Jurnal Informatika: Jurnal pengembangan IT

Vol. 11, No. 2, 2026
ISSN : 2477-5126, DOI:10.30591/jpit.v11i2.2026

Analisis dan Penilaian Manajemen Risiko Keamanan Informasi Menggunakan SNI ISO/IEC 27005:2022 pada Aplikasi One Data Instansi XYZ

Yudhi Prasetya [1], Kalamullah Ramli [2]
[1,2]Fakultas Teknik, Universitas Indonesia, Indonesia
yudhi.prasetya@ui.ac.id, kalamullah.ramli@ui.ac.id

Info Artikel

Riwayat Artikel:

Received 20-02-2026
Revised 26-06-2026
Accepted 01-07-2026

Abstract *– The One Data application at XYZ Agency is a strategic data portal supporting bureaucratic reform and civil service governance. The high strategic value of this managed data increases information security risks. This study aims to design an information security risk management framework for the application based on SNI ISO/IEC 27005:2022, prioritize risk treatments, and validate the design using IKASANDI guidelines. Research methods involved inventorying assets, identifying threats and vulnerabilities, formulating risk scenarios, and evaluating risks using a 5x5 consequence-likelihood matrix aligned with PermenPANRB No. 43 of 2021. The evaluation identified 30 assets, 21 threat types, and 61 risk scenarios (33 requiring mitigation, 28 acceptable). Critical findings highlighted insider threats on VMs, operating systems, and web servers; database server availability; privileged account abuse; and data center dependencies. Risk treatment recommendations were mapped to SNI ISO/IEC 27002:2022 and IKASANDI controls. Through simulated validation, the proposed design projected an IKASANDI score increase from 1.65 to 2.24 and an average risk score reduction from 12.07 to 6.31, shifting all scenarios into the acceptable category. In conclusion, applying SNI ISO/IEC 27005:2022 yields a structured risk management design that supports the continuous monitoring and improvement of the information security management system for the One Data Application.*

Keywords: *IKASANDI, Information Security Risk Management, One Data Application, SNI ISO/IEC 27005:2022, SNI ISO/IEC 27002:2022*

Corresponding Author:

Yudhi Prasetya

Email: yudhi.prasetya@ui.ac.id

Abstrak *– Aplikasi One Data di Instansi XYZ merupakan portal data strategis yang mendukung reformasi birokrasi dan tata kelola aparatur sipil negara. Tingginya nilai strategis data tersebut meningkatkan risiko keamanan informasi. Penelitian ini bertujuan merancang kerangka manajemen risiko keamanan informasi pada aplikasi tersebut mengacu pada SNI ISO/IEC 27005:2022, memprioritaskan perlakuan risiko, dan memvalidasi rancangan menggunakan pedoman IKASANDI. Metode penelitian meliputi inventarisasi aset, identifikasi ancaman dan kerentanan, perumusan skenario risiko, serta evaluasi risiko menggunakan matriks 5×5 konsekuensi-kemungkinan yang selaras dengan PermenPANRB No. 43 Tahun 2021. Evaluasi mengidentifikasi 30 aset, 21 jenis ancaman, dan 61 skenario risiko (33 memerlukan mitigasi, 28 dapat diterima). Temuan kritis menyoroti insider threat pada VM, sistem operasi, dan web server; ketersediaan database; penyalahgunaan akun privilese; serta ketergantungan pada data center. Rekomendasi perlakuan risiko dipetakan pada kontrol SNI ISO/IEC 27002:2022 dan IKASANDI. Melalui validasi berbasis simulasi, rancangan yang diusulkan memproyeksikan peningkatan skor IKASANDI dari 1,65 menjadi 2,24 dan penurunan rata-rata skor risiko dari 12,07 menjadi 6,31, menempatkan seluruh skenario ke dalam kategori dapat diterima. Kesimpulannya, penerapan SNI ISO/IEC 27005:2022 menghasilkan rancangan manajemen risiko terstruktur yang mendukung pemantauan dan peningkatan berkelanjutan sistem manajemen keamanan informasi pada Aplikasi One Data .*

Kata Kunci*: Aplikasi One Data, IKASANDI, Manajemen Risiko Keamanan Informasi, SNI ISO/IEC 27005:2022, SNI ISO/IEC 27002:2022*

I. PENDAHULUAN

Transformasi digital pemerintahan melalui Sistem Pemerintahan Berbasis Elektronik (SPBE) menempatkan data sebagai fondasi layanan publik dan pengambilan keputusan yang akurat, terukur, serta lintas unit [1]. Dalam konteks tersebut, kebijakan Satu Data Indonesia menekankan tata kelola data pemerintah agar menghasilkan data yang akurat, mutakhir, terpadu, dan dapat dipertanggungjawabkan untuk mendukung perumusan kebijakan berbasis bukti [2]. Sejalan dengan arah tersebut, Aplikasi One Data di Instansi XYZ memegang peran krusial sebagai portal data strategis yang mendukung reformasi birokrasi dan tata kelola aparatur sipil negara melalui penyediaan data terintegrasi bagi pengambilan keputusan dan peningkatan kualitas layanan administrasi kepegawaian [3].

Pada praktiknya, pengamanan aplikasi strategis sering kali masih didominasi pendekatan kontrol teknis yang bersifat parsial, sementara proses manajemen risiko yang formal mulai dari penetapan konteks, penilaian, hingga perlakuan risiko belum sepenuhnya terdokumentasi dan terukur [4]. Akibatnya, organisasi menghadapi beberapa

persoalan: (i) identifikasi aset, ancaman, dan kerentanan belum membentuk peta risiko; (ii) penilaian risiko belum konsisten karena kriteria konsekuensi dan kemungkinan tidak ditetapkan secara jelas; (iii) prioritas perlakuan risiko belum selalu selaras dengan tingkat risiko tertinggi; dan (iv) efektivitas rancangan kontrol belum divalidasi menggunakan indikator kapabilitas/maturitas yang dapat menunjukkan peningkatan pengelolaan keamanan. Di lingkungan pemerintahan, kebutuhan akan proses yang sistematis dan terukur juga selaras dengan pedoman manajemen risiko yang memfasilitasi penggunaan kriteria konsekuensi–kemungkinan dan sebagai dasar evaluasi dan pengambilan keputusan risiko pada layanan aplikasi e-*government* [4].

SNI ISO/IEC 27005 menyediakan panduan terstruktur untuk mengidentifikasi, menganalisis, mengevaluasi, dan menangani risiko keamanan informasi sebagai bagian dari *Information Security Management System* (ISMS) berbasis ISO/IEC 27001 [5]. Agar hasil penilaian risiko dapat diturunkan menjadi kontrol operasional, SNI ISO/IEC 27002:2022 digunakan sebagai katalog kontrol yang mencakup aspek organisasi, manusia, fisik, dan teknologi, termasuk autentikasi, pengelolaan akses, pencadangan, logging, keamanan aplikasi, dan pengelolaan perubahan [6]. Dengan demikian, kombinasi SNI ISO/IEC 27005 dan SNI ISO/IEC 27002 dapat digunakan untuk memastikan bahwa proses identifikasi risiko tidak hanya berhenti pada pemetaan risiko, tetapi juga menghasilkan rekomendasi kontrol yang dapat diterapkan secara operasional.

Meskipun demikian, sejumlah penelitian terdahulu menunjukkan bahwa penerapan ISO/IEC 27005 umumnya masih berfokus pada penyusunan *risk registe*r dan rekomendasi kontrol, serta belum banyak dikaitkan dengan instrumen pengukuran kematangan keamanan siber yang relevan dengan konteks instansi pemerintah. Beberapa penelitian juga belum secara spesifik mengaitkan penilaian risiko dengan aset teknis aplikasi, seperti *database*, API, *web server*, *virtual machine*, *WAF*, dan infrastruktur *data center*. Ringkasan penelitian terdahulu dan *GAP* penelitian disajikan pada Tabel 1.

TABEL 1
PENELITIAN TERDAHULU

Rujukan	Fokus dan Pendekatan	*GAP* Penelitian
Rasyid dan Aji [7]	SNI ISO/IEC 27005 pada Integrated School Management System dan pemetaan kontrol ISO/IEC 27002	Belum mengaitkan hasil perlakuan risiko dengan instrumen kematangan keamanan siber
Utami et al. [14]	Penilaian risiko website menggunakan DREAD dan ISO 27005	Belum mengaitkan hasil perlakuan risiko dengan instrumen kematangan keamanan siber dan belum menggunakan kontrol yang terstandar
Arianty [18]	Evaluasi implementasi ISMS pada BSN dengan wawancara, analisis dokumen, dan observasi.	Bersifat level organisasi, belum fokus pada risiko teknis aplikasi, database, API, dan arsitektur layanan
Barraza de la Paz et al. [8]	Tinjauan metodologi manajemen risiko pada organisasi kompleks	Bersifat umum dan belum spesifik pada layanan SPBE

Berdasarkan perbandingan tersebut, *research gap* penelitian ini terletak pada kebutuhan untuk menilai risiko keamanan informasi secara lebih teknis pada *level* aset aplikasi, sekaligus mengaitkannya dengan indikator kematangan keamanan siber yang relevan bagi instansi pemerintah. Dalam konteks sektor publik Indonesia, ruang penguatan tersebut menjadi penting karena rancangan perlakuan risiko idealnya menghasilkan daftar kontrol serta menunjukkan keterukuran peningkatan kapabilitas keamanan melalui instrumen nasional. BSSN memfasilitasi penilaian kematangan tersebut melalui instrumen IKASANDI yang digunakan untuk mengukur tingkat kematangan keamanan siber dan sandi pada organisasi/PSE, sehingga dapat menjadi dasar perencanaan peningkatan keamanan yang lebih terarah [10]. Pendekatan serupa juga sejalan dengan penggunaan berbagai instrumen penilaian kematangan keamanan informasi BSSN, seperti Indeks KAMI dan pengukuran kematangan keamanan siber sektor publik [11].

Dengan demikian, kebaruan penelitian ini tidak hanya terletak pada penggunaan SNI ISO/IEC 27005:2022 sebagai kerangka manajemen risiko, tetapi juga pada integrasinya dengan kontrol operasional SNI ISO/IEC 27002:2022 dan instrumen IKASANDI sebagai dasar simulasi peningkatan kematangan keamanan informasi.

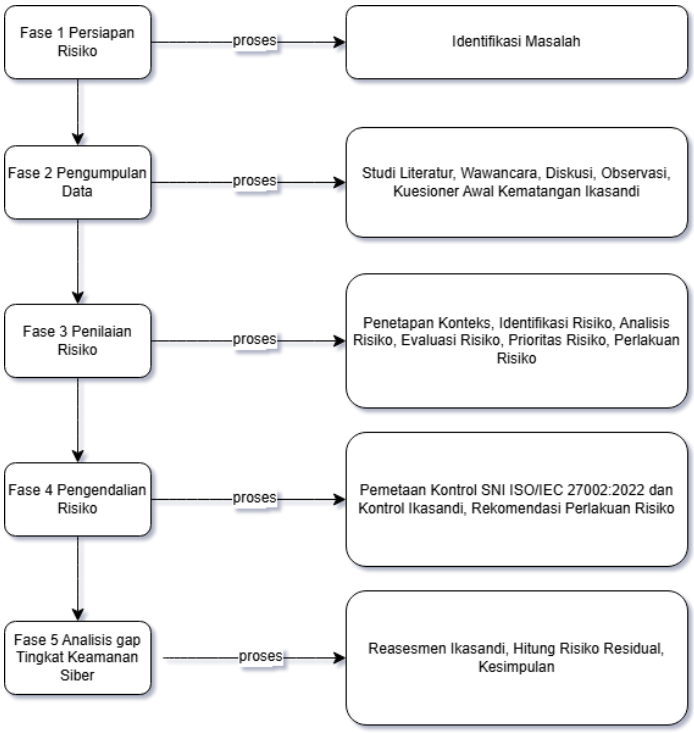
Proses analisis dan evaluasi risiko dalam penelitian ini menggunakan kriteria konsekuensi-kemungkinan dan matriks risiko 5×5 yang merujuk pada PermenPANRB Nomor 43 Tahun 2021. Penggunaan rujukan tersebut bertujuan menjaga konsistensi penilaian risiko dalam konteks tata kelola instansi sektor publik [12]. Hasil penilaian risiko kemudian digunakan untuk menetapkan prioritas perlakuan risiko, memetakan rekomendasi kontrol terhadap SNI ISO/IEC 27002:2022, dan mengevaluasi rancangan melalui proyeksi skor IKASANDI. Dengan pendekatan tersebut, rancangan manajemen risiko yang dihasilkan diharapkan tidak hanya komprehensif secara dokumentasi, tetapi juga operasional untuk mendukung monitoring dan perbaikan berkelanjutan ISMS pada Aplikasi One Data Instansi XYZ.

Penelitian ini bertujuan merancang dan mengevaluasi rancangan manajemen risiko keamanan informasi pada Aplikasi One Data Instansi XYZ menggunakan SNI ISO/IEC 27005:2022. Secara khusus, penelitian ini bertujuan menetapkan prioritas perlakuan risiko, memetakan rekomendasi kontrol terhadap SNI ISO/IEC 27002:2022, serta

memvalidasi rancangan melalui proyeksi peningkatan skor IKASANDI. Kontribusi ilmiah penelitian ini adalah model integrasi SNI ISO/IEC 27005-SNI ISO/IEC 27002-IKASANDI dalam konteks aplikasi One Data sektor publik. Adapun kontribusi praktisnya adalah penyusunan *risk regis*ter, prioritas mitigasi, dan kontrol yang dapat digunakan oleh instansi pemerintah pengelola layanan SPBE.

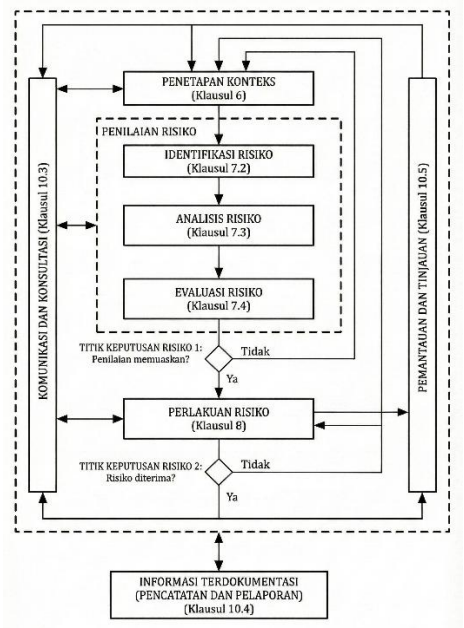
II. METODE

Penelitian ini terdiri dari 5 fase, yaitu (1) fase persiapan, (2) fase pengumpulan data, (3) fase penilaian risiko, (4) fase pengendalian risiko, (5) fase Analisis *gap* tingkat kematangan keamanan siber. Gambar 1 di bawah ini menggambarkan dan menjelaskan beberapa fase penelitian yang dilakukan.



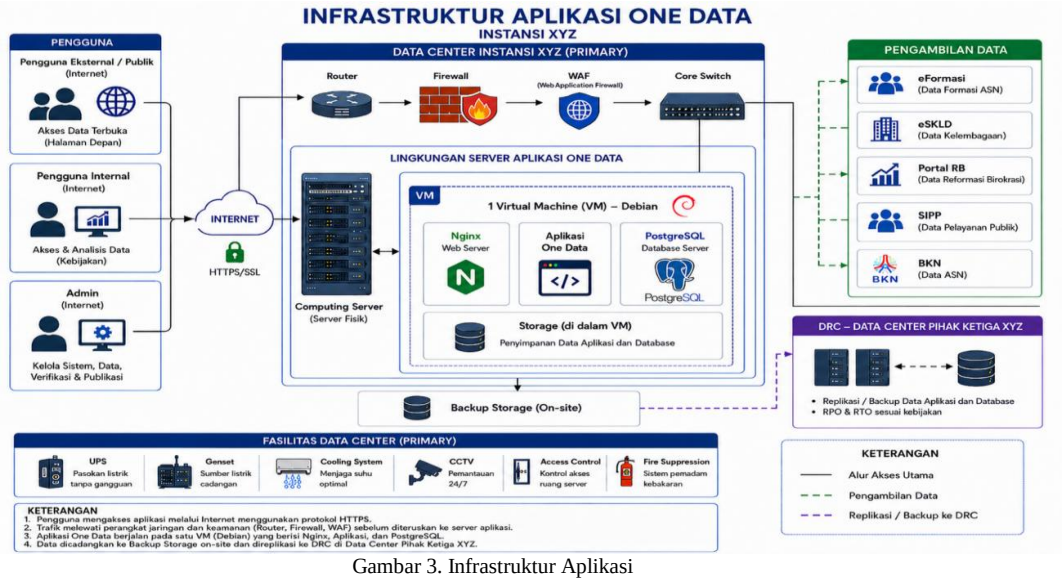
Gambar 1. Alur Penelitian

Gambar 2 menyajikan kerangka operasional manajemen risiko keamanan informasi berdasarkan SNI ISO/IEC 27005:2022 [5] yang diterapkan secara sistematis pada Aplikasi One Data Instansi XYZ. Alur ini diawali dengan penetapan konteks (Klausul 6) untuk mendefinisikan kriteria penilaian, disusul tahap penilaian risiko yang meliputi identifikasi, analisis, dan evaluasi skenario risiko (Klausul 7) guna mengukur dampak terhadap aspek kerahasiaan, integritas, dan ketersediaan. Karakteristik iteratif dari standar ini ditunjukkan melalui titik keputusan pasca-evaluasi untuk memastikan akurasi data sebelum berlanjut ke perencanaan perlakuan risiko (Klausul 8) yang bertujuan menurunkan tingkat risiko ke ambang batas penerimaan. Seluruh siklus didukung oleh mekanisme komunikasi, pemantauan berkelanjutan, serta dokumentasi yang konsisten (Klausul 10) untuk menjamin efektivitas kendali dan perbaikan berkelanjutan pada sistem manajemen keamanan informasi di lingkungan instansi.



Gambar 2. Proses Manajemen Risiko Keamanan Informasi

Arsitektur Aplikasi One Data Instansi XYZ terdiri atas lapisan pengguna, pusat data utama, dan *disaster recovery center* (DRC). Pengguna eksternal, pengguna internal, dan admin mengakses aplikasi melalui internet menggunakan HTTPS/SSL, kemudian trafik diteruskan melalui *router*, *firewall*, WAF, dan *core switch* menuju lingkungan server aplikasi. Aplikasi berjalan pada VM berbasis Debian yang memuat Nginx sebagai web server, aplikasi One Data, PostgreSQL sebagai database server, serta storage internal. Sistem juga didukung *backup storage* on-site, fasilitas data center seperti UPS, genset, *cooling system*, CCTV, access control, dan fire suppression system. Data aplikasi terintegrasi dengan eFormasi, eSKLD, Portal RB, SIPP, dan BKN, serta direplikasi ke DRC pihak ketiga untuk mendukung ketersediaan layanan sesuai kebijakan RPO dan RTO..



Gambar 3. Infrastruktur Aplikasi

A. Persiapan Risiko

Pada fase ini dilakukan identifikasi masalah yang melatarbelakangi perlunya perancangan manajemen risiko keamanan informasi pada Aplikasi One Data Instansi XYZ, termasuk penetapan ruang lingkup objek kajian, pemangku kepentingan yang terlibat, serta asumsi dan batasan penelitian. Selain itu, fase persiapan berfokus pada pengumpulan pemahaman awal mengenai proses bisnis, arsitektur layanan, serta karakteristik data strategis yang dikelola, sehingga konteks risiko dapat dirumuskan secara tepat

B. Pengumpulan Data

Pengumpulan data dilakukan melalui studi literatur, telaah dokumen internal, observasi teknis dan operasional, wawancara, diskusi, serta pengisian instrumen IKASANDI. Wawancara dan diskusi melibatkan 11 responden yang dipilih secara *purposive* karena memiliki pengetahuan langsung terhadap proses bisnis, aset, kontrol eksisting, insiden, dan pengambilan keputusan risiko pada Aplikasi One Data. Pendekatan pengumpulan data melalui kombinasi dokumen, observasi, dan wawancara ini lazim digunakan dalam perancangan manajemen risiko keamanan informasi berbasis standar [13]. Data responden dan fokus validasi disajikan pada Tabel 2. Sedangkan Observasi operasional digunakan untuk memverifikasi kondisi aktual di lapangan, khususnya terkait pengelolaan akses, konfigurasi, dan alur layanan, sekaligus melengkapi informasi dari dokumen dan wawancara. Pada fase ini juga dilakukan pengukuran awal tingkat kematangan keamanan siber menggunakan instrumen IKASANDI sebagai dasar sebelum rekomendasi perlakuan risiko disusun, sejalan dengan praktik pengukuran kematangan keamanan informasi di lingkungan pemerintah Indonesia [9].

TABEL 2
DATA RESPONDEN

Responden	Jumlah	Fokus Data	Masa Kerja Pada Unit Terkait
Manajemen/Pemilik Risiko	2	Konteks, prioritas, dampak, dan penerimaan risiko	1 tahun; 19 tahun
Pengelola Aplikasi	2	Proses bisnis dan fitur aplikasi	11 tahun; 6 tahun
System Administrator	2	Server, VM, OS, dan web server	8 tahun; 6 tahun
Pengelola Infrastruktur/Jaringan	2	Firewall, router, switch, bandwidth, konektivitas, daya dan fasilitas data center	14 tahun; 7 tahun
Pengelola Keamanan Informasi	2	Kontrol keamanan, monitoring, insiden, dan IKASANDI	13 tahun; 19 tahun
App Developer & Database Administrator	1	Coding, bug, integrasi API, perubahan aplikasi, Database, backup, restore	4 tahun

Tabel 3 menyajikan domain penilaian IKASANDI yang digunakan untuk mengukur tingkat kematangan keamanan siber dan persandian pada organisasi. Instrumen ini terdiri atas lima domain utama, yaitu Identifikasi, Proteksi, Deteksi, Penanggulangan dan Pemulihan, serta Persandian, dengan total 216 pertanyaan. Domain Proteksi memiliki jumlah pertanyaan terbanyak, yaitu 79 pertanyaan, sehingga menunjukkan bahwa aspek pengamanan identitas, data, aplikasi, jaringan, dan sumber daya manusia menjadi komponen penting dalam evaluasi kematangan keamanan siber.

TABEL 3
DOMAIN IKASANDI

Domain	Kategori	Jumlah Pertanyaan
Identifikasi	(1) Peran dan Tanggung Jawab Organisasi, (2) Strategi, Kebijakan, dan Prosedur Keamanan Siber, (3) Aset Informasi, (4) Menilai dan Mengelola Risiko Keamanan Siber, (5) Mengelola Risiko Rantai Pasok	59
Proteksi	(1) Identitas, Autentikasi, dan Kendali Akses Aset Fisik, (2) Data, (3) Aplikasi, (4) Jaringan, (5) Sumber Daya Manusia	79
Deteksi	(1) Mengelola Deteksi Peristiwa Siber, (2) Menganalisis Anomali dan Peristiwa Siber, (3) Memantau Peristiwa Siber Berkelanjutan	12
Penanggulangan dan Pemulihan	(1) Menyusun Perencanaan Penanggulangan dan Pemulihan Insiden Siber, (2) Menganalisis dan Melaporkan Insiden Siber, (3) Melaksanakan Penanggulangan dan Pemulihan Insiden Siber, (4) Meningkatkan Keamanan Setelah Terjadinya Insiden Siber	27

Persandian	(1) Kebijakan Pengamanan Informasi, (2) Pengelolaan Sumber Daya, (3) Pengamanan Sistem Elektronik dan Informasi Non Elektronik, (4) Layanan Keamanan Informasi, (5) Pola Hubungan Komunikasi Sandi	39

C. Penilaian Risiko

Penilaian risiko merupakan tahap inti untuk menilai tingkat risiko keamanan informasi pada Aplikasi One Data Instansi XYZ secara sistematis dengan mengacu pada SNI ISO/IEC 27005:2022 [5]. Pada tahap ini dilakukan penetapan konteks risiko, penentuan ruang lingkup aset, tujuan keamanan informasi (kerahasiaan, integritas, dan ketersediaan), asumsi, serta kriteria penilaian [14]. Identifikasi 61 skenario risiko dilakukan melalui empat langkah: (1) memetakan 30 aset ke pemilik dan responden terkait; (2) menghubungkan aset dengan ancaman T-1 sampai T-21 dan kerentanan yang ditemukan dari dokumen, observasi, dan wawancara; (3) merumuskan skenario risiko dalam bentuk kombinasi aset-ancaman-dampak; dan (4) memvalidasi kelayakan skenario kepada responden sesuai fokus data. Skor konsekuensi dan kemungkinan diberikan melalui konsensus peneliti dan responden terkait dengan menggunakan kriteria pada Tabel 4 dan Tabel 5, kemudian dievaluasi melalui matriks risiko 5x5 pada Tabel 6. Teknik analisis data yang digunakan bersifat campuran: data kualitatif digunakan untuk menginterpretasikan konteks ancaman dan kelemahan kontrol, sedangkan data kuantitatif digunakan untuk menghitung skor risiko, kategori risiko, skor residual, dan perubahan skor IKASANDI.

D. Pengendalian Risiko

Fase ini merupakan fase perlakuan risiko terhadap risiko prioritas yang telah ditetapkan pada fase penilaian risiko. Pada tahap ini, setiap risiko yang berada di atas ambang penerimaan dianalisis untuk menentukan opsi perlakuan yang paling tepat, terutama mitigasi melalui penerapan atau penguatan kontrol keamanan informasi [16]. Rekomendasi kontrol disusun dengan memetakan kebutuhan pengendalian terhadap kontrol SNI ISO/IEC 27002:2022, kemudian disejajarkan dengan kontrol pada pedoman IKASANDI agar rancangan yang diusulkan relevan dengan konteks penerapan di instansi pemerintah [17]. Hasil dari fase ini adalah daftar rekomendasi perlakuan risiko dan rencana tindak lanjut untuk evaluasi risiko residual dan validasi peningkatan kematangan keamanan melalui instrumen IKASANDI.

E. Analisis Gap Tingkat Kematangan Keamanan Siber

Rekomendasi kontrol yang telah disusun pada fase pengendalian risiko dievaluasi dengan membandingkan kondisi sebelum dan sesudah penerapan kontrol, baik dari sisi tingkat risiko maupun tingkat kematangan keamanan. Analisis *gap* dilakukan dengan reasesmen menggunakan instrumen IKASANDI untuk mengidentifikasi perbedaan maturitas sebelum dan sesudah rancangan diterapkan. Selain itu, dilakukan perhitungan risiko residual untuk memastikan bahwa perlakuan risiko yang diusulkan mampu menurunkan skor risiko ke ambang penerimaan yang ditetapkan, mengikuti proses evaluasi residual risk sebagaimana diuraikan dalam standar ISO/IEC 27005 dan kerangka manajemen risiko. Hasil dari fase ini berupa ringkasan *gap* kematangan keamanan siber dan *gap* risiko.

III. HASIL DAN PEMBAHASAN

Analisis penelitian ini didasarkan pada skor tingkat Keamanan Siber dan berfokus pada langkah-langkah perencanaan manajemen risiko keamanan informasi berdasarkan standar SNI ISO/IEC 27005:2022 dengan kontrol keamanan informasi berdasarkan standar SNI ISO/IEC 27002:2022.

A. Penetapan Konteks

Menentukan konteks risiko keamanan informasi dengan organisasi tentang kriteria risiko yaitu: (1) Kriteria Konsekuensi, (2) Kriteria Kemungkinan, (3) Kriteria Tingkat Risiko, dan (4) Kriteria Penerimaan Risiko. Kriteria tersebut kemudian ditetapkan dan dipelihara agar penilaian risiko berikutnya berlangsung konsisten, terukur, dan dapat dipertanggungjawabkan.

1. Kriteria Konsekuensi

Kriteria konsekuensi digunakan untuk mengukur besarnya dampak risiko pada dimensi operasional, ketersediaan data, dan reputasi organisasi menggunakan skala 1 (Tidak Signifikan) hingga 5 (Sangat Signifikan). Sebagaimana dirinci dalam Tabel 4, tingkat konsekuensi terendah ditandai oleh gangguan layanan kurang dari satu jam tanpa kerusakan data, sedangkan tingkat tertinggi mencakup gangguan lebih dari 24 jam, kehilangan data permanen tanpa cadangan, hingga pemberitaan negatif berskala internasional. Penetapan parameter ini berfungsi sebagai standar objektif agar penilaian risiko pada Aplikasi One Data dapat dilakukan secara konsisten.

TABEL 4
KRITERIA KONSEKUENSI

Tingkat Konsekuensi	Konsekuensi Operasional	Konsekuensi Ketersediaan Data	Konsekuensi Reputasi
Tidak Signifikan (1)	Gangguan terhadap layanan kurang dari 1 jam.	Tidak ada kehilangan atau kerusakan data.	Tidak ada dampak terhadap reputasi dan kepercayaan organisasi.
Kurang Signifikan (2)	Gangguan terhadap layanan dalam rentang waktu 1-2 jam.	Data memerlukan koreksi minor atau tidak tersedia sementara, namun dapat dipulihkan dengan cepat.	Menimbulkan ketidakpuasan internal atau keluhan pelanggan minor yang tidak terekspos ke publik.
Moderat (3)	Gangguan terhadap layanan dalam rentang waktu 2-12 jam.	Data rusak/hilang, tetapi ada cadangan yang dapat dipulihkan.	Pemberitaan negatif di media massa lokal
Signifikan (4)	Gangguan terhadap layanan dalam rentang waktu 12-24 jam.	Data rusak/hilang dan tidak ada cadangan.	Pemberitaan negatif di media massa nasional
Sangat Signifikan (5)	Gangguan terhadap layanan lebih dari 24 jam	Data rusak/hilang dan tidak ada cadangan.	Pemberitaan negatif di media massa nasional dan internasional

2. Kriteria Kemungkinan

Kriteria kemungkinan digunakan untuk mengukur frekuensi terjadinya risiko dalam kurun waktu satu tahun dengan menggunakan skala penilaian 1 (Sangat Jarang) hingga 5 (Sangat Sering). Sebagaimana dirinci dalam Tabel 5, tingkat terendah merepresentasikan kejadian sebanyak satu kali per tahun, sedangkan tingkat tertinggi mencakup frekuensi lebih dari 12 kali per tahun. Kriteria kemungkinan ini ditetapkan sebagai standar objektif agar klasifikasi ancaman terhadap Aplikasi One Data dapat dilakukan secara terukur.

TABEL 5
KRITERIA KEMUNGKINAN

Tingkat Kemungkinan	Kriteria
Sangat Jarang (1)	Dapat Terjadi 1 Kali Per tahun
Jarang (2)	Dapat Terjadi 2 Sampai 5 Kali Per tahun
Cukup Sering (3)	Dapat Terjadi 6 Sampai 9 Kali Per tahun
Sering (4)	Dapat Terjadi 10 Sampai 12 Kali Per tahun
Sangat Sering (5)	Dapat Terjadi Lebih dari 12 Kali Per tahun

3. Kriteria Tingkat Risiko

Kriteria tingkat risiko ditentukan melalui matriks analisis risiko 5×5 yang menghubungkan skor kemungkinan dan konsekuensi guna menghasilkan skor risiko antara 1 hingga 25. Sebagaimana ditunjukkan dalam Tabel 6, pemetaan ini memungkinkan tingkat risiko. Penggunaan matriks ini merujuk pada PermenPANRB Nomor 43 Tahun 2021 [12].

TABEL 6
KRITERIA TINGKAT RISIKO

Matrix Analisis Risiko		Tingkat Konsekuensi				
		Tidak Signifikan (1)	Kurang Signifikan (2)	Moderat (3)	Signifikan (4)	Sangat Signifikan (5)
Kemungkinan	Sangat Sering (5)	9	15	18	23	25
	Sering (4)	6	12	16	19	24
	Cukup Sering (3)	4	10	14	17	22
	Jarang (2)	2	7	11	13	21
	Sangat Jarang (1)	1	3	5	8	20

4. Kriteria Penerimaan Risiko

Kriteria penerimaan risiko menentukan rentang keputusan penanganan terhadap hasil evaluasi risiko yang telah dilakukan. Berdasarkan Tabel 7, risiko diklasifikasikan ke dalam 5 kategori, di mana skor 11 hingga 25

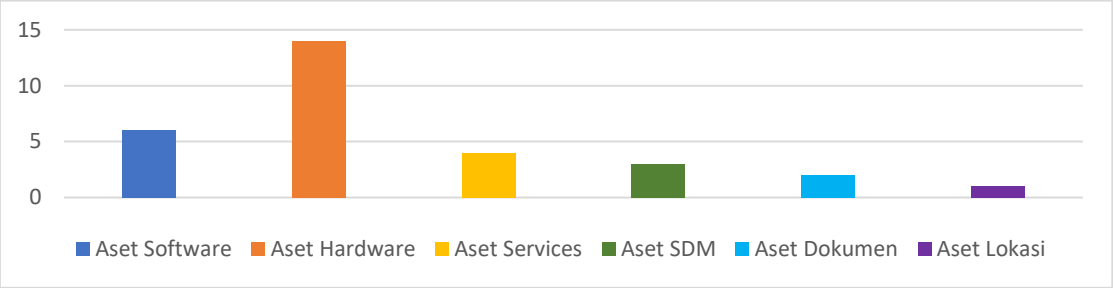
(kategori Sedang hingga Sangat Tinggi) diwajibkan untuk dilakukan mitigasi (*Mitigate*), sedangkan skor 1 hingga 10 (kategori Sangat Rendah hingga Rendah) dinyatakan dapat diterima (*Accept*). Penetapan kriteria ini mengacu pada PermenPANRB Nomor 43 Tahun 2021 [12].

TABEL 7
KRITERIA PENERIMAAN RISIKO

Tingkat Risiko	Skor Risiko	Kriteria Risiko
Sangat Tinggi	21-25	*Mitigate*
Tinggi	16-20	*Mitigate*
Sedang	11-15	*Mitigate*
Rendah	6-10	*Accept*
Sangat Rendah	1-5	*Accept*

B. Identifikasi Aset

Berdasarkan inventarisasi yang dilakukan, teridentifikasi sebanyak 30 aset yang mendukung operasional Aplikasi One Data. Aset-aset tersebut dikelompokkan ke dalam beberapa kategori seperti *Software*, *Hardware*, *Services*, SDM, Dokumen, dan Lokasi. Berdasarkan hasil pemetaan pada Gambar 3, diketahui bahwa Aset *Hardware* merupakan aset dengan jumlah terbanyak, yang mencakup server, perangkat jaringan, serta perangkat keras pendukung lainnya. Distribusi ini menunjukkan bahwa tingkat ketergantungan sangat dipengaruhi oleh aset *Hardware*.



Gambar 3. Jumlah Aset Perkategori

C. Identifikasi Ancaman

Identifikasi ancaman menghasilkan 21 jenis ancaman yang diklasifikasikan ke dalam empat kategori utama: ancaman lingkungan, kegagalan infrastruktur, tindakan manusia, dan ancaman organisasional. Sebagaimana dirinci dalam Tabel 8, daftar ini mencakup faktor fisik seperti kebakaran dan banjir, kendala teknis seperti kegagalan sistem, hingga faktor manusia seperti serangan malware dan ancaman orang dalam (*insider threat*).

TABEL 8
DAFTAR ANCAMAN

Kategori	Kode Ancaman	Deskripsi Ancaman
Ancaman Lingkungan	T-1	Kebakaran
	T-2	Banjir
	T-3	Gempa Bumi
	T-4	Ledakan
Kegagalan Infrastruktur	T-5	Kegagalan sistem pendingin atau ventilasi
	T-6	UPS tidak bekerja
	T-7	Sistem gagal berfungsi
Tindakan Manusia	T-8	Penyalahgunaan Hak (Akses pihak yang tidak berhak, mengambil dokumen tanpa izin, memodifikasi dokumen)
	T-9	Aplikasi tidak bisa diakses (aplikasi mati, aplikasi error, jaringan terputus)
	T-10	Terjadi kesalahan fungsional pada aplikasi saat beroperasi (Bug Aplikasi)
	T-11	Penyalahgunaan Hak (memodifikasi, mencuri akun, dan serangan untuk mendapatkan akun)
	T-12	Social Engineering
	T-13	Terinfeksi Malware

	T-14	Antivirus tidak berjalan/Out of Date
	T-15	Penggunaan perangkat yang tidak sah
	T-16	Terorisme, penyerangan, sabotase
	T-17	Ancaman Orang Dalam (*Insider Threat*)
	T-18	Kerusakan/kehilangan
Ancaman	T-19	Penggunaan perangkat yang salah
Organisasional	T-20	Ketersediaan personil
	T-21	Kegagalan penyedia layanan

D. Evaluasi Risiko

Gambar 4 menyajikan pemetaan dari 61 skenario risiko sehingga dapat dievaluasi secara visual sebaran aset dan ancaman dengan tingkat risiko mulai dari sangat rendah hingga sangat tinggi. Hasil analisis menunjukkan sebanyak 33 skenario risiko berada pada zona sedang hingga tinggi yang memerlukan mitigasi (*mitigate*), sedangkan 28 skenario lainnya berada pada zona rendah hingga sangat rendah yang dapat diterima (*accept*).

Aset / Ancaman	T-1	T-2	T-3	T-4	T-5	T-6	T-7	T-8	T-9	T-10	T-11	T-12	T-13	T-14	T-15	T-16	T-17	T-18	T-19	T-20	T-21	T-22	T-23	T-24	T-25	T-26	T-27	T-28
A-1 - Aplikasi One Data									10	7	11		11				5											
A-2 - Virtual Machine (VM)							5										20											
A-3 - Sistem Operasi (OS)							11										20											
A-4 - Web server							11										20											
A-5 - Database Server									16								5											
A-6 - Antivirus & Malware														5			3											
A-7 - Computing Server																		20										
A-8 - Storage Server																		20										
A-9 - Backup Storage Server																		20										
A-10 - Core Switch																		20										
A-11 - Router																		20										
A-12 - PDU	20																	20										
A-13 - Firewall																		20										
A-14 - UPS	20					20																						
A-15 - Cooling Sistem					7																1							
A-16 - Laptop Pengelola Server											20		2					1										
A-17 - Access Control																		5			5							
A-18 - CCTV																		11			5							
A-19 - Fire Suppression System							20																					
A-20 - Genset																		20										
A-21 - Listrik																					1							
A-22 - Bandwith																					20							
A-23 - Domain																					3							
A-24 - IP Address																			10		3							
A-25 - Management Level												8					8			3								
A-26 - System Administrator												13					20		20	20								
A-27 - App Developer												8					20		3	20								
A-28 - Dokumen Konfigurasi Aplikasi dan Jaringan								5										5										
A-29 - Dokumen Penggunaan Aplikasi								1										1										
A-30 - Data Center Instansi XYZ	20		20	20												20					7							
Jumlah	3	0	1	1	1	1	4	2	2	1	2	3	2	1	0	1	9	13	3	3	8	0	0	0	0	0	0	0

Gambar 4. Pemetaan Risiko

E. Prioritas Risiko

Prioritas risiko pada Tabel 9 dilakukan agar instansi dapat mengalokasikan sumber daya secara efektif untuk menangani risiko yang memiliki dampak paling kritis (*mitigate*) terhadap operasional Aplikasi One Data sebelum beralih ke risiko yang berada pada kategori dapat diterima (*accept*)

TABEL 9
PRIORITAS RISIKO

No	Kode Risiko	Kode Aset	Kode Ancaman	Skor Risiko	Tingkat Risiko	Kriteria Risiko
1	R7	A-2	T-17	20	Tinggi	Mitigate
2	R9	A-3	T-17	20	Tinggi	Mitigate
3	R11	A-4	T-17	20	Tinggi	Mitigate
4	R16	A-7	T-18	20	Tinggi	Mitigate
5	R17	A-8	T-18	20	Tinggi	Mitigate
6	R18	A-9	T-18	20	Tinggi	Mitigate
7	R19	A-10	T-18	20	Tinggi	Mitigate
8	R20	A-11	T-18	20	Tinggi	Mitigate
9	R21	A-12	T-1	20	Tinggi	Mitigate
10	R22	A-12	T-18	20	Tinggi	Mitigate
11	R23	A-13	T-18	20	Tinggi	Mitigate
12	R24	A-14	T-1	20	Tinggi	Mitigate
13	R25	A-14	T-6	20	Tinggi	Mitigate

14	R28	A-16	T-11	20	Tinggi	Mitigate
15	R35	A-19	T-7	20	Tinggi	Mitigate
16	R36	A-20	T-18	20	Tinggi	Mitigate
17	R38	A-22	T-21	20	Tinggi	Mitigate
18	R46	A-26	T-17	20	Tinggi	Mitigate
19	R47	A-26	T-19	20	Tinggi	Mitigate
20	R48	A-26	T-20	20	Tinggi	Mitigate
21	R50	A-27	T-17	20	Tinggi	Mitigate
22	R52	A-27	T-20	20	Tinggi	Mitigate
23	R57	A-30	T-1	20	Tinggi	Mitigate
24	R58	A-30	T-3	20	Tinggi	Mitigate
25	R59	A-30	T-4	20	Tinggi	Mitigate
26	R60	A-30	T-16	20	Tinggi	Mitigate
27	R12	A-5	T-9	16	Tinggi	Mitigate
28	R45	A-26	T-12	13	Sedang	Mitigate
29	R3	A-1	T-11	11	Sedang	Mitigate
30	R4	A-1	T-13	11	Sedang	Mitigate
31	R8	A-3	T-7	11	Sedang	Mitigate
32	R10	A-4	T-7	11	Sedang	Mitigate
33	R33	A-18	T-18	11	Sedang	Mitigate
34	R1	A-1	T-9	10	Rendah	Accept
35	R40	A-24	T-19	10	Rendah	Accept
36	R42	A-25	T-12	8	Rendah	Accept
37	R43	A-25	T-17	8	Rendah	Accept
38	R49	A-27	T-12	8	Rendah	Accept
39	R2	A-1	T-10	7	Rendah	Accept
40	R26	A-15	T-5	7	Rendah	Accept
41	R61	A-30	T-21	7	Rendah	Accept
42	R5	A-1	T-17	5	Sangat Rendah	Accept
43	R6	A-2	T-7	5	Sangat Rendah	Accept
44	R13	A-5	T-17	5	Sangat Rendah	Accept
45	R14	A-6	T-14	5	Sangat Rendah	Accept
46	R31	A-17	T-18	5	Sangat Rendah	Accept
47	R32	A-17	T-21	5	Sangat Rendah	Accept
48	R34	A-18	T-21	5	Sangat Rendah	Accept
49	R53	A-28	T-8	5	Sangat Rendah	Accept
50	R54	A-28	T-18	5	Sangat Rendah	Accept
51	R15	A-6	T-17	3	Sangat Rendah	Accept
52	R39	A-23	T-21	3	Sangat Rendah	Accept
53	R41	A-24	T-21	3	Sangat Rendah	Accept
54	R44	A-25	T-20	3	Sangat Rendah	Accept
55	R51	A-27	T-19	3	Sangat Rendah	Accept
56	R29	A-16	T-13	2	Sangat Rendah	Accept
57	R27	A-15	T-21	1	Sangat Rendah	Accept
58	R30	A-16	T-18	1	Sangat Rendah	Accept
59	R37	A-21	T-21	1	Sangat Rendah	Accept
60	R55	A-29	T-8	1	Sangat Rendah	Accept
61	R56	A-29	T-18	1	Sangat Rendah	Accept

F. Perlakuan Risiko

Perlakuan risiko dalam penelitian ini dirumuskan melalui kontrol SNI ISO/IEC 27002:2022 yang disejajarkan secara spesifik dengan sub kategori kontrol dalam instrumen IKASANDI. Langkah ini berfungsi untuk merekomendasikan perlakuan risiko menjadi langkah detail operasional yang tidak hanya menurunkan skor risiko, tetapi juga menjadi instrumen untuk mengukur peningkatan kematangan keamanan siber organisasi. Sebagaimana ditunjukkan dalam Tabel 10, pendekatan ini menjamin bahwa rancangan manajemen risiko pada Aplikasi One Data memiliki keterukuran yang nyata terhadap standar keamanan siber dan persandian yang berlaku di lingkungan instansi pemerintah.

TABEL 10
PERLAKUAN RISIKO

Risiko	Kontrol ISO 27002:2022	Sub Kategori IKASANDI
R3	8.28 Pengkodean yang aman & 8.5 Autentikasi aman	Menerapkan dan meninjau secara konsisten ketetapan terkait prinsip pengembangan aplikasi yang aman (secure coding) yang digunakan untuk pengembangan aplikasi secara internal (in-house) maupun yang melibatkan pihak eksternal, termasuk proses source code review (baik secara manual atau menggunakan piranti lunak) sebelum dijalankan di lingkungan produksi (PR 4.40) Menetapkan dan menerapkan secara konsisten pengelolaan identitas elektronik yang mencakup proses otentikasi (username & password) (termasuk mengganti password default, kompleksitas password, umur password dan mekanisme reset password) (PR 1.2) Menetapkan dan memberlakukan kebijakan yang mengatur pelanggaran terhadap proses otentikasi tersebut (PR 1.3) Memastikan sistem dan aplikasi mendukung penggantian password secara otomatis, termasuk pengaturan untuk profil pengguna yang berbeda (misal admin dan pengguna biasa), pengaturan kompleksitas, penonaktifan password, dan larangan penggunaan kembali password lama untuk semua infrastruktur dan aplikasi (PR 1.6)
R4	8.7 Proteksi terhadap perangkat perusak	Mengaktifkan, memutakhirkan, dan memastikan antivirus/ antimalware mampu mendeteksi, mengisolir serta menghapus ancaman virus/ malware pada setiap perangkat endpoints dan server (PR 5.73)
R7	8.3 Pembatasan akses informasi, 8.13 Pencadangan informasi dan 8.18 Penggunaan program utilitas privilese	Menetapkan dan menerapkan secara konsisten definisi tingkatan akses yang berbeda untuk setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut (PR 1.1) Menganalisis penggunaan akses (user access review) dan peninjauan hak akses, serta frekuensi pelaksanaannya ditetapkan dan diterapkan secara konsisten (PR 1.8) Menetapkan dan menerapkan metode pencegahan perubahan yang tidak terotorisasi terhadap file system (PR 4.64) Memiliki fasilitas cadangan (kantor alternatif dan/atau DRC) dengan sumber daya redundan untuk digunakan apabila terjadi gangguan terhadap fasilitas kantor utama dan pusat data (DC) (GU 1.13) Menetapkan dan menerapkan prosedur back-up untuk semua data kritikal dan uji coba pengembalian data (restore) termasuk memastikan data integrity yang direview secara berkala (GU 1.7)
R8	8.9 Manajemen konfigurasi & 8.16 Pemonitoran aktivitas	Menerapkan kemampuan deteksi yang sudah dikonfigurasi untuk menerima data log yang diperlukan dari semua sistem sesuai lingkup operasional (DE 1.4) Menetapkan dan menerapkan secara konsisten proses pengelolaan konfigurasi perangkat komputasi (server, perangkat jaringan, sistem operasi dan aplikasi) (PR 4.50)
R10	8.9 Manajemen konfigurasi & 8.23 Pemfilteran web	Menetapkan dan menerapkan secara konsisten proses pengelolaan konfigurasi perangkat komputasi (server, perangkat jaringan, sistem operasi dan aplikasi) (PR 4.50) Menggunakan Web Application Firewall (WAF) untuk melindungi seluruh aplikasi web Organisasi (PR 4.62)
R9, R11	8.2 Hak akses privilese & 8.13 Pencadangan informasi	Menetapkan dan menerapkan secara konsisten kerangka kerja pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) (ID 2.9) Menetapkan dan menerapkan secara konsisten definisi tingkatan akses yang berbeda untuk setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut (PR 1.1) Menetapkan dan menerapkan secara konsisten prosedur spesifik untuk menganalisis penggunaan akses (user access review) dan peninjauan hak akses, serta frekuensi pelaksanaannya (PR 1.8) Menetapkan dan menerapkan metode pencegahan perubahan yang tidak terotorisasi terhadap file system (PR 4.64) Memiliki fasilitas cadangan (kantor alternatif dan/atau DRC) dengan sumber daya redundan untuk digunakan apabila terjadi gangguan terhadap fasilitas kantor utama dan pusat data (DC) (GU 1.13)

		Menetapkan dan menerapkan prosedur back-up untuk semua data kritikal dan uji coba pengembalian data (restore) termasuk memastikan data integrity yang direview secara berkala (GU 1.7)
R12	8.16 Pemonitoran aktivitas & 8.13 Pencadangan informasi	Membentuk fungsi atau unit kerja yang bertugas memantau ketersediaan/aktivitas/kinerja sistem dan mendeteksi adanya peristiwa siber (baik internal maupun eksternal) sesuai dengan lingkup operasional yang ada, termasuk adanya keterlibatan pihak ketiga (DE 1.1) Memastikan ketersediaan SDM dengan jumlah dan kompetensi yang memadai untuk memantau ketersediaan/aktivitas/kinerja sistem, mendeteksi peristiwa siber dan mengawaki perangkat deteksi (DE 1.3) Menetapkan dan menerapkan prosedur back-up untuk semua data kritikal dan uji coba pengembalian data (restore) termasuk memastikan data integrity yang direview secara berkala (GU 1.7)
R16	7.4 Pemonitoran keamanan fisik & 8.14 Redundansi fasilitas pemrosesan informasi	Membentuk fungsi atau unit kerja yang bertugas memantau ketersediaan/aktivitas/kinerja sistem dan mendeteksi adanya peristiwa siber (baik internal maupun eksternal) sesuai dengan lingkup operasional yang ada, termasuk adanya keterlibatan pihak ketiga (DE 1.1) Memiliki fasilitas cadangan (kantor alternatif dan/atau DRC) dengan sumber daya redundan untuk digunakan apabila terjadi gangguan terhadap fasilitas kantor utama dan pusat data (DC) (GU 1.13)
R17	8.14 Redundansi fasilitas pemrosesan informasi & 8.13 Pencadangan informasi	Menetapkan dan menerapkan prosedur back-up untuk semua data kritikal dan uji coba pengembalian data (restore) termasuk memastikan data integrity yang direview secara berkala (GU 1.7) Memiliki fasilitas cadangan (kantor alternatif dan/atau DRC) dengan sumber daya redundan untuk digunakan apabila terjadi gangguan terhadap fasilitas kantor utama dan pusat data (DC) (GU 1.13)
R18	8.13 Pencadangan informasi	Memiliki fasilitas cadangan (kantor alternatif dan/atau DRC) dengan sumber daya redundan untuk digunakan apabila terjadi gangguan terhadap fasilitas kantor utama dan pusat data (DC) (GU 1.13) Menetapkan dan menerapkan prosedur back-up untuk semua data kritikal dan uji coba pengembalian data (restore) termasuk memastikan data integrity yang direview secara berkala (GU 1.7)
R19, R20, R23, R36	8.14 Redundansi fasilitas pemrosesan informasi	Memastikan ketersediaan fasilitas cadangan (kantor alternatif dan/atau DRC) dengan sumber daya (daya listrik, jaringan internet, infrastruktur pendukung, infrastruktur komputasi dan jaringan cadangan) redundan untuk digunakan apabila terjadi gangguan karena insiden siber terhadap fasilitas kantor utama dan pusat data (DC) (GU 1.13) Memastikan sistem pasokan daya listrik (generator, UPS, grounding, penangkal petir) yang sesuai dengan beban penggunaan daya operasional/darurat dengan redundansi yang sesuai dengan asesmen risiko pada infrastruktur komputasi/ ruang server/ data center tersedia, terpelihara dan diuji secara rutin (PR 2.17)
R21, R33	7.4 Pemonitoran keamanan fisik	Memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting ditetapkan dan diterapkan secara konsisten (PR 2.18) Menetapkan dan menerapkan rencana pemulihan berbagai skenario bencana (disaster recovery plan), yang kemudian disimulasikan, direviu, dievaluasi secara berkala untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan (GU 3.21) Menetapkan dan menerapkan secara konsisten pengamanan lokasi fisik/kerja sesuai dengan zonasi klasifikasi aset! (Zonasi = merah kuning hijau) (CCTV, kunci masuk, log book, security, dsb) (PR 2.12)
R22, R60	7.1 Perimeter keamanan fisik & 7.2 Entri fisik	Menetapkan dan menerapkan secara konsisten pengelolaan akses ke fasilitas fisik menggunakan kunci fisik dan elektronik (PR 2.13) Memastikan ketersediaan fasilitas cadangan (kantor alternatif dan/atau DRC) dengan sumber daya (daya listrik, jaringan internet, infrastruktur pendukung, infrastruktur komputasi dan jaringan cadangan) redundan untuk digunakan apabila terjadi gangguan karena insiden siber terhadap fasilitas kantor utama dan pusat data (DC) (GU 1.13) Mengamankan lokasi fisik/kerja sesuai dengan zonasi klasifikasi aset sudah ditetapkan dan diterapkan secara konsisten (Zonasi = merah kuning hijau) (CCTV, kunci masuk, log book, security, dsb) (PR 2.12)

R24, R35, R57, R58, R59	7.3 Mengamankan kantor, ruangan, dan fasilitas	Membangun infrastruktur komputasi/ ruang server/ data center menggunakan material yang aman dari risiko kebakaran dan berada pada lokasi/ lingkungan yang aman (PR 2.14) Memastikan ketersediaan, pemeliharaan, dan pengujian rutin sistem pemadam api (termasuk smoke detector, alarm, APAR) yang sesuai dengan volume ruangan maupun tipe dan jumlah perangkat pada ruang infrastruktur komputasi/ ruang server/ data center (PR 2.15) Memastikan ketersediaan, pemeliharaan, dan pengujian rutin sistem pengatur lingkungan (suhu dan kelembaban) sesuai dengan volume ruangan maupun tipe dan jumlah perangkat pada ruang infrastruktur komputasi/ ruang server/ data center (PR 2.16) Menetapkan dan menerapkan secara konsisten peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll) (PR 2.19)
R25	7.12 Keamanan perkabelan & 8.14 Redundansi fasilitas pemrosesan informasi	Memastikan ketersediaan Business Impact Analysis (BIA) yang mencakup penentuan Recovery Time Objective (RTO) dan Recovery Point Objective (RPO) yang ditinjau ulang validitasnya secara berkala (GU 1.11) Memastikan ketersediaan fasilitas cadangan (kantor alternatif dan/atau DRC) dengan sumber daya (daya listrik, jaringan internet, infrastruktur pendukung, infrastruktur komputasi dan jaringan cadangan) redundan untuk digunakan apabila terjadi gangguan karena insiden siber terhadap fasilitas kantor utama dan pusat data (DC) (GU 1.13)
R28	8.5 Autentikasi aman & 5.15 Kontrol akses	Menetapkan dan menerapkan secara konsisten definisi tingkatan akses yang berbeda untuk setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut! (PR 1.1) Menetapkan dan menerapkan secara konsisten pengelolaan identitas elektronik yang mencakup proses otentikasi (username & password) (termasuk mengganti password default, kompleksitas password, umur password dan mekanisme reset password) (PR 1.2) Menetapkan dan memberlakukan kebijakan yang mengatur pelanggaran terhadap proses otentikasi tersebut (PR 1.3) Menetapkan dan menerapkan persyaratan dan prosedur yang jelas untuk pemberian akses, otentikasi, dan otorisasi dalam penggunaan aset informasi (PR 1.5) Memastikan sistem dan aplikasi mendukung penggantian password secara otomatis, termasuk pengaturan untuk profil pengguna yang berbeda (misal admin dan pengguna biasa), pengaturan kompleksitas, penonaktifan password, dan larangan penggunaan kembali password lama untuk semua infrastruktur dan aplikasi (PR 1.6)
R38	5.30 Kesiapan TIK untuk kontinuitas bisnis	Memiliki fasilitas cadangan (kantor alternatif dan/atau DRC) dengan sumber daya redundan untuk digunakan apabila terjadi gangguan terhadap fasilitas kantor utama dan pusat data (DC) (GU 1.13)
R45	6.3 Kesadaran, pendidikan, dan pelatihan keamanan informasi	Menetapkan dan menerapkan program kesadaran keamanan informasi secara berkala dan berkelanjutan, termasuk melakukan evaluasi kepatuhan pegawai (PR 6.75) Menetapkan program kerja pelatihan keamanan siber untuk semua karyawan sesuai dengan uraian tugas dan wewenangnya (PR 6.77) Menerapkan program untuk menguji pemahaman kesadaran informasi melalui simulasi serangan sosial engineering secara berkala (misal phising) (PR 6.78)
R46	5.2 Peran dan tanggung jawab keamanan informasi & 6.8 Perjanjian konfidensialitas atau nirungkap	Memastikan ketersediaan fungsi atau bagian yang secara spesifik mempunyai tugas, tanggungjawab, dan wewenang yang jelas untuk mengelola keamanan informasi (ID 1.1) Mendefinisikan dan mengalokasikan tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (business continuity dan disaster recovery plans) (ID 1.7)
R47	8.18 Penggunaan program utilitas privilese & 8.32 Manajemen perubahan	Menetapkan dan menerapkan kerangka kerja pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten (ID 2.9)

R48, R52	5.37 Prosedur operasi terdokumentasi & 5.2 Peran dan tanggung jawab keamanan informasi	Memastikan ketersediaan fungsi atau bagian yang secara spesifik mempunyai tugas, tanggungjawab, dan wewenang yang jelas untuk mengelola keamanan informasi (ID 1.1) Mendokumentasikan, mensosialisasikan, dan meninjau secara berkala seluruh kebijakan, standar, dan prosedur keamanan informasi (ID 1.5)
R50	8.28 Pengkodean yang aman & 8.4 Akses ke kode sumber	Menerapkan proses pengembangan sistem yang aman (Secure SDLC) di organisasi Anda dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan (PR 4.39) Menerapkan dan meninjau secara konsisten ketetapan terkait prinsip pengembangan aplikasi yang aman (secure coding) yang digunakan untuk pengembangan aplikasi secara internal (in-house) maupun yang melibatkan pihak eksternal, termasuk proses source code review (baik secara manual atau menggunakan piranti lunak) sebelum dijalankan di lingkungan produksi (PR 4.40) Melakukan pemisahan lingkungan pengembangan dengan lingkungan operasional dan mengelola akses kepada pengembang termasuk pengawasan dan tinjauannya (PR 4.41)

G. Analisis GAP Tingkat Kematangan Keamanan Siber

Analisis *gap* tingkat kematangan siber dilakukan melalui reasesmen menggunakan instrumen IKASANDI guna membandingkan kondisi sebelum dan sesudah rancangan kontrol diterapkan. Berdasarkan data pada Tabel 11, total skor kematangan meningkat dari 1,65 menjadi 2,24 dengan selisih sebesar 0,59. Peningkatan paling besar terlihat pada domain Proteksi (PR) yang naik sebesar 1,00 poin, sehingga status kematangannya berhasil meningkat dari Level 2 (Berulang) menjadi Level 3 (Terdefinisi). Sedangkan untuk total masih berada pada Level 2, kenaikan skor pada seluruh domain (Identifikasi, Proteksi, Deteksi, serta Penanggulangan dan Pemulihan) menunjukkan bahwa rancangan manajemen risiko yang diusulkan mampu memperkuat tata kelola keamanan siber pada Aplikasi One Data secara terstruktur.

TABEL 11
ANALISIS *GAP* IKASANDI

Kategori	Skor Sebelum	Skor Sesudah	Selisih	Kategori Sebelum	Kategori Sesudah
Identifikasi (ID)	1,07	1,33	0,26	Level 1 - Awal	Level 1 - Awal
Proteksi (PR)	2,25	3,25	1,00	Level 2 - Berulang	Level 3 - Terdefinisi
Deteksi (DE)	1,64	2,14	0,50	Level 2 - Berulang	Level 2 - Berulang
Penanggulangan dan Pemulihan (GU)	1,48	2,01	0,53	Level 1 - Awal	Level 2 - Berulang
Total	1,65	2,24	0,59	Level 2 - Berulang	Level 2 - Berulang

Analisis gap juga dilakukan terhadap tingkat risiko residual sebagai validasi berbasis estimasi atas efektivitas rencana mitigasi pada setiap skenario risiko. Sebagaimana ditunjukkan pada Tabel 12, estimasi risiko residual setelah penerapan rancangan perlakuan risiko menunjukkan penurunan rata-rata skor risiko dari 12,07 menjadi 6,31. Penurunan paling signifikan terlihat pada risiko prioritas tinggi (seperti R7, R9, dan R11) yang turun sebesar 12 poin, sehingga berubah dari kategori Mitigate ke Accept. Temuan ini mengindikasikan bahwa, berdasarkan penilaian risiko menggunakan matriks yang sama dan asumsi kontrol yang diusulkan telah diterapkan, seluruh 61 skenario risiko diproyeksikan berada di bawah ambang batas penerimaan. Dengan demikian, rancangan perlakuan risiko yang disusun diperkirakan efektif dalam meminimalkan potensi dampak dan kemungkinan ancaman pada operasional aplikasi.

TABEL 12
ANALISIS *GAP* RISIKO

Kode Risiko	Skor Sebelum	Skor Sesudah	Selisih
R1	10 (Accept)	10 (Accept)	0
R2	7 (Accept)	7 (Accept)	0
R3	11 (Mitigate)	5 (Accept)	6
R4	11 (Mitigate)	5 (Accept)	6
R5	5 (Accept)	5 (Accept)	0
R6	5 (Accept)	5 (Accept)	0
R7	20 (Mitigate)	8 (Accept)	12
R8	11 (Mitigate)	5 (Accept)	6
R9	20 (Mitigate)	8 (Accept)	12
R10	11 (Mitigate)	5 (Accept)	6
R11	20 (Mitigate)	8 (Accept)	12

R12	16 (Mitigate)	10 (Accept)	6
R13	5 (Accept)	5 (Accept)	0
R14	5 (Accept)	5 (Accept)	0
R15	3 (Accept)	3 (Accept)	0
R16	20 (Mitigate)	8 (Accept)	12
R17	20 (Mitigate)	8 (Accept)	12
R18	20 (Mitigate)	8 (Accept)	12
R19	20 (Mitigate)	8 (Accept)	12
R20	20 (Mitigate)	8 (Accept)	12
R21	20 (Mitigate)	8 (Accept)	12
R22	20 (Mitigate)	8 (Accept)	12
R23	20 (Mitigate)	8 (Accept)	12
R24	20 (Mitigate)	8 (Accept)	12
R25	20 (Mitigate)	8 (Accept)	12
R26	7 (Accept)	7 (Accept)	0
R27	1 (Accept)	1 (Accept)	0
R28	20 (Mitigate)	8 (Accept)	12
R29	2 (Accept)	2 (Accept)	0
R30	1 (Accept)	1 (Accept)	0
R31	5 (Accept)	5 (Accept)	0
R32	5 (Accept)	5 (Accept)	0
R33	11 (Mitigate)	7 (Accept)	4
R34	5 (Accept)	5 (Accept)	0
R35	20 (Mitigate)	8 (Accept)	12
R36	20 (Mitigate)	8 (Accept)	12
R37	1 (Accept)	1 (Accept)	0
R38	20 (Mitigate)	8 (Accept)	12
R39	3 (Accept)	3 (Accept)	0
R40	10 (Accept)	10 (Accept)	0
R41	3 (Accept)	3 (Accept)	0
R42	8 (Accept)	8 (Accept)	0
R43	8 (Accept)	8 (Accept)	0
R44	3 (Accept)	3 (Accept)	0
R45	13 (Mitigate)	8 (Accept)	5
R46	20 (Mitigate)	8 (Accept)	12
R47	20 (Mitigate)	8 (Accept)	12
R48	20 (Mitigate)	8 (Accept)	12
R49	8 (Accept)	8 (Accept)	0
R50	20 (Mitigate)	8 (Accept)	12
R51	3 (Accept)	3 (Accept)	0
R52	20 (Mitigate)	8 (Accept)	12
R53	5 (Accept)	5 (Accept)	0
R54	5 (Accept)	5 (Accept)	0
R55	1 (Accept)	1 (Accept)	0
R56	1 (Accept)	1 (Accept)	0
R57	20 (Mitigate)	8 (Accept)	12
R58	20 (Mitigate)	8 (Accept)	12
R59	20 (Mitigate)	8 (Accept)	12
R60	20 (Mitigate)	8 (Accept)	12
R61	7 (Accept)	7 (Accept)	0
RATA-RATA	12,07	6,31	

H. Analisis terhadap Penerapan Kontrol Keamanan

Kendala utama implementasi kontrol terletak pada kebutuhan koordinasi lintas pemilik aset, biaya redundansi dan DRC, keterbatasan personel keamanan, risiko downtime saat hardening, serta kebutuhan *evidence* yang konsisten untuk memenuhi indikator IKASANDI. Kontrol seperti *secure coding*, *source code review*, MFA atau kebijakan password kuat, pembatasan akses database, *backup-restore*, *logging*, dan change management tidak dapat dinilai

efektif hanya dari dokumen; seluruhnya memerlukan prosedur operasional, bukti pelaksanaan, uji berkala, serta peninjauan oleh *risk owner*. Keterbatasan penelitian ini adalah mitigasi masih berbasis rancangan dan simulasi, belum mencakup penetration test aktif pada produksi, belum mengukur dampak kinerja setelah kontrol diterapkan, dan belum melakukan audit kepatuhan pasca-implementasi.

I. Implikasi Praktis bagi Instansi Pemerintah

Implikasi praktis penelitian ini bagi instansi pemerintah lain yang menerapkan layanan One Data adalah pentingnya menjadikan manajemen risiko keamanan informasi sebagai bagian dari tata kelola teknis aplikasi, bukan hanya sebagai dokumen administratif. Instansi perlu memulai proses pengamanan dengan memetakan arsitektur sistem, aliran data, aset kritis, dependensi layanan, dan aktor pengguna untuk memperoleh dasar penilaian risiko yang lebih akurat. Hasil penilaian risiko kemudian dapat digunakan untuk menetapkan prioritas mitigasi pada area yang paling kritis, seperti pengelolaan akses privilese, keamanan database, integrasi API, *backup-restore*, *logging*, monitoring, dan perlindungan infrastruktur pusat data. Selain itu, penerapan kontrol keamanan perlu dikaitkan dengan kerangka Secure SDLC agar aspek keamanan diperhatikan sejak tahap perancangan, pengembangan, pengujian, hingga operasional aplikasi. Dengan pendekatan ini, instansi pemerintah dapat menyusun peta jalan peningkatan keamanan yang lebih terukur, selaras dengan standar SNI ISO/IEC 27002:2022, dan dapat dievaluasi secara berkala menggunakan instrumen kematangan nasional seperti IKASANDI.

IV. SIMPULAN

Berdasarkan hasil identifikasi terhadap 30 aset dan 21 jenis ancaman, teridentifikasi 61 skenario risiko yang terdiri dari 33 risiko prioritas untuk dimitigasi dan 28 risiko dalam kategori dapat diterima. Validasi terhadap rancangan yang diselaraskan dengan kategori IKASANDI dan terbukti efektif meningkatkan kapabilitas keamanan instansi XYZ, ditunjukkan oleh kenaikan skor kematangan keamanan siber dari 1,65 menjadi 2,24 serta menurunkan rata-rata skor risiko sebesar 47,7%, dari 12,07 menjadi 6,31, sehingga seluruh skenario risiko berada dalam ambang batas penerimaan organisasi. Penelitian selanjutnya dapat dikembangkan pada tahap implementasi kontrol secara teknis dan pelaksanaan audit kepatuhan pasca penerapan untuk memastikan efektivitas kontrol dalam jangka panjang serta menjamin keberlanjutan peningkatan Sistem Manajemen Keamanan Informasi. Selain itu, kajian lanjutan mengenai integrasi manajemen risiko ke dalam seluruh siklus hidup pengembangan sistem (SDLC) dapat menjadi fokus untuk memperkuat aspek keamanan aplikasi secara preventif sejak tahap rancang bangun.

UCAPAN TERIMAKASIH

Penulis menyampaikan terima kasih yang kepada Fakultas Teknik Universitas Indonesia atas dukungan akademik, bimbingan, serta fasilitas penelitian yang diberikan selama proses penyusunan ini. Terima kasih juga disampaikan kepada Kementerian Komunikasi dan Digital (KOMDIGI) atas dukungan pendanaan melalui program beasiswa yang telah diberikan, sehingga penelitian mengenai manajemen risiko keamanan informasi pada Aplikasi One Data ini dapat terlaksana dan diselesaikan dengan baik.

DAFTAR PUSTAKA

[1] B. D. Kencono, H. H. Putri, and T. W. Handoko, “Transformasi Pemerintahan Digital: Tantangan dalam Perkembangan Sistem Pemerintahan Berbasis Elektronik (SPBE) di Indonesia.” [Online]. Available: http://Jiip.stkipyapisdompu.ac.id

[2] Nuryana and Junaidi, “Implementasi Kebijakan Penyelenggaraan Satu Data Indonesia di Dinas Komunikasi dan Informatika Provinsi Kepulauan Bangka Belitung,” *Jurnal Pemerintahan dan Politik*, vol. 10, no. 2, pp. 356–383, Apr. 2025, doi: 10.36982/jpp.v10i2.5266.

[3] D. Wulandari, S. F. S. Gumilang, and R. Mulyana, “PERANCANGAN ENTERPRISE ARCHITECTURE LAYANAN SPBE (E-GOVERNMENT) DI LINGKUNGAN PEMKAB SUKABUMI,” *JURTEKSI (Jurnal Teknologi dan Sistem Informasi)*, vol. 8, no. 1, pp. 19–26, Dec. 2021, doi: 10.33330/jurteksi.v8i1.1204.

[4] P. Amalia Fakultas Ekonomi Dan Bisnis Islam and M. Irwan Padli Nasution Fakultas Ekonomi Dan Bisnis Islam, “TANTANGAN TERKINI DALAM KEAMANAN INFORMASI ANALISIS RESIKO DAN UPAYA PERLINDUNGAN,” *Jurnal Ekonomi Bisnis dan Manajemen*, vol. 2, no. 1, 2024, doi: 10.59024/jise.v2i1.5279.

[5] Badan Standardisasi Nasional, “SNI ISO/IEC 27005:2022 Keamanan informasi, keamanan siber, dan proteksi privasi—Panduan manajemen risiko keamanan informasi,” 2022.

[6] Badan Standardisasi Nasional, “SNI ISO/IEC 27002:2022 Keamanan informasi, keamanan siber, dan proteksi privasi—Kontrol keamanan informasi,” 2022.

[7] R. Muhamad Rasyid and R. Fathoni Aji, “Perancangan Manajemen Risiko Keamanan Informasi Menggunakan SNI ISO/IEC 27005: Studi Kasus Integrated School Management System milik PT XYZ,” *Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)*, vol. 10, pp. 226–235, [Online]. Available: https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

[8] J. V. Barraza de la Paz, L. A. Rodríguez-Picón, V. Morales-Rocha, and S. V. Torres-Argüelles, “A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0,” May 01, 2023, *MDPI*. doi: 10.3390/systems11050218.

[9] T. Hardiana and S. Suhardi, “Desain Instrumen Pengukuran Tingkat Kematangan Keamanan Siber Sektor Pemerintahan,” *Jurnal Pendidikan dan Teknologi Indonesia*, vol. 5, no. 11, pp. 3393–3310, Nov. 2025, doi: 10.52436/1.jpti.1124.

[10] Badan Siber dan Sandi Negara, “Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021,” 2021.

[11] M. Syaeful Bahry and B. Sugiantoro, “Evaluasi Tingkat Keamanan Indeks KAMI (Studi Kasus : Universitas X),” 2024.

[12] Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi, "Peraturan Menteri PANRB Nomor 43 Tahun 2021 tentang Manajemen Risiko di Lingkungan Kementerian PANRB," 2021.
[13] Asriyanik and Prajoko, "PENGEMBANGAN APLIKASI PENILAIAN RISIKO KEAMANAN INFORMASI BERBASIS ISO 27005 MENGGUNAKAN METODE PROTOTYPING," *Jurnal Ilmiah SANTIKA*, vol. 8, 2018.
[14] Gina Cahya Utami, Aden Bahtiar Supramaji, and Khairunnisak Nur Isnaini, "Penilaian Risiko Keamanan Informasi pada Website dengan Metode DREAD dan ISO 27005:2018," *JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia)*, vol. 8, no. 1, pp. 47–56, Feb. 2023, doi: 10.32528/justindo.v8i1.219.
[15] H. D. Hadmanto, R. Fathoni Aji, J. P. Nurahman, * Hendra, and D. Hadmanto, "Jurna1 Restikom : Riset Teknik Informatika dan Komputer," vol. 3, no. 2, pp. 60–69, 2021, [Online]. Available: https://restikom.nusaputra.ac.id
[16] G. Gioferi and Y. Yulhendri, "Penilaian Risiko TI Pada Website DosenIT Dengan Framework ISO 31000 Dan ISO 27002," *Jurnal Teknologi Dan Sistem Informasi Bisnis*, vol. 5, no. 4, pp. 409–419, Oct. 2023, doi: 10.47233/jteksis.v5i4.897.
[17] M. Andriana, I. Sembiring, and K. D. Hartomo, "SOP of Information System Security on Koperasi Simpan Pinjam Using ISO/IEC 27002:2013," *TRANSFORMATIKA*, vol. 18, no. 1, pp. 25–35, 2020.
[18] K. P. Arianty, "Analysis of Information Security Management System Implementation at BSN," Jurnal Informatika: Jurnal Pengembangan IT, vol. 10, no. 1, 2025, doi: 10.30591/jpit.v10i1.8211