Analisis Kesiapan Enterprise di Sektor Finansial dalam Penerapan Undang-Undang Perlindungan Data Pribadi

Delfindra Faiz Noorhadi
24917014

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer
Konsentrasi Sistem Informasi Enterprise
Program Studi Informatika Program Magister
Fakultas Teknologi Industri
Universitas Islam Indonesia
2026

Lembar Pengesahan Pembimbing

Analisis Kesiapan Enterprise di Sektor Finansial dalam Penerapan Undang-Undang Perlindungan Data Pribadi

Delfindra Faiz Noorhadi

24917014

Yogyakarta, 3 Agustus 2026

Pembimbing

Mukhammad Andri Setiawan, S.T., M.Sc., Ph.D.,

Lembar Pengesahan Penguji

Analisis Kesiapan Enterprise di Sektor Finansial dalam Penerapan Undang-Undang Perlindungan Data Pribadi

Delfindra Faiz Noorhadi

24917014

Yogyakarta, 3 Agustus 2026

Tim Penguji,

Mukhammad Andri Setiawan, S.T., M.Sc., Ph.D.
Ketua

Ir. Irving Vitra Paputungan, S.T., M.Sc., Ph.D.
Anggota I

18/08/2026

Dr. Hendrik, S.T., M.Eng.
Anggota II

Mengetahui,
Ketua Program Studi Informatika Program Magister
Universitas Islam Indonesia

Ir. Irving Vitra Paputungan, S.T., M.Sc., Ph.D.

Abstrak

Analisis Kesiapan Enterprise di Sektor Finansial dalam Penerapan Undang-Undang Perlindungan Data Pribadi

Sejak diberlakukannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), sektor perbankan Indonesia dituntut untuk memperkuat tata kelola perlindungan data dan menyesuaikan sistem informasi dengan prinsip privacy engineering. Namun, hingga saat ini belum tersedia model evaluasi yang mampu mengukur kesiapan organisasi secara komprehensif berdasarkan ketentuan UU PDP. Penelitian ini bertujuan mengevaluasi kesiapan organisasi dan aspek teknis dalam implementasi UU PDP pada salah satu Bank KBMI Kelompok IV. Penelitian menggunakan pendekatan studi kasus dengan metode kualitatif melalui wawancara terhadap Business Branch Manager dan Department Head Application Developer. Evaluasi dilakukan menggunakan integrasi model Context, Input, Process, Product (CIPP) dan Capability Maturity Model Integration (CMMI) untuk menilai aspek tata kelola, sumber daya, proses operasional, dampak implementasi kebijakan dan tingkat kematangan organisasi. Hasil penelitian menunjukkan tingkat kematangan organisasi sebesar 3,69 yang berada pada Level 3 (Defined), hal ini menunjukkan bahwa proses telah terdokumentasi dan diterapkan secara konsisten. Penelitian ini juga mengidentifikasi gap regulasi antara hak Right to be Forgotten dalam UU PDP dan kewajiban retensi data pada sektor keuangan. Sebagai rekomendasi, penelitian mengusulkan mapping UU PDP terhadap ISO 27001 dan ISO 27701 serta arsitektur kepatuhan berbasis Plan-Do-Check-Act (PDCA) yang mengadopsi mekanisme data masking dan pseudonymization. Kerangka yang diusulkan diharapkan dapat menjadi acuan dalam meningkatkan kesiapan implementasi perlindungan data pribadi di sektor perbankan Indonesia.

Kata kunci

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

Abstract

Analysis of Enterprise Readiness in the Financial Sector in the Implementation of Personal Data Protection Laws

Since the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law), Indonesia's banking sector has been required to strengthen data protection governance and align its information systems with the principles of privacy engineering. However, to date, there is no evaluation model available that can comprehensively measure an organization's readiness based on the provisions of the PDP Law. This study aims to evaluate organizational readiness and technical aspects in the implementation of the PDP Law at one of the KBMI Group IV banks. The study employs a case study approach using qualitative methods through interviews with the Business Branch Manager and the Department Head of Application Development. The evaluation was conducted by integrating the Context, Input, Process, Product (CIPP) model and the Capability Maturity Model Integration (CMMI) to assess governance aspects, resources, operational processes, the impact of policy implementation, and the organization's maturity level. The results showed an organizational maturity level of 3.69, which falls under Level 3 (Defined); this indicates that processes have been documented and are consistently applied. The study also identified a regulatory gap between the "Right to be Forgotten" under the PDP Law and data retention obligations in the financial sector. As a recommendation, the study proposes mapping the Personal Data Protection Act (PDP Act) against ISO 27001 and ISO 27701, as well as a Plan-Do-Check-Act (PDCA)-based compliance architecture that adopts data masking and pseudonymization mechanisms. The proposed framework is expected to serve as a reference for enhancing readiness for the implementation of personal data protection in Indonesia's banking sector.

Keywords

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

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, 3 Agustus 2026





Delfindra Faiz Noorhadi, S.Kom.

Daftar Publikasi

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. https://doi.org/10.63158/journalisi.v8i3.1623

Kontributor	Jenis Kontribusi
Delfindra Faiz Noorhadi	Mendesain eksperimen (60%) Menulis *paper* (70%)
Mukhammad Andri Setiawan	Mendesain eksperimen (40%) Menulis dan mengedit *paper* (30%)

Halaman Kontribusi

"**Tidak ada kontribusi dari pihak lain**"

Halaman Persembahan

Dedicated to myself, who has survived this far, who is always willing to learn, process and progress even with the ups and downs of life.

I also dedicate these words to my family, especially to my parents, whose unwavering support and love have been my pillars of strength. Thank you for everything you have done and continue to do.

I hope this thesis is just the beginning of my journey in academic research and contribution.

Cheers to many more good things further!

Kata Pengantar

Assalamu'alaikum Wr. Wb.

Puji syukur atas kehadirat Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya, Shalawat serta salam semoga tercurahkan kepada junjungan kita Nabi Muhammad SAW, para keluarga, sahabat dan seluruh umatnya sehingga penulis dapat menyelesaikan Tesis dengan judul "Analisis Kesiapan Enterprise di Sektor Finansial dalam Penerapan Undang-Undang Perlindungan Data Pribadi".

Penulis menyadari bahwa ada begitu banyak pihak yang telah turut membantu penulis dalam menyelesaikan penelitian tugas akhir ini sehingga penulis mengucapkan terimakasih kepada seluruh pihak yang telah membimbing dan membantu dalam keseluruhan aktivitas tugas akhir yang dijalani oleh penulis selama ini.

Oleh karena itu, penulis mengucapkan terima kasih kepada pihak dibawah ini:

1) Papa dan Mama selaku kedua orang tua penulis yang selalu memberikan dukungan dan semangat bagi penulis.
2) Bapak Prof. Dr. Ir. Hari Purnomo., M.T., IPU, ASEAN.Eng, selaku Rektor Universitas Islam Indonesia.
3) Bapak Mukhammad Andri Setiawan, S.T., M.Sc., Ph.D., selaku dosen pembimbing yang berkenan meluangkan waktu untuk membimbing dan mengarahkan penulis selama penyusunan tesis.
4) Bapak Ir. Irving Vitra Paputungan, S.T., M.Sc., Ph.D., selaku dosen penguji yang telah bersedia memberikan kritik dan saran terhadap tesis.
5) Bapak Kholid Haryono, S.T., M.Kom., selaku dosen penguji yang telah bersedia memberikan kritik dan saran terhadap tesis.
6) Bapak Dr. Hendrik, S.T., M.Eng., selaku dosen penguji yang telah bersedia memberikan kritik dan saran terhadap tesis.
7) Bank KBMI Kelompok IV Wilayah & Pusat yang telah memberikan memberikan bantuan dalam proses pengumpulan data yang diperlukan dalam menyusun tugas akhir.
8) Seluruh pihak yang telah memberikan motivasi dan dukungan dalam berbagai bentuk yang tidak dapat disebutkan satu per satu.

Penulis telah berusaha sebaik mungkin dalam menyusun Tesis ini, namun penulis menyadari bahwa masih terdapat kekurangan dalam Tesis ini. Oleh karena itu, penulis sangat

mengharapkan saran dan kritik yang bersifat membangun dari semua pihak. Penulis berharap semoga tugas akhir ini berguna dapat bermanfaat bagi pembaca dan pihak-pihak lain yang berkepentingan.

Wassalamualaikum Wr. Wb.

Yogyakarta, 3 Agustus 2026



Delfindra Faiz Noorhadi

Daftar Isi

Lembar Pengesahan Pembimbing i

Lembar Pengesahan Penguji ii

Abstrak iii

Abstract iv

Pernyataan Keaslian Tulisan v

Daftar Publikasi vi

Halaman Kontribusi vii

Halaman Persembahan viii

Kata Pengantar ix

Daftar Isi xi

Daftar Tabel xiv

Daftar Gambar xv

Daftar Rumus xvi

Glosarium xvii

BAB 1 Pendahuluan 1

1.1 Latar Belakang 1

1.2 Rumusan Masalah 3

1.3 Batasan Masalah 3

1.4 Tujuan Penelitian 4

1.5 Manfaat Penelitian 4

1.6 Metodologi Penelitian 5

1.7 Sistematika Penulisan 6

BAB 2 Tinjauan Pustaka 7

2.1 Data Privacy 7

2.2 General Data Protection Regulation (GDPR) 10

2.3 Undang-Undang Perlindungan Data Pribadi 12
2.4 ISO 27001 14
2.5 ISO 27701 15
2.6 Context, Input, Process, Product (CIPP) 16
2.7 Capability Maturity Model Integration (CMMI) 18
2.8 Plan Do Check Act (PDCA) 19
2.9 Penelitian Terdahulu 20
BAB 3 Metodologi 28
3.1 Alur Penelitian 28
3.2 Timeline Penelitian 32
3.3 Instrumen Penelitian 35
3.3.1 Matriks Kesiapan Organisasi 35
3.3.2 Instrumen Wawancara 40
3.4 Teknik Analisis Data 45
3.4.1 CIPP Model 45
3.4.2 CMMI Model 45
BAB 4 Hasil dan Pembahasan 48
4.1 Analisis Framework 48
4.1.1 COBIT 48
4.1.2 ITIL 49
4.1.3 ISO 9001 50
4.1.4 ISO 27001 50
4.2 Mapping *Framework* 52
4.2.1 Mapping ISO 27001 & ISO 27701 Terhadap UU PDP 53
4.2.2 Mapping ISO 27001 & ISO 27701 Terhadap POJK 68
4.2.3 Mapping Gap & Overlapping Regulasi 77
4.3 Analisis Kesiapan 81

4.3.1 Kesiapan dari Sisi Context 82
4.3.2 Kesiapan dari Sisi Input 85
4.3.3 Kesiapan dari Sisi Process 88
4.3.4 Kesiapan dari Sisi Product 91
4.3.5 Maturity Level Organisasi 95
4.4 PDCA Framework 105
BAB 5 Kesimpulan dan Saran 110
5.1 Kesimpulan 110
5.2 Saran 112
Daftar Pustaka 113
LAMPIRAN 120

Daftar Tabel

Tabel 2. 1 Prinsip Perlindungan Data Pribadi 8
Tabel 2. 2 Fokus Evaluasi UU PDP 18
Tabel 2. 3 Penelitian Terdahulu..... 25
Tabel 3. 2 Matriks Pengukuran Kesiapan Organisasi 35
Tabel 3. 3 Daftar Pertanyaan Wawancara 40
Tabel 3. 4 Enam Domain Score..... 46
Tabel 4. 1 Mapping UU PDP dengan ISO terkait Hak Subjek Data 53
Tabel 4. 2 Mapping UU PDP dengan ISO terkait Pemrosesan Data..... 56
Tabel 4. 3 Mapping UU PDP dengan ISO terkait Kewajiban Pengendali dan Prosesor..... 58
Tabel 4. 4 Mapping UU PDP dengan ISO terkait Transfer Data dan Sanksi..... 66
Tabel 4. 5 Mapping POJK dengan ISO terkait Perlindungan Konsumen 68
Tabel 4. 6 Mapping POJK dengan ISO terkait Penanganan Sengketa & Pelaporan..... 73
Tabel 4. 7 Mapping POJK dengan ISO terkait Sanksi 75
Tabel 4. 8 Overlapping regulasi dengan ISO 77
Tabel 4. 9 Gap regulasi dengan ISO..... 79
Tabel 4. 10 Analisis dari Sisi Context 82
Tabel 4. 11 Analisis dari Sisi Input 85
Tabel 4. 12 Analisis dari Sisi Process 88
Tabel 4. 13 Analisis dari Sisi Product 91
Tabel 4. 14 Maturity Level Organisasi..... 95
Tabel 4. 15 Tingkat *Maturity* dalam setiap area..... 103
Tabel 4. 16 PDCA Cycle 105

Daftar Gambar

Gambar 1. 1 Alur Penelitian 5
Gambar 2. 1 *Maturity Level* di CMMI 19
Gambar 3. 1 Alur Penelitian 28
Gambar 3. 2 *Timeline Penelitian* 32
Gambar 4. 1 *Overall Maturity Score* 104

Daftar Rumus

Rumus 3. 1 *Unweighted Mean* 47
Rumus 4. 1 *Unweighted Mean Area* 101

Glosarium

CIPP	- Model evaluasi yang menilai kesiapan organisasi melalui empat dimensi: *context*, *input*, *process* dan *product*.
CMMI	- Model yang digunakan untuk menilai *maturity* dan kapabilitas proses organisasi.
Data Hoarding	- Praktik penyimpanan data secara berlebihan tanpa batasan waktu yang jelas, meskipun data tersebut sudah tidak lagi relevan.
Data Masking	- Proses menyembunyikan data dengan memodifikasi huruf dan angka aslinya
Data Subject Right	- Hak-hak yang dimiliki individu atas data pribadinya, termasuk hak untuk mengakses, memperbaiki dan menghapus data tersebut.
PII	- Setiap informasi yang dapat digunakan untuk mengidentifikasi individu tertentu, baik secara langsung maupun tidak langsung.
PII Controller	- Pihak yang menentukan tujuan dan cara pemrosesan data pribadi serta bertanggung jawab atas kepatuhan pemrosesan tersebut terhadap ketentuan hukum yang berlaku.
PII Processor	- Pihak yang memproses data pribadi atas nama dan sesuai instruksi dari pengendali data tanpa menentukan sendiri tujuan pemrosesan.
Right to be Forgotten	- Hak subjek data untuk meminta penghapusan data pribadinya dari suatu sistem atau organisasi
Pseudonymization	- Teknik de-identifikasi yang menggantikan nilai-nilai data sensitif dengan token yang dihasilkan secara kriptografi

BAB 1
Pendahuluan

1.1 Latar Belakang

Saat ini isu keamanan data khususnya *data breach*, semakin menjadi perhatian penting bagi organisasi publik maupun swasta (Putri et al., 2020). Data dari Kementerian Komunikasi dan Informatika menunjukkan bahwa 47,8% organisasi belum memahami Perlindungan Data Pribadi dan ketentuan-ketentuan di dalamnya (Direktur Jenderal Aplikasi Informatika, 2021). Kondisi ini diperkuat oleh laporan dari Badan Siber dan Sandi Negara (BSSN) yang mencatat 330 juta anomali trafik serta 241 indikasi *data breach* sepanjang 2024 yang menggambarkan rentannya kondisi keamanan siber nasional (Direktorat Operasi Keamanan Siber, 2024). Untuk menjawab tantangan tersebut, pemerintah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang mulai berlaku pada Oktober 2024 (Presiden Republik Indonesia, 2022).

UU Perlindungan Data Pribadi (UU PDP) dirancang untuk melindungi data pribadi dari penyalahgunaan, akses ilegal dan kebocoran data. Undang-undang ini membagi data pribadi menjadi dua kategori, yaitu data pribadi umum dan data pribadi spesifik (Presiden Republik Indonesia, 2022). Dalam praktiknya, implementasi UU PDP menghadapi berbagai hambatan, termasuk rendahnya kesadaran organisasi, kesiapan teknis yang belum merata dan perlunya pedoman tata kelola yang lebih terstruktur (Direktur Jenderal Aplikasi Informatika, 2021)**.** Temuan ini menggambarkan bahwa kepatuhan terhadap regulasi membutuhkan investasi yang tidak sedikit (Li et al., 2019). Oleh karena itu, dibutuhkan pendekatan yang sistematis untuk memastikan kepatuhan terhadap regulasi.

Sektor-sektor dengan risiko tinggi terhadap pelanggaran data khususnya pada *finance industries* menjadi sangat relevan dalam konteks perlindungan data pribadi (Komandla, 2023; Paul et al., 2023). Perbankan dipandang sebagai sektor yang paling rentan karena memiliki dua potensi risiko utama, yaitu keamanan data konsumen dan kesalahan dalam proses transaksi (Subawa, 2020). Selain itu, sektor perbankan memiliki standar yang ketat dalam pengelolaan data pribadi karena operasionalnya sangat bergantung pada pengumpulan, penyimpanan dan pemrosesan data nasabah dalam jumlah besar, termasuk data keuangan, transaksi, identitas dan biometrik (Baker, 2017; Otoritas Jasa Keuangan, 2014). Pada Mei 2023, Bank BSI mengalami serangan *ransomware* yang dikenal sebagai

LockBit 3.0. Serangan ini mengakibatkan berbagai data nasabah bocor (Antoine et al., 2025). Insiden BSI menjadi peringatan keras bagi ekosistem perbankan nasional.

Penelitian ini difokuskan pada Kelompok Bank berdasarkan Modal Inti 4 (KBMI Kelompok IV), yaitu kelompok bank dengan modal inti menengah hingga besar yang mengelola aset antara lebih dari Rp14 triliun hingga di atas Rp70 triliun (Otoritas Jasa Keuangan, 2021). Objek penelitian ini tergolong sebagai Bank Sistemik sesuai POJK No. 2/POJK.03/2018, dimana kegagalan pada bank dengan karakteristik tersebut berpotensi menimbulkan efek domino terhadap institusi keuangan lain, memicu risiko penarikan dana secara masif (*bank run*) dan mengganggu stabilitas sistem keuangan nasional (Ellis et al., 2022; Otoritas Jasa Keuangan, 2018). Kondisi ini menegaskan urgensi penerapan standar keamanan informasi yang telah teruji secara global untuk merespons kompleksitas risiko yang dihadapi.

Peran International Organization for Standardization (ISO) menjadi penting karena menyediakan spesifikasi teknis yang mengatur bagaimana sebuah sistem, produk atau proses harus beroperasi (Kosanke, 2006). Implementasi ISO 27001 membantu organisasi menekan biaya kerugian akibat insiden keamanan informasi serta meningkatkan kepercayaan konsumen dan keunggulan kompetitif (Wu et al., 2022). Selain itu, ISO 27001 menyediakan kerangka kerja manajemen terbaik untuk menerapkan dan memelihara keamanan informasi (Sharma & Dash, 2012). Namun, ISO 27001 belum mencakup aspek privasi secara menyeluruh. Oleh karena itu, ISO 27701 hadir sebagai perluasan ISO 27001 dengan fokus pada pengelolaan data pribadi (ISO/IEC 27701:2019, 2019). Penerapan ISO 27701 membantu organisasi memenuhi tuntutan privasi yang semakin meningkat seiring perkembangan teknologi dan regulasi (Nuruddeen et al., 2025).

Efektivitas implementasi ini tidak dapat dinilai hanya dari hasil akhir, melainkan harus melalui proses evaluasi yang sistematis dan menyeluruh. Untuk melakukan evaluasi dipilih *Context, Input, Process, Product* (CIPP) dan *Capability Maturity Model Integration* (CMMI). CIPP adalah *framework* untuk memandu evaluasi formatif dan sumatif evaluasi proyek, program, personil, produk, institusi dan sistem (Stufflebeam, 2003). (Kaivanpanah & Zarrin, 2025) menunjukan bahwa penerapan CIPP dapat mengidentifakasi hambatan kritis dalam evaluasi. Selain itu digunakan CMMI, tujuan dari penerapan model ini adalah untuk membantu organisasi dalam mengukur tingkat kematangan dan kemampuan prosesnya, mengidentifikasi prioritas perbaikan dan memberikan panduan dalam pelaksanaan implementasi (Khatibian et al., 2010; Najmi et al., 2010). Oleh karena itu, kedua model

tersebut digunakan untuk menilai efektivitas penerapan kebijakan perlindungan data pribadi sesuai dengan ketentuan perundangan yang berlaku di sektor perbankan.

Meskipun berbagai penelitian telah membahas implikasi hukum perlindungan data pribadi, masih terdapat kesenjangan dalam penerjemahan ketentuan regulatif ke dalam arsitektur operasional organisasi. Untuk mengatasi hal tersebut, penelitian ini menganalisis kepatuhan privasi data dan kesiapan operasional pada salah satu bank sistemik Indonesia (KBMI Kelompok IV). Kontribusi utama penelitian ini terletak pada integrasi model CIPP dan CMMI dalam arsitektur berbasis *Plan-Do-Check-Act* (PDCA) yang didukung oleh pemetaan kontrol ISO 27001 dan ISO 27701. Pendekatan ini memungkinkan evaluasi yang sistematis terhadap tata kelola, tingkat kematangan proses dan keselarasan regulasi dalam konteks perlindungan data pribadi. Penelitian ini menjawab dua pertanyaan utama: (RQ1) Bagaimana tingkat kesiapan organisasi perbankan dalam mengimplementasikan UU PDP dapat diukur menggunakan kerangka *CIPP* dan *CMMI* dan (RQ2) Bagaimana ISO 27001 dan ISO 27701 dapat *dimappingkan* terhadap ketentuan UU PDP dan regulasi OJK untuk mengidentifikasi *gap* kepatuhan pada sektor perbankan serta implikasi konseptual apa yang dapat diusulkan untuk mengatasi *gap* kepatuhan yang teridentifikasi?.

1.2 Rumusan Masalah

Berdasarkan penjelasan yang sudah dituliskan pada latar belakang, berikut adalah beberapa rumusan masalah, yaitu:

a. Bagaimana kesiapan sektor perbankan Indonesia, khususnya bank berkategori sistemik (Bank KBMI Kelompok IV), dalam merespons kewajiban kepatuhan yang diatur oleh UU Perlindungan Data Pribadi?
b. Bagaimana keterkaitan antara standar teknis seperti ISO 27001 dan ISO 27701 dengan kewajiban hukum yang diatur dalam UU PDP dan regulasi OJK, karena belum ada *mapping* yang eksplisit antara standar teknis dengan regulasi tersebut.

1.3 Batasan Masalah

Agar masalah yang dibahas tidak meluas dan mengakibatkan pembahasan menjadi tidak jelas dan mendalam maka pada penelitian ini, penulis membatasi masalah yang diteliti, yaitu:

a. Konteks dalam penelitian ini hanya fokus pada sektor perbankan.
b. Pengambilan data hanya dilakukan di 1 Bank KBMI Kelompok IV.

c. Penelitian ini hanya fokus pada perlindungan data pribadi.
d. Hasil *mapping* bersifat akademis dan tidak merepresentasikan pandangan atau interpretasi resmi dari Otoritas Jasa Keuangan (OJK) maupun Kementerian Komunikasi dan Digital (Komdigi).

1.4 Tujuan Penelitian

Untuk menjawab rumusan masalah maka tujuan dari penelitian ini adalah sebagai berikut:

a. Mengukur tingkat kesiapan organisasi perbankan, khususnya pada bank berkategori sistemik (Bank KBMI Kelompok IV), dalam mengimplementasikan ketentuan UU Perlindungan Data Pribadi.
b. Menyusun *mapping* antara ISO 27001 dan ISO 27701 dengan ketentuan UU PDP serta regulasi OJK, untuk mengidentifikasi *gap* kepatuhan yang ada pada sektor perbankan, dan mengusulkan implikasi konseptual berupa kerangka kerja *Plan-Do-Check-Act* (PDCA).

1.5 Manfaat Penelitian

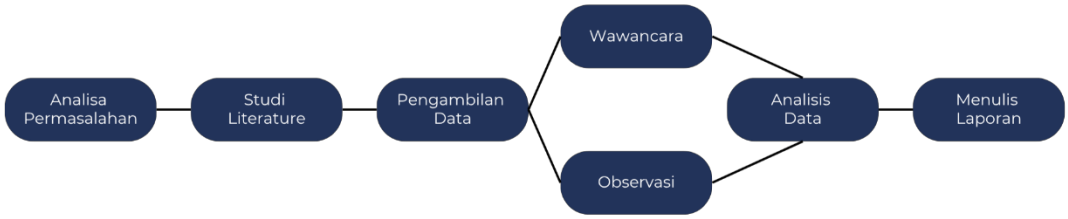
a. Academic perspective

Bagi lingkungan akademik, penelitian ini akan memberikan pemahaman bagaimana penerapan *framework* seperti ISO 27000 *series* dalam konteks perlindungan data pribadi diterapkan di organisasi khususnya perbankan. Selain itu dengan adanya penelitian ini, diharapkan sektor perbankan dapat menyesuaikan kebijakan dan praktik pengelolaan data pribadinya agar selaras dengan regulasi dari UU PDP.

b. Practical perspective

Bagi organisasi, penelitian ini akan memberikan *assesment report* yang menyediakan *gap analysis* antara praktik pengelolaan data pribadi yang telah diterapkan dengan ketentuan dalam UU PDP. Hasil asesmen ini akan digunakan untuk merancang *framework* dan *implementation guidelines* yang sesuai bagi sektor perbankan, hal ini termasuk penyusunan evaluation matriks untuk menilai tingkat kesiapan dan kepatuhan organisasi terhadap regulasi. Selain itu, penelitian ini juga bertujuan untuk meningkatkan kesadaran baik *stakeholders* dan staf terhadap pentingnya perlindungan data sesuai dengan peran dan tanggung jawab masing-masing sehingga potensi *data breach* dapat diminimalisir.

1.6 Metodologi Penelitian



Gambar 1. 1 Alur Penelitian

Penelitian ini terdiri dari 5 tahapan utama sebagaimana ditunjukkan pada Gambar 1. 1 Alur Penelitian, yaitu:

1. Analisis Permasalahan

   Pada tahap ini, penulis melakukan identifikasi masalah mengenai penerapan undang-undang perlindungan data pribadi di Indonesia, bagaimana penerapannya di *enterprise* dan apakah organisasi sudah pada *comply* dengan regulasi ini.

2. Studi Literature

   Tahapan berikutnya Adalah studi literature, hal ini bertujuan untuk menemukan teori-teori dan *framework* yang akan digunakan.

3. Pengambilan Data

   Dalam pengambilan data primer dilakukan dengan 2 metode, yaitu:

   a. Wawancara

      Wawancara dilakukan dengan *Business Branch Manager* dan *Department Head Application Developer* salah satu Bank KBMI. Wawancara ini bertujuan untuk menggali lebih dalam terkait pemahaman, implementasi kebijakan, tantangan dan *best practices* yang diterapkan dalam pengelolaan keamanan informasi dan data nasabah.

   b. Observasi

      Observasi dilakukan terhadap berbagai dokumen dan artefak organisasi seperti standar operasional prosedur (SOP) mengenai pengamanan data pribadi dan prosedur penanganan insiden apabila terjadi kebocoran data dan pelanggaran terhadap sistem keamanan informasi.

4. Analisis Data

   Di tahap ini, data-data yang sudah dikumpulkan melalui wawancara dan observasi dianalisis secara sistematis untuk memperoleh pemahaman yang lebih mendalam. Analisis dilakukan menggunakan metode CIPP dan CMMI.

5. Menulis Laporan

   Pada tahap terakhir, dilakukan proses penyusunan laporan secara menyeluruh yang merangkum seluruh hasil temuan dan analisis yang telah dikumpulkan.

1.7 Sistematika Penulisan

Untuk memudahkan dalam pembahasan penelitian ini maka penulis membuat sistematika penulisan sebagai berikut:

BAB 1 Pendahuluan

Bab ini menjelaskan mengenai masalah yang akan diteliti. Secara lebih detail bab ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian dan sistematika penelitian.

BAB 2 Tinjauan Pustaka

Bab ini menjelaskan mengenai teori-teori yang digunakan dalam penelitian ini dan beberapa penelitian terdahulu. Secara lebih detail bab ini berisi *data privacy,* General Data Protection*,* undang-undang perlindungan data pribadi, CIPP, CMMI, ISO 27001, ISO 27701, *Plan Do Check Act* dan penelitian terdahulu.

BAB 3 Metodologi

Bab ini menjelaskan alur penelitian, lokasi dan waktu penelitian dan *tools* yang digunakan dalam penelitian ini.

BAB 4 Hasil dan Pembahasan

Bab ini menjelaskan hasil dari penelitian dan implementansi *framework* dan *tools* yang digunakan.

BAB 5 Kesimpulan dan Saran

Bab ini menjelaskan kesimpulan akhir dari penelitian ini dan juga menjelaskan terkait penelitian lanjutan yang akan dilakukan di masa depan.

BAB 2
Tinjauan Pustaka

2.1 Data Privacy

Pada tahun 1948, United Nations Universal Declaration of Human Right pada artikel 12 menyatakan bahwa "Tidak seorang pun boleh dikenai campur tangan sewenang-wenang terhadap privasinya, keluarganya, rumahnya, atau surat-menyuratnya, maupun serangan terhadap kehormatan dan reputasinya. Setiap orang berhak atas perlindungan hukum terhadap campur tangan atau serangan semacam itu" (United Nations, 2015). Artikel tersebut menyoroti data pribadi seperti nama, alamat, agama harus dilindungi karena mengandung informasi yang krusial (Morić et al., 2024).

Data pribadi menurut Undang-undang Perlindungan Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau non elektronik (Presiden Republik Indonesia, 2022). Sedangkan menurut General Data Protection Regulation (GDPR), data pribadi adalah informasi apapun yang berkaitan dengan orang alami yang telah diidentifikasi atau dapat diidentifikasi (subjek data); orang yang dapat diidentifikasi adalah orang yang dapat diidentifikasi secara langsung atau tidak langsung, khususnya dengan merujuk pada pengidentifikasi seperti nama, nomor identifikasi, data lokasi, pengidentifikasi daring, atau satu atau lebih faktor yang spesifik terhadap identitas fisik, fisiologis, genetik, mental, ekonomi, budaya atau sosial dari orang tersebut (General Data Protection, 2018).

Berdasarkan UU PDP, data pribadi dibagi menjadi 2 jenis, yaitu:

a. Data pribadi umum: nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan dan data pribadi yang dikombinasikan untuk mengidentifikasi seseorang.
b. Data pribadi spesifik: data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi dan data lainnya sesuai dengan ketentuan peraturan perundang-undangan.

GDPR menerapkan 7 prinsip perlindungan data pribadi yang ditulis pada artikel 5 dan semua entitas baik *data controller* dan *data processor* harus memastikan bahwa individu atau organisasi harus *comply* terhadap regulasi tersebut (General Data Protection, 2018; Štarchoň & Pikulík, 2019). Berikut adalah penjelasan dari prinsip perlindungan data pribadi pada Tabel 2. 1 Prinsip Perlindungan Data Pribadi.

Tabel 2. 1 Prinsip Perlindungan Data Pribadi

Prinsip	Definisi
Fairness, lawfulness, transparency	Data pribadi harus diproses secara sah, adil dan transparan terhadap subjek data
Purpose limitation	Data pribadi harus dikumpulkan untuk tujuan yang spesifik, jelas dan sah dan tidak diproses lebih lanjut dengan cara yang tidak sesuai dengan tujuan tersebut
Data minimization	Data pribadi harus memadai, relevan dan dibatasi pada apa yang diperlukan sehubungan dengan tujuan pengolahan data tersebut
Accuracy	Data pribadi harus akurat dan jika diperlukan, diperbarui secara berkala
Storage limitation	Data pribadi harus disimpan dalam bentuk yang memungkinkan identifikasi subjek data tidak lebih lama dari yang diperlukan untuk tujuan pemrosesan data pribadi tersebut
Integrity and confidentiality	Data pribadi harus diproses dengan cara yang memastikan keamanan yang memadai terhadap data pribadi, termasuk perlindungan terhadap pemrosesan yang tidak sah atau melanggar hukum, serta terhadap kehilangan, kerusakan atau kerusakan yang tidak disengaja, dengan menggunakan langkah-langkah teknis atau organisasi yang sesuai
Accountability	Pengendali data bertanggung jawab atas dan harus dapat membuktikan kepatuhan terhadap GDPR

Untuk memahami secara lebih mendalam terkait prinsip-prinsip perlindungan data pribadi yang dibuat oleh GDPR, berikut adalah penjelasannya:

a. *Fairness, lawfulness, transparency*

   Prinsip ini menekankan bahwa pemrosesan data pribadi harus memiliki dasar hukum yang jelas, dilakukan secara adil terhadap subjek data yang datanya diproses dan transparan. Organisasi harus secara terbuka menginformasikan kepada subjek data mengenai bagaimana data mereka dikumpulkan, digunakan dan dibagikan. Tidak boleh ada proses tersembunyi atau penggunaan data di luar sepengetahuan subjek data.

b. *Purpose limitation*

   Prinsip ini menekankan bahwa data pribadi hanya boleh dikumpulkan untuk tujuan yang spesifik, eksplisit dan sah. Artinya, organisasi tidak dapat mengumpulkan data untuk satu tujuan dan menggunakannya untuk tujuan lain yang tidak sesuai tanpa persetujuan terlebih dahulu kepada subjek data dan tujuan pemrosesan harus ditentukan sejak awal pengumpulan data.

c. *Data minimization*

   Prinsip ini menekankan bahwa organisasi hanya boleh mengumpulkan dan memproses data pribadi yang relevan dan terbatas pada apa yang diperlukan untuk mencapai tujuan pemrosesan yang telah ditetapkan. Prinsip ini melarang pengumpulan data secara berlebihan yang tidak memiliki kaitan langsung dengan tujuan yang telah disampaikan kepada subjek data.

d. *Accuracy*

   Prinsip ini menekankan bahwa data pribadi yang diproses harus akurat dan selalu diperbarui jika diperlukan. Organisasi harus mengambil tindakan untuk memastikan bahwa data yang tidak akurat dengan mempertimbangkan tujuan pemrosesannya, segera dihapus atau diperbaiki.

e. *Storage limitation*

   Prinsip ini menekankan bahwa data pribadi tidak boleh disimpan dalam format yang memungkinkan identifikasi individu lebih lama dari yang diperlukan untuk tujuan pemrosesan. Setelah tujuan tersebut tercapai, data harus dihapus atau dianonimkan kecuali ada kewajiban hukum lain yang mengharuskan penyimpanan lebih lama.

f. Integrity and confidentiality

Prinsip ini menekankan bahwa organisasi untuk memastikan keamanan data pribadi melalui langkah-langkah teknis dan organisasional yang memadai. Data harus dilindungi dari pemrosesan yang tidak sah atau melanggar hukum serta dari kehilangan, kehancuran atau kerusakan yang tidak disengaja. Ini sering kali melibatkan penggunaan enkripsi, kontrol akses dan protokol keamanan lainnya.

g. Accountability

Prinsip ini menekankan bahwa pengendali data bertanggung jawab untuk mematuhi semua prinsip GDPR dan harus dapat menunjukkan kepatuhan tersebut. Hal ini berarti organisasi harus mendokumentasikan proses pengolahan data dengan melakukan penilaian dampak perlindungan data dan jika diperlukan dapat menunjuk *Data Protection Officer* dalam kondisi tertentu.

2.2 General Data Protection Regulation (GDPR)

General Data Protection Regulation (GDPR), data pribadi adalah informasi apapun yang berkaitan dengan orang alami yang telah diidentifikasi atau dapat diidentifikasi (subjek data); orang yang dapat diidentifikasi adalah orang yang dapat diidentifikasi secara langsung atau tidak langsung, khususnya dengan merujuk pada pengidentifikasi seperti nama, nomor identifikasi, data lokasi, pengidentifikasi daring, atau satu atau lebih faktor yang spesifik terhadap identitas fisik, fisiologis, genetik, mental, ekonomi, budaya atau sosial dari orang alami (General Data Protection, 2018).

GDPR dirancang untuk melindungi informasi pelanggan yang sensitif, termasuk informasi pribadi yang dapat diidentifikasi dari penyalahgunaan, penggunaan yang tidak semestinya, atau pengungkapan oleh pihak yang tidak berwenang. GDPR adalah kumpulan aturan dan regulasi yang mendefinisikan cara *Personally Identifiable Information* (PII) harus digunakan, ditransfer dan dilindungi. GDPR berlaku untuk setiap organisasi yang berlokasi di Uni Eropa, serta organisasi non Uni Eropa yang memproses data warga negara Uni Eropa (Mangini et al., 2020). Berdasarkan GDPR, pelanggaran terhadap kewajiban perlindungan data pribadi dapat dikenakan sanksi berupa denda. Besaran sanksi tersebut dapat mencapai maksimal 4% dari total omzet global tahunan atau €100 juta, bergantung pada nilai yang lebih besar di antara keduanya (Albrecht, 2016). Di dalam GDPR terdapat 8 hak yang mengatur terkait perlindungan data (General Data Protection, 2018; Wolters, 2018), yaitu:

a. *Right to be Informed*

   Hak ini dijelaskan pada *Article* 12 yang tujuannya untuk memperoleh konfirmasi apakah data pribadinya diproses, mendapatkan salinan data serta informasi yang jelas tentang tujuan, retensi, penerima data dan hak-hak lain yang relevan.

b. *Right of Access*

   Hak ini dijelaskan pada *Article* 15 yang memberikan hak kepada subjek data untuk mendapatkan salinan data yang diproses. Selain itu, pengendali data wajib memberikan informasi mengenai data tersebut dan operasi pemrosesan yang dilakukan. Sesuai dengan *Article* 12, informasi ini harus disajikan dalam bentuk yang ringkas, transparan, mudah dipahami dan mudah diakses menggunakan bahasa yang jelas dan sederhana.

c. *Right to Rectification*

   Hak ini dijelaskan pada *Article* 16 yang tujuannya untuk memperbaiki data pribadi yang tidak akurat atau melengkapi data yang belum lengkap. Pengendali data wajib memberitahu pihak ketiga yang menerima data tersebut.

d. *Right to Erasure / Right to be Forgotten*

   Hak ini dijelaskan pada *Article* 17 yang tujuannya untuk meminta penghapusan data pribadi dalam kondisi tertentu, seperti data tidak lagi diperlukan, persetujuan dicabut, atau pemrosesan melanggar hukum.

e. *Right to Restrict Processing*

   Hak ini dijelaskan pada *Article* 18 yang menjelaskan dasar-dasar hak untuk membatasi pemrosesan data pribadi berlaku. Pertama, hak ini dapat menjadi solusi sementara jika terdapat perselisihan mengenai keakuratan data pribadi atau mengenai pelaksanaan hak untuk menolak. Selanjutnya, hak untuk membatasi pemrosesan data pribadi dapat menjadi alternatif untuk penghapusan data pribadi jika subjek data membutuhkannya sehubungan dengan tuntutan hukum atau menentang penghapusan data yang diproses secara ilegal dengan alasan lain.

f. *Right to Data Portability*

   Hak ini dijelaskan pada *Article* 20 yang tujuannya untuk membatasi pemrosesan data, misalnya saat terjadi sengketa keakuratan data atau saat menunggu hasil keberatan. Data tetap boleh disimpan tetapi tidak boleh diproses kecuali untuk alasan tertentu.

g. *Right to Object*

Hak ini dijelaskan pada *Article* 21 yang tujuannya untuk menolak pemrosesan data dalam kondisi tertentu, terutama untuk *direct marketing*.

h. *Right in Relation to Automated Decision Making and Profiling*

Hak ini dijelaskan pada *Article* 22 yang tujuannya untuk tidak menjadikan subjek keputusan yang sepenuhnya otomatis yang berdampak secara hukum kecuali ada dasar kontrak dan hukum.

2.3 Undang-Undang Perlindungan Data Pribadi

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau non elektronik (Presiden Republik Indonesia, 2022).

UU PDP mengatur hak-hak yang dimiliki oleh subjek data pribadi. Dalam Pasal 5 sampai Pasal 13, terdapat sembilan hak utama yang memberikan perlindungan hukum serta memastikan kendali penuh subjek data terhadap informasi pribadinya, detail dari hak-hak tersebut akan dijelaskan sebagai berikut:

a. Hak untuk mendapatkan informasi

Subjek data berhak memperoleh informasi yang jelas dan lengkap mengenai identitas pengendali data, dasar kepentingan pemrosesan, tujuan pengumpulan, jenis dan relevansi data pribadi yang diproses, jangka waktu penyimpanan dan rincian pihak yang menerima data pribadi tersebut.

b. Hak untuk melengkapi, memperbarui dan/atau memperbaiki kesalahan dan/atau ketidakakuratan data pribadi

Subjek data dapat mengajukan permintaan kepada pengendali data untuk melengkapi, memperbarui dan/atau memperbaiki data pribadi yang tidak akurat, tidak lengkap atau sudah tidak relevan sehingga kualitas dan akurasi data tetap terjaga.

c. Hak untuk mengakses dan memperoleh salinan data pribadi

Subjek data berhak meminta penghapusan data pribadinya, baik karena tujuan pemrosesan telah tercapai, persetujuan telah dicabut, atau data telah diproses secara melawan hukum.

d. Hak untuk mengakhiri pemrosesan, menghapus dan/ atau memusnahkan data pribadi

   Subjek data dapat meminta pembatasan pemrosesan data pribadinya, misalnya saat terjadi perselisihan mengenai keakuratan data atau keberatan terhadap pemrosesan untuk tujuan tertentu sehingga penggunaan data dapat dikendalikan sementara waktu.

e. Hak untuk menarik kembali persetujuan pemrosesan data pribadi

   Subjek data berhak menarik kembali persetujuan tersebut kapanpun dan setelahnya pengendali data dilarang memproses data untuk tujuan yang bersangkutan.

f. Hak untuk mengajukan keberatan

   Subjek data dapat mengajukan keberatan terhadap pemrosesan data pribadinya apabila pemrosesan tersebut dilakukan untuk tujuan lain yang berpotensi merugikan.

g. Hak untuk menunda atau membatasi pemrosesan data pribadi

   Subjek data berhak untuk meminta agar penggunaan datanya dihentikan sementara waktu dalam kondisi tertentu.

h. Hak untuk menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi

   Subjek data berhak memperoleh ganti rugi atas kerugian materil maupun non materil yang dideritanya, apabila terjadi pelanggaran perlindungan data pribadi yang mengakibatkan kerugian.

i. Hak untuk mendapatkan, menggunakan dan mengirimkan data pribadi

   Subjek data berhak memperoleh salinan data pribadinya dalam format yang dapat diakses, menggunakan data tersebut sesuai kebutuhannya dan mengirimkan data tersebut kepada pihak atau pengendali data lain tanpa hambatan dari pengendali data asal.

Undang-Undang Nomor 27 Tahun 2022 telah menetapkan mekanisme sanksi terhadap setiap individu maupun organisasi yang melanggar ketentuan perlindungan data pribadi. Ketentuan sanksi ini tercantum pada Pasal 57 yang memuat dua sanksi utama, yaitu:

a. Sanksi Administratif
   - Peringatan tertulis
   - Penghentian sementara kegiatan pemrosesan data pribadi
   - Penghapusan atau pemusnahan data pribadi

b. Sanksi Denda

Denda paling tinggi 2 (dua) persen dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran.

2.4 ISO 27001

ISO 27001 yang merupakan standar yang dibuat untuk membangun, menerapkan, mengoperasikan, memantau, meninjau, memelihara dan meningkatkan Sistem Manajemen Keamanan Informasi (Gillies, 2011). Selain itu, ISO 27001 merupakan standar internasional untuk sistem manajemen keamanan informasi (*Information Security Management System*) yang menyediakan *framework* untuk mengelola risiko keamanan informasi melalui pengendalian kebijakan, prosedur dan kontrol teknis (ISO/IEC 27001:2022, 2022). Tujuan dari implementasi ISO 27001 adalah untuk tiga pilar utama keamanan informasi (*CIA Triad*).

- *Confidentiality*

  Prinsip ini mengimplikasikan bahwa data dan informasi yang diwakili oleh data tersebut harus dilindungi sedemikian rupa sehingga penggunaannya dibatasi hanya untuk tujuan yang diizinkan oleh pihak yang berwenang (Camp, 1999).

- *Integrity*

  Prinsip ini mengacu pada jaminan bahwa data tidak akan diubah tanpa izin yang sesuai. Di sinilah keakuratan spesifikasi menjadi penting karena hal ini memastikan bahwa sistem sesuai dengan tujuan, sesuai dengan persyaratan yang ditetapkan oleh berbagai pemangku kepentingan, seperti pemilik dan pengguna (Samonas & Coss, 2014).

- *Availability*

  Prinsip ini memastikan bahwa informasi dan aset terkait dapat diakses dan digunakan sesuai permintaan oleh pengguna yang berwenang kapanpun dibutuhkan (Samonas & Coss, 2014).

Information Security Management System adalah *main concept* dalam ISO 27001. *Information Security Management System* didefinisikan sebagai serangkaian kebijakan yang ditetapkan oleh suatu organisasi untuk mendefinisikan, membangun, mengembangkan dan memelihara keamanan sistem komputer mereka berdasarkan sumber daya perangkat keras dan perangkat lunak (Susanto et al., 2011).

Dalam ISO 27001 terdapat 4 *domain* yang mencakup 93 *controls* yaitu:

- *Organizational control*

  Terdiri dari 37 *controls* yang bertujuan untuk membuat *framework* dan tata kelola untuk keamanan informasi.

- *People control*

  Terdiri dari 8 *controls* yang bertujuan untuk memastikan bahwa setiap individu memahami dan bertanggungjawab atas keamanan informasi.

- *Physical control*

  Terdiri dari 14 *controls* yang bertujuan untuk mencegah akses yang tidak bertanggung jawab yang dapat merusak dan mengintervensi informasi.

- *Technological control*

  Terdiri dari 34 *controls* yang bertujuan untuk memastikan bahwa operasional berjalan aman dan menjaga dari serangan dari luar.

2.5 ISO 27701

ISO/IEC 27701 adalah ekstensi privasi dari ISO/IEC 27001 Manajemen Keamanan Informasi dan ISO/IEC 27002 Kontrol Keamanan. Standar internasional untuk sistem manajemen informasi privasi (PIMS), standar ini memberikan panduan tentang perlindungan privasi, termasuk cara organisasi mengelola informasi pribadi dan membantu dalam membuktikan kepatuhan terhadap peraturan privasi di seluruh dunia (ISO/IEC 27701:2019, 2019). ISO/IEC 27701:2019 menyediakan kerangka kerja untuk membantu organisasi dalam menetapkan perlindungan data pribadi dan privasi serta kepatuhan terhadap berbagai peraturan perundang-undangan dalam lingkungan regulasi yang bervariasi. Perbedaan dalam undang-undang privasi data di seluruh dunia diakui sebagai hambatan bagi organisasi yang beroperasi di pasar internasional (Bougiakiotis, 2020). ISO/IEC 27701:2019 dirancang sebagai standar inovatif dalam bidang privasi supaya memastikan bahwa semua organisasi, baik kecil maupun besar yang beroperasi di yurisdiksi yang berbeda dan beroperasi di berbagai sektor industri, dapat secara efisien melindungi dan mengelola informasi pribadi yang mereka miliki (Anwar & Gill, 2020). Dalam ISO 27701 terdapat beberapa *clause* yang menjelaskan terkait PIMS (ISO/IEC 27701:2019, 2019):

a. *Clause 5* (*PIMS specific requirements related to* ISO/IEC 27001)

   Fokus pada perluasan persyaratan keamanan informasi dari ISO/IEC 27001 untuk memasukkan perlindungan privasi. Persyaratan terkait kepemimpinan, perencanaan, dukungan, operasional, evaluasi kinerja dan perbaikan dari ISO/IEC 27001 harus dipertimbangkan dan diperluas secara sesuai untuk memastikan perlindungan privasi.

b. *Clause 6* (*PIMS specific guidance related to* ISO/IEC 27002)

   Fokus pada perluasan panduan keamanan informasi dari ISO/IEC 27002 untuk memasukkan perlindungan privasi. Misalnya organisasi perlu mempertimbangkan panduan implementasi tambahan terkait kebijakan keamanan informasi untuk memasukkan pernyataan privasi yang relevan, berdasarkan persyaratan kepatuhan, kontrak dan pemangku kepentingan.

c. *Clause 7* (*Additional guidance for PII controllers*)

   Klausul ini mencakup panduan implementasi khusus dari *Privacy Information Management System* (PIMS) untuk pengendali *Personally Identifiable Information* (PII). Hal ini berkaitan dengan kontrol yang tercantum dalam *Annex A*.

d. *Clause 8* (*Additional guidance for PII Processors*)

   Klausul ini mencakup panduan implementasi khusus *Privacy Information Management System* (PIMS) untuk pemroses *Personally Identifiable Information* (PII). Hal ini berkaitan dengan kontrol yang tercantum dalam *Annex B*.

2.6 Context, Input, Process, Product (CIPP)

Context, Input, Process, Product (CIPP) adalah *framework* yang komprehensif untuk memandu evaluasi formatif dan sumatif evaluasi proyek, program, personil, produk, institusi dan sistem (Stufflebeam, 2003). Dengan bantuan model ini, evaluasi dapat dilakukan secara sistematis, memenuhi kebutuhan umum evaluasi. Elemen penting yang membedakan model ini dari model lain adalah fokusnya pada konteks dalam evaluasi proses pembelajaran dan pengembangan (Stufflebeam, 2003; Stufflebeam & Coryn, 2014).

Dalam penelitian ini, CIPP digunakan untuk mengevaluasi penerapan kebijakan perlindungan data pribadi berdasarkan undang-undang perlindungan data pribadi dalam organisasi di sektor keuangan. Terdapat 4 komponen dalam CIPP, berikut adalah penjelasan masing-masing komponen:

a. *Context*

Context bertujuan untuk menilai kebutuhan, permasalahan dan peluang yang ada dalam konteks atau lingkungan yang telah ditentukan (Stufflebeam & Coryn, 2014). Tujuan evaluasi konteks adalah untuk mendefinisikan, mengidentifikasi dan menangani kebutuhan populasi sasaran, mengidentifikasi masalah, serta menilai apakah tujuan-tujuan tersebut responsif terhadap kebutuhan yang diinginkan atau tidak (Stufflebeam, 2003; Stufflebeam & Coryn, 2014). Melalui evaluasi ini, organisasi dapat merumuskan tujuan dan sasaran kebijakan yang sejalan dengan tantangan dan kebutuhan sesuai kondisi di lapangan. Dalam implementasi UU PDP, Context mencakup analisis terhadap tingkat kesadaran organisasi terkait pentingnya perlindungan data, kepatuhan terhadap regulasi dan ekspektasi para *stakeholders* terhadap keamanan dan privasi.

b. *Input*

Input bertujuan untuk menilai strategi, kebijakan dan sumber daya yang disiapkan untuk mencapai tujuan program (Stufflebeam, 2003). Aspek ini mencakup kesiapan organisasi baik dari sisi perencanaan teknis, ketersediaan sumber daya, anggaran dan infrastruktur yang diperlukan untuk mendukung pelaksanaan regulasi ini.

c. *Process*

Process adalah tahap di mana masukan digunakan secara efektif untuk mencapai tujuan, sasaran dan sasaran produk yang diinginkan (Aziz et al., 2018; Stufflebeam, 2003). Tujuannya adalah untuk melakukan pemantauan pelaksanaan kebijakan di lapangan dan menilai apakah pelaksanaannya sudah berjalan sesuai rencana yang telah ditetapkan. Aspek ini membantu untuk mengidentifikasi kendala operasional, penyimpangan dan area perbaikan selama fase implementasi berlangsung.

d. *Product*

Product bertujuan untuk menilai efektivitas dan dampak kebijakan terhadap pencapaian tujuan yang sudah dirumuskan di awal program (Stufflebeam, 2003). Penilaiannya mencakup *output, outcome* dan dampak jangka panjang (*impact*) yang dihasilkan dari penerapan kebijakan ini.

Keempat aspek CIPP dapat dilihat pada Tabel 2. 2 Fokus Evaluasi UU PDP, di bawah ini:

Tabel 2. 2 Fokus Evaluasi UU PDP

Aspek	Fokus Evaluasi
Context	Relevansi dan kebutuhan UU PDP di organisasi
Input	Sumber daya dan strategi yang digunakan
Process	Pelaksanaan dan implementasi UU PDP
Product	Hasil dan dampak implementasi

2.7 Capability Maturity Model Integration (CMMI)

Capability Maturity Model Integration (CMMI) adalah adalah model terintegrasi yang digunakan untuk menilai *maturity level* dan kapabilitas proses organisasi melalui pendekatan bertahap maupun berkelanjutan. Tujuan penerapan CMMI adalah membantu organisasi memahami sejauh mana tingkat kematangan proses internal, mengidentifikasi area yang masih perlu diperbaiki dan memberikan panduan untuk mencapai efisiensi dan efektivitas yang lebih tinggi (Khatibian et al., 2010). Melalui penerapan CMMI, organisasi dapat membangun proses yang terdokumentasi dengan baik, terukur dan dapat diulang sehingga tercipta *continues improvment* dalam pengelolaan sumber daya dan pencapaian tujuan bisnisnya.

Dalam penelitian ini CMMI berperan sebagai *framework* untuk menyediakan struktur yang sistematis dan terukur. Model ini digunakan untuk menilai sejauh mana kebijakan, prosedur dan aktivitas organisasi telah berjalan secara konsisten (Walhidayah & Surendro, 2025). Terdapat 5 *level* dalam CMMI untuk menilai *maturity level* dari organisasi (De Carolis et al., 2017; Khatibian et al., 2010), berikut ini adalah penjelasan dari setiap level (De Carolis et al., 2017; Yassien, 2020):

1. *Level 1* (*Initial*)

   Pada tahap ini, proses dalam organisasi masih bersifat tidak terstruktur, belum terdokumentasi dan berjalan secara reaktif terhadap situasi yang muncul.

2. *Level 2* (*Managed*)

   Pada tahap ini, proses mulai dikelola dalam konteks proyek individual. Setiap proyek sudah memiliki dokumentasi dan mekanisme pengendalian tertentu, meskipun belum terintegrasi secara menyeluruh antar unit organisasi.

3. *Level 3* (*Defined*)

   Pada tahap ini, organisasi telah memiliki proses yang terdokumentasi, terstandarisasi dan diintegrasikan di seluruh bagian.

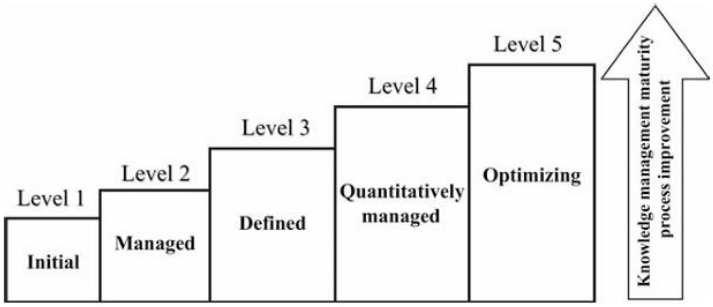
4. *Level 4* (*Quantitatively Managed*)

   Pada tahap ini, organisasi mulai melakukan pengukuran dan pengendalian kinerja proses secara kuantitatif, data dan metrik digunakan untuk mengevaluasi efektivitas dan efisiensi setiap proses yang dijalankan.

5. *Level 5* (*Optimizing*)

   Pada tahap ini organisasi berfokus pada perbaikan berkelanjutan "*continuous process improvement*" dan inovasi.

Gambar 2. 1 *Maturity Level* di CMMI, menunjukkan 5 *level maturity* pada model CMMI.



Gambar 2. 1 *Maturity Level* di CMMI

2.8 Plan Do Check Act (PDCA)

Plan Do Check Act (PDCA) merupakan metode manajemen mutu yang berfungsi sebagai pendekatan untuk melakukan peningkatan berkelanjutan dan telah banyak digunakan dalam berbagai sektor, termasuk industri jasa maupun manufaktur (Isniah, Purba, et al., 2020). Siklus PDCA bertujuan untuk menetapkan, menerapkan, memantau dan memperbaiki efektivitas Sistem Manajemen Keamanan Informasi (*ISMS*) suatu organisasi (Susanto et al., 2011). Setiap fase dalam siklus PDCA memiliki tujuan dan serangkaian aktivitas yang membentuk loop umpan balik untuk perbaikan berkelanjutan yang dimulai dari *Plan, Do, Check, Act* (Jagtap & Teli, 2015). Berikut ini adalah penjelasan dari 4 fase dalam PDCA (Isniah et al., 2020; Realyvásquez-Vargas et al., 2018):

- *Plan*

  Pada fase ini, organisasi mengidentifikasi berbagai peluang perbaikan dan menetapkan prioritas untuk setiap area yang perlu ditingkatkan, selain itu kondisi aktual dianalisis terlebih dahulu berdasarkan data yang valid dan konsisten, akar

penyebab permasalahan ditelusuri kemudian alternatif solusi dirumuskan sebagai dasar penyusunan rencana aksi yang terstruktur.

- *Do*

  Pada fase ini, aktivitas perbaikan dijalankan, didokumentasikan dan dipantau secara sistematis. Selain menjalankan rencana utama, organisasi juga mempertimbangkan kejadian tak terduga, wawasan baru dan pengetahuan yang diperoleh selama proses berjalan sehingga pembelajaran dapat berlangsung secara berkelanjutan.

- *Check*

  Pada fase ini, organisasi mengevaluasi efektivitas tindakan yang telah dilakukan. Hasil penerapan pada fase ini dibandingkan dengan kondisi awal untuk melihat apakah terdapat peningkatan yang signifikan dan apakah target yang direncanakan telah tercapai.

- *Act*

  Pada fase ini berfokus pada pengambilan keputusan lanjutan berdasarkan hasil evaluasi. Jika perbaikan dinilai berhasil maka proses yang telah terbukti efektif dapat distandardisasi dan dijadikan prosedur tetap. Tetapi, apabila hasilnya belum memuaskan maka dilakukan pengujian ulang, revisi strategi atau pengulangan siklus dari tahap awal.

2.9 Penelitian Terdahulu

Dari latar belakang yang sudah dijelaskan sebelumnya, terdapat beberapa penelitian yang membahas topik yang beririsan dengan penelitian ini, yang secara garis besar dapat dikelompokkan ke dalam tiga klaster:

A. Implementasi UU PDP di Indonesia

- Personal Data Protection Law in Indonesia: Challenges and Opportunities

  Syailendra et al. (2024) menganalisis tantangan dan peluang yang muncul setelah diberlakukannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dengan menggunakan pendekatan kualitatif. Penelitian tersebut menunjukkan bahwa regulasi perlindungan data pribadi di Indonesia sebenarnya telah tersebar dalam berbagai peraturan sebelum lahirnya UU PDP. Selain itu, studi ini mengidentifikasi sejumlah hambatan implementasi, termasuk rendahnya tingkat kesadaran organisasi dan

keterbatasan kesiapan teknis dalam memenuhi kewajiban kepatuhan. Temuan tersebut mengindikasikan masih adanya kesenjangan antara tuntutan regulasi dan kemampuan organisasi dalam mengimplementasikan perlindungan data pribadi secara efektif.

- Managing Indonesian Data Breach Notification in the Financial Services Sector: A Case for One-Stop Notification Model

  Algamar et al. (2024) menganalisis mekanisme notifikasi pelanggaran data pada sektor jasa keuangan Indonesia dengan membandingkannya terhadap praktik yang diterapkan dalam General Data Protection Regulation (GDPR) di Uni Eropa. Hasil penelitian menunjukkan bahwa keberadaan berbagai regulasi yang saling beririsan seperti UU ITE, UU PDP serta ketentuan dari Otoritas Jasa Keuangan (OJK) dan Bank Indonesia, menimbulkan kompleksitas kepatuhan bagi institusi keuangan. Sebagai solusi, penelitian ini mengusulkan model one-stop notification untuk menyederhanakan proses pelaporan pelanggaran data dan meningkatkan efektivitas tata kelola kepatuhan.

- Implementation and Challenges of the Personal Data Protection Law in Indonesia

  Razi et al. (2024) menganalisis implementasi UU PDP di Indonesia dengan menyoroti berbagai tantangan yang dihadapi organisasi dalam proses penerapannya. Studi ini menemukan bahwa faktor-faktor seperti rendahnya kesadaran terhadap perlindungan data, keterbatasan sumber daya teknis serta hambatan struktural menjadi kendala utama dalam mencapai kepatuhan yang optimal. Temuan tersebut menunjukkan bahwa banyak organisasi masih berada pada tahap awal dalam mengadopsi praktik perlindungan data yang sesuai dengan persyaratan regulasi.

Ketiga penelitian ini mengidentifikasi adanya *gap* antara tuntutan regulasi dan kesiapan dari organisasi, namun belum ada yang menyediakan instrumen pengukuran yang terstruktur untuk mengukur tingkat kesiapan tersebut secara sistematis, ketiganya bersifat deskriptif-kualitatif tanpa kerangka penilaian maturitas.

B. Implementasi ISO 27001 dan ISO 27701

- ISO 27001 in Banking: An Evaluation of Its Implementation and Effectiveness in Enhancing Information Security

Kuzankah et al. (2023) menganalisis implementasi ISO 27001 di sektor perbankan dan dampaknya terhadap peningkatan keamanan informasi organisasi. Hasil penelitian menunjukkan bahwa penerapan ISO 27001 berkontribusi pada penguatan manajemen risiko, peningkatan kemampuan respons terhadap insiden keamanan serta perbaikan efektivitas pengendalian keamanan informasi. Selain itu, penelitian ini menyoroti pentingnya keseimbangan antara kebutuhan keamanan informasi dan efisiensi operasional dalam lingkungan perbankan yang semakin terdigitalisasi.

- Standardization of Information Security Management in the Banking Sector using the ISO 27001:2022 Framework

  Ryanto & Tundjungsari (2024) menganalisis penerapan standar ISO 27001:2022 pada sektor perbankan Indonesia melalui studi kasus di Bank Victoria International Tbk. Penelitian ini menekankan pentingnya standardisasi sistem manajemen keamanan informasi dalam menghadapi berbagai ancaman siber, termasuk kebocoran data dan serangan eksternal. Hasil penelitian menunjukkan bahwa implementasi ISO 27001:2022 dapat memperkuat mekanisme pengendalian keamanan dan mendukung peningkatan ketahanan organisasi terhadap risiko keamanan informasi.
- ISO/IEC 27701 Standard: Threats and Opportunities for GDPR Certification

  (Lachaud, 2020) menganalisis bahwa ISO 27701 dirancang untuk membantu organisasi dalam mengidentifikasi, mengelola dan melindungi informasi pribadi secara menyeluruh dan terdokumentasi sesuai dengan praktik dan standar hukum yang berlaku. Standar ini memberikan panduan yang sistematis dan rinci bagi organisasi yang berperan sebagai pengendali data (*PII Controllers*) maupun pemroses data (*PII Processors*) dengan menetapkan kontrol, kebijakan dan prosedur yang dapat langsung diintegrasikan ke dalam sistem manajemen keamanan informasi yang sudah ada.
- Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model

  (Anwar & Gill, 2020) menganalisis bahwa kemunculan ISO/IEC 27701:2019 dilatarbelakangi oleh kebutuhan yang mendesak terkait standar yang dapat menjembatani antara praktik keamanan yang bersifat teknis dengan kepatuhan terhadap regulasi perlindungan data, khususnya General Data Protection Regulation di Uni Eropa yang terkenal sangat ketat. GDPR sering dianggap

sebagai regulasi perlindungan data paling komprehensif saat ini, namun dalam implementasinya tidak mudah untuk dilakukan. Banyak organisasi mengalami kesulitan dalam memahami dan memenuhi persyaratan GDPR karena kompleksitas teknis dan legal yang sangat tinggi. ISO 27701 berfungsi sebagai *tools* bagi organisasi untuk menerjemahkan ketentuan hukum GDPR ke dalam kontrol operasional dan proses manajemen. Dengan kata lain, ISO 27701 menyediakan *framework* teknis dan manajerial agar organisasi dapat selaras dengan prinsip-prinsip regulasi perlindungan data pribadi.

Keempat penelitian tersebut menegaskan efektivitas ISO 27001 dan ISO 27701 sebagai kerangka teknis perlindungan data. Namun, masih terdapat *gap* penelitian karena standar tersebut belum dipetakan secara sistematis terhadap persyaratan UU PDP Indonesia dan regulasi sektoral OJK yang menjadi landasan penelitian ini.

C. Implementasi Maturity Model

- Evaluating Maturity Models in Healthcare Information Systems: A Comprehensive Review

  Gomes & Romão (2025) melakukan tinjauan literatur terhadap berbagai *maturity models* yang digunakan dalam sistem informasi kesehatan. Penelitian tersebut mengidentifikasi 45 model kematangan yang diterapkan dalam berbagai konteks organisasi dengan sebagian besar mengadopsi prinsip-prinsip yang berasal dari *Capability Maturity Model Integration* (CMMI). Hasil kajian menunjukkan bahwa model kematangan memberikan kerangka yang sistematis untuk menilai, merencanakan dan meningkatkan kapabilitas proses organisasi. Temuan ini memberikan landasan teoritis yang kuat bagi penggunaan CMMI sebagai instrumen evaluasi kematangan proses dalam konteks kepatuhan perlindungan data pribadi.

- Evaluation of English for Banking Purposes (EBP) Courses Using Stufflebeam's Context, Input, Process and Product (CIPP) Model

  (Kaivanpanah & Zarrin, 2025) menerapkan model *Context, Input, Process and Product* (CIPP) untuk mengevaluasi efektivitas program *English for Banking Purposes* (EBP) di Bank Melli Iran melalui pendekatan *mixed-methods*. Penelitian ini menunjukkan bahwa model CIPP dapat digunakan sebagai kerangka evaluasi yang komprehensif untuk mengidentifikasi kesenjangan antara kebutuhan organisasi, sumber daya yang tersedia, proses implementasi

dan hasil yang dicapai sehingga memberikan landasan metodologis yang kuat bagi penggunaan CIPP dalam mengevaluasi kesiapan organisasi dan mengidentifikasi area perbaikan pada konteks institusional.

Meskipun kedua penelitian membuktikan validitas CMMI dan CIPP sebagai kerangka evaluasi yang kuat, penerapannya dilakukan pada konteks pendidikan, pelatihan perbankan dan kesehatan sehingga masih terdapat kesenjangan penelitian dalam penerapannya pada *domain* kepatuhan perlindungan data pribadi.

Berdasarkan sintesis dari ketiga klaster diatas, didapatkan beberapa *research gap* yang menjadi landasan penelitian ini.

- Beberapa penelitian terkait implementasi UU PDP masih didominasi pendekatan deskriptif dan belum didukung instrumen yang mampu mengukur kesiapan organisasi secara sistematis.
- Penelitian terkait ISO 27001 dan ISO 27701 belum memetakan standar tersebut secara eksplisit terhadap kerangka hukum Indonesia.
- Integrasi CIPP dan CMMI sebagai kerangka evaluasi belum pernah diterapkan dalam konteks kepatuhan perlindungan data pada sektor perbankan Indonesia.

Oleh karena itu, kebaruan penelitian ini terletak pada integrasi model *Context, Input, Process and Product* (CIPP), *Capability Maturity Model Integration* (CMMI) serta pemetaan kontrol ISO 27001 dan ISO 27701 ke dalam arsitektur kepatuhan berbasis *Plan-Do-Check-Act* (PDCA). Melalui pendekatan tersebut, penelitian ini tidak hanya mengevaluasi tingkat kesiapan dan kematangan organisasi dalam menghadapi implementasi UU PDP pada sektor perbankan tetapi juga menghasilkan kerangka kerja konseptual yang dapat digunakan untuk mengidentifikasi kesenjangan kepatuhan dan merumuskan rekomendasi implementasi perlindungan data pribadi yang lebih terstruktur dan selaras dengan standar internasional. Dari penjelasan di atas, dirangkum pada Tabel 2. 3 Penelitian Terdahulu.

Tabel 2. 3 Penelitian Terdahulu

Artikel	Metode Pengumpulan Data	Metode Analisis Data	Temuan
Personal Data Protection Law in Indonesia: Challenges and Opportunities (Syailendra et al., 2024)	Data sekunder: studi dokumen hukum, peraturan perundang-undangan dan literatur	Content analysis terhadap regulasi dan literatur yang relevan	UU PDP menandai langkah dalam perlindungan data di Indonesia akan tetapi implementasinya menghadapi berbagai hambatan seperti rendahnya kesadaran organisasi, ketidaksiapan teknis dan ketidakjelasan pedoman teknis dari pemerintah
Managing Indonesian Data Breach Notification in the Financial Services Sector (Algamar et al., 2024)	Data sekunder: analisis dokumen regulasi (UU ITE, UU PDP, regulasi OJK/BI) dan GDPR Eropa	Analisis komparatif regulasi dengan pendekatan case-based reasoning dari praktik internasional (GDPR) dan diterapkan ke konteks Indonesia	Terdapat patchwork regulasi yang tumpang tindih antara UU PDP, UU ITE dan regulasi OJK/BI dalam kewajiban notifikasi pelanggaran data
Implementation and Challenges of the Personal Data Protection Law in Indonesia (Razi et al., 2024)	Data sekunder: studi literatur, dokumen kebijakan pemerintah dan laporan implementasi UU PDP	Analisis deskriptif terhadap kondisi aktual implementasi UU PDP di berbagai sektor termasuk sektor keuangan	Masih terdapat kesenjangan antara kewajiban regulasi UU PDP dan kesiapan aktual organisasi di Indonesia
ISO 27001 in Banking: An Evaluation of Its Implementation	Data sekunder: review literatur, laporan industri perbankan,	Analisis evaluatif terhadap literatur dan temuan empiris dari	ISO 27001 terbukti meningkatkan postur keamanan informasi bank

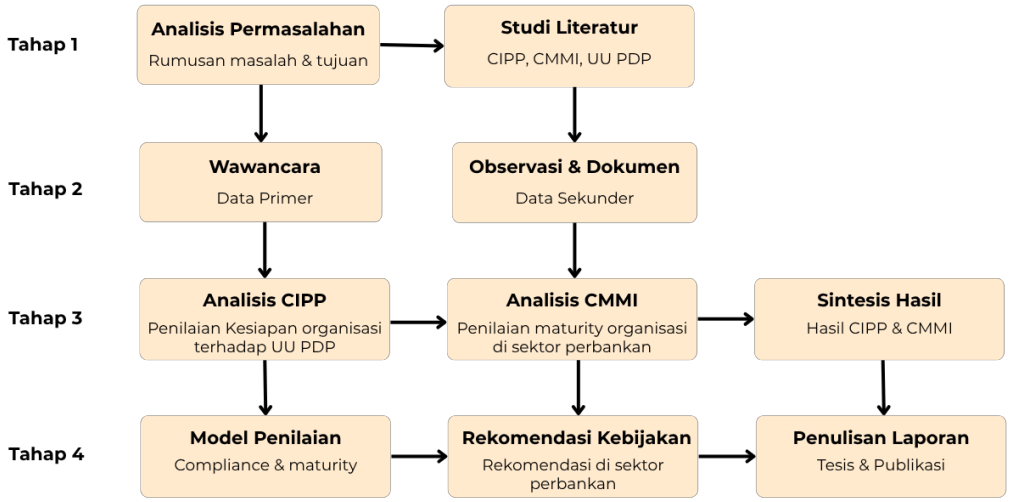
Artikel	Metode Pengumpulan Data	Metode Analisis Data	Temuan
and Effectiveness in Enhancing Information Security (Sarah Kuzankah et al., 2023)	standar ISO 27001 dan studi kasus implementasi di berbagai bank	berbagai studi terkait implementasi ISO 27001 di sektor perbankan	secara signifikan melalui peningkatan manajemen risiko dan kemampuan respons insiden namun terdapat kendala terutama tantangan biaya implementasi dan keseimbangan dengan efisiensi operasional
Standardization of Information Security Management in the Banking Sector using the ISO 27001:2022 *Framework* (Ryanto & Tundjungsari, 2024)	Data primer: wawancara (in-*depth interview*) dan *Focus Group Discussion* (FGD) dengan staf keamanan informasi dan manajemen Bank Victoria International Tbk Indonesia	Analisis kualitatif terhadap data wawancara dan FGD, evaluasi kesesuaian praktik keamanan siber bank dengan kontrol ISO 27001:2022	Implementasi ISO 27001:2022 di Bank Victoria International terbukti efektif dalam mencegah kebocoran data dan serangan siber
ISO/IEC 27701 Standard: Threats and Opportunities for GDPR Certification (Lachaud, 2020)	Data sekunder: analisis dokumen standar ISO/IEC 27701, regulasi GDPR, skema sertifikasi GDPR dan literatur hukum privasi	Analisis komparatif antara persyaratan ISO/IEC 27701 dengan kerangka sertifikasi GDPR	ISO 27701 memiliki potensi besar sebagai mekanisme sertifikasi GDPR namun juga mengandung risiko seperti cakupan yang terlalu luas dan kompleksitas implementasi

Artikel	Metode Pengumpulan Data	Metode Analisis Data	Temuan
Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model (Anwar & Gill, 2020)	Data sekunder: analisis dokumen ISO 27701, persyaratan GDPR dan studi literatur terkait kepatuhan privasi	*Semantic mapping* antara persyaratan ISO 27701 dengan kewajiban GDPR dan pengembangan model kepatuhan menggunakan pendekatan design science	Mengembangkan model kepatuhan terintegrasi yang memetakan 138 persyaratan ISO 27701 ke dalam 99 persyaratan GDPR
Evaluating Maturity Models in Healthcare Information Systems: A Comprehensive Review (Gomes & Romão, 2025)	Data sekunder: *systematic literature review* terhadap 50 *Maturity Model*	*Systematic Literature Review* dan sintesis temuan dari berbagai studi *maturity model*	Model CIPP terbukti efektif sebagai alat evaluasi komprehensif dalam konteks perbankan, evaluasi CIPP berhasil mengidentifikasi hambatan dalam setiap komponen program secara sistematis
Evaluation of English for Banking Purposes (EBP) Courses Using Stufflebeam's Context, Input, Process and Product (CIPP) Model (Kaivanpanah & Zarrin, 2025)	Data primer: kuesioner dan wawancara dengan instruktur dan peserta program EBP perbankan; data sekunder: dokumen kurikulum dan materi pelatihan	Analisis CIPP (*Context, Input, Process, Product*)	Model kematangan berbasis CMMI terbukti efektif membantu organisasi merencanakan dan mengoptimalkan implementasi sistem informasi

BAB 3
Metodologi

3.1 Alur Penelitian

Penelitian ini dilaksanakan melalui empat tahapan utama sebagaimana ditunjukkan pada Gambar 3. 1 Alur Penelitian, yang terdiri analisis permasalahan hingga penulisan laporan akhir. Berikut adalah penjelasan dari masing-masing tahapan:



Gambar 3. 1 Alur Penelitian

1. Tahap 1
   a. Analisis Permasalahan

      Pada tahap awal penelitian, penulis melakukan identifikasi mengenai isu penerapan Undang-Undang Perlindungan Data Pribadi di Indonesia. Identifikasi ini mencakup bagaimana aturan tersebut dijalankan dalam konteks organisasi, sejauh mana organisasi menyesuaikan kebijakannya agar selaras dengan ketentuan hukum yang berlaku dan tantangan yang muncul dalam proses implementasinya. Tahap ini juga berfungsi untuk memetakan gap antara regulasi dengan praktik di lapangan sehingga dapat diketahui apakah organisasi telah sepenuhnya *comply* atau masih terdapat aspek-aspek yang belum terpenuhi. Dengan demikian, analisis permasalahan bukan hanya berfokus pada aspek hukum saja, melainkan juga pada dimensi teknis, manajerial dan budaya yang mempengaruhi efektivitas penerapan UU PDP pada organisasi.

b. Studi Literatur

Tahapan berikutnya adalah studi literatur yang bertujuan untuk memahami teori, konsep dan *framework* yang relevan dengan topik penelitian. Studi ini mencakup penelusuran sumber-sumber akademik seperti jurnal, buku, laporan penelitian, regulasi dan *framework* seperti ISO 27001 dan ISO 27701 yang memiliki keterkaitan erat dengan tata kelola keamanan informasi dan perlindungan data pribadi. Dengan studi literatur, penulis dapat memperoleh landasan teoritis yang kuat serta membangun kerangka konseptual yang akan digunakan dalam analisis. Selain itu, studi literatur juga membantu penulis untuk mengidentifikasi *best practices* dari berbagai negara atau institusi lain yang sudah lebih dahulu menerapkan regulasi serupa sehingga hasil penelitian ini memiliki pembanding yang valid.

2. Tahap 2

Pengambilan Data

Pengambilan data dalam penelitian ini dilakukan melalui pendekatan data primer dengan dua metode utama, yaitu wawancara dan observasi. Kedua metode ini dipilih agar data yang diperoleh tidak hanya berupa informasi dari dokumen tetapi juga mencerminkan realitas yang terjadi di lapangan.

a. Wawancara

Wawancara dilakukan secara mendalam dengan pihak-pihak yang memiliki otoritas dan tanggung jawab langsung terhadap pengelolaan data pribadi nasabah di salah satu Bank KBMI. Responden pertama adalah *Business Branch Manager* pada tingkat cabang. Pemilihan jabatan ini didasarkan pada pertimbangan bahwa manajer cabang memiliki tanggung jawab langsung atas seluruh kegiatan operasional cabang, termasuk pengelolaan data nasabah dalam proses layanan perbankan sehari-hari. Posisi ini dinilai paling kompeten untuk menggambarkan bagaimana kebijakan perlindungan data pribadi diterapkan pada level operasional, mencakup prosedur penanganan data nasabah, mekanisme persetujuan (*consent*) serta pengendalian akses data di lingkungan cabang. Responden kedua adalah *Development Head Application* pada kantor pusat. Pemilihan jabatan ini didasarkan pada pertimbangan bahwa posisi tersebut bertanggung jawab atas perencanaan dan pengembangan aplikasi yang memproses data pribadi nasabah secara teknis.

Responden ini memiliki visibilitas langsung terhadap bagaimana prinsip privacy by design diterapkan sejak tahap perancangan sistem, termasuk mekanisme enkripsi, pengelolaan akses berbasis peran dan *audit trail* pada sistem aplikasi perbankan. Melalui wawancara ini, penulis berupaya menggali pemahaman terkait implementasi kebijakan, tingkat kesadaran organisasi terhadap pentingnya perlindungan data, tantangan yang dihadapi dan *best practices* yang sudah diterapkan. Data yang diperoleh dari wawancara ini menjadi bahan penting untuk menilai sejauh mana kesiapan dan kesesuaian organisasi dengan UU PDP serta mengidentifikasi area yang masih membutuhkan perbaikan.

b. Observasi

Selain wawancara, metode observasi digunakan untuk memperoleh data yang bersifat objektif. Observasi dilakukan dengan cara mempelajari berbagai dokumen, arsip dan artefak organisasi seperti Standar Operasional Prosedur (SOP) mengenai pengamanan data pribadi, laporan audit keamanan informasi maupun dokumen berhubungan dengan perlindungan data. Penulis juga mengamati secara langsung bagaimana mekanisme pengendalian keamanan diterapkan di lingkungan kerja termasuk langkah-langkah teknis dalam mencegah kebocoran data serta prosedur mitigasi jika terjadi insiden. Dengan demikian, observasi ini memberikan validasi tambahan terhadap hasil wawancara dan memperkaya pemahaman mengenai konsistensi antara kebijakan tertulis dengan praktik nyata di lapangan.

3. Tahap 3

Analisis Data

Pada tahap ini, seluruh data yang telah dikumpulkan melalui wawancara dan observasi dianalisis secara sistematis untuk memperoleh pemahaman yang lebih mendalam. Analisis dilakukan dengan mengintegrasikan *Context, Input, Process, Product Model* (CIPP) dan *Capability Maturity Model Integration* (CMMI) sehingga menghasilkan *output* yang tidak hanya menilai kesiapan tetapi juga tingkat kematangan implementasinya. Dalam penelitian ini, CIPP berfungsi sebagai kerangka evaluasi untuk mengidentifikasi kesiapan organisasi dalam menerapkan perlindungan data pribadi berdasarkan empat aspek utama, yaitu *context, input, process dan product*. Melalui keempat aspek tersebut, CIPP

membantu mengevaluasi kondisi organisasi, sumber daya yang tersedia, pelaksanaan proses, serta hasil implementasi yang telah dicapai. Hasil evaluasi ini memberikan gambaran menyeluruh mengenai faktor-faktor yang mendukung maupun menghambat penerapan kebijakan perlindungan data. Kemudian, CMMI digunakan untuk mengukur tingkat kematangan implementasi berdasarkan hasil evaluasi yang diperoleh dari model CIPP. Setiap temuan pada aspek konteks, masukan, proses dan hasil dipetakan ke dalam area proses CMMI agar dapat mengetahui sejauh mana praktik yang diterapkan telah terstandarisasi, terdokumentasi, dikelola dan dikembangkan secara berkelanjutan. Hasil pengukuran tersebut menjadi dasar dalam menyusun rekomendasi strategis untuk meningkatkan tata kelola keamanan informasi, memperbaiki proses yang masih belum optimal, serta mendukung keberlanjutan kepatuhan organisasi terhadap Undang-Undang Pelindungan Data Pribadi. Dengan demikian, kedua model tersebut saling melengkapi dalam proses analisis. CIPP berfungsi untuk mengidentifikasi dan mengevaluasi aspek-aspek yang memengaruhi kesiapan organisasi sedangkan CMMI digunakan untuk mengukur tingkat kematangan implementasi dari aspek-aspek yang telah dievaluasi sehingga menghasilkan rekomendasi perbaikan yang lebih terarah.

4. Tahap 4

a. Perancangan Model

Pengembangan model dilakukan dengan menggunakan pendekatan PDCA (*Plan-Do-Check-Act*) *Cycle* yang memungkinkan organisasi untuk merencanakan, menerapkan, mengevaluasi dan meningkatkan pengelolaan keamanan informasi dan perlindungan data pribadi secara berkelanjutan. Siklus PDCA bertujuan untuk menetapkan, menerapkan, memantau dan memperbaiki efektivitas Sistem Manajemen Keamanan Informasi (ISMS) suatu organisasi (Susanto et al., 2011). Setiap fase dalam siklus PDCA memiliki tujuan dan serangkaian aktivitas yang membentuk loop umpan balik untuk perbaikan berkelanjutan yang dimulai dari *Plan, Do, Check, Act* (Jagtap & Teli, 2015). Dengan menjadikan PDCA sebagai pendekatan, setiap tahapan dapat diselaraskan ke dalam tahapan perencanaan, implementasi, evaluasi dan perbaikan berkelanjutan secara konsisten. Oleh karena itu, bagian selanjutnya akan menguraikan usulan PDCA *Framework* yang menggambarkan pemetaan

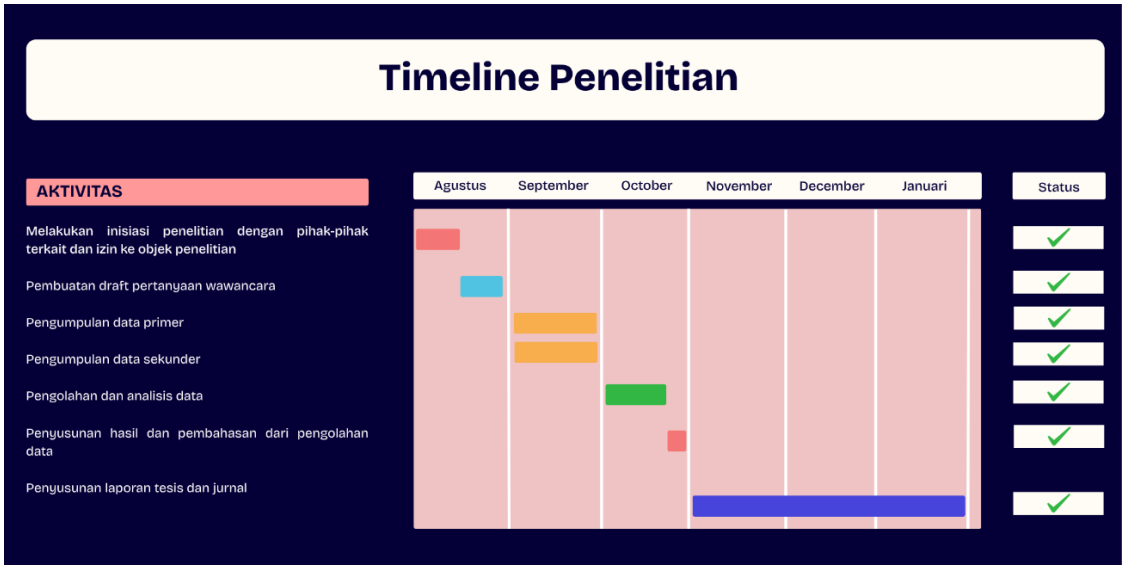
aktivitas, kontrol dan mekanisme evaluasi dalam setiap fase PDCA untuk mendukung kepatuhan terhadap UU PDP melalui integrasi ISO 27001 dan ISO 27701.

b. Menulis Laporan

Tahap terakhir adalah proses penyusunan laporan penelitian yang merangkum seluruh hasil temuan, analisis dan rekomendasi. Penyusunan laporan dilakukan dengan mengikuti struktur ilmiah, mulai dari pendahuluan, tinjauan pustaka, metodologi penelitian, hasil dan pembahasan hingga kesimpulan. Pada bagian ini, penulis tidak hanya mendeskripsikan hasil temuan tetapi juga mengaitkannya dengan teori dan studi literatur yang sudah dibahas sebelumnya. Laporan ini juga menjadi wadah untuk menyajikan rekomendasi praktis bagi organisasi, khususnya terkait langkah-langkah yang perlu dilakukan untuk meningkatkan perlindungan data pribadi dan mematuhi regulasi. Dengan demikian, laporan penelitian tidak hanya bermanfaat secara akademik tetapi juga memiliki nilai praktis sebagai rujukan bagi organisasi dalam memperkuat tata kelola data pribadi.

3.2 Timeline Penelitian

Berdasarkan penjelasan dari latar belakang, rumusan masalah dan metodologi yang telah dipaparkan sebelumnya maka disusunlah *timeline* penelitian sebagai acuan dalam menjalankan setiap fase penelitian ini agar lebih sistematis dan terstruktur. Berikut ini adalah *timeline* dari penelitian ini, yang disajikan pada Gambar 3. 2 *Timeline Penelitian*:



Gambar 3. 2 *Timeline Penelitian*

a. Agustus 2025

Pada bulan Agustus 2025, kegiatan penelitian diawali dengan tahap inisiasi yaitu melakukan koordinasi awal dengan pihak-pihak terkait serta mengurus perizinan untuk memperoleh akses ke objek penelitian yaitu dari pihak Bank KBMI Kelompok IV dari cabang dan pusat. Pada minggu pertama hingga minggu kedua, fokus utama adalah memastikan kesepakatan dan izin resmi agar proses pengumpulan data dapat berjalan lancar. Selanjutnya, pada minggu ketiga hingga minggu keempat, penulis menyusun draft pertanyaan wawancara yang digunakan untuk menggali informasi dari narasumber.

b. September 2025

Pada bulan September 2025, kegiatan penelitian berlanjut pada tahap pengumpulan data, baik data primer dan sekunder. Pengumpulan data primer dilakukan melalui wawancara dan observasi langsung dengan pihak Bank KBMI Kelompok IV dari cabang dan pusat, sedangkan data sekunder diperoleh dari dokumen, laporan, maupun regulasi yang mendukung. Seluruh kegiatan ini berlangsung sepanjang bulan September dengan tujuan memperoleh data yang komprehensif dan beragam sebagai dasar analisis.

c. Oktober 2025

Pada bulan Oktober 2025, penelitian memasuki tahap pengolahan dan analisis data. Kegiatan ini berlangsung dari minggu pertama hingga minggu ketiga, di mana seluruh data yang telah terkumpul diolah dan dianalisis untuk menemukan pola serta jawaban atas rumusan masalah penelitian. Kemudian, pada minggu keempat, hasil analisis tersebut mulai disusun dalam bentuk narasi pembahasan yang terstruktur sehingga dapat memberikan gambaran menyeluruh terkait kondisi aktual yang ditemukan di lapangan.

d. November 2025

Pada bulan November 2025, kegiatan penelitian difokuskan pada penyusunan hasil penelitian. Tahapan ini meliputi penyempurnaan pembahasan untuk memastikan bahwa seluruh temuan yang dihasilkan telah sesuai dengan kerangka teoritis yang digunakan. Hasil sementara penelitian juga dievaluasi untuk memastikan kualitas dan relevansinya terhadap tujuan penelitian.

e. Desember 2025

Pada bulan Desember 2025, penelitian diarahkan pada penyusunan laporan akhir. Pada tahap ini, penulis merangkum seluruh hasil penelitian dalam bentuk laporan tesis

lengkap yang mencakup seluruh bab penelitian, mulai dari pendahuluan hingga kesimpulan. Selain itu, penulis juga menyusun artikel ilmiah atau jurnal sebagai bentuk publikasi akademik dari hasil penelitian ini.

f. Januari 2026

Pada bulan Januari 2026, kegiatan penelitian difokuskan pada tahap finalisasi yaitu penyempurnaan laporan tesis serta persiapan untuk ujian tesis. Pada tahap ini, laporan akhir diperiksa kembali agar sesuai dengan ketentuan akademik. Dengan demikian, keseluruhan rangkaian kegiatan penelitian diharapkan dapat selesai tepat waktu dan menghasilkan kontribusi yang signifikan baik secara akademis maupun praktis.

3.3 Instrumen Penelitian

3.3.1 Matriks Kesiapan Organisasi

Kesiapan organisasi adalah pandangan, kepercayaan, sikap dan ekspektasi para anggota organisasi terhadap sejauh mana organisasi memiliki kemampuan dan kesiapan untuk menerima, mengadopsi dan menjalankan perubahan untuk mendorong peningkatan kinerja secara menyeluruh (Susyanto, 2019). Dalam penelitian ini, kesiapan yang dimaksud adalah sejauh mana organisasi memiliki budaya kerja, sumber daya dan tata kelola untuk mendukung implementasi Undang-Undang Perlindungan Data Pribadi (UU PDP) secara efektif. Berikut ini adalah matriks pengukuran yang dapat digunakan untuk mengukur tingkat kesiapan organisasi yang disajikan pada Tabel 3. 1 Matriks Pengukuran Kesiapan Organisasi.

Tabel 3. 1 Matriks Pengukuran Kesiapan Organisasi

Area Kepatuhan	Persyaratan	Pasal Terkait	Matriks Pengukuran
Pemrosesan Data	Memiliki dasar hukum yang sah untuk setiap kegiatan pemrosesan data pribadi	Pasal 20	• Terdapat *mapping* untuk setiap pemrosesan data • Terdapat dokumentasi dasar hukum untuk setiap aktivitas pemrosesan (contoh: formulir persetujuan, klausul kontrak, dll)
	Pemrosesan dilakukan secara terbatas, spesifik, sah dan transparan	Pasal 16 ayat (2), Pasal 27	• Pengumpulan data dibatasi hanya pada data yang relevan dengan tujuan yang telah ditetapkan • Dalam *privacy policy* disebutkan secara spesifik tujuan pengumpulan dari setiap data

Area Kepatuhan	Persyaratan	Pasal Terkait	Matriks Pengukuran
	Memastikan akurasi, kelengkapan dan konsistensi data	Pasal 29	• Terdapat proses verifikasi data pada saat pengumpulan data • Adanya prosedur untuk pembaruan data secara berkala atau *by request*
Hak Subjek Data	Memberikan informasi yang jelas kepada Subjek Data Pribadi	Pasal 5, Pasal 21	• Tersedia Pemberitahuan Privasi (*Privacy Notice*) yang mudah diakses dan dipahami, memuat informasi sesuai Pasal 21
	Memberikan hak akses dan salinan data kepada Subjek Data	Pasal 7, Pasal 32	• Terdapat prosedur untuk memverifikasi identitas pemohon • Dapat menyediakan data dan rekam jejak pemrosesan dalam waktu 3x24 jam sejak permintaan diterima
	Memfasilitasi hak untuk memperbaiki dan memperbarui data	Pasal 6, Pasal 30	• Terdapat prosedur untuk menerima dan memproses permintaan perbaikan data • Dapat melakukan perbaikan atau pembaruan dilakukan dalam waktu 3x24 jam sejak permintaan diterima
	Memfasilitasi hak untuk menghapus dan memusnahkan data	Pasal 8, Pasal 43, Pasal 44	• Terdapat Prosedur penghapusan/pemusnahan data tersedia jika tujuan tercapai, persetujuan ditarik kembali, atau ada permintaan • Terdapat bukti bahwa data telah dihapus/dimusnahkan

Area Kepatuhan	Persyaratan	Pasal Terkait	Matriks Pengukuran
Kewajiban Pengendali dan Prosesor	Mendapatkan persetujuan yang sah dan eksplisit	Pasal 20 ayat (2) huruf a, Pasal 21-24	• Terdapat Formulir persetujuan dibuat secara tertulis atau terekam, mudah dipahami, menggunakan bahasa sederhana dan jelas • Terdapat sistem untuk mencatat dan mengelola bukti persetujuan
	Melakukan pemrosesan data anak dan penyandang disabilitas secara khusus	Pasal 25, Pasal 26	• Terdapat mekanisme verifikasi usia • Terdapat prosedur untuk mendapatkan persetujuan dari orang tua/wali anak atau penyandang disabilitas/walinya
	Melakukan perekaman seluruh kegiatan pemrosesan data	Pasal 31	• Membuat dan memelihara Catatan Kegiatan Pemrosesan (*Record of Processing Activities/RoPA*)
	Melakukan pengawasan terhadap pihak yang terlibat dalam pemrosesan	Pasal 37, Pasal 51	• Terdapat perjanjian pemrosesan data dengan Prosesor Data (*Data Processing Agreement*)
Keamanan dan Manajemen Risiko	Melindungi dan memastikan keamanan data pribadi	Pasal 35, Pasal 39	• Menerapkan protokol enkripsi dan kontrol akses untuk keamanan data • Melakukan penilaian tingkat keamanan berdasarkan sifat dan risiko data

Area Kepatuhan	Persyaratan	Pasal Terkait	Matriks Pengukuran
	Menjaga kerahasiaan data pribadi	Pasal 36	• Terdapat perjanjian kerahasiaan (*Non Disclosure Agreement*) untuk pihak yang dapat mengakses data
	Memberitahukan kegagalan pelindungan data (*data breach*)	Pasal 46	• Terdapat Prosedur Standar Operasi (SOP) penanganan insiden kebocoran data yang mencakup kewajiban lapor secara tertulis kepada Subjek Data dan Lembaga dalam waktu 3x24 jam
Transfer Data Pribadi	Memastikan pelindungan data dalam transfer lintas negara	Pasal 56	• Terdapat daftar negara tujuan transfer data dan penilaian tingkat perlindungan data di negara tersebut
Tata Kelola dan Akuntabilitas	Menunjuk Pejabat/Petugas Fungsi Pelindungan Data Pribadi (DPO)	Pasal 53, Pasal 54	• Melakukan penilaian apakah organisasi wajib menunjuk DPO berdasarkan kriteria di Pasal 53
	Menunjukkan pertanggungjawaban (*accountability*)	Pasal 47	• Terdapat dokumentasi semua kebijakan, prosedur dan tindakan kepatuhan yang telah diambil
	Menangani pengalihan data akibat aksi korporasi (merger, akuisisi, dll)	Pasal 48	• Terdapat prosedur untuk memberitahukan pengalihan data kepada subjek data sebelum dan sesudah aksi korporasi

Level:

a. 1: Tidak Ada (Proses atau kontrol sama sekali belum ada, tidak terdokumentasi dan tidak disadari)
b. 2: Dasar (Ada kesadaran akan kebutuhan proses atau kontrol. Beberapa praktik dasar sudah mulai diterapkan tapi masih belum standar, tidak konsisten antar departemen dan belum terdokumentasi secara resmi)
c. 3: Terdefinisi (Proses atau kontrol sudah didefinisikan, didokumentasikan secara resmi dan dikomunikasikan ke seluruh unit / divisi terkait)
d. 4: Terkelola (Proses yang sudah terdefinisi tidak hanya dijalankan tapi juga dipantau, diukur efektivitasnya dan dievaluasi secara berkala

3.3.2 Instrumen Wawancara

Untuk memperoleh data primer, penelitian ini menyusun wawancara semi-terstruktur yang disusun berdasarkan empat dimensi dalam model *Context, Input, Process, Product* (CIPP). Penyusunan wawancara ini bertujuan untuk memastikan bahwa proses pengumpulan data dilakukan secara terarah, konsisten dan mampu menggali informasi yang relevan dengan tujuan penelitian. Setiap pertanyaan disusun untuk mengeksplorasi kondisi organisasi, ketersediaan sumber daya, implementasi proses perlindungan data pribadi dan hasil atau dampak penerapan kebijakan perlindungan data sesuai dengan masing-masing dimensi CIPP. Hasil wawancara kemudian digunakan sebagai acuan utama dalam proses pengumpulan data dari dua responden penelitian, yaitu *Business Branch Manager* dan *Department Head Application Developer* yang dipilih karena mewakili perspektif bisnis dan teknologi informasi dalam implementasi perlindungan data pribadi. Rincian pertanyaan wawancara yang digunakan dalam penelitian ini disajikan pada Tabel 3. 2 Daftar Pertanyaan Wawancara.

Tabel 3. 2 Daftar Pertanyaan Wawancara

CIPP Model	Tujuan	Responden	Pertanyaan	Referensi
Context	Memahami situasi, kebutuhan dan pendorong utama sebelum dan saat awal implementasi UU PDP	*Stakeholders*	• Sebelum UU PDP disahkan dan menjadi perhatian utama, bagaimana pandangan dan tingkat kesadaran Bank KBMI mengenai pentingnya perlindungan data pribadi nasabah? Apa yang menjadi pemicu utama kesadaran tersebut? • Apa pendorong utama bagi organisasi ini untuk memprioritaskan kepatuhan terhadap UU PDP? Apakah dorongan tersebut murni karena kewajiban hukum atau ada faktor lain seperti tuntutan nasabah atau reputasi?	• (Reksoprodjo et al., 2024) • (Nugraha & Nasyuha, 2024) • (Presiden Republik

CIPP Model	Tujuan	Responden	Pertanyaan	Referensi
			• Apakah inisiatif untuk sertifikasi dengan standar ISO 27001 dan ISO 27701 sudah ada sebelum UU PDP menjadi fokus, atau justru UU PDP yang mendorong adopsi standar-standar ini sebagai *framework*?	Indonesia, 2022) • (ISO/IEC 27001:2022, 2022) • (ISO/IEC 27701:2019, 2019)
	Memahami kesiapan teknis dari *developers* terkait privasi data	*Developers*	• Bagaimana persepsi tim *developers* mengenai integrasi persyaratan UU PDP dan ISO 27001 dalam aktivitas pengembangan aplikasi? Apakah hal ini dipandang sebagai hambatan teknis atau sebagai standar yang perlu diadopsi? • Sebelum regulasi ini diberlakukan, sejauh mana tingkat *awareness developers* terkait isu privasi data nasabah?	
Input	Mengidentifikasi sumber daya, kebijakan dan perencanaan yang dialokasikan untuk implementasi UU PDP	*Stakeholders*	• Sumber daya apa saja misalnya, anggaran khusus, pembentukan tim / departemen baru, pengadaan teknologi yang organisasi ini alokasikan secara spesifik untuk mempersiapkan dan mengimplementasikan UU PDP? • Kebijakan dan prosedur apa yang Bank KBMI kembangkan atau revisi sebagai landasan untuk program kepatuhan UU PDP?	

CIPP Model	Tujuan	Responden	Pertanyaan	Referensi
			• Bagaimana struktur organisasi Bank KBMI terkait perlindungan data? Apakah Bank KBMI telah menunjuk fungsi DPO sesuai perintah UU PDP? • Pelatihan dan program peningkatan kesadaran seperti apa yang diberikan kepada karyawan di semua tingkatan untuk memastikan mereka memahami kewajiban berdasarkan UU PDP dan kebijakan internal?	
	Mengidentifikasi sumber daya teknis dan tools yang dibutuhkan	*Developers*	• Apakah unit bisnis / unit *compliance* sudah memberikan *technical requirements* terkait regulasi privasi data? • Tools apa saja yang digunakan organisasi untuk mengamankan data dari nasabah? Apakah ada *tools* atau *platform* tertentu yang diwajibkan?	
Process	Memahami langkah-langkah, aktivitas dan tantangan yang terjadi selama proses implementasi	*Stakeholders*	• Bisa dijelaskan langkah-langkah konkret yang telah dan sedang dilakukan dalam proses implementasi? • Bagaimana organisasi memonitor, meninjau dan mengaudit efektivitas dari kontrol yang telah diimplementasikan? Apakah ada audit internal atau eksternal yang secara spesifik mengacu pada kepatuhan UU PDP?	

CIPP Model	Tujuan	Responden	Pertanyaan	Referensi
			• Apa tantangan terbesar yang dihadapi selama proses implementasi ini?	
	Menganalisis mekanisme teknis implementasi kontrol privasi dalam Siklus Hidup Pengembangan Sistem	*Developers*	• Bagaimana mekanisme teknis penghapusan data "*Right to be Forgotten*" diimplementasikan untuk memastikan data benar-benar tidak dapat dipulihkan? • Bagaimana arsitektur sistem dirancang untuk memfasilitasi permintaan portabilitas data nasabah sehingga format yang dihasilkan aman, terstandarisasi dan dapat dibaca oleh mesin?	
Product	Mengevaluasi dampak, hasil dan efektivitas dari keseluruhan program implementasi	*Stakeholders*	• Dilihat dari sudut pandang organisasi, sejauh mana implementasi yang telah dilakukan berhasil membawa organisasi selaras dengan aspek hukum UU PDP? • Selain pemenuhan aspek hukum, bagaimana Bapak menilai dampak implementasi ini terhadap penguatan postur perlindungan data pribadi secara keseluruhan? Apakah Bapak melihat adanya peningkatan dalam keamanan data nasabah? Apakah ada penurunan jumlah atau dampak dari insiden kebocoran data sejak program ini diimplementasikan?	

CIPP Model	Tujuan	Responden	Pertanyaan	Referensi
			• Secara keseluruhan, apakah dengan penerapan ISO 27001 dan ISO 27701 terbukti efektif membantu organisasi untuk selaras dengan regulasi UU PDP? Di area mana standar ini paling memberikan nilai tambah? • Melihat ke depan, apa langkah selanjutnya bagi organisasi dalam menjaga dan terus meningkatkan kematangan program perlindungan data pribadi pasca implementasi awal UU PDP? • Apa dampak implementasi UU PDP terhadap: ▪ Proses bisnis inti misalnya, pembukaan rekening, pengajuan kredit? ▪ Hubungan dan kepercayaan dengan nasabah? ▪ Inovasi produk dan layanan digital?	
	Mengevaluasi efektivitas, performa dan keamanan sistem aplikasi pasca implementasi UU PDP	Developers	• Berdasarkan monitoring, apakah implementasi fitur keamanan tambahan seperti enkripsi *end-to-end* berdampak signifikan terhadap latensi sistem atau waktu respons aplikasi? • Bagaimana mekanisme pencatatan "*logging*" dirancang agar tetap informatif untuk penelusuran insiden "*debugging*" tanpa mengekspos data sensitif nasabah secara terbuka?	

3.4 Teknik Analisis Data

3.4.1 CIPP Model

Tahap pertama analisis dilakukan menggunakan model *Context, Input, Process, Product* (CIPP) sebagai kerangka evaluasi kualitatif. Seluruh data yang diperoleh dari wawancara dianalisis dengan mengelompokkan informasi ke dalam empat dimensi utama CIPP sehingga diperoleh gambaran menyeluruh mengenai kesiapan organisasi dalam mengimplementasikan perlindungan data pribadi sesuai ketentuan UU PDP. Pada dimensi *context*, analisis difokuskan pada identifikasi latar belakang organisasi, kebutuhan implementasi, regulasi yang menjadi dasar penerapan serta komitmen manajemen terhadap perlindungan data pribadi. Dimensi *input* digunakan untuk mengevaluasi kesiapan sumber daya organisasi, meliputi struktur organisasi, kebijakan, prosedur, infrastruktur teknologi serta kompetensi sumber daya manusia yang mendukung implementasi perlindungan data. Selanjutnya, dimensi *process* diarahkan untuk mengidentifikasi bagaimana kebijakan dan prosedur tersebut diterapkan dalam kegiatan operasional, termasuk mekanisme pengelolaan data pribadi, pengendalian keamanan informasi, pemantauan kepatuhan serta proses evaluasi yang dilakukan organisasi. Terakhir, dimensi *product* digunakan untuk menilai hasil implementasi, manfaat yang diperoleh organisasi serta tingkat pencapaian terhadap tujuan perlindungan data pribadi. Selama proses analisis, peneliti melakukan *thematic analysis* yang muncul dari hasil wawancara sehingga dapat menggambarkan kondisi aktual organisasi pada masing-masing dimensi CIPP. Proses ini dilakukan untuk meningkatkan kredibilitas hasil penelitian dengan memastikan adanya konsistensi antara informasi yang disampaikan oleh responden dengan bukti terdokumentasi yang dimiliki organisasi.

3.4.2 CMMI Model

Setelah analisis menggunakan model CIPP dilakukan, hasil evaluasi selanjutnya dikonversi menjadi pengukuran menggunakan kerangka *Capability Maturity Model Integration* (CMMI). Tahapan ini bertujuan untuk memberikan ukuran objektif terhadap tingkat kematangan organisasi dalam memenuhi persyaratan perlindungan data pribadi berdasarkan UU PDP. Untuk menjamin transparansi dalam penelitian, prosedur penilaian pada setiap *domain* kepatuhan dirancang secara sistematis. Setiap persyaratan kepatuhan yang tercantum pada Tabel 3. 1 Matriks Pengukuran Kesiapan

Organisasi, diberikan skor tingkat kematangan pada skala 1 hingga 4 berdasarkan bukti yang diperoleh dari dua sumber utama, yaitu hasil wawancara dengan dua responden dan dokumen internal organisasi. Skor 4 (*Quantitatively Managed*) diberikan apabila bukti dari wawancara dan dokumentasi menunjukkan bahwa praktik yang dinilai telah diterapkan secara menyeluruh, dipantau secara berkala serta didukung oleh mekanisme evaluasi yang terukur. Skor 3 (*Defined*) diberikan ketika proses telah terdokumentasi dan dikomunikasikan secara formal, namun belum didukung oleh pengukuran kinerja yang sistematis. Skor 2 (*Managed*) menunjukkan bahwa praktik dasar telah tersedia dan dijalankan tetapi implementasinya masih belum konsisten atau belum terdokumentasi secara formal. Sementara itu, skor 1 (*Initial*) diberikan apabila belum terdapat proses yang jelas atau praktik yang dapat diidentifikasi terkait persyaratan yang dinilai. Selanjutnya, nilai *maturity* untuk masing-masing dari enam *domain* kepatuhan dihitung menggunakan rata-rata dari seluruh skor persyaratan yang berada dalam *domain* tersebut. Pendekatan ini memungkinkan penilaian tingkat *maturity* dilakukan secara terstruktur dan konsisten sehingga menghasilkan gambaran yang lebih objektif mengenai kondisi kepatuhan organisasi terhadap persyaratan perlindungan data pribadi dan tata kelola keamanan informasi. Berikut ini adalah 6 *domain score* yang digunakan dalam penelitian ini yang dijelaskan pada tabel Tabel 3. 3 Enam *Domain Score*.

Tabel 3. 3 Enam *Domain Score*

No.	Domain	Jumlah Persyaratan
1	Pemrosesan Data	3
2	Hak Subjek Data	4
3	Kewajiban Pengendali dan Prosesor	4
4	Keamanan dan Manajemen Risiko	3
5	Transfer Data Pribadi	1
6	Tata Kelola dan Akuntabilitas	3
Total		18

Untuk menghasilkan evaluasi pada tingkat organisasi secara keseluruhan, skor pada setiap persyaratan kemudian disintesis menggunakan kerangka *Capability Maturity Model Integration* (CMMI) yang dimodifikasi dan diterapkan pada enam area kepatuhan utama. Selanjutnya, nilai *Overall Maturity Score* dihitung untuk merepresentasikan tingkat kematangan organisasi secara menyeluruh yang ditunjukan pada Rumus 3. 1 *Unweighted Mean*:

$$M_{Total} = \frac{1}{n}\sum_{i=1}^{n} C_i \tag{3.1}$$

Rumus 3. 1 *Unweighted Mean*

$^{M}Total$: Skor *maturity level* secara keseluruhan

n : Jumlah *domain* kepatuhan

C_i: Skor rata-rata pada *domain* kepatuhan

BAB 4
Hasil dan Pembahasan

4.1 Analisis Framework

Pada penelitian ini, subjek penelitiannya adalah salah satu Bank KBMI, berdasarkan hasil wawancara dan observasi dokumen dari Bank KBMI, diketahui bahwa Bank KBMI menggunakan beberapa *framework* dalam tata kelola IT, yaitu COBIT, ITIL, ISO 9001 dan ISO 27001. Penggunaan *framework-framework* ini dilakukan untuk memperkuat ketahanan Bank terhadap berbagai risiko baik dari dalam atau dari luar organisasi seperti kemampuan terhadap perubahan regulasi, serangan siber dan ketidakpastian bisnis. Di Bank KBMI tata kelola teknologi informasi digunakan untuk memastikan bahwa IT Bank KBMI selaras dengan tujuan strategis dalam mendukung pencapaian nilai bisnis yang optimal. Penerapan tata kelola ini bertujuan untuk mengelola risiko di bidang IT, meningkatkan efektivitas dan efisiensi dan memastikan bahwa IT di Bank KBMI selaras dengan regulasi yang berlaku. Berikut ini adalah penjelasan dari masing-masing *framework.*

4.1.1 COBIT

COBIT adalah kerangka kerja tata kelola IT yang dikembangkan oleh *Information Systems Audit and Control Association* (ISACA) yang bertujuan untuk memberikan panduan terstruktur dalam menyelaraskan proses IT dengan tujuan bisnis. COBIT membantu organisasi memenuhi persyaratan kepatuhan, mengurangi risiko dan mengelola IT organisasi (ISACA, 2019).

Di Bank KBMI, COBIT digunakan sebagai *framework* dalam mengelola IT agar dapat mendukung kebutuhan para *stakeholders* baik internal maupun eksternal. Dengan pendekatan ini, COBIT memungkinkan Bank KBMI memetakan keterkaitan antara tujuan IT dengan tujuan bisnis secara jelas sehingga *stakeholders* dapat memprioritaskan inisiatif teknologi yang memberikan dampak langsung pada pencapaian target bisnis. *Framework* ini juga menyediakan mekanisme untuk mengukur tingkat kematangan (*maturity level*) dari setiap proses IT yang dijalankan sehingga organisasi dapat menilai sejauh mana proses-proses tersebut telah optimal dan di mana diperlukan perbaikan. Selain itu, penerapan COBIT di Bank KBMI berfokus pada penciptaan sinergi yang kuat antara strategi bisnis dan strategi IT dengan perhatian khusus pada informasi dan data sebagai aset strategis. COBIT

menyediakan *domain-domain* yang dapat membantu memastikan bahwa setiap aktivitas IT selaras dengan strategi organisasi, meminimalkan risiko operasional dan meningkatkan *value* yang diberikan kepada organisasi.

Dengan penggunaan *framework* ini, Bank KBMI dapat memastikan bahwa pengelolaan IT tidak hanya memenuhi persyaratan regulasi tetapi juga mendukung inovasi, kelincahan organisasi dalam menghadapi perubahan lingkungan bisnis yang adaptif. Hal ini pada akhirnya menciptakan tata kelola IT yang lebih proaktif dan mampu memberikan *business value* yang optimal bagi organisasi.

4.1.2 ITIL

ITIL adalah *framework* yang dikembangkan oleh *UK's Office of Government Commerce* (OGC) untuk membuat *best practice* dalam manajemen layananan teknologi informasi dan komunikasi (Potgieter et al., 2005). ITIL menyediakan kerangka kerja untuk membantu organisasi merancang, menyampaikan, mengoperasikan dan terus meningkatkan layanan IT sehingga mendukung pencapaian tujuan bisnis.

Di Bank KBMI, ITIL berperan penting dalam menyelaraskan layanan pendukung IT dengan strategi bisnis organisasi. ITIL menitikberatkan pada penyusunan proses, prosedur, *task* dan penetapan *service level* yang terukur untuk memastikan layanan IT memenuhi kebutuhan pengguna internal maupun eksternal. Dengan adanya standar ini, Bank KBMI dapat menjamin konsistensi kualitas layanan, meningkatkan kepuasan pengguna dan meminimalkan gangguan operasional yang berpotensi memengaruhi layanan kepada nasabah.

Selain itu, ITIL juga menyediakan *framework* untuk evaluasi yang memungkinkan organisasi mengidentifikasi area yang membutuhkan perbaikan dan melakukan peningkatan secara berkelanjutan. Dengan pendekatan *service lifecycle*, ITIL membantu Bank KBMI memastikan setiap fase, mulai dari *service strategy, service design, service transition, service operation* sampai *continual service improvement* dilakukan dengan kontrol yang baik dan terdokumentasi.

Dengan penerapan *framework* ini, Bank KBMI memperoleh *baseline* untuk perencanaan, implementasi dan pengukuran kinerja layanan IT. Hal ini juga mendukung *value creation* bagi bisnis karena memungkinkan IT bertindak sebagai *enabler*, bukan sekadar fungsi pendukung (*back office*). Penerapan ITIL, juga membantu menjaga kompetensi tim IT, mendukung koordinasi antar unit dan

memastikan layanan IT dapat beradaptasi terhadap perubahan kebutuhan bisnis dan regulasi.

4.1.3 ISO 9001

ISO 9001 adalah standar internasional untuk sistem manajemen mutu (*Quality Management System*) yang diterbitkan oleh *International Organization for Standardization* (*ISO*) (ISO 9001:2015, 2015). Bank KBMI telah menerapkan kerangka kerja ini sejak tahun 2007, khususnya pada area *IT Operation* dan *IT Security Management* untuk memastikan seluruh proses yang dilakukan mengikuti prinsip mutu yang sudah terstandarisasi.

Tujuan penerapan *framework* ISO 9001 adalah memastikan organisasi mampu memenuhi kebutuhan dan ekspektasi stakeholders secara konsisten, termasuk nasabah dan regulator. Standar ini menekankan pentingnya dokumentasi proses, pengendalian prosedur dan pemantauan hasil agar penyampaian layanan dapat dipastikan sesuai kualitas yang diharapkan. Pendekatan yang digunakan dalam ISO 9001 bersifat berbasis risiko (*Risk Based Thinking*) yang berarti setiap proses dianalisis terlebih dahulu untuk mengidentifikasi potensi kegagalan, dampak terhadap operasional dan langkah mitigasi yang diperlukan.

Selain itu, penerapan *framework* ISO 9001 di Bank KBMI juga mendorong budaya *continuous improvement* atau perbaikan berkelanjutan. Siklus PDCA (*Plan-Do-Check-Act*) menjadi kerangka utama yang memandu organisasi dalam merencanakan, melaksanakan, mengevaluasi dan memperbaiki proses agar kualitas tetap terjaga. Dengan pendekatan ini, efek negatif yang dapat menimbulkan kerugian bagi organisasi dapat diminimalkan dan unit IT dapat selalu bersikap proaktif untuk memperbaiki sistem serta memastikan kesesuaian dengan perkembangan kebutuhan bisnis maupun tuntutan regulasi.

4.1.4 ISO 27001

ISO 27001 merupakan standar internasional yang secara khusus mengatur *Information Security Management System* (ISMS), yaitu sebuah sistem manajemen yang memberikan kerangka kerja terstruktur untuk mengelola risiko keamanan informasi (ISO/IEC 27001:2022, 2022). Standar ini membantu organisasi mengidentifikasi aset informasi penting, menilai risiko yang terkait dan menerapkan kontrol teknis dan prosedural yang diperlukan untuk melindungi kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan informasi (*availability*).

Implementasi ISO 27001 di Bank KBMI bertujuan untuk memperkuat postur keamanan IT secara menyeluruh, memastikan bahwa proses bisnis *digital banking* berlangsung dengan aman dan membangun citra positif baik dari nasabah dan *business partner*. Penerapan standar ini mencakup serangkaian aktivitas, mulai dari perencanaan kebijakan keamanan informasi, penetapan tanggung jawab, penerapan kontrol akses, enkripsi, pengelolaan insiden, pemantauan dan *logging* aktivitas sampai evaluasi berkelanjutan melalui audit internal dan eksternal. Penerapan ISO 27001 juga memiliki dampak strategis terhadap posisi kompetitif Bank KBMI di industri perbankan dan *fintech*. Dengan penggunaan ISO 27001, Bank KBMI dapat menunjukkan kepada nasabah dan *business partner* bahwa sistem keamanannya telah memenuhi standar sehingga dapat meningkatkan reputasi dan citra positif organisasi. Dari perspektif kepatuhan, implementasi standar ini memudahkan Bank KBMI dalam memenuhi persyaratan regulator seperti OJK, BI dan UU PDP karena sebagian besar pasal terkait perlindungan data pribadi selaras dengan *framework* ini. Secara keseluruhan, manfaat dari penerapan *framework* ini meliputi:

1. Menjadikan Bank KBMI lebih kompetitif di industri *fintech* dan perbankan dan dapat memberikan citra positif bagi nasabah dan *business partner*.
2. Meningkatkan tata kelola keamanan informasi sesuai dengan regulasi yang berlaku sehingga dapat mempermudah izin dari regulator.
3. Memberikan kemudahan dalam meningkatkan kontrol terkait keamanan informasi di proses bisnis *digital banking.*

Berdasarkan penjelasan diatas, diketahui bahwa penerapan 4 *framework* (COBIT, ITIL, ISO 9001 dan ISO 27001) di Bank KBMI memberikan fondasi yang kuat untuk tata kelola IT. Peran masing-masing *framework* ini saling melengkapi satu dengan lain, seperti COBIT yang berperan untuk mengukur tingkat *maturity* organisasi, ITIL berperan untuk memastikan layanan IT yang konsisten dan terukur, ISO 9001 yang berperan untuk menjamin kualitas/mutu dan *continues improvement* dan ISO 27001 yang berperan untuk membangun sistem keamanan informasi yang terstruktur. Kombinasi dari *framework-framework* tersebut membantu Bank KBMI untuk menciptakan tata kelola IT yang tidak hanya efektif dan efisien tetapi juga siap untuk menjawab tantangan regulasi yang terus berkembang. Namun, untuk benar-benar menilai sejauh mana penerapan *framework-framework* ini mendukung kepatuhan terhadap UU Perlindungan Data Pribadi, diperlukan pemetaan yang lebih terperinci. Pemetaan (*Mapping*) ini bertujuan untuk melihat keterkaitan antara setiap kontrol

atau proses dalam *framework* dengan pasal-pasal yang diatur dalam UU PDP. Dengan cara ini, organisasi dapat mengidentifikasi area yang sudah selaras, area yang perlu ditingkatkan dan potensi celah kepatuhan yang harus segera diperbaiki.

4.2 Mapping *Framework*

Untuk menjaga pembahasan tetap fokus pada rumusan masalah dan tujuan penelitian, pada bagian ini akan secara khusus membahas proses *mapping* antara ISO 27001 dan ISO 27701 dengan regulasi perlindungan data pribadi yang berlaku di Indonesia, khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan ketentuan pendukung dari regulator sektor keuangan seperti Otoritas Jasa Keuangan (OJK).

Mapping ini dilakukan untuk mengidentifikasi sejauh mana kontrol yang terdapat pada ISO 27001 yang berfokus pada *Information Security Management System* (ISMS) dan ISO 27701 yang menambahkan fokus pada *Privacy Information Management System* (PIMS) mampu mendukung pemenuhan kewajiban hukum yang diatur dalam UU PDP. Proses *mapping* mencakup analisis hubungan antara klausul, kontrol dan tujuan keamanan pada kedua standar dengan pasal-pasal UU PDP yang mengatur prinsip pemrosesan data, hak subjek data, kewajiban pengendali data, manajemen insiden kebocoran data, transfer data lintas negara dan kewajiban penunjukan *Data Protection Officer* (DPO).

Melalui *mapping* ini, diharapkan dapat diperoleh gambaran yang lebih jelas mengenai area yang sudah sepenuhnya *comply*, area yang perlu dilakukan perbaikan atau penguatan dan area yang mungkin belum tercakup sama sekali. Hasil analisis ini menjadi dasar untuk memberikan rekomendasi perbaikan yang bersifat praktis bagi organisasi di sektor perbankan sehingga tata kelola keamanan informasi terutama di sektor perlindungan data pribadi dapat lebih efektif mendukung kepatuhan terhadap UU PDP maupun regulasi lain yang relevan di sektor perbankan dan *fintech* yang ada Indonesia.

4.2.1 Mapping ISO 27001 & ISO 27701 Terhadap UU PDP

Implementasi ISO 27001 dan ISO 27701 sebagai model kerangka kerja dapat menjadi pendekatan strategis untuk menjembatani gap kepatuhan terhadap Undang-Undang Perlindungan Data Pribadi (UU PDP) di sektor keuangan, khususnya perbankan. Integrasi kedua standar ini memungkinkan organisasi untuk menyelaraskan pengelolaan keamanan informasi melalui *Information Security Management System* (ISMS) dengan pengelolaan privasi data melalui *Privacy Information Management System* (PIMS) dalam satu kerangka tata kelola yang terpadu.

Melalui proses mapping antara klausul dan kontrol ISO 27001 dan ISO 27701 dengan pasal-pasal dalam UU PDP, institusi perbankan dapat mengidentifikasi kesesuaian, celah dan tumpang tindih antara standar internasional dan regulasi nasional. Pendekatan ini tidak hanya membantu memastikan bahwa aspek teknis dan operasional pengamanan data telah terpenuhi tetapi juga memperkuat aspek kepatuhan hukum, akuntabilitas dan perlindungan hak subjek data. Berikut ini adalah mapping antara UU PDP dengan ISO 27001 dan ISO 27701.

a. Hak Subjek Data

Bagian ini menjelaskan keterkaitan antara pasal-pasal dalam UU PDP dengan *clause* dan *control* pada ISO 27001 dan ISO 27701. Tujuannya adalah untuk menunjukkan bagaimana standar ISO dapat digunakan sebagai kerangka dalam melindungi hak-hak individu terkait data pribadinya. Berikut adalah penjelasan dari *mapping* dari UU PDP dengan ISO terkait Hak Subjek Data yang dijelaskan pada Tabel 4. 1 Mapping UU PDP dengan ISO terkait Hak Subjek Data.

Tabel 4. 1 Mapping UU PDP dengan ISO terkait Hak Subjek Data

Hak Subjek Data			
UU PDP	ISO 27001	ISO 27701	Justifikasi
Pasal 5: Hak untuk mendapatkan informasi	*A.18.1.4 (Privacy and protection of personally identifiable information)*	*A.7.3.3 (Providing information to PII principals)*	Hak ini memastikan kewajiban pengendali data untuk memberikan informasi kepada subjek data mengenai penggunaan data pribadinya secara transparan. ISO 27001 dan 27701 mendukung

			prinsip ini dengan mekanisme perlindungan dan penyediaan akses terhadap informasi pribadi.
Pasal 6: Hak untuk memperbaiki dan melengkapi data	*A.18.1.4 (Privacy and protection of personally identifiable information)*	*A.7.3.6 (Access, correction and/or erasure)*	Hak ini memastikan bahwa subjek data dapat memperbarui atau mengoreksi data yang tidak salah. ISO 27701 menegaskan hal ini melalui kontrol yang memungkinkan individu meminta perbaikan atau penghapusan data yang salah.
Pasal 7: Hak untuk mendapatkan akses dan salinan data	*A.9.2.5 (Review of user access rights),* *A.9.4.1 (Information access restriction)*	*A.7.3.5 (Providing mechanism to object to PII processing)*	Hak ini memastikan agar subjek data dapat memeriksa bagaimana datanya digunakan. ISO mendukung hal ini dengan pengendalian akses dan mekanisme keberatan atas pemrosesan data.
Pasal 8: Hak untuk mengakhiri pemrosesan dan menghapus data	*A.8.3.2 (Disposal of media)*	*A.7.3.6 (Access, correction and/or erasure),* *A.7.4.8 (Disposal)*	Hak ini memastikan bahwa subjek data untuk menghentikan pemrosesan dan meminta penghapusan data. ISO mengatur prosedur penghapusan data secara aman untuk mencegah penyalahgunaan data.
Pasal 9: Hak untuk menarik kembali persetujuan	*A.18.1.4 (Privacy and protection of personally identifiable information)*	*A.7.3.4 (Providing mechanism to modify or withdraw consent)*	Hak ini memastikan bahwa subjek data dapat mencabut persetujuan penggunaan data pribadi. ISO 27701 mengatur mekanisme untuk mengelola perubahan atau penarikan persetujuan secara transparan dan terdokumentasi.
Pasal 10: Hak untuk mengajukan keberatan atas	*A.18.1.4 (Privacy and protection of personally identifiable information)*	*A.7.3.4 (Providing mechanism to modify or withdraw consent)*	Hak ini memastikan bahwa subjek data dapat untuk menolak pemrosesan otomatis, termasuk pemrofilan. ISO 27001 memastikan perlindungan terhadap data yang dapat diidentifikasi sementara ISO

pemrosesan otomatis/pemrofilan			27701 menyediakan mekanisme bagi subjek data untuk menolak atau menarik kembali persetujuan atas pemrosesan otomatis.
Pasal 11: Hak untuk menunda atau membatasi pemrosesan data	*A.18.1.4 (Privacy and protection of personally identifiable information)*	*A.7.3.4 (Providing mechanism to modify or withdraw consent)*	Hak ini memastikan bahwa subjek data dapat meminta penghentian sementara atau pembatasan pemrosesan data pribadinya. ISO 27701 menyediakan mekanisme yang memungkinkan perubahan atau pencabutan persetujuan bagi subjek data jika merasa data mereka digunakan melampaui tujuan awal pengumpulan.
Pasal 12: Hak untuk menggugat dan menerima ganti rugi	*A.16.1.1 (Responsibilities and procedures)*	*Clause 6.13.1.1 (Responsibilities and procedures)*	Hak ini memastikan bahwa subjek data dapat mengajukan gugatan dan memperoleh kompensasi apabila terjadi pelanggaran terhadap data pribadinya. ISO menekankan pentingnya tanggung jawab organisasi dan prosedur yang jelas untuk menangani insiden pelanggaran, termasuk investigasi, pelaporan dan penyelesaian masalah secara transparan.
Pasal 13: Hak atas portabilitas data	*A.13.2.1 (Information transfer policies and procedures)*	*A.7.5 (PII sharing, transfer and disclosure)*	Hak ini memastikan bahwa subjek data dapat memperoleh kendali atas data pribadinya. ISO 27001 mengatur kebijakan transfer data yang aman sedangkan ISO 27701 menetapkan prosedur untuk berbagi dan pengungkapan *Personally Identifiable Information* (PII) untuk memastikan bahwa perpindahan data dilakukan tanpa melanggar hak privasi subjek data.

b. Pemrosesan Data

Bagian ini menjelaskan keterkaitan antara pasal-pasal dalam UU PDP dengan *clause* dan *control* pada ISO 27001 dan ISO 27701. Tujuannya adalah untuk mengatur pengelolaan dan pemrosesan data pribadi. Berikut adalah penjelasan dari *mapping* dari UU PDP dengan ISO terkait Pemrosesan Data yang dijelaskan pada Tabel 4. 2 Mapping UU PDP dengan ISO terkait Pemrosesan Data.

Tabel 4. 2 Mapping UU PDP dengan ISO terkait Pemrosesan Data

Pemrosesan Data			
UU PDP	ISO 27001	ISO 27701	Penjelasan
Pasal 16: Definisi dari siklus hidup data dari pengumpulan sampai pemusnahan	*Clause 4 (Context of the organization), A.8 (Asset management), A.18.1.4 (Privacy and protection of personally identifiable information)*	*Clause 7.2 (Conditions for collection and processing), Clause 7.4 (Privacy by design and privacy by default)*	Pasal ini mendefinisikan seluruh siklus hidup data pribadi, mulai dari pengumpulan, penyimpanan, pemrosesan sampai pemusnahannya. ISO 27001 menetapkan konteks organisasi, klasifikasi aset dan perlindungan data pribadi dalam setiap tahapan. Sementara ISO 27701 menegaskan pentingnya penerapan prinsip *privacy by design dan privacy by default* untuk memastikan bahwa perlindungan data ada sejak tahap perancangan sistem sampai pemusnahan data.
Pasal 17: Mengatur pemasangan alat pemroses data visual di tempat umum	*A.11 (Physical and environmental security)*	*A.7.3.3 (Providing information to PII principals)*	Pasal ini mendefinisikan tanggung jawab organisasi dalam melindungi privasi individu di area publik melalui pengawasan visual seperti *CCTV*.

Pasal 18: Mengatur kondisi jika ada dua atau lebih pengendali data yang memproses data bersama	*A.15 (Supplier relationships), A.15.1.2 (Addressing security within supplier agreements)*	*A.7.2.7 (Joint PII controller)*	Pasal ini mendefinisikan pentingnya kejelasan tanggung jawab antar pihak yang bersama-sama memproses data pribadi. ISO 27001 menekankan keamanan dalam hubungan dengan pihak ketiga melalui perjanjian kerja sama yang mengatur peran, tanggung jawab dan kewajiban keamanan informasi. Sementara ISO 27701 memperkuat hal ini dengan kewajiban adanya kontrak antara pengendali dan pemroses data (*PII processors*).

c. Kewajiban Pengendali & Prosesor

Bagian ini menjelaskan keterkaitan antara kewajiban hukum pengendali dan prosesor data pribadi yang diatur dalam UU PDP dengan *clause* pengendalian dari ISO 27001 dan ISO 27701. Tujuannya adalah menunjukkan bagaimana organisasi dapat membangun sistem manajemen keamanan dan privasi yang sesuai dengan prinsip *accountability, transparency* dan *lawful processing*. Berikut adalah penjelasan dari *mapping* dari UU PDP dengan ISO terkait Kewajiban Pengendali dan Prosesor yang dijelaskan pada Tabel 4. 3 Mapping UU PDP dengan ISO terkait Kewajiban Pengendali dan Prosesor.

Tabel 4. 3 Mapping UU PDP dengan ISO terkait Kewajiban Pengendali dan Prosesor

Kewajiban Pengendali dan Prosesor			
UU PDP	ISO 27001	ISO 27701	Penjelasan
Pasal 20: Pengendali data wajib memiliki dasar hukum untuk memproses data	*A.18.1.4 (Privacy and protection of personally identifiable information)*	*A.7.2.2 (Identify lawful basis)*	Pasal ini menjelaskan bahwa setiap kegiatan pemrosesan data harus memiliki dasar hukum yang jelas. ISO mendukung kewajiban pengendali untuk mendokumentasikan tujuan pemrosesan agar sesuai dengan prinsip *lawfulness* dan *purpose limitation*
Pasal 21: Pada saat meminta persetujuan, pengendali data wajib memberikan informasi yang jelas tentang legalitas, tujuan, jenis	*A.18.1.4 (Privacy and protection of personally identifiable information)*	*A.7.3.2 (Determining information for PII principals), A.7.3.3 (Providing information to PII principals)*	Pasal ini menjelaskan bahwa pengendali harus memastikan bahwa subjek data memahami seluruh aspek pemrosesan. ISO mendukung ketentuan ini dengan mewajibkan organisasi memberikan informasi yang sesuai kepada subjek data mengenai tujuan, dasar hukum dan masa retensi data.

data, masa retensi dan hak subjek data			
Pasal 22 - 24: Mengatur bahwa persetujuan harus tertulis atau terekam, disajikan dengan bahasa sederhana dan jelas dan pengendali data wajib bisa menunjukkan bukti persetujuan tersebut	*A.18.1.4 (Privacy and protection of personally identifiable information)*	*A.7.2.3 (Determine when and how consent is to be obtained), A.7.2.4 (Obtain and record consent)*	Pasal ini menjelaskan bahwa bentuk persetujuan harus eksplisit dan terdokumentasi. ISO mendukung ketentuan ini melalui penerapan *Privacy Impact Assessment* (PIA) untuk memastikan proses pengumpulan persetujuan memenuhi prinsip keterbukaan.
Pasal 25 - 26: Aturan khusus untuk pemrosesan data anak (wajib ada persetujuan orang tua/wali) dan penyandang disabilitas	*A.18.1.4 (Privacy and protection of personally identifiable information)*	*A.7.2.2 (Identify lawful basis)*	Pasal ini menjelaskan bahwa data pribadi kelompok rentan seperti anak-anak atau penyandang disabilitas memerlukan perlindungan khusus. ISO mengatur hal ini dengan menekankan perlunya identifikasi dasar hukum spesifik sebelum memproses data kategori sensitif.
Pasal 27 - 29: Kewajiban untuk memproses data secara terbatas, sesuai tujuan dan memastikan akurasinya	*A.8.2.2 (Labelling of information), A.8.1.3 (Acceptable use of assets)*	*A.7.4.2 (Limit processing), A.7.4.3 (Accuracy and quality), A.7.4.4 (PII minimization objectives)*	Pasal ini menjelaskan bahwa pengendali data wajib memastikan data yang diproses akurat, relevan dan terbatas pada tujuan yang telah ditentukan. ISO mendukung prinsip ini melalui penerapan *data minimization* dan *accuracy control.*

Pasal 30: Kewajiban memperbarui / memperbaiki data yang tidak akurat paling lambat 3x24 jam setelah menerima permintaan	*A.12.1.2 (Change management), A.18.1.3 (Protection of records)*	*A.7.3.6 (Access, correction and/or erasure)*	Pasal ini menjelaskan bahwa organisasi wajib memberikan hak koreksi bagi subjek data secara cepat. ISO 27701 menegaskan mekanisme koreksi sedangkan ISO 27001 memastikan perubahan tersebut terdokumentasi dalam sistem yang aman.
Pasal 31: Kewajiban merekam seluruh kegiatan pemrosesan data	*A.12.4.1 (Event logging), A.12.4.3 (Administrator and operator logs)*	*A.7.2.8 (Records related to processing PII)*	Pasal ini menjelaskan bahwa setiap aktivitas pemrosesan data harus dapat dilacak dan diaudit. ISO 27001 mewajibkan pencatatan (*logging*) aktivitas keamanan sedangkan ISO 27701 memperluas cakupannya pada pencatatan seluruh proses pemrosesan data pribadi.
Pasal 32: Kewajiban memberikan akses kepada subjek data atas data mereka paling lambat 3x24 jam setelah menerima permintaan	*A.9 (Access control)*	*A.7.3.6 (Access, correction and/or erasure), A.7.3.8 (Providing copy of PII processed)*	Pasal ini menjelaskan bahwa subjek data memiliki hak penuh untuk mengakses data pribadinya. ISO 27701 mendukung hal ini dengan menyediakan mekanisme permintaan akses sementara ISO 27001 memastikan keamanan proses tersebut.
Pasal 33: Kewajiban menolak memberikan akses perubahan terhadap	*A.9.4.1 (Information access restriction)*	*A.7.3.9 (Handling requests)*	Pasal ini menjelaskan bahwa pengendali dapat menolak permintaan perubahan data jika bertentangan dengan hukum atau tujuan pengumpulan. ISO mendukung kontrol akses ketat untuk mencegah manipulasi data tanpa izin.

data pribadi kepada subjek data pribadi			
Pasal 34: Kewajiban melakukan penilaian dampak pelindungan data (DPIA) untuk pemrosesan berisiko tinggi	*Clause 6.1.2 (Information security risk assessment)*	*A.7.2.5 (Privacy impact assessment)*	Pasal ini menjelaskan bahwa setiap kegiatan pemrosesan yang berisiko tinggi terhadap privasi wajib dilakukan penilaian dampak. ISO mengintegrasikan hal ini melalui *privacy risk assessment*.
Pasal 35: Kewajiban melindungi dan memastikan keamanan data dengan langkah teknis operasional dan penentuan tingkat keamanan berdasarkan risiko	*A.9 (Access control), A.10 (Cryptography), A.12 (Operations security)*	*Clause 6.2 (Information security policies)*	Pasal ini menjelaskan bahwa perlindungan wajib diterapkan secara menyeluruh. ISO menekankan kontrol akses, enkripsi dan kebijakan keamanan.
Pasal 36: Kewajiban menjaga kerahasiaan data pribadi	*A.13.2.4 (Confidentiality or non-disclosure agreements)*	*Clause 6.10.2.4 (Confidentiality or non-disclosure agreements)*	Pasal ini menjelaskan bahwa pengendali dan prosesor wajib menjamin kerahasiaan data pribadi serta mencegah penyebaran informasi kepada pihak yang tidak berwenang. ISO mendukung hal ini melalui penerapan perjanjian kerahasiaan.

Pasal 37: Kewajiban melakukan pengawasan terhadap semua pihak yang terlibat dalam pemrosesan di bawah kendalinya	*A.15.2.1 (Monitoring and review of supplier services)*	*A.7.2.6 (Contracts with PII processors)*	Pasal ini menjelaskan bahwa setiap pihak ketiga yang terlibat dalam pemrosesan harus tunduk pada pengawasan dan evaluasi secara berkala. ISO mengharuskan perjanjian formal yang mendefinisikan peran, tanggung jawab dan mekanisme audit.
Pasal 38 – 39: Kewajiban melindungi data dari pemrosesan tidak sah dan mencegah akses tidak sah, salah satunya dengan sistem elektronik yang andal dan aman	*A.9 (Access control), A.12 (Operations security), A.14 (System acquisition, development and maintenance)*	*Clause 7.4 (Privacy by design and privacy by default)*	Pasal ini menjelaskan bahwa sistem elektronik yang digunakan untuk memproses data harus andal dan aman dari akses ilegal. ISO mengatur kontrol akses dan pengamanan operasional keamanan dalam siklus pengembangan sistem.
Pasal 40: Kewajiban menghentikan pemrosesan paling lambat 3x24 jam jika subjek data menarik persetujuannya	*A.9.4.1 (Information access restriction)*	*A.7.3.4 (Providing mechanism to modify or withdraw consent)*	Pasal ini menjelaskan bahwa pengendali data wajib menghentikan seluruh aktivitas pemrosesan data pribadi dalam waktu paling lama 3x24 jam setelah subjek data mencabut persetujuannya. ISO 27701 mendukung hal ini melalui penyediaan mekanisme untuk modifikasi atau pencabutan persetujuan sementara ISO 27001 mengatur pembatasan akses agar data tidak lagi diproses setelah pencabutan terjadi.

Pasal 41: Kewajiban melakukan penundaan dan pembatasan pemrosesan baik sebagian maupun seluruhnya paling lambat 3x24	*A.9.4.1 (Information access restriction)*	*A.7.3.4 (Providing mechanism to modify or withdraw consent), A.7.3.5 (Providing mechanism to object to PII processing)*	Pasal ini menjelaskan bahwa pengendali data wajib menghormati hak subjek data untuk membatasi atau menunda pemrosesan data pribadinya. ISO 27701 menyediakan mekanisme keberatan (*objection mechanism*) terhadap pemrosesan sedangkan ISO 27001 memastikan pembatasan akses diterapkan segera setelah permintaan diajukan.
Pasal 42 – 45: Kewajiban untuk mengakhiri pemrosesan, menghapus atau memusnahkan data jika tujuan sudah tercapai, masa retensi berakhir atau ada permintaan dan memberitahukannya kepada subjek data	*A.8.3.2 (Disposal of media), A.11.2.7 (Secure disposal or reuse of equipment)*	*A.7.4.5 (PII de-identification and deletion at the end of processing), A.7.4.7 (Retention), A.7.4.8 (Disposal)*	Pasal ini menjelaskan bahwa pengendali harus mengakhiri pemrosesan dan menghapus data pribadi ketika tujuan pemrosesan telah tercapai, masa retensi berakhir atau atas permintaan subjek data. ISO 27701 mengatur mekanisme penghapusan dan de-identification data pribadi untuk menjamin tidak ada informasi yang tersisa sementara ISO 27001 memastikan penghapusan dilakukan dengan aman, baik pada media fisik maupun digital.
Pasal 46: Jika terjadi kegagalan pelindungan data (*data breach*), wajib memberitahukan secara	*A.16.1.5 (Response to information security incidents)*	*Clause 6.13.1.1 (Responsibilities and procedures),*	Pasal ini menjelaskan bahwa setiap pelanggaran data wajib dilaporkan kepada otoritas yang berwajib dan subjek data secara cepat. ISO menegaskan pentingnya sistem pelaporan dan respon

tertulis kepada subjek data dan lembaga paling lambat 3x24 jam		*Clause 6.13.1.5 (Response to information security incidents)*	insiden yang terintegrasi untuk menjaga transparansi dan mitigasi risiko jika terjadi kebocoran data.
Pasal 47: Pengendali data wajib bertanggung jawab dan mampu menunjukkan pertanggungjawabannya atas seluruh pemrosesan data	*Clause 5 (Leadership), Clause 9 (Performance evaluation)*	*Clause 5.3 (Leadership), Clause 7.2.8 (Records related to processing PII)*	Pasal ini menjelaskan bahwa tanggung jawab atas seluruh kegiatan pemrosesan berada pada pimpinan organisasi. ISO menegaskan peran manajemen dalam memastikan efektivitas sistem keamanan dan kepatuhan terhadap regulasi.
Pasal 51: Prosesor data wajib memproses data hanya berdasarkan perintah dari pengendali data. Jika melanggar, tanggung jawab beralih ke Prosesor.	*A.15 (Supplier relationships)*	*Clause 7.2.6 (Contracts with PII processors)*	Pasal ini menjelaskan bahwa prosesor data hanya dapat memproses data berdasarkan instruksi dari pengendali data. ISO mengharuskan adanya kontrak yang menetapkan tanggung jawab dan kewenangan prosesor secara tegas.
Pasal 53: Kewajiban menunjuk seorang DPO jika melakukan pemrosesan untuk pelayanan publik,	*A.6.1.1 (Information security roles and responsibilities)*	*Clause 6.3.1.2 (Segregation of duties)*	Pasal ini menjelaskan bahwa organisasi yang memproses data pribadi dalam skala besar, baik untuk kepentingan publik maupun kegiatan bersifat sistematis, wajib menunjuk seorang pejabat perlindungan data atau *Data Protection Officer* (DPO). ISO 27001 mengatur bahwa setiap organisasi harus memiliki

memantau data skala besar secara sistematis / memproses data spesifik / skala besar			peran dan tanggung jawab keamanan informasi yang jelas sementara ISO 27701 menegaskan pemisahan fungsi (*segregation of duties*) untuk memastikan independensi DPO.
Pasal 54: Tugas DPO meliputi pemberian saran, pemantauan dan koordinasi terkait pemrosesan data	*A.6.1.1 (Information security roles and responsibilities)*	*Clause 6.3.1.2 (Segregation of duties)*	Pasal ini menjelaskan bahwa DPO bertanggung jawab memberikan masukan strategis kepada manajemen, melakukan pengawasan atas kegiatan pemrosesan data dan memastikan koordinasi antar divisi terkait kebijakan privasi dan keamanan data. ISO 27001 menekankan pentingnya definisi tanggung jawab dan pelaporan yang jelas untuk setiap peran keamanan sedangkan ISO 27701 menegaskan pentingnya pemisahan peran agar DPO dapat bekerja secara independen.

d. Transfer Data & Sanksi

Bagian ini menjelaskan hubungan antara ketentuan transfer data pribadi dan sanksi hukum dalam UU PDP dengan ISO 27001 dan ISO 27701. Fokusnya adalah bagaimana kedua standar ini mengatur keamanan dan akuntabilitas dalam transfer lintas negara, penegakan kepatuhan dan respon terhadap pelanggaran keamanan data. Berikut adalah penjelasan dari *mapping* dari UU PDP dengan ISO terkait Transfer Data dan Sanksi yang dijelaskan pada Tabel 4. 4 Mapping UU PDP dengan ISO terkait Transfer Data dan Sanksi.

Tabel 4. 4 Mapping UU PDP dengan ISO terkait Transfer Data dan Sanksi

Transfer Data dan Sanksi			
UU PDP	ISO 27001	ISO 27701	Penjelasan
Pasal 55 – 56: Aturan mengenai transfer data, baik di dalam maupun ke luar wilayah Indonesia, termasuk syarat tingkat pelindungan yang setara atau lebih tinggi	*A.13.2 (Information transfer), A.13.2.1 (Information transfer policies and procedures), A.13.2.2 (Agreements on information transfer)*	*Clause 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)*	Pasal ini memastikan bahwa setiap transfer data pribadi antar subjek data atau lintas negara dilakukan dengan jaminan perlindungan yang setara. ISO 27001 menekankan perlunya kebijakan dan perjanjian formal dalam transfer data sedangkan ISO 27701 menambahkan dimensi privasi dengan keharusan mengidentifikasi dasar hukum, negara tujuan dan tingkat perlindungan yang berlaku di negara penerima.

Pasal 57: Jenis-jenis sanksi administratif, mulai dari peringatan tertulis hingga denda maksimal 2% dari pendapatan tahunan	*A.18.1 (Compliance with legal and contractual requirements), A.16.1.5 (Response to information security incidents)*	*Clause 6.13.1.1 (Responsibilities and procedures), Clause 6.15.1.1 (Identification of applicable legislation and contractual requirements)*	Pasal ini menjelaskan terkait sanksi jika organisasi melanggar regulasi. ISO 27001 menegaskan kepatuhan terhadap regulasi dan kontrak sebagai bagian dari tanggung jawab keamanan informasi sedangkan ISO 27701 memperluas cakupan dengan memasukkan identifikasi peraturan privasi dan kewajiban hukum yang berlaku.
Pasal 65 – 66: Larangan spesifik seperti memperoleh atau menggunakan data pribadi secara melawan hukum	*A.9.1.1 (Access control policy), A.5.1.1 (Policies for information security)*	*A.7.2.1 (Identify and document purpose), A.7.2.2 (Identify lawful basis)*	Pasal ini menjelaskan terkait pelarangan pengumpulan dan penggunaan data tanpa dasar hukum yang sah. ISO 27001 mengatur kontrol akses dan kebijakan keamanan sementara ISO 27701 menegaskan keharusan mendokumentasikan tujuan dan dasar hukum pemrosesan sebelum data digunakan.
Pasal 67 – 73: Ketentuan pidana, termasuk denda dan hukuman penjara untuk pelanggaran berat	*A.18.1.1 (Identification of applicable legislation and contractual requirements), A.16.1.7 (Collection of evidence)*	*A.7.2.5 (Privacy impact assessment), Clause 6.13.1.5 (Response to information security incidents)*	Pasal ini mengatur konsekuensi hukum bagi pelanggaran serius terkait data pribadi. ISO 27001 mengatur kewajiban dokumentasi hukum dan pengumpulan bukti dalam investigasi insiden keamanan sementara ISO 27701 menambahkan analisis *Privacy Impact Assessment* dan mekanisme respon cepat terhadap insiden data.

4.2.2 Mapping ISO 27001 & ISO 27701 Terhadap POJK

Mapping antara ISO 27001 dan ISO 27701 dengan Peraturan OJK No. 6 Tahun 2022 dilakukan untuk menilai sejauh mana penerapan *Information Security Management System* (ISMS) dan *Privacy Information Management System* (PIMS) mendukung kepatuhan organisasi terhadap ketentuan regulasi yang berlaku. Berikut ini adalah *mapping* antara Peraturan OJK No. 6 Tahun 2022 dengan ISO 27001 dan ISO 27701.

a. Perlindungan Konsumen

Bagian ini menjelaskan terkait tanggung jawab lembaga jasa keuangan dalam memastikan perlindungan terhadap hak-hak konsumen, terutama yang berhubungan dengan keamanan dan privasi data pribadi. Regulasi ini menekankan pentingnya transparansi, akurasi informasi dan persetujuan eksplisit sebelum pemrosesan data dilakukan. Berikut adalah penjelasan dari *mapping* dari POJK dengan ISO terkait Perlindungan Konsumen yang dijelaskan pada Tabel 4. 5 Mapping POJK dengan ISO terkait Perlindungan Konsumen.

Tabel 4. 5 Mapping POJK dengan ISO terkait Perlindungan Konsumen

Perlindungan Konsumen			
POJK	ISO 27001	ISO 27701	Penjelasan
Pasal 11: Memberikan data/informasi pribadi konsumen ke pihak lain tanpa persetujuan dan menggunakan data pribadi konsumen yang sudah putus hubungan atau calon konsumen yang ditolak/menarik permohonan	*A.13.2.1 (Information transfer policies and procedures),* *A.8.3.2 (Disposal of media)*	*A.7.2.2 (Identify lawful basis), A.7.2.4 (Obtain and record consent),* *A.7.4.8 (Disposal)*	Pasal ini menjelaskan bahwa lembaga keuangan dilarang memberikan data pribadi konsumen kepada pihak ketiga tanpa dasar hukum atau persetujuan eksplisit. ISO 27701 mendukung prinsip ini melalui kewajiban identifikasi dasar hukum dan mekanisme pencatatan persetujuan sedangkan ISO 27001 memastikan keamanan data yang sudah tidak relevan dengan kebijakan penghapusan yang terkontrol.

Pasal 12 – 15: Kewajiban merancang dan menguji produk agar sesuai dan tidak merugikan target Konsumen	*Clause 6.1.2 (Information security risk assessment), A.14.2.1 (Secure development policy)*	*Clause 7.4 (Privacy by design and privacy by default), A7.2.5 (Privacy impact assessment)*	Pasal ini menjelaskan bahwa lembaga keuangan harus memastikan sistemnya dirancang untuk menjamin keamanan dan privasi data pribadi. ISO 27701 mengatur penerapan *privacy by design* sedangkan ISO 27001 menekankan analisis risiko dan pengendalian keamanan untuk melindungi data konsumen secara menyeluruh.
Pasal 16 – 17: Kewajiban menyediakan informasi produk yang jelas, akurat, tidak menyesatkan dan dalam bentuk ringkasan informasi	*A.18.1.4 (Privacy and protection of personally identifiable information)*	*A.7.3.2 (Determining information for PII principals), A.7.3.3 (Providing information to PII principals)*	Pasal ini menjelaskan bahwa lembaga keuangan wajib menyampaikan informasi yang akurat dan transparan kepada konsumen. ISO 27701 memastikan individu menerima informasi yang cukup tentang penggunaan datanya sedangkan ISO 27001 mengatur perlindungan atas data pribadi yang diproses.
Pasal 18 – 19: Mengatur waktu dan cara penyampaian informasi serta ringkasan produk kepada calon konsumen	*A.18.1.1 (Identification of applicable legislation and contractual requirements)*	*A.7.3.2 (Determining information for PII principals), A.7.3.3 (Providing information to PII principals)*	Pasal ini menjelaskan bahwa penyampaian informasi harus dilakukan secara tepat waktu, sesuai peraturan dan mudah dipahami. ISO 27701 menegaskan hak subjek data untuk memperoleh informasi terkait pengunaan datanya sedangkan ISO 27001 memastikan proses komunikasi dilakukan sesuai ketentuan hukum.
Pasal 21: Wajib mencantumkan pernyataan	*A.18.1.1 (Identification of applicable legislation and*	*A.6.15.1.1 (Identification of applicable legislation*	Pasal ini menjelaskan bahwa lembaga keuangan wajib menampilkan pernyataan pengawasan otoritas untuk

"Berizin dan diawasi oleh Otoritas Jasa Keuangan" dalam setiap iklan atau promosi	*contractual requirements)*	*and contractual requirements)*	menjamin transparansi dan kepercayaan publik. ISO mendukungnya melalui identifikasi dan kepatuhan terhadap persyaratan hukum.
Pasal 25: Dilarang melakukan penawaran melalui sarana komunikasi pribadi (telepon, SMS, WA, dll.), tanpa persetujuan calon konsumen. Jika ada persetujuan, penawaran hanya boleh dilakukan Senin-Sabtu jam 08:00-18:00 waktu setempat	*A.18.1.4 (Privacy and protection of personally identifiable information)*	*A.7.2.4 (Obtain and record consent),* *A.7.3.5 (Providing mechanism to object to PII processing),* *B.8.2.3 (Marketing and advertising use)*	Pasal ini menjelaskan bahwa lembaga keuangan dilarang menghubungi calon konsumen melalui sarana pribadi tanpa izin. ISO 27701 mengatur mekanisme persetujuan dan keberatan untuk pemrosesan data dalam konteks pemasaran sedangkan ISO 27001 menegaskan perlindungan atas data pribadi dalam komunikasi elektronik.
Pasal 29: Wajib melakukan konfirmasi pemahaman Konsumen atas isi perjanjian sebelum tanda tangan	*A.18.1.4 (Privacy and protection of personally identifiable information)*	*A.7.2.4 (Obtain and record consent),* *A.7.3.3 (Providing information to PII principals)*	Pasal ini menjelaskan bahwa lembaga keuangan wajib memastikan konsumen memahami isi perjanjian secara utuh sebelum menyetujuinya. ISO 27701 mendukung prinsip *informed consent* sementara ISO 27001 memastikan data yang dikumpulkan selama proses terlindungi dari manipulasi dan penyalahgunaan.
Pasal 30: Dilarang mencantumkan klausula	*A.18.1.1 (Identification of applicable legislation and*	*A.7.2.6 (Contracts with PII processors),*	Pasal ini menjelaskan bahwa lembaga keuangan dilarang melepas tanggung jawab hukum terhadap

eksonerasi (pengalihan tanggung jawab) dalam perjanjian baku	*contractual requirements)*	*A.7.2.7 (Joint PII controller)*	keamanan data konsumen melalui perjanjian. ISO 27701 memperkuatnya melalui ketentuan hubungan antara pengendali dan pemroses data sementara ISO 27001 memastikan kepatuhan hukum dalam kontrak bisnis.
Pasal 31 – 32: Kewajiban memberitahukan dan mendapatkan konfirmasi dari konsumen jika ada perubahan ketentuan dalam perjanjian	*A.12.1.2 (Change management)*	*A7.3.2 (Determining information for PII principals),* *A.7.3.4 (Providing mechanism to modify or withdraw consent)*	Pasal ini menjelaskan bahwa setiap perubahan ketentuan harus disampaikan dan dikonfirmasi oleh konsumen. ISO 27701 menjamin hak individu untuk menarik atau memperbarui persetujuan sedangkan ISO 27001 mengatur manajemen perubahan untuk memastikan integritas sistem informasi.
Pasal 35: Wajib memberikan akses yang setara dan mendukung layanan khusus untuk konsumen penyandang disabilitas dan lanjut usia	*A.18.1.1 (Identification of applicable legislation and contractual requirements)*	*A.7.3.3 (Providing information to PII principals)*	Pasal ini menjelaskan bahwa lembaga keuangan wajib memastikan layanan dapat diakses oleh seluruh konsumen tanpa diskriminasi. ISO 27701 menekankan prinsip keadilan dalam akses informasi sedangkan ISO 27001 mengatur kepatuhan terhadap ketentuan hukum terkait layanan.
Pasal 36: Wajib menjaga keamanan dana dan/atau aset konsumen	*Clause 4 (Context of the organization),*	*Clause 5.1 (General)*	Pasal ini menjelaskan bahwa lembaga keuangan wajib menjaga keamanan aset finansial dan data konsumen melalui penerapan manajemen risiko. ISO 27001 memberikan panduan untuk penilaian risiko keamanan

	Clause 6.1.2 (Information security risk assessment)		sedangkan ISO 27701 menegaskan tanggung jawab organisasi dalam menjaga integritas dan kepercayaan data pribadi.
Pasal 37 – 38: Wajib memberikan laporan posisi saldo/mutasi secara akurat dan tepat waktu	*A.12.4.1 (Event logging), A.18.1.3 (Protection of records)*	*A.7.4.3 (Accuracy and quality),* *A.7.3.8 (Providing copy of PII processed)*	Pasal ini menjelaskan bahwa lembaga keuangan wajib memberikan informasi transaksi secara akurat, lengkap dan tepat waktu. ISO 27701 menjamin akurasi serta hak konsumen untuk memperoleh salinan data pribadinya sedangkan ISO 27001 memastikan pencatatan dan perlindungan data transaksi melalui kontrol audit yang terdokumentasi.
Pasal 39: Wajib melaksanakan instruksi konsumen sesuai perjanjian	*A.18.1.1 (Identification of applicable legislation and contractual requirements),* ***A.12.1.1*** *(Documented operating procedures)*	*A.7.3.9 (Handling requests)*	Pasal ini menjelaskan bahwa lembaga keuangan wajib melaksanakan instruksi konsumen sesuai ketentuan kontrak. ISO 27701 mengatur mekanisme penanganan permintaan dari individu terkait data pribadinya sedangkan ISO 27001 memastikan adanya prosedur yang terdokumentasi.

b. Penanganan Sengketa & Pelaporan

Bagian ini menjelaskan terkait mekanisme penyelesaian sengketa dan kewajiban pelaporan dalam kerangka perlindungan konsumen. Ketentuan ini memastikan bahwa konsumen memiliki akses terhadap proses pengaduan yang adil, transparan, tanpa biaya tambahan dan menjamin hak untuk melanjutkan penyelesaian melalui lembaga mediasi atau pengadilan apabila tidak tercapai kesepakatan. Berikut adalah penjelasan dari *mapping* dari POJK dengan ISO terkait Penanganan Sengketa & Pelaporan yang dijelaskan pada Tabel 4. 6 Mapping POJK dengan ISO terkait Penanganan Sengketa & Pelaporan.

Tabel 4. 6 Mapping POJK dengan ISO terkait Penanganan Sengketa & Pelaporan

Penanganan Sengketa & Pelaporan			
POJK	ISO 27001	ISO 27701	Penjelasan
Pasal 41: Layanan pengaduan oleh POJK tidak boleh dikenakan biaya	*A.18.1.1 (Identification of applicable legislation and contractual requirements)*	*A.7.3.9 (Handling requests)*	Pasal ini menjelaskan bahwa setiap layanan pengaduan yang disediakan oleh lembaga jasa keuangan di bawah POJK harus diberikan secara gratis kepada konsumen. ISO 27701 mendukung prinsip ini melalui pengaturan tentang penanganan permintaan atau keluhan dari subjek data tanpa dikenai biaya sementara ISO 27001 memastikan adanya identifikasi dan kepatuhan terhadap kewajiban hukum yang berlaku.

Pasal 42: Jika pengaduan tidak mencapai kesepakatan, konsumen dapat melanjutkan penyelesaian sengketa melalui LAPS Sektor Jasa Keuangan atau pengadilan	*A.18.1.1 (Identification of applicable legislation and contractual requirements)*	*A.7.3.1 (Determining and fulfilling obligations to PII principals)*	Pasal ini menjelaskan bahwa jika proses pengaduan internal tidak mencapai kesepakatan, konsumen berhak melanjutkan penyelesaian melalui lembaga alternatif atau jalur hukum. ISO 27701 menegaskan tanggung jawab organisasi untuk memenuhi kewajiban terhadap subjek data yang datanya diproses sementara ISO 27001 memastikan seluruh proses tunduk pada peraturan hukum yang berlaku.
Pasal 43: Wajib melakukan penilaian sendiri (*self assessment*) terhadap pemenuhan ketentuan POJK ini dan melaporkannya ke OJK setiap tahun	*Clause 9.1 (Monitoring, measurement, analysis and evaluation),* *9.2 (Internal audit)*	*Clause 5.7.1 (Monitoring, measurement, analysis and evaluation),* *Clause 5.7.2 (Internal audit)*	Pasal ini menjelaskan bahwa lembaga wajib melakukan evaluasi internal untuk memastikan kepatuhan terhadap ketentuan perlindungan konsumen. ISO mendukung hal ini melalui mekanisme audit internal secara berkala.

c. Sanksi

Bagian ini menjelaskan terkait penerapan sanksi terhadap pelanggaran ketentuan perlindungan konsumen dan kewajiban lembaga jasa keuangan dalam menjaga integritas sistem pengelolaan data pribadi. Ketentuan ini mengatur bahwa lembaga keuangan harus memiliki unit khusus perlindungan konsumen dan memastikan keterlibatan pimpinan dan dewan pengawas dalam pelaksanaan dan pengawasan kepatuhan. Berikut adalah penjelasan dari *mapping* dari POJK dengan ISO terkait Sanksi yang dijelaskan pada Tabel 4. 7 Mapping POJK dengan ISO terkait Sanksi.

Tabel 4. 7 Mapping POJK dengan ISO terkait Sanksi

Sanksi			
POJK	ISO 27001	ISO 27701	Penjelasan
Pasal 46: Wajib memiliki fungsi atau unit untuk pelaksanaan perlindungan konsumen	*A.6.1.1 (Information security roles and responsibilities)*	*Clause 6.3.1.1 (Information security roles and responsibilities)*	Pasal ini menjelaskan bahwa setiap lembaga jasa keuangan wajib membentuk unit atau fungsi khusus yang bertanggung jawab terhadap perlindungan konsumen. ISO sama-menekankan pentingnya definisi tanggung jawab yang jelas dan pembagian peran dalam pelaksanaan keamanan dan privasi informasi.
Pasal 48: Direksi wajib bertanggung jawab atas kepatuhan POJK ini dan Dewan Komisaris wajib mengawasinya	*Clause 5.1 (Leadership and commitment),* *9.3 (Management review)*	*Clause 5.3.1 (Leadership and commitment),* *Clause 5.7.3 (Management review)*	Pasal ini menjelaskan bahwa tanggung jawab tertinggi terhadap kepatuhan berada pada jajaran direksi dan dewan komisaris. ISO 27001 mengharuskan pimpinan untuk menunjukkan komitmen terhadap keamanan

			informasi melalui kebijakan dan alokasi sumber daya sementara ISO 27701 menegaskan peran pimpinan dalam mengarahkan dan meninjau efektivitas kebijakan privasi organisasi.
Pasal 44, 45, 50, 53, 55: Merinci berbagai sanksi administratif untuk setiap pelanggaran, mulai dari peringatan tertulis, denda sampai pencabutan izin usaha	*A.18.1.1 (Identification of applicable legislation and contractual requirements)*	*A.6.15.1.1 (Identification of applicable legislation and contractual requirements)*	Pasal ini menjelaskan bahwa pelanggaran terhadap ketentuan perlindungan konsumen dapat dikenakan sanksi administratif yang beragam sesuai tingkat pelanggaran. ISO mendukung prinsip ini melalui keharusan organisasi untuk mengidentifikasi dan mematuhi semua ketentuan hukum dan kontraktual yang berlaku, termasuk konsekuensi dan penegakan hukumnya.

4.2.3 Mapping Gap & Overlapping Regulasi

Dari hasil mapping antara regulasi yang mengatur perlindungan data pribadi yaitu UU PDP dan POJK dengan ISO 27001 dan ISO 27701, ditemukan bahwa terdapat sejumlah *overlapping* dan *gap*. Berikut ini adalah beberapa *overlapping* dan *gap* yang terjadi, sebagai berikut:

a. Overlapping

Bagian ini menjelaskan area di mana ketentuan dalam regulasi dan standar ISO saling beririsan atau mengatur aspek yang sama. Berdasarkan hasil *mapping*, ditemukan beberapa tumpang tindih yang dijelaskan pada Tabel 4. 8 Overlapping regulasi dengan ISO:

Tabel 4. 8 Overlapping regulasi dengan ISO

Area	Implementasi dalam UU PDP	Implementasi dalam POJK	Penjelasan
Prinsip kerahasiaan dan keamanan data	Mewajibkan pengendali data untuk menjaga kerahasiaan data pribadi dan melindunginya dari pemrosesan yang tidak sah	Mewajibkan Pelaku Usaha Jasa Keuangan (PUJK) menjaga kerahasiaan dan keamanan data konsumen dan secara eksplisit melarang pemberian data pribadi konsumen kepada pihak lain tanpa dasar yang sah	Prinsip Sejalan. Kedua regulasi ini menjadikan keamanan dan kerahasiaan data sebagai kewajiban inti. POJK fokus melindungi "data konsumen" sedangkan UU PDP melindungi semua "Data Pribadi"
Persetujuan	Menjadikan "persetujuan yang sah secara eksplisit dari subjek data pribadi" sebagai salah satu dasar hukum utama pemrosesan data.	Mengharuskan adanya persetujuan dari konsumen untuk memberikan data / informasi pribadi mereka kepada pihak lain atau untuk	Prinsip Sejalan. Kedua regulasi ini menjadikan persetujuan sebagai pilar tetapi UU PDP mendefinisikan standar

	Pengendali data wajib menunjukkan bukti persetujuan	penawaran produk melalui sarana komunikasi pribadi	persetujuan jauh lebih ketat dan detail
Transparansi Pemrosesan Data	Mewajibkan pemrosesan data pribadi dilakukan secara transparan. Saat meminta persetujuan, pengendali data wajib menyampaikan informasi mengenai legalitas, tujuan, jenis dan relevansi data yang diproses.	Menerapkan prinsip keterbukaan dan transparansi informasi. PUJK wajib menyediakan informasi produk / layanan yang jelas, akurat dan benar	Prinsip Sejalan. Kedua regulasi ini mendorong transparansi. POJK fokus pada transparansi produk/layanan sedangkan UU PDP fokus pada transparansi mengapa dan bagaimana data pribadi seseorang diproses
Keterlibatan Pihak Ketiga	Mengatur hubungan hukum antara pengendali data dan prosesor data, dimana prosesor data wajib memproses data berdasarkan perintah pengendali data. Tanggung jawab utama tetap pada pengendali data	PUJK wajib bertanggung jawab atas kerugian konsumen yang muncul akibat kesalahan atau kelalaian pihak ketiga yang bekerja untuk atau mewakili kepentingan PUJK	Prinsip Sejalan. Kedua regulasi ini menegaskan tanggung jawab pengendali data saat datanya dikelola pihak lain
Hak Dasar Konsumen / Subjek Data	Memberikan serangkaian hak dasar kepada subjek data seperti hak untuk mengakses data, hak memperbaiki data dan hak menarik kembali persetujuan	Memberikan hak kepada konsumen untuk mengajukan pengaduan dan mendapatkan penanganan sengketa	Prinsip Sejalan. Hak untuk mengajukan pengaduan di POJK sejalan dengan hak-hak dasar di UU PDP tetapi UU PDP menyediakan daftar hak yang lebih luas

b. Gap

Bagian ini menjelaskan area di mana regulasi belum secara eksplisit mengatur aspek yang sudah menjadi ketentuan dalam ISO 27001 atau ISO 27701. Berdasarkan hasil *mapping*, ditemukan beberapa *gap* yang dijelaskan pada Tabel 4. 9 Gap regulasi dengan ISO:

Tabel 4. 9 Gap regulasi dengan ISO

Area	Implementasi dalam UU PDP	Implementasi dalam POJK
Dasar hukum pemrosesan	Terdapat 6 dasar hukum pemrosesan data terdapat pada Pasal 20 ayat 2 termasuk persetujuan, pemenuhan kontrak, kewajiban hukum, kepentingan vital, tugas publik dan kepentingan yang sah	POJK hanya terdapat "persetujuan" untuk seluruh aktivitas
Hak-Hak subjek data	Terdapat beberapa hak-hak baru dan spesifik • Hak untuk menghapus data • Hak atas portabilitas data • Hak untuk menolak pemrofilan otomatis	POJK tidak mengatur ini
Kewajiban Baru	• Penunjukan *Data Protection Officer* (DPO) • Penilaian Dampak Pelindungan Data (*Data Protection Impact Assessment - DPIA*) • Notifikasi Pelanggaran Data (*Data Breach Notification*)	POJK tidak mengatur ini

Transfer Data Lintas Batas	Pasal 56 mengatur secara ketat syarat transfer data ke luar negeri yaitu negara tujuan harus punya tingkat perlindungan setara atau ada pelindungan yang memadai & mengikat atau telah mendapat persetujuan subjek data.	POJK tidak mengatur ini secara spesifik. Pengendali data hanya menggunakan layanan cloud atau berbagi data dengan grup internasional.
Sanksi	Sanksi lebih berat: • Sanksi Administratif Denda hingga 2% dari pendapatan tahunan • Sanksi Pidana Pidana penjara hingga 6 tahun dan denda hingga Rp 6 Miliar bagi individu dan denda hingga 10 kali lipat bagi korporasi	POJK hanya mengatur sanksi administratif yaitu denda maksimal Rp 15 Miliar

4.3 Analisis Kesiapan

Berdasarkan pembahasan sebelumnya, terdapat sejumlah irisan pengaturan antara Undang-Undang Perlindungan Data Pribadi (UU PDP) dan regulasi Otoritas Jasa Keuangan (POJK) terkait tata kelola keamanan informasi serta perlindungan data konsumen pada sektor keuangan. Meskipun memiliki tujuan yang serupa, yaitu melindungi data dan menjaga kepercayaan publik, perbedaan dalam ruang lingkup, terminologi, dan mekanisme pengawasan menuntut pemahaman yang komprehensif dari organisasi.

Untuk menilai kesiapan organisasi dalam mengimplementasikan ketentuan UU PDP, penelitian ini menggunakan model *Context, Input, Process, and Product* (CIPP) yang dikembangkan oleh Stufflebeam. Model tersebut digunakan untuk mengevaluasi aspek konteks, sumber daya, proses implementasi, serta hasil yang dicapai, sehingga memberikan gambaran menyeluruh mengenai tingkat kesiapan organisasi dari perspektif kepatuhan dan efektivitas operasional.

Data penelitian diperoleh melalui wawancara mendalam dengan dua informan kunci dari salah satu bank KBMI, yaitu *Business Branch Manager* dan *Department Head Application Developer*. Wawancara tersebut memberikan pemahaman mengenai sejauh mana kebijakan, prosedur dan praktik organisasi telah diselaraskan dengan prinsip-prinsip yang diatur dalam UU PDP. Hasil evaluasi ini selanjutnya digunakan untuk mengidentifikasi tingkat kesiapan organisasi, menemukan area yang masih memerlukan perbaikan, serta menjadi dasar dalam penyusunan rekomendasi strategis untuk memperkuat tata kelola perlindungan data pribadi dan mendukung integrasi standar ISO 27001 dan ISO 27701 dengan regulasi yang berlaku.

4.3.1 Kesiapan dari Sisi Context

Komponen *Context* digunakan untuk menilai kebutuhan, permasalahan dan peluang dalam suatu lingkungan tertentu (Stufflebeam & Coryn, 2014). Evaluasi *Context* bertujuan mengidentifikasi kebutuhan sasaran, memahami permasalahan serta menilai apakah tujuan yang ditetapkan sesuai dengan kondisi nyata (Stufflebeam, 2003). Berikut adalah Analisis dari Sisi *Context* yang dijelaskan pada Tabel 4. 10 Analisis dari Sisi Context.

Tabel 4. 10 Analisis dari Sisi Context

CIPP Model	Pertanyaan	Responden	Jawaban
Context	Sebelum UU PDP disahkan dan menjadi perhatian utama, bagaimana pandangan dan tingkat kesadaran Bank KBMI mengenai pentingnya perlindungan data pribadi nasabah? Apa yang menjadi pemicu utama kesadaran tersebut?	*Business Branch Manager*	Kesadaran pelindungan data sudah terbentuk kuat sebelum UU PDP ini ada yang berakar pada dua konsep utama yaitu Rahasia Jabatan dan Rahasia Bank.
	Apa pendorong utama bagi organisasi ini untuk memprioritaskan kepatuhan terhadap UU PDP? Apakah dorongan tersebut murni karena kewajiban hukum atau ada faktor lain seperti tuntutan nasabah atau reputasi?		Pendorong utama bersifat *top down* "didorong regulasi" yaitu kepatuhan wajib terhadap Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI). Faktor utamanya adalah mitigasi risiko reputasi. Pelanggaran data dinilai berdampak langsung pada reputasi dan kepercayaan publik yang dapat memicu komplain dari nasabah.

	Apakah inisiatif untuk sertifikasi dengan standar ISO 27001 dan ISO 27701 sudah ada sebelum UU PDP menjadi fokus atau justru UU PDP yang mendorong adopsi standar-standar ini sebagai *framework*?		Inisiatif ISO 27001 sudah ada sebelumnya. Namun, UU PDP mendorong adopsi yang lebih komprehensif untuk memastikan perlindungan data yang mendalam, tidak hanya sekadar patuh pada regulasi.
	Bagaimana persepsi tim *developers* mengenai integrasi persyaratan UU PDP dan ISO 27001 dalam aktivitas pengembangan aplikasi? Apakah hal ini dipandang sebagai hambatan teknis atau sebagai standar yang perlu diadopsi?	*Department Head Application Developer*	Developer memandang integrasi regulasi ini bukan sebagai blocker, melainkan sebagai standar baru yang wajib diadopsi. Keamanan data kini dianggap sebagai bagian dari setiap fase pengembangan hingga operasional aplikasi.
	Sebelum regulasi ini diberlakukan, sejauh mana tingkat *awareness developers* terkait isu privasi data nasabah?		Tingkat *awareness* sebelumnya sangat bervariasi "tidak merata", tergantung pada jenis aplikasi dan data yang mereka pegang. Kehadiran UU PDP berfungsi sebagai penyetara pemahaman "*unifying framework*". Regulasi ini memaksa semua developer memiliki *knowledge* yang seragam tentang siklus hidup data, mulai dari cara disimpan, digunakan, diarsipkan sampai dimusnahkan.

Hasil wawancara pada aspek *Context* menunjukkan bahwa kesadaran perlindungan data di sektor perbankan telah ada sebelum UU PDP, terutama berlandaskan prinsip kerahasiaan bank. Namun, UU PDP berperan sebagai penguat regulatif yang menstandarkan praktik perlindungan data secara lebih sistematis. Kepatuhan terhadap UU PDP didorong terutama oleh faktor regulasi dan mitigasi risiko reputasi dengan tekanan top down dari OJK dan Bank Indonesia. Penerapan ISO 27001 yang telah berjalan sebelumnya diperluas melalui adopsi ISO 27701 untuk membentuk kerangka keamanan dan privasi data yang terintegrasi. Bagi pengembang aplikasi, UU PDP berfungsi sebagai unifying *framework* yang menyelaraskan tingkat awareness dan memastikan perlindungan data diimplementasikan secara konsisten sepanjang siklus pengembangan sistem.

4.3.2 Kesiapan dari Sisi Input

Komponen *Input* digunakan untuk menilai kesiapan organisasi dari aspek strategi, kebijakan, sumber daya, anggaran dan infrastruktur yang diperlukan untuk mendukung implementasi (Stufflebeam, 2003). Berikut adalah Analisis dari Sisi *Input* yang dijelaskan pada Tabel 4. 11 Analisis dari Sisi Input.

Tabel 4. 11 Analisis dari Sisi Input

CIPP Model	Pertanyaan	Responden	Jawaban
Input	Sumber daya apa saja misalnya, anggaran khusus, pembentukan tim / departemen baru, pengadaan teknologi yang organisasi ini alokasikan secara spesifik untuk mempersiapkan dan mengimplementasikan UU PDP?	*Business Branch Manager*	Organisasi telah melakukan sejumlah penyesuaian, termasuk alokasi anggaran khusus, penyempurnaan aspek legal, modifikasi proses bisnis misalnya pembukaan rekening & promo serta program sosialisasi internal.
	Kebijakan dan prosedur apa yang Bank KBMI kembangkan atau revisi sebagai landasan untuk program kepatuhan UU PDP?		Kebijakan dan prosedur internal telah disesuaikan dan diperbarui pasca UU PDP. Fokus utamanya adalah memastikan penerapan praktis di setiap fungsi melalui sosialisasi kepada seluruh pegawai.
	Bagaimana struktur organisasi Bank KBMI terkait perlindungan data? Apakah Bank KBMI telah menunjuk fungsi DPO sesuai perintah UU PDP?		Struktur organisasi sudah dilengkapi dengan fungsi *Data Protection Officer* (DPO) di bawah divisi *Compliance*. Selain itu, setiap unit / divisi memiliki *PIC* perlindungan data untuk memastikan koordinasi yang efektif. Struktur ini

			diperkuat dengan sistem keamanan internal seperti tautan rahasia dan kontrol akses terbatas.
	Pelatihan dan program peningkatan kesadaran seperti apa yang diberikan kepada karyawan di semua tingkatan untuk memastikan mereka memahami kewajiban berdasarkan UU PDP dan kebijakan internal?		Organisasi melakukan program pelatihan dan awareness secara rutin dan bertingkat seperti kegiatan bulanan dan sharing moments. Terdapat juga reminder dan monitoring berkala untuk memperkuat pemahaman pegawai mengenai tanggung jawab terhadap perlindungan data pribadi.
	Apakah unit bisnis / unit compliance sudah memberikan *technical requirements* terkait regulasi privasi data?	*Department Head Application Developer*	Sudah ada pedoman perusahaan "*corporate guidelines*" dari unit terkait. Tugas tim developer adalah menerjemahkan pedoman tersebut menjadi *technical requirement* yang spesifik dan unik untuk setiap aplikasi, mengingat setiap aplikasi memiliki karakteristik yang berbeda-beda.
	Tools apa saja yang digunakan organisasi untuk mengamankan data dari nasabah? Apakah ada *tools* atau *platform* tertentu yang diwajibkan?		Organisasi menggunakan kombinasi *tools* enkripsi dan mekanisme *security testing* berkala. Pengujian ini krusial untuk memastikan setiap versi rilis aplikasi tetap *comply* dengan standar keamanan terkini dan mendapatkan dukungan keamanan yang memadai.

Hasil wawancara pada aspek *Input* menunjukkan bahwa Bank KBMI kelompok III & IV telah melakukan penyesuaian struktural dalam merespons UU PDP. Penyediaan anggaran khusus dan pembentukan fungsi *Data Protection Officer* (DPO) di bawah divisi *Compliance* mencerminkan kesiapan tata kelola, bukan sekadar pemenuhan administratif. Kesiapan ini diperkuat melalui penyesuaian proses bisnis seperti prosedur pembukaan rekening yang mengindikasikan penerapan prinsip *privacy by design* hingga level operasional melalui penunjukan *PIC* di setiap unit kerja. Dari sisi teknis, temuan menunjukkan adanya integrasi yang kuat antara kebijakan korporat dan implementasi sistem. Penerjemahan corporate guidelines ke dalam technical requirements bagi pengembang aplikasi menandakan bahwa kepatuhan telah terinternalisasi pada arsitektur sistem. Penerapan enkripsi, security testing berkala dan program peningkatan kesadaran SDM secara rutin mencerminkan pendekatan yang mengombinasikan penguatan kontrol teknis dan kesiapan manusia dalam memitigasi risiko kebocoran data.

4.3.3 Kesiapan dari Sisi Process

Process merupakan tahap di mana input dimanfaatkan secara efektif untuk mencapai tujuan, sasaran dan hasil yang diharapkan (Aziz et al., 2018; Stufflebeam, 2003). Tahap ini berfokus pada pemantauan pelaksanaan kebijakan di lapangan untuk memastikan implementasi berjalan sesuai rencana, sekaligus mengidentifikasi hambatan, penyimpangan dan area yang memerlukan perbaikan selama proses berlangsung. Berikut adalah Analisis dari Sisi *Process* yang dijelaskan pada Tabel 4. 12 Analisis dari Sisi Process.

Tabel 4. 12 Analisis dari Sisi Process

CIPP Model	Pertanyaan	Responden	Jawaban
Process	Bisa dijelaskan langkah-langkah konkret yang telah dan sedang dilakukan dalam proses implementasi?	*Business Branch Manager*	Organisasi menerapkan UU PDP melalui serangkaian proses terstruktur, mulai dari pemetaan data, penetapan peran, pelaksanaan *Risk Assessment* dan *DPIA*, penyusunan *Privacy Notice*, pengelolaan hak subjek data, manajemen vendor dan prosedur insiden 72 jam. Seluruh aktivitas ini dijalankan secara terintegrasi untuk memastikan kesiapan operasional.
	Bagaimana organisasi memonitor, meninjau dan mengaudit efektivitas dari kontrol yang telah diimplementasikan? Apakah ada audit internal atau eksternal yang secara spesifik mengacu pada kepatuhan UU PDP?		Efektivitas kontrol dievaluasi melalui monitoring internal oleh pimpinan unit dan audit berkala berbasis COBIT 2019 dan ISO 27001. Audit ini menilai kesesuaian penerapan kontrol keamanan dan kepatuhan terhadap ketentuan UU PDP.

	Apa tantangan terbesar yang dihadapi selama proses implementasi ini?		Hambatan utama meliputi kebutuhan sosialisasi yang berkelanjutan, pengawasan kepatuhan vendor, pembangunan budaya perlindungan data lintas unit dan kendala teknis seperti legacy system, data silo dan tumpang tindih regulasi.
	Bagaimana mekanisme teknis penghapusan data "*Right to be Forgotten*" diimplementasikan untuk memastikan data benar-benar tidak dapat dipulihkan?	*Department Head Application Developer*	Penghapusan data tidak dapat dilakukan sepenuhnya karena kewajiban retensi BI / OJK selama 7–10 tahun. Implementasi dilakukan secara selektif sesuai ketentuan retensi dengan fokus pada pembatasan akses dan penghapusan data yang tidak lagi diperlukan.
	Bagaimana arsitektur sistem dirancang untuk memfasilitasi permintaan portabilitas data nasabah sehingga format yang dihasilkan aman, terstandarisasi dan dapat dibaca oleh mesin?		Sistem portabilitas dirancang menggunakan format standar seperti *JSON/XML* dengan protokol berbasis ISO. Semua transmisi dienkripsi dan menggunakan jalur dedicated untuk memastikan keamanan dan integritas data selama proses pemindahan.

Hasil wawancara pada aspek *Process* menunjukkan bahwa implementasi UU PDP telah dijalankan secara operasional melalui mekanisme pengendalian risiko berlapis, bukan sekadar kepatuhan administratif. Proses kepatuhan diintegrasikan ke dalam siklus hidup data, mulai dari data mapping, pelaksanaan *Data Protection Impact Assessment* (DPIA) sebagai langkah preventif dan prosedur respons insiden dalam batas waktu 72 jam. Keberlanjutan dan validitas proses ini dijaga melalui audit berkala berbasis COBIT 2019 dan ISO 27001 yang berfungsi sebagai mekanisme pengawasan ganda terhadap efektivitas kontrol internal. Meski demikian, implementasi dihadapkan pada tantangan struktural dan teknis. Terdapat potensi konflik antara pemenuhan hak subjek data, khususnya Right to be Forgotten dan kewajiban retensi data perbankan sesuai ketentuan OJK/BI, untuk menjembatani konflik ini, organisasi tidak melakukan hard delete tetapi mengadopsi pendekatan data masking & data anonymization sehingga organisasi cenderung menerapkan penghapusan selektif dan pembatasan akses. Di sisi lain, keberadaan *legacy system* dan *data fragmentation* masih menghambat interoperabilitas, meskipun adopsi standar pertukaran data seperti JSON/XML mulai dilakukan sebagai upaya mitigasi.

4.3.4 Kesiapan dari Sisi Product

Product bertujuan untuk menilai efektivitas dan dampak kebijakan terhadap pencapaian tujuan yang sudah dirumuskan di awal program (Stufflebeam, 2003). Penilaiannya mencakup *output, outcome* dan *impact* yang dihasilkan dari penerapan kebijakan ini. Berikut adalah Analisis dari Sisi *Product* yang dijelaskan pada Tabel 4. 13 Analisis dari Sisi Product.

Tabel 4. 13 Analisis dari Sisi Product

CIPP Model	Pertanyaan	Responden	Jawaban
Product	Dilihat dari sudut pandang organisasi, sejauh mana implementasi yang telah dilakukan berhasil membawa organisasi selaras dengan aspek hukum UU PDP?	*Business Branch Manager*	Implementasi dinilai sudah selaras dengan ketentuan UU PDP dan mampu memperkuat prinsip kerahasiaan data nasabah. Pendekatan yang dilakukan tidak hanya bersifat pemenuhan hukum tetapi juga meningkatkan rasa aman dan kepercayaan nasabah sebagai bagian dari tata kelola organisasi.
	Selain pemenuhan aspek hukum, bagaimana Bapak menilai dampak implementasi ini terhadap penguatan postur perlindungan data pribadi secara keseluruhan? Apakah Bapak melihat adanya peningkatan dalam keamanan data nasabah? Apakah ada penurunan jumlah atau dampak dari insiden kebocoran data sejak program ini diimplementasikan?		Dampaknya terlihat signifikan, reputasi bank tetap terjaga dan tidak ditemukan insiden kebocoran data sejak program berjalan serta meningkatnya persepsi keamanan nasabah. Penguatan ini dicapai melalui monitoring dan evaluasi internal yang lebih ketat.

	Secara keseluruhan, apakah dengan penerapan ISO 27001 dan ISO 27701 terbukti efektif membantu organisasi untuk selaras dengan regulasi UU PDP? Di area mana standar ini paling memberikan nilai tambah?		Keduanya terbukti efektif, khususnya ISO 27701 yang berperan sebagai compliance enabler yang melengkapi ISO 27001. Nilai tambah terbesarnya meliputi penguatan tata kelola privasi, pemenuhan hak subjek data, pengelolaan *ROPA* dan pelaksanaan *DPIA* sebagai dasar pemenuhan UU PDP.
	Melihat ke depan, apa langkah selanjutnya bagi organisasi dalam menjaga dan terus meningkatkan kematangan program perlindungan data pribadi pasca implementasi awal UU PDP?		Fokus ke depan diarahkan pada pembentukan budaya privasi yang berkelanjutan melalui pelatihan internal. Mindset perlindungan data perlu menjadi bagian dari *customer experience* sehingga dapat memperkuat kepercayaan dan keunggulan kompetitif organisasi.
	Apa dampak implementasi UU PDP terhadap: ▪ Proses bisnis inti misalnya, pembukaan rekening & pengajuan kredit? ▪ Hubungan dan kepercayaan dengan nasabah? ▪ Inovasi produk dan layanan digital?		Dampaknya bersifat positif, proses bisnis menyesuaikan mekanisme consent untuk keperluan promosi dan notifikasi, hubungan dengan nasabah semakin kuat melalui peningkatan kepercayaan dan inovasi layanan digital meningkat karena nasabah merasa datanya aman.
	Berdasarkan monitoring, apakah implementasi fitur keamanan tambahan	*Department Head*	Monitoring menunjukkan bahwa enkripsi tidak menyebabkan penurunan performa yang signifikan. Kemajuan teknologi

	seperti enkripsi end-to-end berdampak signifikan terhadap latensi sistem atau waktu respons aplikasi?	*Application Developer*	perangkat keras dan pengelolaan *SLA* memungkinkan waktu respons tetap stabil meskipun proses enkripsi dan dekripsi ditambahkan.
	Bagaimana mekanisme pencatatan "*logging*" dirancang agar tetap informatif untuk penelusuran insiden "*debugging*" tanpa mengekspos data sensitif nasabah secara terbuka?		Mekanisme logging menggunakan penyimpanan berbasis database terenkripsi dengan akses yang sangat dibatasi. Log tidak disimpan dalam plain text dan hanya admin tertentu di lingkungan *Production* atau *Security* yang memiliki akses. Dengan desain ini, proses *debugging* tetap dapat dilakukan tanpa membuka data sensitif nasabah.

Hasil wawancara pada aspek *Product* menunjukkan bahwa integrasi ISO 27001 dan ISO 27701 telah menggeser kepatuhan dari sekadar *regulatory checklist* menjadi aset strategis organisasi. Efektivitasnya tercermin dari tidak ditemukannya insiden kebocoran data sejak implementasi yang beriringan dengan meningkatnya persepsi keamanan dan kepercayaan nasabah. ISO 27701 berperan sebagai *compliance enabler* yang memperjelas implementasi mandat teknis UU PDP seperti *ROPA*, *DPIA* dan pemenuhan hak subjek data yang tidak sepenuhnya terakomodasi oleh standar keamanan umum. Secara jangka panjang, dampak implementasi melampaui aspek teknis menuju penguatan keberlanjutan bisnis. Perlindungan data terinternalisasi sebagai budaya privasi yang terintegrasi dalam *customer experience* sehingga menjadi faktor diferensiasi kompetitif. Dengan demikian, *output* dari sistem ini bukan hanya kepatuhan hukum tetapi penguatan kepercayaan pasar dan ketahanan reputasi yang esensial bagi institusi keuangan di era digital berisiko tinggi.

4.3.5 Maturity Level Organisasi

Dari pembahasan sebelumnya diketahui bahwa salah satu Bank KBMI sudah comply terhadap perlindungan data nasabah sebelum UU PDP disahkan tetapi dalam penelitian ini, penulis juga menggunakan matriks kesiapan organisasi untuk menilai bagaimana kesiapan salah satu Bank KBMI ini diukur dari pasal-pasal di UU PDP. *Capability Maturity Model Integration* (CMMI) dipilih karena mampu memberikan gambaran mengenai tingkat kemampuan organisasi dalam mengelola dan meningkatkan prosesnya secara berkelanjutan. Berikut ini adalah hasil matriks *maturity level* dari salah satu Bank KBMI yang dijelaskan pada Tabel 4. 14 Maturity Level Organisasi:

Tabel 4. 14 Maturity Level Organisasi

Area Kepatuhan	Persyaratan	Pasal Terkait	Matriks Pengukuran	Skala 1-4
Pemrosesan Data	Memiliki dasar hukum yang sah untuk setiap kegiatan pemrosesan data pribadi	Pasal 20	• Terdapat *mapping* untuk setiap pemrosesan data • Terdapat dokumentasi dasar hukum untuk setiap aktivitas pemrosesan (contoh: formulir persetujuan, klausul kontrak, dll)	4
	Pemrosesan dilakukan secara terbatas, spesifik, sah dan transparan	Pasal 16 ayat (2), Pasal 27	• Pengumpulan data dibatasi hanya pada data yang relevan dengan tujuan yang telah ditetapkan • Dalam *privacy policy* disebutkan secara spesifik tujuan pengumpulan dari setiap data	4

Area Kepatuhan	Persyaratan	Pasal Terkait	Matriks Pengukuran	Skala 1-4
	Memastikan akurasi, kelengkapan dan konsistensi data	Pasal 29	• Terdapat proses verifikasi data pada saat pengumpulan data • Adanya prosedur untuk pembaruan data secara berkala atau *by request*	4
Hak Subjek Data	Memberikan informasi yang jelas kepada Subjek Data Pribadi	Pasal 5, Pasal 21	• Tersedia Pemberitahuan Privasi (*Privacy Notice*) yang mudah diakses dan dipahami, memuat informasi sesuai Pasal 21	4
	Memberikan hak akses dan salinan data kepada Subjek Data	Pasal 7, Pasal 32	• Terdapat prosedur untuk memverifikasi identitas pemohon • Dapat menyediakan data dan rekam jejak pemrosesan dalam waktu 3x24 jam sejak permintaan diterima	4
	Memfasilitasi hak untuk memperbaiki dan memperbarui data	Pasal 6, Pasal 30	• Terdapat prosedur untuk menerima dan memproses permintaan perbaikan data • Dapat melakukan perbaikan atau pembaruan dilakukan dalam waktu 3x24 jam sejak permintaan diterima	3

Area Kepatuhan	Persyaratan	Pasal Terkait	Matriks Pengukuran	Skala 1-4
	Memfasilitasi hak untuk menghapus dan memusnahkan data	Pasal 8, Pasal 43, Pasal 44	• Terdapat Prosedur penghapusan / pemusnahan data tersedia jika tujuan tercapai, persetujuan ditarik kembali, atau ada permintaan • Terdapat bukti bahwa data telah dihapus / dimusnahkan	4
Kewajiban Pengendali dan Prosesor	Mendapatkan persetujuan yang sah dan eksplisit	Pasal 20 ayat (2) huruf a, Pasal 21-24	• Terdapat Formulir persetujuan dibuat secara tertulis atau terekam, mudah dipahami, menggunakan bahasa sederhana dan jelas • Terdapat sistem untuk mencatat dan mengelola bukti persetujuan	4
	Melakukan pemrosesan data anak dan penyandang disabilitas secara khusus	Pasal 25, Pasal 26	• Terdapat mekanisme verifikasi usia • Terdapat prosedur untuk mendapatkan persetujuan dari orang tua/wali anak atau penyandang disabilitas/walinya	3
	Melakukan perekaman seluruh kegiatan pemrosesan data	Pasal 31	• Membuat dan memelihara Catatan Kegiatan Pemrosesan (*Record of Processing Activities/RoPA*)	4

Area Kepatuhan	Persyaratan	Pasal Terkait	Matriks Pengukuran	Skala 1-4
	Melakukan pengawasan terhadap pihak yang terlibat dalam pemrosesan	Pasal 37, Pasal 51	• Terdapat perjanjian pemrosesan data dengan Prosesor Data (*Data Processing Agreement*)	4
Keamanan dan Manajemen Risiko	Melindungi dan memastikan keamanan data pribadi	Pasal 35, Pasal 39	• Menerapkan protokol enkripsi dan kontrol akses untuk keamanan data • Melakukan penilaian tingkat keamanan berdasarkan sifat dan risiko data	4
	Menjaga kerahasiaan data pribadi	Pasal 36	• Terdapat perjanjian kerahasiaan (*Non Disclosure Agreement*) untuk pihak yang dapat mengakses data	4
	Memberitahukan kegagalan pelindungan data (*data breach*)	Pasal 46	• Terdapat Prosedur Standar Operasi (SOP) penanganan insiden kebocoran data yang mencakup kewajiban lapor secara tertulis kepada Subjek Data dan Lembaga dalam waktu 3x24 jam	3
Transfer Data Pribadi	Memastikan pelindungan data dalam transfer lintas negara	Pasal 56	• Terdapat daftar negara tujuan transfer data dan penilaian tingkat perlindungan data di negara tersebut	3

Area Kepatuhan	Persyaratan	Pasal Terkait	Matriks Pengukuran	Skala 1-4
Tata Kelola dan Akuntabilitas	Menunjuk Pejabat / Petugas Fungsi Pelindungan Data Pribadi (DPO)	Pasal 53, Pasal 54	• Melakukan penilaian apakah organisasi wajib menunjuk DPO berdasarkan kriteria di Pasal 53	4
	Menunjukkan pertanggungjawaban (*accountability*)	Pasal 47	• Terdapat dokumentasi semua kebijakan, prosedur dan tindakan kepatuhan yang telah diambil	4
	Menangani pengalihan data akibat aksi korporasi (merger, akuisisi, dll)	Pasal 48	• Terdapat prosedur untuk memberitahukan pengalihan data kepada subjek data sebelum dan sesudah aksi korporasi	4

Untuk menentukan *maturity level* suatu organisasi, penulis menggunakan pendekatan *Capability Maturity Model Integration* (CMMI) sebagai model untuk melakukan evaluasi. Proses perhitungan tingkat *maturity* ini dilakukan melalui dua tahapan utama yang menekankan pada objektivitas dan transparansi analisis data.

Tahap pertama, dilakukan penilaian terhadap setiap area kepatuhan dengan menghitung nilai rata-rata dari skor seluruh item atau indikator yang ada di dalamnya. Setiap indikator merepresentasikan sejauh mana organisasi telah memenuhi persyaratan yang ditetapkan dalam masing-masing *domain maturity*. Tahapan ini menjadi fondasi penting karena memberikan gambaran terhadap konsistensi penerapan kebijakan dan prosedur di setiap area. Tahap kedua berfokus pada perhitungan *Overall Maturity Score*, yaitu skor rata-rata dari seluruh area kepatuhan yang telah dievaluasi sebelumnya. Nilai ini menggambarkan tingkat kematangan organisasi secara keseluruhan. Skor *maturity* organisasi dihitung menggunakan metode *unweighted mean* yang sudah dijelaskan sebelumnya pada Rumus 3. 1 *Unweighted Mean*:

$$M_{Total} = \frac{1}{n}\sum_{i=1}^{n} C_i \tag{3.1}$$

Rumus 3. 1 *Unweighted Mean*

$^{M}Total$: Skor *maturity level* secara keseluruhan

n : Jumlah *domain* kepatuhan

C_i: Skor rata-rata pada *domain* kepatuhan

Pendekatan ini didasarkan pada asumsi bobot yang setara "*equal weighting*". Prinsip ini berpedoman bahwa setiap area yang diukur memiliki tingkat kepentingan yang sama terhadap keseluruhan model kematangan organisasi. Dengan kata lain, tidak ada satu area yang dianggap lebih dominan atau lebih berpengaruh dibandingkan area lainnya dalam menentukan *maturity level.* Beberapa penelitian sebelumnya seperti yang dilakukan oleh (Becker et al., 2009; Mettler, 2011) juga menggunakan pendekatan ini. Dalam metode ini, setiap area evaluasi diberikan nilai yang setara karena diasumsikan bahwa seluruh aspek memiliki kontribusi seimbang terhadap representasi *maturity level* secara keseluruhan. Pendekatan ini juga menghindari bias interpretasi yang dapat timbul akibat pembobotan yang tidak proporsional.

Dalam konteks kepatuhan terhadap Undang-Undang Perlindungan Data Pribadi (UU PDP), penerapan prinsip *equal weighting* memiliki relevansi yang kuat. Hal ini karena pelanggaran

atau kegagalan pada satu area kepatuhan dapat berimplikasi serius terhadap reputasi, kepercayaan publik dan integritas sistem secara keseluruhan. Dengan demikian, kegagalan dalam satu dimensi kepatuhan dipandang memiliki tingkat urgensi yang sama dengan kegagalan pada dimensi lainnya. Berikut ini adalah perhitungan dari setiap area untuk menilai *maturity level* organisasi yang ditunjukan pada Rumus 4. 1 *Unweighted Mean Area*:

$$M_{Area} = \frac{\sum_{i=1}^{n} S_i}{n} \tag{4.1}$$

Rumus 4. 1 *Unweighted Mean Area*

$^{M}Area$: Skor rata-rata area kepatuhan

S_i: Skor item persyaratan

n : Jumlah item persyaratan

$\sum_{i=1}^{n}$: Total Skor

a. Pemrosesan Data

   Pada area pemrosesan data, terdapat 3 persyaratan penilaian yang menjadi dasar perhitungan tingkat *maturity*. Penilaian dilakukan dengan melakukan rata-rata skor dari masing-masing persyaratan yang ada. Hasil perhitungan rata-ratanya adalah sebagai berikut:

$$M_{Area} = \frac{4 + 4 + 4}{3} = 4$$

   Dengan hasil perhitungan tersebut, area pemrosesan data memperoleh skor *maturity* 4 yang mengindikasikan bahwa pengelolaan proses data telah mencapai tingkat pemenuhan yang konsisten dan berada pada level yang *mature.*

b. Hak Subjek Data

   Pada area hak subjek data, terdapat 4 persyaratan yang mencerminkan bagaimana organisasi memenuhi hak-hak pemilik data "*data subject*". Hasil perhitungan rata-ratanya adalah sebagai berikut:

$$M_{Area} = \frac{4 + 4 + 3 + 4}{4} = 3.75$$

   Dengan hasil perhitungan tersebut, area ini menunjukkan bahwa pemenuhan hak subjek data sudah berjalan baik tetapi masih terdapat ruang penyempurnaan agar mencapai *maturity* yang optimal.

c. Kewajiban Pengendali dan Prosesor

Pada area kewajiban pengendali dan prosesor, terdapat 4 persyaratan yang berkaitan dengan kepatuhan organisasi sebagai *data controller* dan *data processor* Hasil perhitungan rata-ratanya adalah sebagai berikut:

$$M_{Area} = \frac{4 + 3 + 4 + 4}{4} = 3.75$$

Dengan hasil perhitungan tersebut, area ini menunjukkan bahwa tanggung jawab pengendali dan pemroses data sudah dipenuhi dan sudah berjalan baik tetapi masih terdapat ruang penyempurnaan agar mencapai *maturity* yang optimal.

d. Keamanan dan Manajemen Risiko

Pada area keamanan dan manajemen risiko, terdapat 3 persyaratan yang berkaitan bagaimana organisasi dalam mengelola keamanan informasi dan risiko terkait perlindungan data pribadi. Hasil perhitungan rata-ratanya adalah sebagai berikut:

$$M_{Area} = \frac{4 + 4 + 3}{3} = 3.66$$

Dengan hasil perhitungan tersebut, area ini menunjukkan bahwa proses ini sudah berjalan dengan baik tetapi masih perlu dilakukan peningkatan.

e. Transfer Data Pribadi

Pada area transfer data pribadi, hanya terdapat 1 persyaratan yang berkaitan bagaimana organisasi melakukan manajemen terhadap transfer data pribadi. Hasil perhitungan rata-ratanya adalah sebagai berikut:

$$M_{Area} = \frac{3}{1} = 3$$

Dengan hasil perhitungan tersebut, area ini menunjukkan bahwa proses ini sudah berada pada level 3 (*defined*) tetapi belum optimal sehingga perlu dilakukan peningkatan di area ini.

f. Tata Kelola dan Akuntabilitas

Pada area tata kelola dan akuntabilitas, terdapat 3 persyaratan yang berkaitan dengan mekanisme pengawasan internal, penetapan peran dan dokumentasi pertanggung jawaban terkait data pribadi. Hasil perhitungan rata-ratanya adalah sebagai berikut:

$$M_{Area} = \frac{4 + 4 + 4}{3} = 4$$

Dengan hasil perhitungan tersebut, area pemrosesan data memperoleh skor *maturity* 4 yang mengindikasikan bahwa pengelolaan proses data telah mencapai tingkat pemenuhan yang konsisten dan berada pada level yang *mature.* Berikut ini adalah ringkasan dari perhitungan tingkat *maturity* organisasi yang disajikan pada Tabel 4. 15 Tingkat *Maturity* dalam setiap area.

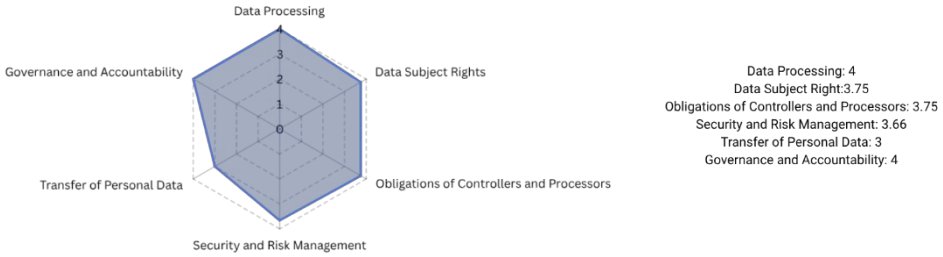
Tabel 4. 15 Tingkat *Maturity* dalam setiap area

Area Kepatuhan	Jumlah Persyaratan	Skor	Penjelasan
Pemrosesan Data	3	4	Pemenuhan sudah konsisten dan telah mencapai tingkat *maturity* yang optimal
Hak Subjek Data	4	3.75	Sudah baik tetapi masih terdapat ruang untuk peningkatan
Kewajiban Pengendali dan Prosesor	4	3.75	Sudah baik tetapi masih terdapat ruang untuk peningkatan
Keamanan dan Manajemen Risiko	3	3.66	Kontrol keamanan cukup baik tetapi masih terdapat ruang untuk peningkatan
Transfer Data Pribadi	1	3	Perlu dilakukan peningkatan terutama terkait kebijakan transfer lintas sistem / yurisdiksi
Tata Kelola dan Akuntabilitas	3	4	Pemenuhan sudah konsisten dan telah mencapai tingkat *maturity* yang optimal

Setelah memperoleh skor masing-masing area kepatuhan, langkah selanjutnya adalah menghitung *Overall Maturity Score* untuk mengetahui posisi tingkat *maturity level* organisasi. Perhitungan ini dilakukan dengan merata-ratakan seluruh skor area menggunakan rumus berikut:

$$M_{Total} = \frac{22.16}{6} = 3.69$$

Hasil akhir menunjukkan bahwa nilai rata-rata keseluruhan adalah 3.69. Skor tersebut menempatkan organisasi pada Level 3 "*Defined*" dalam model *CMMI* tetapi dengan kecenderungan yang sudah mendekati Level 4 "*Quantitatively Managed*", artinya, proses-proses yang terkait dengan kepatuhan data pribadi telah terdokumentasi dengan baik, terstandarisasi dan diterapkan secara konsisten di seluruh divisi.



Gambar 4. 1 *Overall Maturity Score*

Visualisasi pada Gambar 4. 1 *Overall Maturity Score*, memperlihatkan distribusi skor di enam area kepatuhan yang dinilai. Dapat dilihat bahwa area Pemrosesan Data dan Tata Kelola dan Akuntabilitas memperoleh skor tertinggi "4" yang menunjukkan tingkat *maturity* yang paling dominan. Sebaliknya, pada area Transfer Data Pribadi memperoleh skor terendah "3" yang mengindikasikan perlunya penguatan kebijakan kontrol data lintas sistem atau lintas yurisdiksi. Sementara itu, area lain seperti Hak Subjek Data, Kewajiban Pengendali dan Prosesor dan Keamanan dan Manajemen Risiko berada pada rentang 3.66 - 3.75 yang menunjukkan bahwa implementasi sudah berjalan dengan baik tetapi masih dapat ditingkatkan.

4.4 PDCA Framework

Berdasarkan hasil analisis dan mapping tersebut, diperlukan suatu kerangka kerja implementasi yang sistematis agar integrasi ISO 27001 dan ISO 27701 dapat diterapkan secara efektif dan berkelanjutan. Oleh karena itu, pengembangan kerangka kerja selanjutnya dilakukan dengan menggunakan pendekatan PDCA (*Plan-Do-Check-Act*) Cycle yang memungkinkan organisasi untuk merencanakan, menerapkan, mengevaluasi dan meningkatkan pengelolaan keamanan informasi dan perlindungan data pribadi secara berkelanjutan. Siklus PDCA bertujuan untuk menetapkan, menerapkan, memantau dan memperbaiki efektivitas Sistem Manajemen Keamanan Informasi (*ISMS*) suatu organisasi (Susanto et al., 2011). Setiap fase dalam siklus PDCA memiliki tujuan dan serangkaian aktivitas yang membentuk loop umpan balik untuk perbaikan berkelanjutan yang dimulai dari *Plan, Do, Check, Act* (Jagtap & Teli, 2015). Dengan menjadikan PDCA sebagai pendekatan, setiap tahapan dapat diselaraskan ke dalam tahapan perencanaan, implementasi, evaluasi dan perbaikan berkelanjutan secara konsisten. Oleh karena itu, bagian selanjutnya akan menguraikan usulan PDCA *framework* yang menggambarkan pemetaan aktivitas, kontrol dan mekanisme evaluasi dalam setiap fase *PDCA* untuk mendukung kepatuhan terhadap UU PDP melalui integrasi ISO 27001 dan ISO 27701. Berikut ini adalah rancangan dari PDCA *framework* yang disajikan pada Tabel 4. 16 PDCA Cycle.

Tabel 4. 16 PDCA Cycle

Tahap	Aktivitas	Justifikasi	Fokus pada ISO 27701&27701
Plan	• Penyelarasan Konflik Regulasi Merancang kebijakan Pseudonymisation untuk menengahi konflik antara "Hak Penghapusan" (UU PDP) dan "Wajib Retensi 10 Tahun" (OJK).	• CIPP Model: Ditemukan kendala teknis pelaksanaan *Right to be Forgotten* karena benturan antar regulasi • CMMI Model: Area Transfer Data masih pada 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)*

	• Penguatan Mekanisme Transfer Lintas negara Menyusun *Standard Contractual Clauses* dan penilaian kelayakan negara tujuan untuk memperbaiki kelemahan pada transfer data.		• *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	• Penerapan *DPIA & ROPA* Menjalankan Data Protection Impact Assessment untuk produk baru dan memelihara *Record of Processing Activities* secara *real-time*. • Penerapan Enkripsi & *Access Control* Mengimplementasikan enkripsi *end-to-end* dan manajemen akses ketat pada *legacy system*. • *Privacy Culture* Melakukan pelatihan kepada seluruh staf untuk menanamkan mindset bahwa privasi adalah bagian dari *Customer Experience*	• CIPP Model: Keamanan data terbukti meningkatkan kepercayaan nasabah dan menjadi keunggulan kompetitif	• *ISO 27701: A.7.2.5 (Privacy impact assessment) & Clause 7.2.8 (Records related to processing PII)* • *ISO 27001: A.10 (Cryptography) & A.9 (Access Control - A.9.1.1, A.9.2.5, A.9.4.1)*

Check	• Audit Respons Hak Subjek Data Mengukur *SLA* respons permintaan nasabah (akses/hapus/koreksi) apakah konsisten < 3x24 jam. • Review Pihak Ketiga (Vendor) Mengaudit kepatuhan vendor terhadap klausul *Data Processing Agreement* (DPA).	• CMMI Model: Area Hak Subjek Data masih belum optimal • ISO Mapping: Klausul A.15 (*Supplier relationships*) yang mewajibkan monitoring layanan supplier	• *ISO 27701: A.7.3.6 (Access, correction and/or erasure), A.7.3.9 (Handling PII requests) & A.7.3.3 (Providing information to PII principals)* • *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)*
Act	• Sanksi & Terminasi Vendor Memberikan sanksi atau memutus kontrak vendor yang gagal mematuhi standar pelindungan data. • Peningkatan Fitur *Legacy System* Melakukan *patching* atau *upgrade* pada sistem lama yang menjadi penghambat.	• CIPP: Tantangan seperti *legacy system* dan pengawasan kepatuhan vendor masih menjadi tantangan yang serius • ISO Mapping: Klausul A.15 (*Supplier relationships*) yang mewajibkan monitoring layanan supplier	• *ISO 27701: A.7.2.6 (Contracts with PII processors)* • *ISO 27001: A.15 (Supplier relationships), A.14 (System acquisition, development and maintenance) & A.12.1.2 (Change management)*

Dari *framework* tersebut, fase *Plan* memuat sejumlah aktivitas kunci untuk menyelaraskan regulasi dengan ISO 27001 dan ISO 27701. *Pseudonymisation* digunakan sebagai teknik perlindungan data yang diakui secara eksplisit dalam GDPR untuk menurunkan risiko terhadap subjek data tanpa menghambat pemrosesan dan analisis data yang sah karena data yang dipseudonimkan masih dikategorikan sebagai data pribadi (European Data Protection Board, 2025; Mourby et al., 2018). Selain itu, penguatan mekanisme transfer data lintas negara menjadi elemen strategis supaya memastikan aliran data internasional selaras dengan prinsip perlindungan hak subjek data, melalui pendekatan berlapis seperti *adequacy decision, appropriate safeguards dan derogations* (Riswandi & Gultom, 2023). Dalam konteks ini, *Standard Contractual Clauses* (SCCs) berfungsi sebagai instrumen akuntabilitas berbasis organisasi yang mengompensasi keterbatasan perlindungan hukum di negara tujuan transfer melalui kewajiban kontraktual yang diperkuat oleh kontrol teknis dan organisasional, bukan sebagai penilaian menyeluruh atas sistem hukum negara tersebut (Bradford et al., 2021).

Pada fase *Do* dalam siklus PDCA, organisasi menerapkan kontrol operasional untuk memastikan perlindungan data pribadi berjalan konsisten, antara lain melalui pelaksanaan *Data Protection Impact Assessment* (DPIA) pada pengembangan produk serta pemeliharaan *Record of Processing Activities* (ROPA) secara berkelanjutan suapya menjamin akuntabilitas dan transparansi pemrosesan data (Henriksen-Bulmer et al., 2020; Iwaya et al., 2024). Upaya ini diperkuat dengan penerapan enkripsi end-to-end dan kontrol akses berbasis risiko, termasuk pada *legacy system*, sebagai langkah teknis utama dalam mencegah akses tidak sah dan kebocoran data (Ayedh M et al., 2023). Dan didukung oleh penguatan *privacy culture* melalui pelatihan rutin bagi seluruh pegawai.

Pada fase *Check*, organisasi melakukan audit pemenuhan hak subjek data untuk memastikan konsistensi layanan sesuai *service level agreement* (SLA), khususnya terkait hak akses, koreksi dan penghapusan data yang sejalan dengan prinsip ketepatan waktu dan transparansi yang ditekankan dalam regulasi perlindungan data (Bufalieri et al., 2020). Pengawasan ini dilengkapi dengan evaluasi kepatuhan vendor terhadap *Data Processing Agreement* (DPA) supaya memastikan bahwa keterlibatan pihak ketiga tidak melemahkan kontrol perlindungan data (Amaral et al., 2023).

Selanjutnya, pada fase *Act*, ketidakpatuhan ditindaklanjuti melalui tindakan korektif seperti penerapan sanksi atau penghentian kerja sama dengan vendor, sebagai upaya menjaga akuntabilitas dan meminimalkan risiko hukum dan reputasi (Gregory Voss & Bouthinon-Dumas, 2021). Di saat yang sama, perbaikan berkelanjutan dilakukan melalui

peningkatan atau *patching legacy system* yang masih menjadi hambatan teknis sehingga efektivitas pengendalian dan audit perlindungan data dapat terus ditingkatkan (Safitra et al., 2023).

Berdasarkan kerangka tersebut, perlindungan data pribadi yang selaras dengan ISO 27001 dan ISO 27701 menuntut pendekatan yang menggabungkan aspek hukum, teknis dan organisasional secara berkelanjutan melalui siklus PDCA. Instrumen seperti *pseudonymisation*, DPIA dan ROPA berperan penting dalam menekan risiko terhadap hak subjek data tanpa menghambat pemrosesan yang sah, sementara penguatan mekanisme transfer data lintas negara melalui SCCs yang didukung kontrol teknis dan organisasional menjamin akuntabilitas aliran data internasional. Efektivitas tata kelola perlindungan data pada akhirnya ditentukan oleh konsistensi implementasi kontrol teknis, pengawasan kepatuhan dan perbaikan berkelanjutan, bukan sekadar keberadaan kebijakan atau regulasi.

BAB 5
Kesimpulan dan Saran

5.1 Kesimpulan

Penelitian ini dilakukan untuk menjawab dua rumusan masalah mengenai tingkat kesiapan organisasi perbankan dalam mengimplementasikan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan kesesuaian standar ISO 27001 dan ISO 27701 dengan ketentuan hukum yang berlaku. Berdasarkan hasil analisis yang telah dilakukan, diperoleh kesimpulan sebagai berikut:

a. Kesiapan organisasi perbankan terhadap implementasi UU PDP

   Rumusan masalah pertama dijawab melalui penerapan model *Context, Input, Process, Product* (CIPP) yang dipadukan dengan *Capability Maturity Model Integration* (CMMI). Hasil evaluasi menunjukkan bahwa kebijakan dan proses perlindungan data pribadi pada organisasi yang menjadi objek penelitian telah terdokumentasi, diterapkan secara formal dan didukung oleh budaya perlindungan informasi yang telah berkembang sebelum diberlakukannya UU PDP melalui penerapan prinsip kerahasiaan bank. Pengukuran menggunakan CMMI menghasilkan nilai kematangan sebesar 3,69 yang menempatkan organisasi pada Level 3 (*Defined*). Tingkat kematangan tersebut menunjukkan bahwa proses kepatuhan telah terstandarisasi dan dijalankan secara konsisten, meskipun masih diperlukan peningkatan pada aspek pemantauan dan pengendalian yang lebih sistematis. Hasil pengukuran ini menggambarkan kondisi organisasi yang diteliti dan tidak dimaksudkan untuk merepresentasikan tingkat kesiapan seluruh sektor perbankan di Indonesia.

b. Keterkaitan ISO 27001 dan ISO 27701 dengan kewajiban hukum UU PDP dan regulasi OJK

   Rumusan masalah kedua dijawab melalui penyusunan matriks pemetaan yang menghubungkan persyaratan dalam UU PDP dan regulasi OJK dengan kontrol pada ISO 27001 dan ISO 27701. Hasil pemetaan menunjukkan bahwa sebagian besar ketentuan hukum memiliki kesesuaian dengan standar internasional tersebut, namun juga mengungkap adanya potensi konflik regulatif, terutama antara hak *Right to be Forgotten* dalam UU PDP dan kewajiban retensi data yang diwajibkan pada sektor jasa keuangan. Untuk mengatasi permasalahan tersebut, penelitian ini mengusulkan sebuah arsitektur

kepatuhan konseptual berbasis siklus *Plan-Do-Check-Act* (PDCA) yang mengintegrasikan mekanisme *data masking* dan *pseudonymization* sebagai strategi mitigasi risiko privasi. Meskipun demikian, baik matriks pemetaan maupun arsitektur yang diusulkan masih berada pada tahap konseptual dan belum diuji melalui implementasi pada lingkungan operasional sehingga implikasinya terhadap penguatan kepatuhan organisasi masih memerlukan validasi lebih lanjut melalui penerapan pada lingkungan operasional yang sesungguhnya.

Secara keseluruhan, penelitian ini memberikan kontribusi dalam pengembangan kerangka evaluasi kepatuhan perlindungan data pada sektor perbankan melalui integrasi model CIPP, CMMI dan pemetaan kontrol berdasarkan ISO 27001 dan ISO 27701. Pendekatan ini menyediakan mekanisme evaluasi yang sistematis terhadap kesiapan organisasi, mencakup aspek tata kelola, sumber daya, proses operasional hingga keselarasan dengan regulasi yang berlaku. Penelitian ini menggunakan pendekatan studi kasus tunggal dengan melibatkan dua responden yang mewakili perspektif bisnis dan teknologi informasi. Oleh karena itu, hasil penilaian kematangan yang diperoleh hanya mencerminkan kondisi organisasi yang diteliti dan tidak dapat digeneralisasikan sebagai gambaran kesiapan seluruh industri perbankan di Indonesia. Meskipun memiliki keterbatasan tersebut, penelitian ini memberikan kontribusi secara teoretis maupun praktis melalui penyusunan kerangka evaluasi yang terintegrasi untuk menilai kesiapan organisasi dalam memenuhi ketentuan UU PDP. Kerangka yang dihasilkan dapat dimanfaatkan sebagai acuan penilaian internal bagi institusi keuangan dalam menyusun strategi kepatuhan sekaligus mendukung pengembangan tata kelola perlindungan data yang selaras dengan standar internasional. Penelitian selanjutnya disarankan melakukan validasi pada berbagai institusi keuangan dengan karakteristik yang beragam untuk menguji konsistensi dan tingkat generalisasi kerangka yang diusulkan. Selain itu, juga dapat mengeksplorasi pemanfaatan teknologi berbasis *Artificial Intelligence* dan *Natural Language Processing* untuk mengembangkan mekanisme *automated compliance checking*, khususnya dalam melakukan analisis dan audit terhadap dokumen *Data Processing Agreement*, kebijakan privasi serta dokumen kepatuhan lainnya secara lebih efisien dan terukur.

5.2 Saran

Adapun saran dari penelitian ini, yaitu:

1. Saran bagi Organisasi

   Institusi perbankan perlu memperkuat tata kelola perlindungan data pribadi melalui penyelarasan yang lebih sistematis antara ketentuan UU PDP, regulasi Otoritas Jasa Keuangan (OJK) serta standar internasional seperti ISO 27001 dan ISO 27701. Upaya ini dapat dilakukan melalui penyusunan kebijakan privasi yang terintegrasi, peningkatan mekanisme pengawasan kepatuhan dan pembentukan struktur tata kelola yang secara khusus bertanggung jawab terhadap pengelolaan data pribadi. Selain itu, organisasi disarankan untuk mengembangkan mekanisme teknis yang mampu mengakomodasi kebutuhan perlindungan data sekaligus memenuhi kewajiban retensi data sektor keuangan. Implementasi teknologi seperti data *masking* & *pseudonymization* dapat menjadi alternatif untuk meminimalkan risiko pelanggaran privasi tanpa mengabaikan kewajiban regulatif yang berlaku.

2. Saran bagi Regulator

   Regulator perlu mempertimbangkan penyusunan pedoman implementasi yang lebih rinci terkait hubungan antara UU PDP dan regulasi sektoral, khususnya pada sektor perbankan dan jasa keuangan. Pedoman tersebut diharapkan dapat memberikan kejelasan mengenai mekanisme penerapan prinsip-prinsip perlindungan data pribadi, termasuk penanganan potensi konflik antara hak subjek data dan kewajiban retensi data yang diwajibkan oleh regulator sektor keuangan.

3. Saran Penelitian Selanjutnya

   Penelitian ini menggunakan pendekatan studi kasus tunggal pada satu institusi perbankan sehingga hasil yang diperoleh masih terbatas pada konteks organisasi yang diteliti. Oleh karena itu, penelitian selanjutnya disarankan untuk melakukan validasi kerangka kerja yang diusulkan pada berbagai institusi keuangan dengan karakteristik yang berbeda, seperti bank umum, bank digital, perusahaan pembiayaan, maupun perusahaan *fintech*. Selain itu, penelitian selanjutnya dapat mengeksplorasi pemanfaatan *Artificial Intelligence* (AI), *Machine Learning* (ML) dan *Natural Language Processing* (NLP) dalam pengembangan sistem *automated compliance checking* untuk melakukan analisis kesesuaian regulasi, audit *Data Processing Agreement* (DPA) serta pemantauan kepatuhan privasi secara berkelanjutan.

Daftar Pustaka

Albrecht, J. P. (2016). How the GDPR will change the world. European Data Protection Law Review, 2(3), 287–289. https://doi.org/10.21552/EDPL/2016/3/4

Algamar, M. D., Munir, A. B., & Hendro. (2024). Managing Indonesian data breach notification in the financial services sector: A case for one-stop notification model. Journal of Central Banking Law and Institutions, 3(3), 547–584. https://doi.org/10.21098/jcli.v3i3.271

Amaral, O., Azeem, M. I., Abualhaija, S., & Briand, L. C. (2023). NLP-based automated compliance checking of data processing agreements against GDPR. Proceedings of the 45th IEEE/ACM International Conference on Software Engineering (ICSE), 1–26. https://doi.org/10.1109/ICSE48619.2023.00172

Antoine, R. A., Farizqa, N. S., Hasna, A. H., & Pasaribu, M. (2025). Penyalahgunaan data pribadi dalam teknologi transaksi digital di industri perbankan digital (studi kasus PT. Bank Syariah Indonesia). Jurnal Multidisiplin Ilmu Akademik, 2(1), 316–327. https://doi.org/10.61722/jmia.v2i1.3147

Anwar, M. J., & Gill, A. Q. (2020). Developing an integrated ISO 27701 and GDPR based information privacy compliance requirements model. Australasian Conference on Information Systems (ACIS) 2020 Proceedings, 1–12. https://aisel.aisnet.org/acis2020/20

Ayedh, A. T., Wahab, A. W. A., & Idris, M. Y. I. (2023). 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, 13(14), Article 8048. https://doi.org/10.3390/app13148048

Aziz, S., Mahmood, M., & Rehman, Z. (2018). Implementation of CIPP model for quality evaluation at school level: A case study. Journal of Education and Educational Development, 5(1), 189–206.

Baker, L. (2017). The impact of the General Data Protection Regulation on the banking sector: Data subjects' rights, conflicts of laws and Brexit. Journal of Data Protection & Privacy, 1(2), 137–145.

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing maturity models for IT management. Business & Information Systems Engineering, 1(3), 213–222. https://doi.org/10.1007/s12599-009-0044-5

Bougiakiotis, E. (2020). The layered links model: An alternative approach to international privacy regulation. International Data Privacy Law, 11(1), 1–16. https://doi.org/10.1093/idpl/ipaa002

Bradford, L., Aboy, M., & Liddell, K. (2021). Standard contractual clauses for cross-border transfers of health data after Schrems II. *Journal of Law and the Biosciences*, *8*(1), 1–36. https://doi.org/10.1093/jlb/lsab007

Bufalieri, L., La Morgia, M., Mei, A., & Stefa, J. (2020). GDPR: When the right to access personal data becomes a threat. Proceedings of the IEEE International Conference on Web Services (ICWS), 1–8. https://doi.org/10.1109/ICWS49710.2020.00017

Camp, L. J. (1999). Web security and privacy: An American perspective. The Information Society, 15(4), 249–256. https://doi.org/10.1080/019722499128411

De Carolis, A., Macchi, M., Negri, E., & Terzi, S. (2017). A maturity model for assessing the digital readiness of manufacturing companies. IFIP Advances in Information and Communication Technology, 513, 13–20. https://doi.org/10.1007/978-3-319-66923-6_2

Direktorat Operasi Keamanan Siber. (2024). *Lanskap keamanan siber Indonesia 2024*. Badan Siber dan Sandi Negara (BSSN).

Direktur Jenderal Aplikasi Informatika. (2021). *Kesiapan industri dalam pelindungan data pribadi: Survei terhadap perusahaan digital tahun 2021*. Kementerian Komunikasi dan Informatika Republik Indonesia.

Ellis, S., Sharma, S., & Brzeszczyński, J. (2022). Systemic risk measures and regulatory challenges. *Journal of Financial Stability*, *61*, Article 100960. https://doi.org/10.1016/j.jfs.2021.100960

Esgaiar, E., & Foster, S. (2019). Implementation of CIPP model for quality evaluation at Zawia University. *International Journal of Applied Linguistics and English Literature*, *8*(5), 106–115. https://doi.org/10.7575/aiac.ijalel.v.8n.5p.106

European Data Protection Board. (2025). Guidelines 01/2025 on pseudonymisation. https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-012025-pseudonymisation_en.

European Union. (2018). General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council. Official Journal of the European Union. https://GDPR-info.eu/.

Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. *The TQM Journal*, *23*(4), 367–376. https://doi.org/10.1108/17542731111139455

Gomes, J., & Romão, M. (2025). Evaluating maturity models in healthcare information systems: A comprehensive review. *Healthcare*, *13*(15), Article 1847. https://doi.org/10.3390/HEALTHCARE13151847

Gregory Voss, W., & Bouthinon-Dumas, H. (2021). EU General Data Protection Regulation sanctions in theory and in practice. *Santa Clara High Technology Law Journal*, *37*(1), 1–97.

Henriksen-Bulmer, J., Faily, S., & Jeary, S. (2020). DPIA in context: Applying DPIA to assess privacy risks of cyber physical systems. *Future Internet*, *12*(5), Article 93. https://doi.org/10.3390/FI12050093

ISACA. (2019). COBIT 2019 framework: Governance and management objectives. ISACA.

Isniah, S., Hardi Purba, H., & Debora, F. (2020). Plan do check action (PDCA) method: literature review and research issues. *Jurnal Sistem Dan Manajemen Industri*, *4*(1), 72–81. https://doi.org/10.30656/jsmi.v4i1.2186

ISO 9001:2015. (2015). *ISO 9001:2015(en), Quality management systems — Requirements*. https://www.iso.org/obp/ui/#iso:std:iso:9001:ed-5:v1:en

ISO/IEC 27001:2022. (2022). *ISO/IEC 27001:2022(en), Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en

ISO/IEC 27701:2019. (2019). *ISO/IEC 27701:2019(en)*. https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en

Iwaya, L. H., Alaqra, A. S., Hansen, M., & Fischer-Hübner, S. (2024). Privacy impact assessments in the wild: A scoping review. *Array*, *23*, 1–20. https://doi.org/10.1016/j.array.2024.100356

Jagtap, M., & Teli, S. N. (2015). P-D-C-A Cycle As TQM Tool-Continuous Improvement of Warranty. *International Journal on Recent Technologies in Mechanical and Electrical Engineering (IJRMEE)*, *2*(4), 1–5. http://www.ijrmee.org

Kaivanpanah, S., & Zarrin, M. (2025). 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*, *12*(3), 1–26. https://doi.org/10.30479/jmrels.2024.20762.2419

Khatibian, N., Hasan gholoi pour, T., & Abedi Jafari, H. (2010). Measurement of knowledge management maturity level within organizations. *Business Strategy Series*, *11*(1), 54–70. https://doi.org/10.1108/17515631011013113

Komandla, V. (2023). Safeguarding Digital Finance: Advanced Cybersecurity Strategies for Protecting Customer Data in Fintech. *ISAR Journal of Multidisciplinary Research and Studies*, *1*(2), 62–70. https://ssrn.com/abstract=4983180

Kosanke, K. (2006). ISO Standards for Interoperability: a Comparison. *Interoperability of Enterprise Software and Applications*, 55–64.

Lachaud, E. (2020). ISO/IEC 27701: Threats and Opportunities for GDPR Certification. *SSRN Electronic Journal*, *6*(2), 194–210. https://doi.org/10.2139/ssrn.3521250

Li, H., Yu, L., & He, W. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*, *22*(1), 1–6. https://doi.org/10.1080/1097198X.2019.1569186

Mangini, V., Tal, I., & Moldovan, A.-N. (2020, August). *An Empirical Study on the Impact of* GDPR *and Right to be Forgotten - Organisations and Users Perspective*. https://doi.org/10.1145/3407023

Mettler, T. (2011). Maturity assessment models: A design science research approach. *International Journal of Society Systems Science*, *3*(1/2), 81–98.

Morić, Z., Dakic, V., Djekic, D., & Regvart, D. (2024). Protection of Personal Data in the Context of E-Commerce. *Journal of Cybersecurity and Privacy*, *4*(3), 731–761. https://doi.org/10.3390/jcp4030034

Mourby, M., Mackey, E., Elliot, M., Gowans, H., Wallace, S. E., Bell, J., Smith, H., Aidinlis, S., & Kaye, J. (2018). Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. *Computer Law and Security Review*, *34*(2), 222–233. https://doi.org/10.1016/j.clsr.2018.01.002

Najmi, M., Sepehri, M., & Hashemi, S. (2010). The evaluation of business intelligence maturity level in Iranian banking industry. *Proceedings of the 2010 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, 466–470.

Nugraha, A. A., & Nasyuha, A. H. (2024). Integrating ISO 27001 and Indonesia's Personal Data Protection Law for data protection requirement model. *Journal of Information Systems and Informatics*, *6*(2), 1052–1069. https://doi.org/10.51519/journalisi.v6i2.754

Nuruddeen, U., Aimufua, G. I. O., Maijamaa, B., & Bassey, S. (2025). Assessment Of Data Protection And Privacy Implementation In Financial Institutions In Nigeria. *International Journal of Innovative Information Systems & Technology Research*, *13*(4), 125–134. https://doi.org/10.5281/zenodo.17490504

Otoritas Jasa Keuangan. (2014). *Surat Edaran Otoritas Jasa Keuangan Nomor 14/SEOJK.07/2014 tentang kerahasiaan dan keamanan data dan/atau informasi pribadi konsumen*. OJK..

Otoritas Jasa Keuangan. (2018). *Peraturan Otoritas Jasa Keuangan Nomor 2/POJK.03/2018 tentang penerapan bank sistemik dan capital surcharge*. OJK.

Otoritas Jasa Keuangan. (2021). *Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2021 tentang bank umum*. OJK.

Paul, E. O., Callistus, O., Somtobe, O., Esther, T., Somto, K.-A., Clement, O., & Ejimofor, I. (2023). Cybersecurity Strategies for Safeguarding Customer's Data and Preventing Financial Fraud in the United States Financial Sectors. *International Journal on Soft Computing (IJSC)*, *14*(3), 01–16. https://doi.org/10.5121/ijsc.2023.14301

Potgieter, C., Botha, J. H., & Lew, C. (2005). Evidence that use of the ITIL *framework* is effective. *Proceedings of the 18th Annual Conference of the National Advisory Committee on Computing Qualifications (NACCQ)*, 1–6..

Presiden Republik Indonesia. (2022). *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang perlindungan data pribadi*. Sekretariat Negara.

Putri, N. I., Komalasari, R., & Munawar, Z. (2020). Pentingnya Kemanan Data dalam Intelijen Bisnis. *Jurnal Sistem Informasi, J-SIKA*, *2*(2), 41–48.

Razi, F., Tuasikal, H., & Markus, D. P. (2024). Implementation and challenges of the Personal Data Protection Law in Indonesia. *Jurnal Indonesia Sosial Teknologi*, *5*(12), 6559–6565. https://doi.org/10.59141/jist.v5i12.1285

Realyvásquez-Vargas, A., Arredondo-Soto, K. C., Carrillo-Gutiérrez, T., & Ravelo, G. (2018). Applying the Plan-Do-Check-Act (PDCA) cycle to reduce the defects in the manufacturing industry. A case study. *Applied Sciences (Switzerland)*, *8*(11). https://doi.org/10.3390/app8112181

Reksoprodjo, A. A., Dachyar, M., & Pratama, N. R. (2024). A Decision-Making Model for Selecting Personal Data Protection Frameworks for Companies in Indonesia. *Journal of System and Management Sciences*, *14*(2), 156–171. https://doi.org/10.33168/JSMS.2024.0210

Riswandi, B. A., & Gultom, A. M. (2023). Protecting Our Mosts Valuable Personal Data: A Comparison Of Transborder Data Flow Laws In The European Union, United Kingdom, And Indonesia. *Prophetic Law Review*, *5*(2), 179–206. https://doi.org/10.20885/PLR.vol5.iss2.art3

Ryanto, K., & Tundjungsari, V. (2024). Standardization of Information Security Management in the Banking Sector using the ISO 27001:2022 Framework. *Journal La Multiapp*, *5*(4), 361–379. https://doi.org/10.37899/journallamultiapp.v5i4.1399

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A *Framework* for the Future of Cybersecurity. *Sustainability*, *15*(18), 1–32. https://doi.org/10.3390/su151813369

Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3), 21–45

Sarah Kuzankah, E., Zainab Efe, E., Adedolapo, O., & Abimbola Oluwatoyin, A. (2023). ISO 27001 in Banking: an Evaluation of Its Implementation and Effectiveness in Enhancing Information Security. *Finance & Accounting Research Journal*, *5*(12), 405–425. https://doi.org/10.51594/farj.v5i12.684

Sharma, N. K., & Dash, P. K. (2012). Effectiveness of ISO 27001 as an information security management system: An analytical study of financial aspects. *Far East Journal of Psychology and Business*, *9*(3), 42–55.

Štarchoň, P., & Pikulík, T. (2019). GDPR principles in data protection encourage pseudonymization through most popular and full-personalized devices: Mobile phones. *Procedia Computer Science*, *151*, 303–312. https://doi.org/10.1016/j.procs.2019.04.043

Stufflebeam, D. L. (2003). *The CIPP model for evaluation*. Paper presented at the Annual Conference of the Oregon Program Evaluators Network (OPEN), Portland, Oregon.

Stufflebeam, D. L., & Coryn, C. L. S. (2014). *Evaluation theory, models, and applications* (2nd ed.). Jossey-Bass.

Subawa, I. M. M. (2020). Protecting Personal Data in Financial Technology in Indonesia. *International Journal of Business, Economics and Law*, *22*(1), 59–68.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical & Computer Sciences (IJECS-IJENS)*, *11*(5), 23–29.

Susyanto, H. (2019). Pengaruh Kepimpinan, Keterlibatan Karyawan dan Kepuasan Kerja Terhadap Kesiapan untuk Berubah dalam Menghadapi Perubahan Organisasi. *Jurnal Ekonomi, Bisnis, Dan Akuntansi (JEBA)*, *21*(1).

Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal data protection law in Indonesia: Challenges and opportunities. *Indonesia Law Review*, *14*(2), 56–72. https://doi.org/10.15742/ilrev.v14n2.4

Umam, K. A., & Saripah, I. (2018). Using the Context, Input, Process and Product (CIPP) model in the evaluation of training programs. *International Journal of Pedagogy and Teacher Education (IJPTE)*, *2*, 183–194. https://doi.org/10.20961/ijpte.v2i1.26086

United Nations. (2015). *Universal declaration of human rights*. United Nations. https://www.un.org/en/about-us/universal-declaration-of-human-rights

Walhidayah, I., & Surendro, K. (2025). Development of an AI governance model for higher education using the Capability Maturity Model Integration (CMMI). *Jurnal Teknik Informatika (Jutif)*, *6*(4), 2001–2018. https://doi.org/10.52436/1.jutif.2025.6.4.4709

Wolters, P. T. J. (2018). The control by and rights of the data subject under the GDPR. *Journal of Internet Law*, *22*(1), 7–18

Wu, W., Shi, K., Wu, C. H., & Liu, J. (2022). 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*, *30*(3), 1–16. https://doi.org/10.4018/JGIM.20220701.oa2

Yassien, E. (2020). The challenges of capability maturity model integration application in the dynamic environment. *International Journal of Information Systems and Change Management*, *12*(1), 17–34. https://doi.org/10.1504/IJISCM.2020.112045

LAMPIRAN

Transkrip Wawancara

CIPP Model	Pertanyaan	Responden	Jawaban
Context	Sebelum UU PDP disahkan dan menjadi perhatian utama, bagaimana pandangan dan tingkat kesadaran Bank KBMI mengenai pentingnya perlindungan data pribadi nasabah? Apa yang menjadi pemicu utama kesadaran tersebut?	Business Branch Manager	Kalau sebelum Undang-Undang Perlindungan Data Pribadi ini disahkan, sebetulnya perbankan itu sudah mempunyai ketentuan ya, artinya terkait dengan perlindungan data-data dari nasabah yang dituangkan di dalam suatu ketentuan yang namanya rahasia bank dan rahasia jabatan. Rahasia jabatan itu adalah apa yang informasi apapun yang kita ketahui di fungsi jabatan kita, itu kita tidak boleh menginformasikannya keluar. Kemudian untuk rahasia bank sendiri, kami juga sebenarnya ada ketentuan itu, di mana rahasia bank adalah menyangkut ke rahasia lain yang sangat menyangkut terkait dengan Undang-Undang PDP. Kalau misalnya rahasia bank itu adalah semua informasi yang terkait nasabah, baik itu identitas, nama kemudian saldo transaksi dan lain-lain, itu memang harus dirahasiakan dan tidak boleh diinformasikan keluar sesuai dengan ketentuan yang berlaku.
	Apa pendorong utama bagi organisasi ini untuk memprioritaskan kepatuhan terhadap UU PDP?		Ya, sepertinya kalau ini memang harus terkait dengan ketentuan regulasi yang dikeluarkan oleh OJK dan Bank

	Apakah dorongan tersebut murni karena kewajiban hukum atau ada faktor lain seperti tuntutan nasabah atau reputasi?		Indonesia ya mas. Kita harus mematuhi terkait ketentuan rahasia bank dan rahasia jabatan. Tentunya disitu ada ketika ada pelanggaran disitu akan dikenakan sanksi dan itu akan apalagi impactnya itu akan ke risiko reputasi bagi bank itu. Sampai ketika suatu bank itu membocorkan terkait rahasia bank atau data-data dari nasabah, itu yang nanti akan menimbulkan suatu somasi atau komplain. Itu tentunya akan membuat reputasi dari suatu bank itu menjadi tidak baik ya. Dan kami di Bank BNI sangat menjaga ketentuan itu.
	Apakah inisiatif untuk sertifikasi dengan standar ISO 27001 dan ISO 27701 sudah ada sebelum UU PDP menjadi fokus atau justru UU PDP yang mendorong adopsi standar-standar ini sebagai *framework*?		Iya. Jadi inisiatif menerapkan sertifikat ISO 27001 ini sebetulnya itu inisiatifnya sudah berjalan mas. Hanya ini lebih komprehensif lagi ya. Lebih komprehensif lagi selain data dari rahasia bank, rahasia jabatan. Tentunya saat ini kan marak dengan apa yang disebut dengan marketing digital ya. Nah itulah yang lebih komprehensif lagi supaya benar-benar data dari nasi nasabah ini benar-benar lebih terlindungi lagi. Jadi fokus dari organisasi ataupun dari BNI terhadap undang-undang PDP ini tentunya tidak hanya terkait dengan informasi keamanan tetapi juga aspek dari privacy kemudian pengelolaan data pribadi secara menyeluruh. Jadi dikatakan informasi ini sebetulnya sudah melekat di ketentuan rahasia

			bank dan rahasia jabatan cuman ini lebih komprehensif lagi mas. Karena kita kan di dunia perbankan ini dinamis ya. Perkembangan yang dinamis apalagi dengan adanya marketing digital dan sebagainya. Nah itu yang lebih diatur lagi, lebih komprehensif terkait dengan hal ini.
	Bagaimana persepsi tim *developers* mengenai integrasi persyaratan UU PDP dan ISO 27001 dalam aktivitas pengembangan aplikasi? Apakah hal ini dipandang sebagai hambatan teknis atau sebagai standar yang perlu diadopsi?	Department Head Application Developer	Kalau dari sisi developer ya, mengingat keamanan data ini sudah merupakan hal yang menjadi bagian dalam setiap implementasi pengembangan makanya untuk hal tersebut dipandang sebagai suatu standar baru yang perlu diadopsi dari sisi pengembangan hingga nanti ke fase operasional.
	Sebelum regulasi ini diberlakukan, sejauh mana tingkat *awareness developers* terkait isu privasi data nasabah?		Untuk tingkat awareness dari masing-masing developer karena mungkin dari sisi developer kan atas aplikasi yang dikembangkan, kemudian melibatkan data apa, mungkin kan mempunyai pemahaman yang berbeda-beda tapi dengan undang-undang PDP ini bagaimana data tersebut disimpan kemudian nanti digunakan hingga nanti di archive maupun data tersebut sudah tidak digunakan lagi. Dengan knowledge yang masih bervariatif itu dengan implementasi UU PDP ini semuanya diharapkan memiliki pemahaman yang sama.

CIPP Model	Pertanyaan	Responden	Jawaban
Input	Sumber daya apa saja misalnya, anggaran khusus, pembentukan tim / departemen baru, pengadaan teknologi yang organisasi ini alokasikan secara spesifik untuk mempersiapkan dan mengimplementasikan UU PDP?	Business Branch Manager	Untuk mempersiapkan kepatuan terhadap UU PDP ini kami memang telah menyiapkan beberapa penyesuaian, termasuk alokasi anggaran tentunya ada. Termasuk untuk penyesuaian-penyesuaian terhadap aspek legalnya, kemudian penyesuaian-penyesuaian terhadap mungkin kegiatan transaksi pembukaan rekening nasabah di mana bersedia atau tidak nasabah dilakukan katakanlah promo-promo dan sebagainya, itu tergantung dari nasabah customer kami itu. Kalau memang tidak bersedia ditulis tidak ya kami akan tidak melakukan promo-promo melalui digital. Kemudian di sisi dari sumber daya manusia tentunya kami juga menyelenggarakan sosialisasi ya terkait dengan program kesadaran privasi bagi seluruh karyawan di kami untuk memahami kewajiban dan peran masing-masing terhadap kewajiban untuk menjaga data pribadi dari para nasabah customer kami.
	Kebijakan dan prosedur apa yang Bank KBMI kembangkan atau revisi sebagai landasan untuk program kepatuhan UU PDP?		Kebijakan dan prosedur ini tentunya sudah dilakukan penyesuaian setelah Undang-Undang PDP ini diberlakukan. Tentunya kita harus melaksanakan dengan baik termasuk dengan pelaksanaan apa yang tertuang di dalam Undang-Undang PDP tersebut. Intinya dalam Undang-Undang PDP

			tersebut kita sosialisasikan kemudian pegawai kita sosialisasikan untuk bisa diterapkan pada fungsi dan kegiatan kita pada saat melakukan aktivitas perbankan.
	Bagaimana struktur organisasi Bank KBMI terkait perlindungan data? Apakah Bank KBMI telah menunjuk fungsi DPO sesuai perintah UU PDP?		Ada fungsi data protection office itu sudah ada yang secara struktural berada di bawah divisi compliance. Fungsi ini memang menjadi bagian penting dalam pengawasan dan penerapan kebijakan perlindungan data pribadi di lingkungan BNI. Kemudian di setiap divisi atau unit terdapat PIC yang bertanggung jawab atas data nasabah baik yang keluar maupun masuk. Jadi data nasabah itu sangat terlindungi. Bahkan kita pada saat melakukan rapat internal pun kita memakai link-link yang rahasia yang tidak bisa dibuka untuk yang berwenang atau terbatas saja.
	Pelatihan dan program peningkatan kesadaran seperti apa yang diberikan kepada karyawan di semua tingkatan untuk memastikan mereka memahami kewajiban berdasarkan UU PDP dan kebijakan internal?		Intinya program pelatihan dan awareness selalu kami lakukan rutin, terutama mungkin untuk awareness itu kami sampaikan di event-event misalnya sharing moment kemudian kita adakan tiap bulan sekali bulan mutu. Kita selalu sosialisasikan, kita remind dan kita monitor pelaksananya serta kita evaluasi, artinya undang-undang PDP ini bisa terlaksana dengan baik, kemudian idealnya kami juga masing-masing per unit untuk memperdalam, misalnya disitu kan

			secara umum undang-undang PDP di kemukakan, itu di staff frontliner, di tim IT, di marketing kemudian di tim lainnya itu juga lebih didalami lagi supaya mereka dalam di lapangan ketika menjalankan fungsinya benar-benar mentaati undang-undang PDP ini.
	Apakah unit bisnis / unit compliance sudah memberikan *technical requirements* terkait regulasi privasi data?	Department Head Application Developer	Untuk technical requirement dari sisi perusahaan sudah dalam bentuk pedoman perusahaan dan nanti akses tersebut akan diterjemahkan menjadi technical requirement yang spesifik ke masing-masing aplikasi karena tiap-tiap aplikasi kan mempunyai karakteristiknya tersendiri.
	Tools apa saja yang digunakan organisasi untuk mengamankan data dari nasabah? Apakah ada *tools* atau *platform* tertentu yang diwajibkan?		Untuk tools mungkin beberapa kita menggunakan tools enkripsi, baik itu untuk mentransmisikan data maupun untuk menyimpan data dan apa itu untuk setiap pengembangan aplikasi, ada mekanisme testing security dan hal itu dilakukan secara berkala untuk memastikan bahwa setiap versi dari aplikasi ini mendapatkan support dan comply dengan security standard yang berlaku hari ini.

CIPP Model	Pertanyaan	Responden	Jawaban
Process	Bisa dijelaskan langkah-langkah konkret yang telah dan sedang dilakukan dalam proses implementasi?	Business Branch Manager	Untuk menjalankan kepatuan terhadap UU PDP ini langkah-langkah yang sudah dilakukan oleh kami itu memang dilakukan secara sistematis mas, jadi yang pertama dilakukan pemetaan dan inventarisasi data nasabah untuk mengetahui data apa saja yang disimpan kemudian di mana lokasinya. Kemudian setelah itu ditentukan peran dan tanggung jawab masing-masing pihak agar jelas siapa yang mengelola, memproses dan melindungi data tersebut. Setelah itu dilakukan juga penilaian terhadap risiko dan data protection impact assessment-nya untuk proses yang dianggap berisiko tinggi. Kami di organisasi juga menyiapkan namanya privacy notice di mana mekanisme persetujuan konsen bagi nasabah. Membangun alur kerja untuk menangani permintaan hak data, menilai risiko pihak ketiga seperti vendor, menyiapkan prosedur penanganan insiden termasuk notifikasi kebocoran data yang harus dilakukan maksimal di 72 jam. Di saat yang sama karyawan mendapatkan pelatihan. Namun yang terakhir ini artinya kebocoran data kami memang benar-benar consent di situ untuk tidak terjadi di kami karena sangat ketat untuk pemantauannya untuk pelaksanaan UU PDP ini.

	Bagaimana organisasi memonitor, meninjau dan mengaudit efektivitas dari kontrol yang telah diimplementasikan? Apakah ada audit internal atau eksternal yang secara spesifik mengacu pada kepatuhan UU PDP?		Kalau dari sisi pengawasan tentunya mulai dari leaders, kemudian pemimpin bidang sampai branch manager sampai dengan audit internal secara rutin juga melakukan pengawasan terhadap kerangka yang sudah ditetapkan oleh COBIT 2019 dan ISO 27001. Ini juga dilakukan secara audit dan dievaluasi untuk selalu disampaikan hasilnya kepada kami bagaimana kami untuk mengaplikasikannya agar benar-benar bisa terlaksana.
	Apa tantangan terbesar yang dihadapi selama proses implementasi ini?		Sebetulnya tantangan secara umum tidak ada, hanya kita wajib mensosialisasikannya terus, terutama kepada pegawai-pegawai baru ya yang masuk ya. Kemudian unit-unit yang sering membuat artinya di unit pemetaan, pengendalian dan data itu kadang-kadang kita juga tapi kita berkolaborasi kok mas, dengan tim pusat untuk mendapatkan pemetaan dan pengendalian data dimaksud. Pengelolaan vendor ini mas yang terpenting juga, itu juga kami informasikan bahwa ketika sudah menjadi vendor kami, tentunya dia juga harus mematuhi adanya undang undang PDP tadi. Di mana selain budaya organisasi perlu diarahkan semua pegawai melihat perlindungan data sebagai tanggung jawab bersama. Jadi bukan hanya tugas tim IT atau tim compliance saja.

			Bagaimana memahamkan semua pegawai untuk menggunakan standar dan membuat secara standar sehingga membuat organisasi ini perlu membuat peta kontrol yang terintegrasi. Tidak tumpang tindih dan semua berjalan selaras. Kemudian untuk tantangan teknis secara umum memang ada ya mas, karena kan kita ada UU PDP. Tapi sejauh ini dalam perjalanannya seperti legasi silo data, vendor kemudian budaya, overlap standar dan regulasi, kita monitor dengan baik dan itu sudah berjalan dengan baik.
	Bagaimana mekanisme teknis penghapusan data "*Right to be Forgotten*" diimplementasikan untuk memastikan data benar-benar tidak dapat dipulihkan?	Department Head Application Developer	Kalau untuk menutup rekening itu secara historis kan masih ada ya karena apa itu kalau tidak salah kan data nasabah kan disimpan untuk keperluan audit terutama itu 7-10 tahun. Mungkin nanti coba cari literature terkait surat edaran Bank Indonesia atau peraturan OJK.
	Bagaimana arsitektur sistem dirancang untuk memfasilitasi permintaan portabilitas data nasabah sehingga format yang dihasilkan aman, terstandarisasi dan dapat dibaca oleh mesin?		Kalau komunikasi antar sistem kan format standard ya. Misalkan ada JSON, XML atau mungkin ada beberapa juga formal transmisi yang berbasis ISO dan untuk networknya sendiri juga dedicated sih, kecuali mungkin yang lewat publik itu ada proses enkripsi ya dan bahkan beberapa transmisi data antar aplikasi pun juga ada proses enkripsi, terutama untuk data-data sensitif.

CIPP Model	Pertanyaan	Responden	Jawaban
Product	Dilihat dari sudut pandang organisasi, sejauh mana implementasi yang telah dilakukan berhasil membawa organisasi selaras dengan aspek hukum UU PDP?	Business Branch Manager	Kalau ini hasil dari implementasi undang-undang PDP ini setelah dievaluasi memang selaras ya. Karena itu memang dari sejak awal perbankan atau bank didirikan memang yang terkait dengan kerahasiaan nasabah ini sudah dituangkan di dalam ketentuan rahasia bank mas. Contohnya ini ketika diimplementasikan lagi searah dengan perkembangan atau dinamisasi dari transaksi perbankan ini akan lebih baik lagi mas. Karena nasabah tentunya akan merasa lebih aman, lebih safe gitu ya dan datanya benar-benar terlindungi dan itu sudah terbukti ya di para nasabah kami. Artinya sampai dengan saat ini kami selalu komit untuk menjaga kerahasiaan data-data pribadi dari para customer atau nasabah.
	Selain pemenuhan aspek hukum, bagaimana Bapak menilai dampak implementasi ini terhadap penguatan postur perlindungan data pribadi secara keseluruhan? Apakah Bapak melihat adanya peningkatan dalam keamanan data nasabah? Apakah ada penurunan jumlah atau dampak dari insiden kebocoran data sejak program ini diimplementasikan?		Ya, sejak program ini diimplementasikan tentunya sangat baik ya dan itu terbukti dari sampai saat ini kami bisa melaksanakan undang-undang PDP ini dengan baik dan nasabah merasa terlindungi, nasabahnya terbukti sampai saat ini reputasi dari Bank BNI tentunya sangat teruji ya untuk terkait dengan pelindungan data diri nasabah ini dan dengan demikian ketika merasa aman, artinya transaksi bisnisnya bisa meningkat di kami. Untuk kebocoran, alhamdulillah

			sampai saat ini tidak ada, jadi memang kami lakukan ini monitor dan evaluasinya dengan ketat untuk pelaksanaan UU PDP ini.
	Secara keseluruhan, apakah dengan penerapan ISO 27001 dan ISO 27701 terbukti efektif membantu organisasi untuk selaras dengan regulasi UU PDP? Di area mana standar ini paling memberikan nilai tambah?		Tentunya dengan ISO 27701 ini sebagai rangka kerja yang berfungsi sebagai compliance enabler melengkapi ISO 27001 untuk aspek tata kelola privacy, pemenuhan hak subjek data, pencatatan aktivitas proses data serta pelaksanaan DPIA. Dengan demikian ISO 27701 ini dapat digunakan sebagai model mapping untuk membantu suatu organisasi memenuhi berbagai peraturan perlingunan data termasuk UU PDP.
	Melihat ke depan, apa langkah selanjutnya bagi organisasi dalam menjaga dan terus meningkatkan kematangan program perlindungan data pribadi pasca implementasi awal UU PDP?		Selain kita memahami betul bahwa kita bekerja sebagai bankers harus menjaga berkait dengan kerahasiaan bank maka kita tanamkan terus ke segenap pegawai untuk melaksanakan hal ini dengan baik. Karena sekali lagi bahwa transaksi diperbankan itu yang diperlukan selain bisnis, aktivitas bisnis dan lain-lain tentunya suatu hal perlindungan data nasabah, data pribadi nasabah ini menjadi hal yang terpenting dan harus safe, benar-benar safe, terlindungi agar lebih nasabah dalam melaksanakan itu, melaksanakan transaksinya di kami itu lebih nyaman. Jadi kalau strategi saya kira semua sudah dilakukan seperti sosialisasi,

			kemudian pelatihan, kemudian pendalaman di masing-masing unit gitu kan ya dan itu kita tanamkan bahwa memang perlindungan data nasabah itu sangat diperlukan sehingga konkretnya dalam melaksanakan transaksi perbankan di unit-unit kita harus mematuhi hal tersebut karena ini terkait dengan kenyamanan nasabah menjadi kenyamanan customer ketika menjadi nasabah kami, salah satunya adalah minta dilindungi untuk data pribadinya.
	Apa dampak implementasi UU PDP terhadap: ▪ Proses bisnis inti misalnya, pembukaan rekening & pengajuan kredit? ▪ Hubungan dan kepercayaan dengan nasabah? ▪ Inovasi produk dan layanan digital?		Jadi dampak program ini tidak hanya terlihat dari sisi kepatuan hukum tetapi juga di proses bisnis inti dan hubungan nasabah dengan perkembangan inovasi atau digital marketing ya. Jadi proses bisnis inti misalnya di pembukaan rekening kita di situ ada concern di mana nasabah apakah bersedia dihubungi ketika berhubungi tim, ketika ada promo-promo, ada notifikasi dan lain-lain ketika mereka, kita akan lakukan implementasi sesuai dengan apa yang di maui nasabah. Ketika bersedia tentunya proses bisnis akan lebih berkembang karena kan di dalam bisnis bank itu kan terus dinamis ya. Ketika kita sampaikan promo-promo itu misalnya melalui sarana telpon atau WA atau dan lain-lain, dari sisi aspek hukum sudah sesuai dan dari sisi nasabah mungkin itu

			akan ternotif dengan baik dan tentunya hal ini akan menjadi perkembangan bisnis di kita dan untuk pengajuan kredit, misalnya untuk pengajuan kredit pun kami juga melakukan hal yang sama dan nasabah prinsip lebih senang, artinya selain terlindungi, dia juga bisa membuat pilihan bersedia atau tidak ketika ditawarkan untuk notif-notif atau info-info yang berasal dari bank tapi kebanyakan dan sebagian besar mereka mengikuti. Jadi sebetulnya mereka juga ingin ternotif info-info tersebut, mereka kan juga dari sisi kalau yang debitur, pengajuan kredit, tentunya kan mereka juga melaksanakan suatu usaha ya jadi dia juga membuka untuk informasi-informasi ada peluang-peluang apa, usaha yang bisa dikembangkan. Kemudian dari hubungan dan kepercayaan nasabah tentu menjadi hal yang penting juga terkait dengan pelaksanaan hal ini. Dengan nasabah terlindungi data dirinya, maka dia akan merasa nyaman bertransaksi di kami kemudian artinya pelaksanaan dengan UU PDP ini tentunya membuat nasabah lebih terlindungi lagi kemudian untuk inovasi dan produk layan digital seperti saya sampaikan, ketika nasabah sudah tentunya ini suatu perkembangan yang harus mau tidak mau kita ikuti karena

			tentunya adanya penyesuaian UU PDP yang perlindungan data diri nasabah yang komprehensif, nasabah tentunya akan senang juga. Dengan artinya dia memilih mau diinformasikan, di-notify atau tidak, sebagian besar dari kami, sebagian besar dari nasabah kami itu ingin mendapatkan informasi-informasi tersebut, dari sisi kami tentunya dengan senang hati menginformasikan terkait dengan transaksi-transaksi perbakan atau perkembangannya.
	Berdasarkan monitoring, apakah implementasi fitur keamanan tambahan seperti enkripsi end-to-end berdampak signifikan terhadap latensi sistem atau waktu respons aplikasi?	Department Head Application Developer	Kalau untuk proses enkripsi sendiri pastinya kan ada waktu tambahan ya yang diperlukan untuk decrypt maupun encrypt, akan tapi dengan perkembangan teknologi hardware maupun software kan, untuk respon time kita jaga agar sesuai dengan service level agreement yang telah disepakati untuk antar aplikasi.
	Bagaimana mekanisme pencatatan "*logging*" dirancang agar tetap informatif untuk penelusuran insiden "*debugging*" tanpa mengekspos data sensitif nasabah secara terbuka?		Kalau untuk logging kita sih biasanya kita menggunakan standard dari log database dan lognya itu sudah terencrypt sesuai mekanisme security yang ada di database tersebut, jadi tidak plain datanya sehingga mudah untuk dibaca oleh pihak tertentu, untuk akses ke logging tersebut juga spesifik di PIC dan terutama mungkin di teman-teman production ataupun teman-teman security.