Journal of Applied Informatics and Computing (JAIC)
Vol.x, No.x, Juli 201x, pp. xx~xx
e-ISSN: 2548-6861

Analisis Kesenjangan dan Kematangan Sistem Manajemen Keamanan Informasi Berdasarkan ISO/IEC 27001:2022 pada Perusahaan Penyedia Layanan Internet (ISP)

Fajar Budiman [1]*, Antoni Haikal [2]**
* Teknik Informatika, Politeknik Negeri Batam
** Rekayasa Keamanan Siber, Politeknik Negeri Batam
fajar.4332201028@students.polibatam.ac.id [1], antoni@polibatam.ac.id [2]

Article Info

Article history:

Received …
Revised …
Accepted …

Keyword:

gap analysis, IKAS, ISO/IEC 27001:2022, maturity assessment, ISP.

ABSTRACT

Perusahaan Penyedia Layanan Internet (ISP) mengelola data pribadi pelanggan dalam jumlah besar, sehingga penerapan Sistem Manajemen Keamanan Informasi (SMKI) menjadi kebutuhan operasional dan regulasi yang mendesak. Penelitian ini melakukan gap analysis dan penilaian kematangan pada sebuah ISP lokal di Batam menggunakan kerangka ISO/IEC 27001:2022 dan Instrumen Penilaian Kematangan Keamanan Siber (IKAS) dari BSSN. Pendekatan mixed method diterapkan melalui wawancara semi-terstruktur, observasi, telaah dokumen, dan instrumen penilaian terstruktur terhadap enam responden. Hasil gap analysis terhadap 93 kontrol Annex A menunjukkan tingkat kepatuhan sebesar 20,0%, dengan 32 kontrol berjalan parsial dan 48 kontrol belum tersedia. Skor IKAS sebesar 0,29 dari skala 0–5 (Level 1 – Awal) mengindikasikan bahwa praktik keamanan masih bersifat informal dan belum terdokumentasi. Penilaian risiko menghasilkan 10 skenario risiko (2 Critical, 6 High, 2 Medium). Berdasarkan temuan tersebut, penelitian menghasilkan delapan dokumen SMKI kritis meliputi SoA, RTP, Kebijakan Keamanan Informasi, dan lima SOP prioritas. Temuan mengonfirmasi bahwa kontrol Organizational dan People lebih lemah dibanding Technological, dan gap terbesar terdapat pada kontrol yang berkaitan dengan kewajiban UU PDP.

I. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat telah membawa manfaat besar bagi masyarakat. Indonesia sendiri diproyeksikan memiliki nilai ekonomi digital mencapai USD 130 miliar pada 2025 dengan lebih dari 200 juta pengguna internet, menempatkannya di antara pasar online terbesar di dunia [1]. Di saat yang sama, intensitas pertukaran data pribadi di berbagai platform digital meningkat tajam, sehingga memperbesar eksposur terhadap kejahatan siber, seperti pencurian identitas, penipuan daring, peretasan, dan penyalahgunaan data.

Kenyataannya, berbagai insiden kebocoran pada platform besar beberapa tahun terakhir memperlihatkan bahwa pengelolaan keamanan informasi bukan lagi opsi, tetapi keharusan strategis bagi penyelenggara layanan digital agar mampu menjaga kepercayaan pelanggan dan keberlangsungan bisnis. Kendala utama pada era digital adalah melindungi privasi dan data pribadi di tengah pesatnya inovasi teknologi, sehingga organisasi perlu membangun kerangka pengelolaan keamanan informasi yang efektif sekaligus tetap mendukung keberlanjutan layanan.

Pemerintah merespons melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) yang mengatur siklus hidup data pribadi, yaitu pengumpulan, pemrosesan, penyimpanan, pemutakhiran, pemindahtanganan, dan pemusnahan, serta hak subjek data dan kewajiban pengendali atau pemroses data [2]. Di tingkat pengukuran kapabilitas, BSSN menyediakan Instrumen Penilaian Kematangan Keamanan Siber (IKAS) sebagai alat self-assessment untuk memetakan kondisi saat ini, mengidentifikasi kesenjangan, dan menyusun prioritas peningkatan secara terstruktur [3].

e-ISSN: 2548-6861

Pada saat yang sama, ISO/IEC 27001:2022 menyediakan kerangka kerja berbasis risiko untuk membangun dan memelihara SMKI. Standar ini menggunakan pendekatan Plan-Do-Check-Act (PDCA), sehingga pengelolaan keamanan informasi tidak berhenti pada pembuatan dokumen, tetapi berlanjut pada implementasi, evaluasi, dan tindakan perbaikan. Justifikasi penggunaan ISO/IEC 27001:2022 dalam penelitian ini adalah karena standar tersebut memberikan kerangka sistematis untuk mengidentifikasi, mengelola, dan memitigasi risiko keamanan informasi serta menyediakan dasar penyusunan SoA dan Risk Treatment Plan.

Kerangka PDCA memberikan struktur bertahap yang relevan bagi ISP yang baru memulai implementasi SMKI, dimulai dari identifikasi kondisi kekinian melalui gap analysis dan penilaian kematangan, hingga penyusunan dokumen kebijakan, SOP, SoA, dan RTP sebagai rancangan siap implementasi.

Bagi sektor Internet Service Provider (ISP), kebutuhan ini bersifat kritikal karena karakteristik operasionalnya adalah pengelolaan data pelanggan berskala besar. Kondisi tersebut menuntut penerapan SMKI yang bukan hanya patuh terhadap standar global, tetapi juga selaras dengan kepatuhan lokal melalui UU PDP dan mampu menunjukkan tingkat kematangan secara terukur melalui IKAS.

Beberapa studi telah menilai kesiapan atau implementasi ISO/IEC 27001:2022 secara umum pada pusat data dan organisasi lain [7]-[11], tetapi penilaian terpadu belum menjelaskan secara eksplisit bagaimana menerapkan gap analysis ISO/IEC 27001:2022 dan maturity assessment IKAS khususnya di sektor ISP. Karena perusahaan target masih tahap awal, penelitian ini menekankan fokus pada gap analysis terhadap persyaratan ISO/IEC 27001:2022, maturity assessment berbasis IKAS, dan pemetaan rekomendasi dokumen kunci SMKI, seperti kebijakan, SOP kritikal, SoA, dan RTP untuk mempercepat kesiapan menuju penerapan ISO/IEC 27001:2022. Berikut rincian perbandingan sistematis studi-studi terdahulu dirangkum pada Tabel 1.

Tabel 1. Perbandingan studi terdahulu (state of the art)

Studi	**Metode**	**Objek**	**Instrumen**	**Kontribusi vs. Penelitian Ini**
Lajuba & Triwinarko [7] (2024)	Gap analysis kualitatif	Pusat data X	ISO 27001:2022	Pembanding pola Organizational/People lemah; objek beda sektor, level kematangan lebih tinggi
Chavez et al. [8] (2024)	Studi implementasi ISMS	Sektor Internet Services	ISO 27001:2022	Sektor sama (ISP), tanpa integrasi IKAS maupun UU PDP
Sinaga [10] (2024)	Model penilaian kepatuhan	Perguruan tinggi	ISO 27001:2022	Metode penilaian bertingkat sebanding; tanpa dimensi regulasi lokal
Jelita dkk. [11] (2024)	Evaluasi keamanan TI	PT Kano Teknologi Utama	Indeks KAMI 5.0 + ISO 27001:2022	Instrumen self-assessment pemerintah serupa; tidak spesifik ISP, tanpa UU PDP
Wijayanto dkk. [9] (2025)	Implementasi SMKI	PT XYZ	ISO 27001:2022	Sumber metode penilaian risiko likelihood×impact yang diadopsi
Penelitian ini	Gap analysis + IKAS + risk assessment	ISP lokal (ISP-X)	ISO 27001:2022 + IKAS BSSN + UU PDP	Integrasi tiga kerangka sekaligus, spesifik sektor ISP dengan pemetaan regulasi lokal

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk: (1) mengidentifikasi gap antara kondisi SMKI perusahaan saat ini dengan persyaratan kontrol ISO/IEC 27001:2022, (2) mengukur tingkat kematangan SMKI pada perusahaan ISP menggunakan IKAS, dan (3) memberikan rekomendasi perbaikan serta rencana perbaikan dalam bentuk kebijakan, prosedur, kontrol, SoA, dan RTP.

II. DASAR TEORI

Bagian ini merangkum kerangka teoritis yang mendukung penyelesaian tugas akhir dengan menyajikan konsep-konsep dan prinsip-prinsip yang relevan dalam konteks penelitian yang dilakukan.

A. Sistem Manajemen Keamanan Informasi (SMKI) dan ISO/IEC 27001:2022

Keamanan informasi adalah serangkaian kebijakan, proses, dan kontrol untuk melindungi aset informasi dari akses, penggunaan, pengungkapan, perubahan, atau perusakan yang tidak sah[4]. Keamanan informasi bertujuan menjaga kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) aset informasi. SMKI adalah kerangka kebijakan, prosedur, dan kontrol untuk mengelola keamanan informasi secara sistematis [4].

Penelitian ini menggunakan ISO/IEC 27001:2022 sebagai standar acuan karena sifatnya yang berbasis risiko dan berlandaskan siklus Plan-Do-Check-Act (PDCA). Standar ini relevan bagi ISP karena data pelanggan merupakan aset kritis yang perlu dikelola sesuai regulasi dan best practice internasional. Annex A versi 2022 memuat 93 kontrol yang dikelompokkan ke empat domain: Organizational (37), People (8), Physical (14), dan Technological (34) [4], [5].

B. Gap Analysis, SoA, dan RTP

Gap analysis membandingkan kondisi aktual organisasi dengan persyaratan ISO/IEC 27001:2022 untuk mengetahui kontrol yang sudah terpenuhi, masih parsial, atau belum tersedia[5]. Hasil gap analysis menjadi dasar penyusunan Statement of Applicability (SoA), yaitu dokumen yang memuat kontrol applicable, not applicable, justifikasi, status implementasi, dan rekomendasi perbaikan. Setelah risiko diidentifikasi, rekomendasi disusun dalam Risk Treatment Plan (RTP) yang memuat risiko prioritas, opsi perlakuan risiko, kontrol rujukan, PIC, target waktu, dan indikator keberhasilan.

C. Instrumen Penilaian Kematangan Keamanan Siber (IKAS) dan UU PDP dalam Konteks ISP

Instrumen Penilaian Kematangan Keamanan Siber (IKAS) digunakan untuk mengukur tingkat kematangan keamanan siber organisasi [3]. Dalam konteks ISP, pengukuran kematangan penting karena proses bisnis ISP melibatkan registrasi pelanggan, aktivasi layanan, pencatatan layanan, dukungan teknis, dan pengelolaan data pribadi pelanggan. UU PDP relevan karena data pelanggan perlu dikelola melalui prinsip persetujuan pemrosesan data, pemenuhan hak subjek data, keamanan pemrosesan, notifikasi insiden, retensi, dan penghapusan data [2]. Karena itu, penelitian ini memetakan kewajiban UU PDP ke kontrol ISO/IEC 27001:2022 sebagai bagian dari analisis dan rekomendasi perbaikan.

D. Pertanyaan Penelitian

Penelitian ini merupakan studi kasus tunggal (single case, N=1 organisasi) dengan pendekatan mixed method. Sebagai studi kasus tunggal, penelitian ini menggunakan pertanyaan penelitian (research question) untuk mengarahkan pengumpulan dan analisis data [12]. Berdasarkan kajian literatur dan kondisi umum ISP yang baru memulai implementasi SMKI, penelitian ini merumuskan dua pertanyaan penelitian sebagai arah pembahasan hasil:

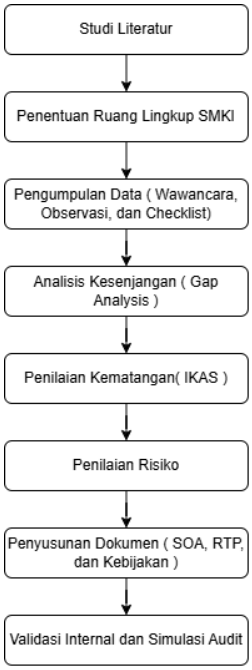
- RQ1: Apakah tingkat kematangan atau pemenuhan kontrol Organizational dan People lebih rendah dibandingkan Technological pada perusahaan ISP.
- RQ2: Apakah gap terbesar terdapat pada kontrol yang terkait kewajiban UU PDP, khususnya perlindungan data pribadi, hak subjek data, dan manajemen insiden.

III. METODE

Penelitian ini menggunakan pendekatan mixed method untuk memperoleh pemahaman menyeluruh mengenai kondisi dan kesiapan organisasi dalam menerapkan SMKI. Pendekatan kualitatif digunakan untuk menggali kondisi keamanan informasi, persepsi stakeholder, proses bisnis, dan tantangan implementasi kontrol keamanan melalui wawancara dan observasi. Untuk menjawab tujuan pertama (identifikasi gap), penelitian menggunakan checklist gap analysis ISO/IEC 27001:2022; untuk tujuan kedua (pengukuran kematangan), digunakan form IKAS BSSN; dan untuk tujuan ketiga (rekomendasi perbaikan), disusun SoA, RTP, dan dokumen SMKI kritikal berdasarkan integrasi hasil gap analysis, penilaian IKAS, pemetaan UU PDP, dan risk register. Pendekatan kuantitatif digunakan untuk mengukur tingkat kematangan dan kepatuhan melalui checklist ISO/IEC 27001:2022 dan form IKAS.

Ketiga instrumen analisis dalam penelitian ini, yaitu checklist gap analysis, form IKAS, dan pemetaan UU PDP, diterapkan terhadap sumber data wawancara, observasi, dan telaah dokumen yang sama, namun menjalankan fungsi analitis yang berbeda dan saling melengkapi. Gap analysis berfungsi sebagai diagnosis, yaitu mengukur kepatuhan ISP-X secara terperinci per kontrol terhadap 93 kontrol teknis Annex A ISO/IEC 27001:2022. Penilaian IKAS berfungsi sebagai konteks pembanding, yaitu menempatkan kondisi keamanan siber ISP-X pada skala kematangan nasional (Level 1-5) yang digunakan BSSN, dengan sudut pandang proses (Identifikasi, Proteksi, Deteksi, Penanggulangan dan Pemulihan) yang berbeda dari struktur kontrol ISO/IEC 27001:2022. Pemetaan UU PDP berfungsi sebagai penegasan kewajiban hukum, yaitu mengidentifikasi kontrol mana yang memiliki konsekuensi regulasi apabila tidak dipenuhi. Ketiga hasil analisis ini selanjutnya diintegrasikan pada tahap penilaian risiko dan penyusunan RTP sebagai dasar penentuan solusi dan prioritas mitigasi.

A. Alur Penelitian



Gambar 1. Alur tahapan penelitian

Penelitian ini dilaksanakan melalui tahapan yang sistematis untuk memastikan seluruh tujuan penelitian tercapai dengan baik. Alur tahapan penelitian (sebagaimana diilustrasikan pada Gambar 1) dijabarkan sebagai berikut:

Tabel 2. Tahapan penelitian dan keluaran penelitian

Tahapan Penelitian	Penjelasan
Studi Literatur	Mempelajari struktur ISO/IEC 27001:2022 (93 kontrol Annex A), Undang-Undang PDP No. 27 Tahun 2022, serta instrumen IKAS dari BSSN. Output: kerangka teori dan daftar kontrol untuk checklist.
Penentuan Ruang Lingkup SMKI	Memfokuskan pada proses pengelolaan data pelanggan (CRM, CS/CRM, NOC, dan infrastruktur pendukung). Mengidentifikasi aset informasi, sistem, unit kerja, dan aspek legal (UU PDP).
Pengumpulan Data	Menggunakan wawancara semi-terstruktur dengan 6 responden (Direktur, Manager IT, Head Admin, Staff NOC, Staff CS, Head Teknisi), observasi langsung, telaah dokumen, serta instrumen checklist ISO/IEC 27001:2022 dan form IKAS.

e-ISSN: 2548-6861

Gap Analysis	Membandingkan 93 kontrol Annex A terhadap kondisi aktual ISP-X. Skor 0 (tidak ada), 1 (parsial), 2 (penuh), atau N/A. Persentase kepatuhan dihitung per domain (Organizational, People, Physical, Technological).
Penilaian Kematangan (IKAS)	Mengisi form IKAS dari BSSN untuk mengukur kematangan pada empat domain: Identifikasi, Proteksi, Deteksi, Penanggulangan & Pemulihan. Nilai akhir (0–5) menentukan level kematangan (Level 1 – Awal hingga Level 5 – Inovatif).
Penilaian Risiko	Identifikasi aset kritis (data pelanggan, CRM, database, backup, dll.), ancaman, dan kerentanan. Penilaian semi-kuantitatif likelihood x impact (skala 1–5) menghasilkan 10 skenario risiko (2 Critical, 6 High, 2 Medium).
Penyusunan Dokumen SMKI	Berdasarkan gap, IKAS, risk register, dan pemetaan UU PDP, disusun 8 dokumen rekomendasi: SoA, RTP, Kebijakan Keamanan Informasi, serta 5 SOP prioritas (Kontrol Akses, Manajemen Insiden, Klasifikasi Informasi, Backup & Recovery, Hak Subjek Data).
Validasi Internal	Tahap lanjutan yang direncanakan dalam desain penelitian untuk memastikan kesesuaian dokumen dengan kondisi aktual dan kapasitas organisasi. Tahap konfirmasi akhir yang dilaksanakan ISP-X pada tahap adopsi SMKI, setelah dokumen selesai disusun (lihat Bab V).

B. Responden dan Instrumen Penelitian

Responden dipilih menggunakan purposive sampling karena penelitian membutuhkan pihak yang memahami proses bisnis dan pengelolaan data pelanggan secara langsung. Responden minimal berjumlah enam orang yang mewakili fungsi manajemen, IT/Infra, NOC, CS/CRM, administrasi/keuangan, dan teknisi. Jumlah enam responden ini dinilai representatif untuk ISP-X mengingat struktur organisasi yang ramping, di mana keenam fungsi tersebut mencakup seluruh lini yang bersinggungan langsung dengan aset informasi dan data pelanggan. Kombinasi responden ini menjaga validitas melalui triangulasi antar sumber, sebagaimana disarankan Creswell dan Plano Clark [6] dalam penelitian mixed method.

Tabel 3. Responden dan keterlibatan dalam penelitian

No	Peran/Jabatan	Keterlibatan dalam Penelitian
1	Direktur/Manajemen	Validasi komitmen, kebijakan, prioritas implementasi, dan dukungan sumber daya.
2	Manager IT/Infra	Validasi inventaris aset, sistem akses, backup, dan kontrol teknis tingkat umum.
3	Head Admin/Finance	Validasi pengelolaan data administrasi pelanggan dan dokumen kontrak.
4	Staff NOC	Validasi proses monitoring jaringan, penanganan insiden, dan log operasional.
5	Staff CS/CRM	Validasi proses pengelolaan data pelanggan, akses CRM, dan alur layanan pelanggan.
6	Head Teknisi	Validasi proses instalasi pelanggan, pengelolaan perangkat di lapangan, dan alur teknis.

Checklist ISO/IEC 27001:2022 menggunakan skala: 0 = tidak ada kontrol atau aktivitas terkait; 1 = kontrol parsial atau belum formal; 2 = kontrol telah diterapkan secara formal dan berkelanjutan.

Rumus kepatuhan checklist gap analysis dinyatakan sebagai berikut:

$$Kepatuhan\ (\%) = (\Sigma\ Skor\ Aktual / (2 \times n)) \times 100$$

Keterangan:

– Σ Skor Aktual = jumlah skor seluruh kontrol applicable, dengan setiap kontrol diberi skor 0 (tidak ada), 1 (parsial), atau 2 (diterapkan penuh);

– 2 = skor maksimum per kontrol, yaitu kondisi kontrol "diterapkan penuh";

– n = jumlah kontrol applicable = 80 kontrol, sesuai hasil pemetaan 93 kontrol Annex A terhadap ruang lingkup penelitian (lihat Bab IV.A).

Skala checklist 0/1/2 pada rumus ini mengadaptasi pendekatan penilaian tingkat kepatuhan kontrol keamanan informasi yang digunakan Nasser [13] dalam studi gap analysis ISO/IEC 27001 pada institusi pendidikan, yang kemudian disesuaikan dengan struktur 93 kontrol Annex A ISO/IEC 27001:2022 dan cakupan Statement of Applicability (SoA) pada penelitian ini.

Checklist ISO/IEC 27001:2022 disusun berdasarkan 93 kontrol Annex A yang dipetakan ke ruang lingkup penelitian, sedangkan form IKAS diperoleh dari format Excel terstruktur BSSN [3]. Form IKAS digunakan untuk menentukan level kematangan organisasi berdasarkan bukti observasi dan wawancara.

Setiap kontrol pada checklist gap analysis dinilai oleh satu narasumber utama yang memiliki kompetensi dan kewenangan langsung atas area kontrol tersebut, sebagaimana dipetakan pada Tabel 3, sehingga desain penelitian ini pada dasarnya menghindari kebutuhan mekanisme resolusi multi-rater untuk sebagian besar kontrol. Sebagai ilustrasi, kontrol terkait inventaris aset informasi (A.5.9) dijawab oleh Manager IT/Infra selaku penanggung jawab langsung, bukan oleh keenam responden sekaligus, sehingga tidak muncul perbedaan skor yang perlu dikonsensuskan. Untuk kontrol yang bersinggungan dengan lebih dari satu fungsi, misalnya kontrol akses (A.8.2) yang melibatkan baik Manager IT/Infra maupun Staff CS/CRM, triangulasi dilakukan melalui observasi langsung dan telaah dokumen sebagai pembanding atas jawaban wawancara, dan skor akhir ditetapkan berdasarkan kondisi yang paling konsisten dengan bukti observasi, bukan berdasarkan rata-rata atau pemungutan suara antar responden. Penelitian ini mengakui keterbatasan bahwa validitas instrumen checklist belum diuji melalui expert judgement atau uji keterbacaan secara formal sebelum digunakan di lapangan, dan hal ini menjadi salah satu rekomendasi untuk penelitian lanjutan.

C. Penilaian Risiko dan Prioritas RTP

Penilaian risiko dilakukan dengan pendekatan semi-kuantitatif mengadopsi metode matriks likelihood × impact

sebagaimana digunakan Wijayanto dkk. [9], dengan formula sebagai berikut:

$$Nilai\ Risiko = Likelihood \times Impact$$

Keterangan: Likelihood dan Impact masing-masing dinilai pada skala ordinal 1–5 berdasarkan hasil wawancara dan observasi terhadap kondisi aktual ISP-X, sehingga rentang Nilai Risiko adalah 1–25. Hasil perkalian dikategorikan ke dalam lima level sebagaimana Tabel 4 berikut.

Tabel 4. Kategorisasi level risiko

Level	Kategori	Nilai Risiko	Tindak Lanjut
I	Informational	1–2	Risiko dapat diterima tanpa pengendalian khusus
II	Low	3–4	Risiko dapat diterima tanpa pengendalian segera
III	Medium	6–9	Perlu pemantauan berkala
IV	High	12–16	Harus ada program penurunan risiko
V	Critical	20–25	Program penurunan risiko segera, prioritas utama

Untuk memudahkan pembacaan warna yang digunakan secara konsisten pada dokumen Risk Treatment Plan (SMKI-RTP-001), Tabel 5 menyajikan matriks Likelihood × Impact secara visual, di mana warna setiap sel merepresentasikan level risiko sesuai kategori pada Tabel 4: hijau (Informational/Low), kuning (Medium), oranye (High), dan merah (Critical).

Tabel 5. Matriks likelihood × impact (heatmap risiko)

Likelihood \ Impact	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Aset kritis diidentifikasi melalui kombinasi wawancara dan observasi langsung pada tahap pengumpulan data, kemudian diverifikasi bersama responden Manager IT dan Direktur untuk memastikan kelengkapan dan relevansinya terhadap proses bisnis inti ISP-X. Aset yang teridentifikasi meliputi data identitas pelanggan, CRM/Simple Apps, database pelanggan, email layanan, kredensial admin, repositori backup, perangkat monitoring/NOC, dan dokumen vendor. Risk assessment workshop melibatkan perwakilan keenam responden agar penilaian mencakup sudut pandang strategis, operasional, dan teknis secara seimbang.

Prioritas implementasi dalam RTP ditentukan berdasarkan: (1) level risiko (Critical dan High didahulukan); (2) keterkaitan dengan data pribadi pelanggan; (3) kewajiban UU PDP; (4) pengaruh terhadap banyak kontrol ISO/IEC 27001:2022; dan (5) kemudahan implementasi relatif. Dengan demikian, RTP tidak difokuskan secara eksklusif pada 48 kontrol dengan skor 0. Sebagaimana ditunjukkan pada Tabel 10, tiga dari sepuluh skenario risiko (R-01, R-05, dan R-09) justru bersumber dari kontrol yang telah berjalan parsial (skor 1), yaitu kontrol akses (A.8.2), backup informasi (A.8.13), dan keamanan fisik (A.7.4/A.7.10), menunjukkan bahwa kontrol parsial pun dapat menghasilkan risiko Critical/High apabila penerapannya belum konsisten atau belum terdokumentasi formal. Seluruh 80 kontrol applicable, baik 48 kontrol berskor 0 maupun 32 kontrol berskor 1, tetap memperoleh rekomendasi perbaikan yang didokumentasikan dalam SoA, sehingga tidak ada kontrol yang dibiarkan tanpa tindak lanjut. RTP secara spesifik mengangkat kontrol, baik berskor 0 maupun 1, yang teridentifikasi menghasilkan risiko Critical dan High sebagai tindakan mitigasi prioritas, sedangkan kontrol dengan risiko lebih rendah dicatat dalam SoA sebagai rencana jangka menengah. Risiko Critical dan High yang terkait data pelanggan, kontrol akses, consent, notifikasi insiden, backup, dan hak subjek data ditempatkan sebagai prioritas implementasi awal.

IV. HASIL DAN PEMBAHASAN

A. Hasil Gap Analysis ISO/IEC 27001:2022

Hasil gap analysis dilakukan terhadap seluruh 93 kontrol Annex A ISO/IEC 27001:2022. Dari 93 kontrol tersebut, sebanyak 80 kontrol dinilai applicable dan 13 kontrol dikategorikan Not Applicable (N/A), seluruhnya berada pada domain Technological (A.8) karena berkaitan dengan konfigurasi teknis perangkat dan beberapa control terkait dengan vendor pihak ketiga (Website) yang berada di luar ruang lingkup evaluasi teknis penelitian ini. Dari 80 kontrol applicable, tidak ada kontrol yang memperoleh skor 2 (diterapkan penuh), sebanyak 32 kontrol memperoleh skor 1 (parsial), dan 48 kontrol memperoleh skor 0 (belum ada). Tingkat kepatuhan keseluruhan dihitung sebagai: 32 / (2 x 80) x 100 = 20,0%.

Tabel 6. Rekapitulasi hasil gap analysis ISO/IEC 27001:2022 per domain

Domain	Total Kontrol	N/A	Applicable	Skor 2	Skor 1	Skor 0	Kepatuhan (%)
Organizational (A.5)	37	0	37	0	10	27	13,5%
People (A.6)	8	0	8	0	3	5	18,8%
Physical (A.7)	14	0	14	0	8	6	28,6%
Technological (A.8)	34	13	21	0	11	10	26,2%
Total	93	13	80	0	32	48	20,0%

Domain Organizational (A.5) memiliki tingkat kepatuhan terendah sebesar 13,5%. Dari 37 kontrol yang seluruhnya applicable, hanya 10 kontrol yang berjalan secara parsial dan 27 kontrol belum tersedia sama sekali. Gap terbesar terdapat pada kontrol-kontrol yang berkaitan dengan kebijakan keamanan informasi (A.5.1), penugasan peran dan tanggung jawab keamanan informasi (A.5.2), inventaris aset (A.5.9,

e-ISSN: 2548-6861

A.5.10), klasifikasi informasi (A.5.12, A.5.13, A.5.14), manajemen insiden (A.5.24-A.5.28), perlindungan PII (A.5.34), dan manajemen pemasok (A.5.19-A.5.23). Tidak adanya kebijakan keamanan informasi formal menjadi akar permasalahan yang berdampak pada hampir seluruh kontrol Organizational, karena kebijakan merupakan dokumen puncak yang menjadi acuan implementasi seluruh kontrol lainnya.

Domain People (A.6) memiliki tingkat kepatuhan 18,8% dengan 3 kontrol parsial dan 5 kontrol tidak ada. Gap utama mencakup: belum adanya program pelatihan dan kesadaran keamanan informasi yang terstruktur (A.6.3), ketentuan formal berupa perjanjian kerahasiaan (Non-Disclosure Agreement) yang mengatur kewajiban keamanan informasi karyawan belum teridentifikasi pada dokumentasi kepegawaian yang ditelaah (A.6.6), demikian pula prosedur formal pengelolaan hak akses bagi karyawan yang keluar atau berganti jabatan (A.6.5). Kontrol yang berjalan secara parsial umumnya adalah proses background screening dasar yang dilakukan secara informal tanpa panduan formal.

Domain Physical (A.7) memiliki tingkat kepatuhan tertinggi kedua sebesar 28,6% dengan 8 kontrol parsial dan 6 kontrol tidak ada. Kontrol yang berjalan parsial umumnya berkaitan dengan pengamanan fisik ruangan server dan perangkat NOC yang sudah dilakukan meskipun belum terdokumentasi dalam kebijakan formal. Gap yang masih ada mencakup penanganan media penyimpanan (A.7.10), pengamanan perangkat clear desk/clear screen (A.7.7), dan pemantauan keamanan fisik secara berkelanjutan (A.7.4).

Domain Technological (A.8) memiliki kepatuhan 26,2% dengan 21 kontrol applicable (13 kontrol berstatus N/A karena teknologi tidak digunakan dalam ruang lingkup). Dari 21 kontrol applicable, 11 kontrol berjalan parsial dan 10 kontrol tidak ada. Kontrol parsial mencakup monitoring jaringan, konfigurasi dasar perangkat, dan aktivitas backup yang sudah dilakukan tetapi belum diformalkan dalam kebijakan dan SOP tertulis. Kontrol yang belum ada mencakup manajemen kerentanan teknis (A.8.8), perlindungan dari malware yang terstruktur (A.8.7), enkripsi data (A.8.24), pengujian keamanan (A.8.29), dan pencatatan/logging yang formal (A.8.15, A.8.16).

Tabel 7. Kontrol prioritas hasil gap analysis

Kode Kontrol	Nama Kontrol	Skor	Gap Utama	Domain
A.5.1	Kebijakan Keamanan Informasi	0	Tidak ada kebijakan keamanan informasi formal	Organizational
A.5.2	Peran dan Tanggung Jawab KI	0	Belum ada penugasan peran SMKI formal	Organizational
A.5.9	Inventaris Aset Informasi	0	Tidak ada inventaris aset terdokumentasi	Organizational
A.5.12	Klasifikasi Informasi	0	Tidak ada skema klasifikasi data	Organizational
A.5.24	Manajemen Insiden - Perencanaan	0	Tidak ada prosedur manajemen insiden	Organizational
A.5.31	Persyaratan Legal/Regulasi	1	UU PDP belum dipetakan ke kebijakan internal	Organizational
A.5.34	Perlindungan PII	0	Tidak ada kebijakan pengelolaan data pribadi	Organizational
A.6.3	Kesadaran KI, Pendidikan, Pelatihan	0	Tidak ada program pelatihan keamanan	People
A.6.6	Perjanjian Kerahasiaan (NDA)	0	Tidak ada NDA atau klausul kerahasiaan	People
A.8.2	Hak Akses (Access Rights)	1	Akses diberikan informal, tidak ada RBAC	Technological
A.8.13	Backup Informasi	1	Backup tidak terjadwal, tidak ada uji restore	Technological
A.8.15	Logging	0	Tidak ada kebijakan logging dan retensi log	Technological
A.8.24	Penggunaan Kriptografi	0	Data pelanggan tidak dienkripsi at-rest	Technological

B. Hasil Penilaian Kematangan IKAS

Penilaian kematangan dilakukan menggunakan form Excel IKAS BSSN v1.2.1 [3] yang mencakup empat domain utama: Identifikasi, Proteksi, Deteksi, dan Penanggulangan & Pemulihan. Setiap domain memiliki sub-indikator yang dinilai berdasarkan bukti observasi, wawancara, dan telaah dokumen. Nilai total kematangan ISP-X adalah 0,29 dari skala 0–5, yang berada pada Level 1 - Awal. Kondisi ini menggambarkan bahwa praktik keamanan informasi masih bersifat informal, reaktif, dan belum terdokumentasi secara konsisten.

Berbeda dengan rumus kepatuhan checklist gap analysis yang dipaparkan eksplisit pada bagian III.B, nilai total IKAS (0,29) tidak diperoleh melalui rata-rata sederhana antar keempat nilai domain (yang menghasilkan 0,2725), melainkan melalui rata-rata terbobot (weighted average) sesuai formula baku yang melekat pada form Excel resmi IKAS BSSN v1.2.1:

$$\textit{Nilai Total IKAS} = (I \times 0{,}25) + (P \times 0{,}30) + (D \times 0{,}25) + (G \times 0{,}20)$$

Keterangan:

– I = nilai domain Identifikasi = 0,32; bobot 25%;

– P = nilai domain Proteksi = 0,41; bobot 30% (bobot tertinggi, mencerminkan penekanan IKAS BSSN pada domain Proteksi);

– D = nilai domain Deteksi = 0,31; bobot 25%;

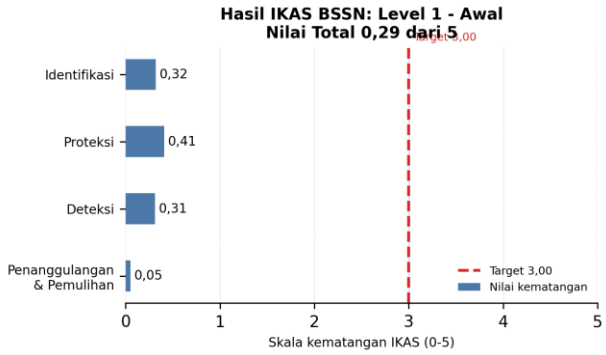
– G = nilai domain Penanggulangan dan Pemulihan = 0,05; bobot 20%;

– hasil akhir dibulatkan ke bawah (rounddown) pada dua desimal.

Perhitungan: (0,32 × 0,25) + (0,41 × 0,30) + (0,31 × 0,25) + (0,05 × 0,20) = 0,2905, dibulatkan ke bawah menjadi 0,29. Bobot I=25%, P=30%, D=25%, G=20% merupakan struktur baku instrumen IKAS BSSN v1.2.1 yang melekat pada rumus form Excel resmi, bobot ini mencerminkan penekanan domain Proteksi sebagai domain dengan kontribusi tertinggi terhadap penilaian kematangan keamanan siber organisasi. Berdasarkan kerangka pembobotan tersebut, hasil evaluasi beserta interpretasi tingkat kematangan untuk setiap domain direkapitulasi pada Tabel 8.

Tabel 8. Hasil penilaian kematangan IKAS per domain

Domain IKAS	Nilai	Level	Interpretasi Kondisi
Identifikasi	0,32	Level 1 - Awal	Inventaris aset, klasifikasi data, dan risk assessment belum tersedia secara formal. Tidak ada dokumentasi aset kritis dan tidak ada penilaian risiko yang pernah dilakukan.
Proteksi	0,41	Level 1 - Awal	Kontrol proteksi berjalan parsial secara informal, belum didukung kebijakan dan SOP formal. Kontrol akses tidak berbasis role, enkripsi belum diterapkan.
Deteksi	0,31	Level 1 - Awal	Monitoring operasional jaringan tersedia secara teknis, tetapi belum diarahkan sebagai security monitoring yang formal. Tidak ada review log keamanan.
Penanggulangan dan Pemulihan	0,05	Level 1 - Awal	Respons insiden dilakukan secara ad-hoc tanpa prosedur formal. Notifikasi dan pemulihan belum memiliki panduan tertulis.
Nilai Total IKAS	0,29	Level 1 - Awal	Keamanan informasi masih informal, belum terorganisir, dan belum memiliki tata kelola SMKI yang konsisten.



Gambar 2. Visualisasi tingkat kematangan IKAS per domain

Visualisasi pada Gambar 2 menunjukkan nilai IKAS ISP-X sebesar 0,29 dari skala 0–5. Nilai tersebut menempatkan organisasi pada Level 1 - Awal, yaitu kondisi awal yang ditandai dengan empat karakteristik utama. Pertama, tidak ada dokumentasi formal tentang aset informasi, risiko, atau kebijakan keamanan. Kedua, praktik keamanan dilakukan secara ad-hoc dan bergantung pada pengetahuan individu, bukan pada prosedur yang terdokumentasi. Ketiga, tidak ada mekanisme pengukuran atau pemantauan keamanan yang konsisten. Keempat, respons terhadap insiden dilakukan reaktif tanpa panduan yang jelas. Nilai tertinggi pada domain Proteksi (0,41) menunjukkan bahwa kontrol teknis yang sudah ada seperti Fortinet NGFW, antivirus, dan UPS menjadi modal awal yang dapat diformalkan. Nilai terendah pada domain Penanggulangan dan Pemulihan (0,05) menunjukkan bahwa seluruh aspek tanggap insiden dan pemulihan perlu dibangun dari awal. Untuk menjembatani kesenjangan tersebut, pada gambar 2 ditetapkan garis batas minimum (target) pada skor 3,00 (Level 3 - Terdefinisi). Penetapan target ini merujuk pada standar minimum penerapan SMKI yang formal, di mana seluruh proses telah didokumentasikan, distandarisasi, dan disahkan melalui kebijakan serta SOP. Target ini selaras dengan prasyarat kepatuhan tata kelola ISO/IEC 27001:2022 dan kewajiban administratif UU PDP yang menuntut adanya bukti tertulis, suatu persyaratan yang secara fundamental tidak dapat dipenuhi apabila organisasi masih beroperasi pada tingkat kematangan reaktif (Level 1 atau 2).

C. Pemetaan Temuan UU PDP terhadap ISO/IEC 27001:2022

Pemetaan kewajiban UU PDP ke kontrol ISO/IEC 27001:2022 dilakukan untuk mengidentifikasi kontrol-kontrol yang memiliki urgensi ganda, yaitu sekaligus menutup gap teknis dan memenuhi kewajiban hukum. Dalam konteks ISP-X, data pelanggan yang dikelola meliputi data identitas (nama, KTP, alamat), data kontak (nomor telepon, email), data layanan (paket, lokasi instalasi, perangkat), dan data transaksi (tagihan, riwayat pembayaran). Seluruh kategori data ini termasuk dalam definisi data pribadi menurut Pasal 4 UU No. 27 Tahun 2022.

Tabel 9. Pemetaan temuan UU PDP terhadap kontrol ISO/IEC 27001:2022

Area UU PDP	Gap Utama	Rekomendasi/Kontrol ISO
Consent/dasar pemrosesan (Ps. 20-28)	Kritis: consent dan privacy notice belum terdokumentasi.	Privacy notice, formulir consent, prosedur penarikan consent; A.5.31, A.5.34.
Hak subjek data (Ps. 5-16)	Tinggi: belum ada SOP permintaan akses, koreksi, atau hapus data.	Kanal pengajuan, target respons, pencatatan permintaan; A.5.34.
Notifikasi kegagalan data (Ps. 46)	Kritis: belum ada prosedur deteksi, eskalasi, dan notifikasi insiden.	SOP Manajemen Insiden dan template notifikasi maksimal 3 x 24 jam; A.5.24-A.5.27.
Keamanan pemrosesan data pribadi	Kritis: akses belum berbasis peran dan masih terjadi sharing password.	RBAC, password policy, review akses, offboarding; A.5.15-A.5.18, A.8.2-A.8.5.
Retensi/penghapusan data	Tinggi: belum ada aturan retensi dan penghapusan data pelanggan.	Kebijakan retensi, jadwal penghapusan, bukti pelaksanaan; A.5.33, A.8.10.
Backup dan pemulihan	Tinggi: backup informal dan uji restore belum terdokumentasi.	SOP Backup & Recovery, RTO/RPO, uji restore berkala; A.8.13.
Vendor/transfer data pihak ketiga	Tinggi: kontrak vendor belum memuat klausul keamanan dan NDA.	Klausul keamanan data, NDA, review pemasok; A.5.14, A.5.19-A.5.23.

Berdasarkan Tabel 9, terdapat tiga area dengan tingkat gap Kritis yang membutuhkan intervensi segera karena berpotensi menimbulkan sanksi administratif berdasarkan UU PDP [2]: (1) tidak adanya mekanisme consent terdokumentasi, yang

e-ISSN: 2548-6861

berarti seluruh pemrosesan data pelanggan saat ini berpotensi tidak memiliki dasar hukum yang sah; (2) tidak adanya prosedur notifikasi insiden, yang merupakan kewajiban hukum dengan tenggat 3 x 24 jam setelah kegagalan pelindungan data pribadi diketahui; dan (3) tidak adanya kontrol akses formal, yang membuka risiko akses tidak sah terhadap data pelanggan.

D. Risk Register dan Risk Treatment Plan

Penilaian risiko dilakukan menggunakan matriks semi-kuantitatif likelihood x impact (1-5) terhadap delapan aset kritis yang diidentifikasi dalam ruang lingkup SMKI. Risk assessment workshop melibatkan enam responden untuk memastikan konsistensi penilaian dari berbagai perspektif. Hasil penilaian menghasilkan 10 skenario risiko yang terdiri atas 2 risiko Critical, 6 risiko High, dan 2 risiko Medium. Ringkasan risk register dan rencana perlakuan risiko disajikan pada Tabel 11, sedangkan detail PIC, target waktu, dan indikator keberhasilan ditempatkan dalam dokumen RTP.

Untuk menunjukkan dasar kemunculan setiap skenario risiko secara eksplisit dan bukan hasil penilaian subjektif, Tabel 10 memetakan kesepuluh risiko pada RTP kembali ke kontrol gap analysis dan domain IKAS yang menjadi sumber temuannya. Kebijakan Keamanan Informasi (SMKI-KKI-001) tidak disertakan pada Tabel 10 karena kedudukannya sebagai dokumen fondasional yang melandasi seluruh kontrol (A.5.1, A.5.2), bukan dokumen yang lahir dari satu skenario risiko tertentu; posisinya sebagai prioritas tertinggi (1-Fondasi) dijelaskan tersendiri pada Tabel 13.

Tabel 10. Traceability risiko RTP terhadap gap analysis dan IKAS

ID	Kontrol Gap Analysis Asal	Domain IKAS Terkait	Dasar Kemunculan Risiko
R-01	A.8.2 (skor 1)	Proteksi (0,41)	Kontrol parsial (akses informal, tanpa RBAC) pada Tabel 7
R-02	A.5.34 (skor 0)	Proteksi (0,41)	Kontrol tidak ada (kebijakan PII) pada Tabel 7
R-03	A.5.24 (skor 0)	Penanggulangan & Pemulihan (0,05)	Kontrol tidak ada (manajemen insiden) pada Tabel 7; nilai IKAS terendah
R-04	A.8.15 (skor 0)	Deteksi (0,31)	Kontrol tidak ada (logging) pada Tabel 7
R-05	A.8.13 (skor 1)	Proteksi (0,41)	Kontrol parsial (backup tidak terjadwal) pada Tabel 7
R-06	A.8.16 (terkait, skor 0)	Deteksi (0,31)	Monitoring teknis ada namun belum diarahkan sebagai security monitoring formal
R-07	A.5.9 (skor 0)	Identifikasi (0,32)	Kontrol tidak ada (inventaris aset) pada Tabel 7; nilai IKAS Identifikasi rendah
R-08	A.6.3 (skor 0)	Proteksi (0,41)	Kontrol tidak ada (kesadaran KI/pelatihan) pada Tabel 7
R-09	A.7.4/A.7.10 (parsial)	Proteksi (0,41)	Kontrol fisik berjalan parsial, belum terdokumentasi formal
R-10	A.5.19–A.5.23 (skor 0)	Identifikasi (0,32)	Kontrol tidak ada (manajemen pemasok) pada Tabel 7

Tabel 11. Ringkasan risk register dan risk treatment plan

ID/Level	Aset Terdampak	Risiko Utama	Rencana Perlakuan
R-01 Critical	Data identitas pelanggan, CRM	Akses tidak sah ke data pelanggan.	RBAC, password policy, review akses, SOP Kontrol Akses.
R-02 Critical	Database pelanggan, formulir registrasi	Pemrosesan PII tanpa consent sah.	Privacy notice, consent, penarikan consent, SOP Hak Subjek Data.
R-03 High	Sistem CRM, email layanan	Kegagalan notifikasi insiden.	SOP Manajemen Insiden, eskalasi, template notifikasi 3 x 24 jam.
R-04 High	Log sistem, CRM, email	Insider threat tanpa jejak audit.	Logging CRM/email, larangan sharing password, review log.
R-05 High	Repositori backup, database	Kegagalan pemulihan data.	Jadwal backup, uji restore triwulanan, dokumentasi RTO/RPO.
R-06 High	Perangkat NOC, jaringan	Aktivitas berbahaya tidak terdeteksi.	Security monitoring NOC dan review log berkala.
R-07 High	Aset informasi (semua)	Kerentanan tidak teridentifikasi.	Inventaris aset, risk assessment tahunan, pembaruan SoA dan risk register.
R-08 High	Karyawan, data pelanggan	Social engineering/kelalaian insider.	Security awareness, NDA karyawan, mekanisme pelaporan insiden.
R-09 Medium	Server, perangkat NOC, ruang server	Akses fisik tidak sah.	Access control ruang server, log tamu, rencana CCTV.
R-10 Medium	Data pelanggan, layanan ISP	Insiden dari vendor/mitra.	Klausul keamanan data, NDA/vendor checklist, review pemasok.

E. Dokumen Rekomendasi SMKI

Berdasarkan integrasi hasil gap analysis, penilaian kematangan IKAS, pemetaan UU PDP, dan risk register, penelitian menghasilkan delapan dokumen rekomendasi SMKI yang bersifat strategis dan manajerial. Ringkasan dokumen ditampilkan pada Tabel 12, termasuk kode dokumen yang digunakan secara konsisten pada penelitian ini dengan format SMKI-[Kategori]-[Nomor Urut], yaitu SOA (Statement of Applicability), RTP (Risk Treatment Plan), KKI (Kebijakan Keamanan Informasi), dan SOP (Standar Prosedur Operasional), diikuti nomor urut penyusunan dokumen. Dokumen-dokumen ini dirancang sebagai paket awal SMKI yang realistis untuk diimplementasikan oleh ISP-X mengingat kondisi kematangan yang masih berada di Level 1.

Tabel 12. Dokumen rekomendasi SMKI prioritas

No	Kode Dokumen	Dokumen	Pokok Isi	Kontrol ISO yang Didukung
1	SMKI-SOA-001	Statement of Applicability (SoA)	Daftar 93 kontrol Annex A, status applicable/N/A, skor kondisi saat ini, justifikasi penerapan/pengecualian, dan rekomendasi perbaikan per kontrol	Seluruh Annex A
2	SMKI-RTP-001	Risk Treatment Plan (RTP)	Daftar 10 skenario risiko, opsi perlakuan risiko, tindakan mitigasi spesifik, PIC, target waktu, dan indikator keberhasilan	A.5.15, A.5.24, A.5.31, A.5.34, A.8.2, A.8.13, A.6.3, A.6.6
3	SMKI-KKI-001	Kebijakan Keamanan Informasi	Komitmen manajemen, tujuan keamanan informasi, ruang lingkup SMKI, peran dan	A.5.1, A.5.2

			tanggung jawab, serta acuan regulasi (ISO 27001, UU PDP)	
4	SMKI-SOP-001	SOP Kontrol Akses	Prinsip least privilege, matriks RBAC, prosedur onboarding/offboarding, password policy, dan jadwal review akses	A.5.15-A.5.18, A.8.2-A.8.5
5	SMKI-SOP-002	SOP Manajemen Insiden	Klasifikasi insiden, alur deteksi-eskalasi-respons-pemulihan, template notifikasi ke regulator dan pelanggan sesuai UU PDP	A.5.24-A.5.27
6	SMKI-SOP-003	SOP Klasifikasi Informasi	Skema klasifikasi data (Publik, Internal, Rahasia, Sangat Rahasia), penandaan, dan penanganan data pelanggan sesuai kategori	A.5.12-A.5.14
7	SMKI-SOP-004	SOP Backup & Recovery	Jadwal backup, jenis backup (full/incremental), lokasi penyimpanan, prosedur restore, target RTO/RPO, dan jadwal uji restore	A.8.13
8	SMKI-SOP-005	SOP Hak Subjek Data	Kanal pengajuan permintaan hak data, prosedur verifikasi identitas pemohon, target waktu respons (maks. 30 hari), dan dokumentasi permintaan	A.5.34

Prioritas implementasi dokumen ditetapkan berdasarkan tingkat risiko dan kewajiban regulasi. Kebijakan Keamanan Informasi harus disusun pertama karena menjadi landasan bagi seluruh dokumen lainnya. SOP Kontrol Akses dan SOP Manajemen Insiden diprioritaskan berikutnya karena berkaitan langsung dengan risiko Critical (R-01 dan R-02) serta kewajiban UU PDP yang bersifat imperatif. SOP Backup & Recovery dan SOP Hak Subjek Data juga bersifat mendesak karena berkaitan dengan risiko High dan kewajiban hukum. SOP Klasifikasi Informasi, SoA, dan RTP dapat disusun paralel setelah kebijakan utama tersedia.

Merujuk pada lima kriteria prioritas yang telah ditetapkan pada bagian III.C (level risiko, keterkaitan data pribadi pelanggan, kewajiban UU PDP, cakupan kontrol ISO/IEC 27001:2022, dan kemudahan implementasi), Tabel 13 menunjukkan operasionalisasi kriteria tersebut terhadap kedelapan dokumen SMKI yang dihasilkan. Dokumen dengan keterkaitan risiko Critical/High dan kewajiban UU PDP berkategori Kritis ditempatkan pada prioritas tertinggi, sementara dokumen dengan cakupan luas namun bergantung pada ketersediaan dokumen lain (SoA, RTP) ditempatkan pada tahap paralel setelah fondasi kebijakan tersedia.

Tabel 13. Dasar penentuan prioritas dokumen SMKI

Dokumen	Risiko & Kewajiban UU PDP	Cakupan Kontrol	Prioritas
Kebijakan Keamanan Informasi	Landasan seluruh kontrol dan kewajiban regulasi	A.5.1, A.5.2	1 – Fondasi
SOP Kontrol Akses	R-01 (Critical); keamanan pemrosesan data (Kritis)	8 kontrol	2 – Mendesak
SOP Manajemen Insiden	R-03 (High); notifikasi kegagalan data (Kritis)	4 kontrol	2 – Mendesak
SOP Hak Subjek Data	R-02 (Critical); consent & hak subjek data (Kritis/Tinggi)	1 kontrol	2 – Mendesak
SOP Backup & Recovery	R-05 (High); backup dan pemulihan (Tinggi)	1 kontrol	3 – Penting
SOP Klasifikasi Informasi	Tidak terhubung risiko Critical/High spesifik	3 kontrol	4 – Paralel
SoA	Mencakup seluruh 10 skenario risiko secara administratif	Seluruh Annex A	4 – Paralel
RTP	Mencakup seluruh 10 skenario risiko	8 kontrol lintas domain	4 – Paralel

Sebagai ilustrasi substansi dokumen yang dihasilkan, Kebijakan Keamanan Informasi (SMKI-KKI-001) memuat ketentuan eksplisit terkait pengelolaan data pelanggan, di antaranya kewajiban memperoleh persetujuan (consent) yang sah sebelum memproses data pribadi kecuali terdapat dasar hukum lain (merujuk UU PDP Pasal 20-28), serta kewajiban notifikasi kepada pelanggan dan Komnas PDP dalam batas waktu 3×24 jam apabila terjadi kegagalan pelindungan data pribadi (merujuk UU PDP Pasal 46). SOP Manajemen Insiden (SMKI-SOP-002) menjabarkan lebih lanjut format notifikasi kepada pelanggan, yang wajib memuat deskripsi singkat insiden, estimasi jumlah pelanggan terdampak, tindakan yang telah dan sedang diambil, serta langkah yang disarankan kepada pelanggan. Pada dokumen Risk Treatment Plan (SMKI-RTP-001), setiap skenario risiko dilengkapi rincian kerentanan spesifik dan tindakan mitigasi konkret; sebagai contoh, risiko R-01 (akses tidak sah terhadap data pelanggan) diidentifikasi memiliki kerentanan berupa ketiadaan Role-Based Access Control (RBAC), praktik berbagi kata sandi antarkaryawan, serta ketiadaan audit trail akses pada sistem CRM, dengan tindakan mitigasi berupa implementasi RBAC, penerapan kebijakan kata sandi dengan rotasi setiap 90 hari, dan aktivasi log akses yang direview mingguan oleh Manager IT.

Sebagai bukti substansi yang bersifat kutipan langsung (bukan ringkasan atau parafrase), berikut disajikan cuplikan verbatim dari dokumen SMKI yang dihasilkan.

> *"Mendapatkan persetujuan (consent) yang sah dari pelanggan sebelum memproses data pribadinya, kecuali terdapat dasar hukum lain yang berlaku (UU PDP Pasal 20-28)."*
>
> *"Memberikan notifikasi kepada pelanggan dan otoritas terkait dalam batas waktu 3x24 jam apabila terjadi kegagalan pelindungan data pribadi (UU PDP Pasal 46)."*
>
> — Kutipan langsung dari Kebijakan Keamanan Informasi (SMKI-KKI-001), Bagian 7 – Kebijakan Pengelolaan Data Pelanggan

Tahap Validasi Internal dan Simulasi Audit yang dicantumkan pada alur metode penelitian (Gambar 1, Tabel 2) merupakan tahap konfirmasi akhir yang secara lazim

e-ISSN: 2548-6861

dilaksanakan oleh pihak organisasi setelah dokumen SMKI diadopsi secara formal. Seluruh dokumen SMKI yang menjadi luaran penelitian ini, yaitu SoA, RTP, Kebijakan Keamanan Informasi, dan lima SOP prioritas, telah selesai disusun secara lengkap berdasarkan hasil gap analysis, penilaian IKAS, dan pemetaan UU PDP, sehingga siap digunakan ISP-X sebagai dasar pelaksanaan validasi internal dan simulasi audit pada tahap adopsi SMKI berikutnya.

F. Pembahasan Pertanyaan Penelitian

Pertanyaan penelitian pertama (RQ1) menanyakan apakah tingkat kematangan atau pemenuhan kontrol Organizational dan People lebih rendah dibandingkan Technological pada perusahaan ISP. Temuan penelitian ini menjawab RQ1 secara afirmatif: kepatuhan domain Organizational hanya 13,5% dan People 18,8%, sedangkan Technological mencapai 26,2%. Pola ini konsisten dengan temuan Lajuba dan Triwinarko [7] pada konteks pusat data, meskipun angka absolut berbeda karena ISP-X masih berada di Level 1 sementara pusat data X berada pada level kematangan yang lebih tinggi. Hal ini menunjukkan bahwa organisasi yang baru memulai SMKI cenderung mengabaikan fondasi tata kelola dan aspek manusia, dan lebih mengandalkan teknologi yang sudah tersedia secara operasional.

Pertanyaan penelitian kedua (RQ2) menanyakan apakah gap terbesar terdapat pada kontrol yang terkait kewajiban UU PDP. Temuan penelitian ini juga menjawab RQ2 secara afirmatif: seluruh kontrol yang dipetakan ke kewajiban UU PDP memperoleh skor 0 kecuali A.5.31 (skor 1). Ini berarti lima dari tujuh area kewajiban UU PDP yang diidentifikasi (consent, hak subjek data, notifikasi insiden, kontrol akses, dan backup) tidak memiliki kontrol sama sekali. Temuan ini mengonfirmasi bahwa integrasi ISO/IEC 27001:2022 dengan UU PDP sebagaimana disarankan Nugraha dan Nasyuha [1] bukan hanya relevan secara akademis, tetapi juga mendesak secara praktis bagi ISP-X.

V. KESIMPULAN

Hasil gap analysis menunjukkan bahwa tingkat kepatuhan ISO/IEC 27001:2022 pada ISP-X adalah 20,0%. Dari 93 kontrol Annex A, 80 kontrol dinilai applicable dan 13 kontrol berada di luar ruang lingkup evaluasi teknis penelitian. Tidak ada kontrol yang terpenuhi penuh, 32 kontrol berjalan parsial, dan 48 kontrol belum tersedia.

Hasil IKAS dari file Excel BSSN v1.2.1 menunjukkan nilai kematangan 0,29 dari skala 0–5, atau Level 1 - Awal. Kondisi ini menggambarkan bahwa praktik keamanan informasi masih bersifat informal, belum terdokumentasi secara memadai, dan belum memiliki tata kelola SMKI yang konsisten.

Risk assessment menghasilkan 10 risiko, terdiri atas 2 Critical, 6 High, dan 2 Medium. Risiko paling prioritas berkaitan dengan akses tidak sah terhadap data pelanggan, pemrosesan PII tanpa consent, kegagalan notifikasi insiden, dan kelemahan backup serta pemulihan.

Rekomendasi perbaikan disusun dalam bentuk SoA, RTP, kebijakan keamanan informasi, dan SOP kritikal. Rekomendasi ini mempertahankan batasan proposal, yaitu fokus pada evaluasi kebijakan, prosedur, kontrol manajerial, dan tata kelola, bukan konfigurasi teknis perangkat.

Penelitian selanjutnya disarankan melaksanakan validasi internal dan simulasi audit terhadap dokumen SMKI yang telah disusun, melibatkan manajemen dan tim teknis ISP-X, sebagai prasyarat sebelum implementasi; memperluas ruang lingkup ke audit teknis konfigurasi perangkat; melakukan pengujian efektivitas kontrol setelah implementasi; menguji validitas instrumen checklist melalui expert judgement secara formal; serta melakukan evaluasi ulang IKAS untuk mengukur peningkatan kematangan setelah roadmap dilaksanakan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Politeknik Negeri Batam, Program Studi Rekayasa Keamanan Siber, serta dosen pembimbing atas bimbingan dan dukungan selama pelaksanaan penelitian ini. Terima kasih juga disampaikan kepada pihak manajemen dan staf ISP-X yang telah bersedia meluangkan waktu sebagai responden dan memberikan akses untuk pengumpulan data.

DAFTAR PUSTAKA

[1] A. A. Nugraha and A. H. Nasyuha, "Integrating ISO 27001 and Indonesia's Personal Data Protection Law for data protection requirement model," Journal of Information Systems and Informatics, vol. 6, no. 2, pp. 1052-1063, 2024, doi: 10.51519/journalisi.v6i2.754.

[2] Republik Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, 2022.

[3] Badan Siber dan Sandi Negara, Panduan Pengisian Instrumen Penilaian Kematangan Keamanan Siber (IKAS), 2024.

[4] ISO/IEC, ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements, 2022.

[5] ISO/IEC, ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security controls, 2022.

[6] J. W. Creswell and V. L. Plano Clark, Designing and Conducting Mixed Methods Research, 3rd ed. Thousand Oaks, CA: SAGE Publications, 2018.

[7] A. S. Lajuba and A. Triwinarko, "Evaluasi penerapan standar ISO/IEC 27001:2022 di pusat data X," Journal of Applied Informatics and Computing, 2024.

[8] J. Chavez, C. Guerrero, and R. Vilchez, "Implementation of ISMS 27001:2022 in Internet Services Sector," IEEE Confluence, 2024.

[9] D. T. Wijayanto, R. R. Saedudin, and M. T. Kurniawan, "Implementasi ISO 27001:2022 sebagai kerangka manajemen keamanan informasi untuk meningkatkan kepatuhan regulasi di PT XYZ," E-Proceedings of Telkom University, 2025.

[10] R. Sinaga, "Pengembangan Model Penilaian Kepatuhan Salah Satu Perguruan Tinggi Terhadap Standar ISO 27001:2022," JuTISI, vol. 9, no. 3, pp. 381-394, 2024, doi: 10.28932/jutisi.v9i3.6850.

[11] L. D. A. Jelita, M. N. Al Azam, and A. Nugroho, "Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/IEC 27001:2022," Jurnal Saintekom, vol. 14, no. 1, pp. 84-94, 2024, doi: 10.33020/saintekom.v14i1.623.
[12] R. K. Yin, Case Study Research and Applications: Design and Methods, 6th ed. Thousand Oaks, CA: SAGE Publications, 2018.
[13] A. A. Nasser, "Information security gap analysis based on ISO 27001:2013 standard: A case study of the Yemeni Academy for Graduate Studies, Sana'a, Yemen," International Journal of Scientific Research in Multidisciplinary Studies, vol. 3, no. 11, pp. 1-7, Dec. 2017.