: 10.3390/systems13010052.

[24] S. A. Mazhar, R. Anjum, A. I. Anwar, and A. A. Khan, "Methods of Data Collection: A Fundamental Tool of Research," *Journal of Integrated Community Health*, vol. 10, no. 01, pp. 6–10, Jun. 2021, doi: 10.24321/2319.9113.202101.

[25] Otoritas Jasa Keuangan, *Peraturan Otoritas Jasa Keuangan Nomor 51/POJK.04/2020 tentang Pemeliharaan Dokumen oleh Bank Umum sebagai Kustodian*. Jakarta: OJK, Dec. 2020.

[26] D. I. Anggraini, P. Oktavia, and H. Putra, "Data Protection Impact Assessment Framework in the Banking Sector in Indonesia to Implement Law of Personal Data Protection," *Journal of Information Systems*, vol. 21, no. 1, pp. 15–34, Apr. 2025, doi: 10.21609/jsi.v21i1.1439.

[27] E. Aristianto, M. H. Hilman, and S. Yazid, "Evaluating ISO Standards for Indonesian PDP Law Compliance: A Regulatory Mapping and Literature Review," *Scientific Journal of Informatics*, vol. 12, no. 1, pp. 145–158, Feb. 2025, doi: 10.15294/sji.v12i1.21538.

[28] M. Mirtsch, K. Blind, C. Koch, and G. Dudek, "Information security management in ICT and non-ICT sector companies: A preventive innovation perspective," *Computers & Security*, vol. 109, pp. 1–23, Jun. 2021, doi: 10.1016/j.cose.2021.102383.

[29] A. Górka–Chowaniec and A. Popek, "Attempt to use the Deming cycle (PDCA) in the process of implementing an information security management system," *International Journal for Quality Research*, vol. 19, no. 2, pp. 371–386, Nov. 2025, doi: 10.24874/IJQR19.02-01.

[30] European Data Protection Board, Guidelines 01/2025 on Pseudonymisation. Brussels: EDPB, Jan. 2025.

[31] B. A. Riswandi and A. M. Gultom, "Protecting our most valuable personal data: A comparison of transborder data flow laws in the European Union, United Kingdom, and Indonesia," *Prophetic Law Review*, vol. 5, no. 2, pp. 179–206, Dec. 2023, doi: 10.20885/PLR.vol5.iss2.art3.

[32] L. Bradford, M. Aboy, and K. Liddell, "Standard contractual clauses for cross-border transfers of health data after Schrems II," *J. Law Biosci*, vol. 8, no. 1, pp. 1–36, Jan. 2021, doi: 10.1093/jlb/lsab007.

[33] J. Henriksen-Bulmer, S. Faily, and S. Jeary, "DPIA in context: Applying DPIA to assess privacy risks of cyber physical systems," *Future Internet*, vol. 12, no. 93, pp. 1–23, May 2020, doi: 10.3390/FI12050093.

[34] L. H. Iwaya, A. S. Alaqra, M. Hansen, and S. Fischer-Hübner, "Privacy impact assessments in the wild: A scoping review," *Array*, vol. 23, pp. 1–20, Jun. 2024, doi: 10.1016/j.array.2024.100356.

[35] A. T. Ayedh M, A. W. A. Wahab, and M. Y. I. Idris, "Systematic Literature Review on Security Access Control Policies and Techniques Based on Privacy Requirements in a BYOD Environment: State of the Art and Future Directions," *Applied Sciences*, vol. 13, no. 14, pp. 1–37, Jul. 2023, doi: 10.3390/app13148048.

[36] L. Bufalieri, M. La Morgia, A. Mei, and J. Stefa, "GDPR: When the right to access personal data becomes a threat," in Proc. IEEE International Conference on Web Services (ICWS), Beijing, China, May 2020, pp. 1–8, doi: 10.1109/ICWS49710.2020.00017.

[37] O. Amaral, M. I. Azeem, S. Abualhaija, and L. C. Briand, "NLP-Based Automated Compliance Checking of Data Processing Agreements Against GDPR," in *IEEE Transactions on Software Engineering*, vol. 49, no. 9, pp. 4282-4303, Sept. 2023, doi: 10.1109/TSE.2023.3288901.

[38] W. Gregory Voss and H. Bouthinon-Dumas, "EU General Data Protection Regulation Sanctions in Theory and in Practice," *Santa Clara High Technology Law Journal*, vol. 37, no. 1, pp. 1–97, Jan. 2021.

[39] M. F. Safitra, M. Lubis, and H. Fakhrurroja, "Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity," *Sustainability*, vol. 15, no. 18, pp. 1–32, Sep. 2023, doi: 10.3390/su151813369.

[40] Lachaud, E, ISO/IEC 27701: Threats and Opportunities for GDPR Certification (January 15, 2020). Available at SSRN: https://ssrn.com/abstract=3521250.

[41] M. J. Anwar and A. Q. Gill, "Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model," in *ACIS 2020 Proceedings*, Wellington: Australasian Conference on Information Systems, 2020, pp. 1–12.

[42] M. Khoje, "Securing Data Platforms: Strategic Masking Techniques for Privacy and Security for B2B Enterprise Data," *International Journal of Computer Trends and Technology*, vol. 71, no. 11, pp. 46–54, Nov. 2023, doi: 10.14445/22312803/ijctt-v71i11p107.