JURNAL ILMIAH SISTEM INFORMASI (JUSI)
VOL 5, No. 2, Mei 2026, pp. 68 - 77
p-ISSN : 2803-1507 (media cetak) | e-ISSN : 2803-1531 (media online)
Link Publikasi: https://ejurnal.provisi.ac.id/index.php/JUISI/issue/view/171

Information Security Evaluation Based on KAMI Index 5.0 (2023) at PT X

Greycia Febrina Michelle*[1], Nickel Modami[2], Ephraim Eleazar Reva Manopo[3], Muhamad Rafly Kurniawan[4], Danendra Rafi Enditama[5], Afifah Trista Ayunda[6]
[1,2,3,4,5,6] Fakultas Sains dan Teknologi, Universitas Pradita
Jl. Gading Serpong Boulevard No.1 Tower 1, 15810, Kabupaten Tangerang, Banten, Indonesia
e-mail: greycia.febrina@student.pradita.ac.id*[1], nickel.modami@student.pradita.ac.id[2], ephraim.eleazar@student.pradita.ac.id[3], muhamad.rafly@student.pradita.ac.id[4], danendra.rafi@student.pradita.ac.id[5], afifah.trista@pradita.ac.id[6]

ARTICLE INFO

Article History:

Received: 02-12-2025
Revised: 28-12-2025
Accepted: 29-12-2025
Published: 21-05-2026

ABSTRACT

The digital transformation in the financial services sector demands robust information security assurance to protect strategic data from increasingly complex cyber threats. PT X, as a strategic institution managing investments and public assets, faces the challenge of balancing Enterprise Resource Planning (ERP) system operations with regulatory compliance for data privacy. This study aims to evaluate the information security maturity level and identify risk gaps at PT X using the Information Security Index (KAMI) Version 5.0 instrument, aligned with ISO/IEC 27001:2022 standards. The research methodology employs a descriptive quantitative approach through interviews, document observation, and dashboard assessment covering seven evaluation areas. Based on the evaluation conducted in November 2025, the Electronic System at PT X is classified in the "High" category with a score of 21. The final evaluation result indicates an "Adequate" (Cukup Baik) status, with varying maturity levels: Governance (III+), Risk Management (III+), Framework (II), Asset Management (II), Technology (III+), and Personal Data Protection (I+). Research findings reveal that while governance aspects and technology controls are well-defined, significant gaps exist in the formalization of framework documentation and PDP Law compliance, which remains at an initial level. In conclusion, strategic improvement priorities must focus on developing data privacy policies and asset lifecycle management to achieve optimal compliance targets.

Keywords: *Information Security, KAMI Index 5.0, Risk Management, ISO/IEC 27001:2022, Maturity Evaluation.*

Abstrak

Transformasi digital di sektor jasa keuangan menuntut adanya jaminan keamanan informasi yang tangguh untuk melindungi data strategis dari ancaman siber yang semakin kompleks. PT X, sebagai institusi strategis yang mengelola investasi dan aset publik, menghadapi tantangan dalam menyeimbangkan operasional sistem Enterprise Resource Planning (ERP) dengan kepatuhan terhadap regulasi privasi data. Penelitian ini bertujuan untuk mengevaluasi tingkat kematangan (maturity level) keamanan informasi dan mengidentifikasi celah risiko pada PT X menggunakan instrumen Indeks Keamanan Informasi (KAMI) Versi 5.0 yang diselaraskan

DOI: https://doi.org/10.51903/etg50932

p-ISSN : 2803-1507 e-ISSN : 2803-1531

dengan standar ISO/IEC 27001:2022. Metodologi penelitian menggunakan pendekatan deskriptif kuantitatif melalui wawancara, observasi dokumen, dan pengisian dashboard assessment yang mencakup tujuh area evaluasi. Berdasarkan evaluasi yang dilakukan pada November 2025, Sistem Elektronik pada PT X diklasifikasikan dalam kategori "Tinggi" dengan skor 21. Hasil akhir evaluasi menunjukkan status "Cukup Baik" dengan rincian tingkat kematangan yang bervariasi: Tata Kelola (III+), Pengelolaan Risiko (III+), Kerangka Kerja (II), Pengelolaan Aset (II), Teknologi (III+), dan Pelindungan Data Pribadi (I+). Temuan penelitian mengungkapkan bahwa meskipun aspek tata kelola dan kontrol teknologi telah terdefinisi dengan baik, terdapat kesenjangan signifikan pada formalisasi dokumentasi kerangka kerja dan kepatuhan terhadap UU PDP yang masih berada pada level awal. Kesimpulannya, prioritas perbaikan strategis harus difokuskan pada penyusunan kebijakan privasi data dan manajemen siklus hidup aset untuk mencapai target kepatuhan yang optimal.

Kata Kunci: *Keamanan Informasi, Indeks KAMI 5.0, Manajemen Risiko, ISO/IEC 27001:2022, Evaluasi Kematangan.*

1. PENDAHULUAN

Adopsi teknologi digital yang masif di berbagai sektor industri telah mengubah paradigma operasional menjadi lebih terintegrasi, namun di sisi lain menciptakan potensi risiko keamanan baru yang semakin kompleks. Regulasi keamanan siber kini memegang peran vital dalam mempromosikan transformasi digital yang aman [1]. Sektor jasa keuangan, khususnya, kini menjadi sasaran utama serangan siber global karena nilai strategis data yang dikelolanya. Hal ini menuntut adanya mekanisme pertahanan yang adaptif dan tangguh, terutama dalam menghadapi tantangan privasi data yang menyertai transformasi digital perbankan [2], [3]. Dalam konteks ini, PT X sebagai institusi yang bergerak di bidang pengelolaan investasi dan keuangan, menghadapi tantangan berat untuk memastikan terjaminnya aspek kerahasiaan, integritas, dan ketersediaan data (Confidentiality, Integrity, Availability) di tengah ancaman yang terus berkembang.

Implementasi teknologi yang masif, seperti penggunaan sistem Enterprise Resource Planning (ERP) berbasis SAP, memerlukan model kematangan manajemen keamanan informasi organisasi yang terstruktur untuk memitigasi risiko kegagalan sistem maupun kebocoran data strategis [4]. Tata kelola siber yang baik juga terbukti berhubungan positif dengan inovasi perusahaan [5]. Namun, penerapan teknologi tanpa evaluasi berkala seringkali menimbulkan celah keamanan baru yang tidak terdeteksi, yang dapat menghambat pencapaian tujuan strategis perusahaan [6]. Selain aspek teknis, faktor manusia juga memegang peranan krusial dalam ekosistem keamanan siber. Kurangnya kesadaran keamanan (security awareness) di kalangan karyawan seringkali menjadi celah masuknya serangan melalui social engineering [7]. Lebih lanjut, dampak finansial yang ditimbulkan akibat insiden keamanan tidak hanya terbatas pada kerugian operasional langsung, tetapi juga mencakup biaya pemulihan reputasi jangka panjang yang signifikan bagi institusi keuangan [8]. Dalam ekosistem yang saling terhubung ini, keamanan informasi bukan lagi sekadar opsi, melainkan kebutuhan mendasar untuk menjamin keberlangsungan bisnis dan kepercayaan pemangku kepentingan.

Untuk memastikan standar keamanan yang memadai, Badan Siber dan Sandi Negara (BSSN) telah menetapkan instrumen evaluasi berupa Indeks Keamanan Informasi (KAMI). Instrumen ini dirancang untuk memotret tingkat kesiapan dan kematangan keamanan informasi di setiap instansi. Penelitian terdahulu yang dilakukan oleh [9], [10] menunjukkan bahwa penggunaan Indeks KAMI (Versi 4.0 dan 4.1) efektif dalam mengidentifikasi celah keamanan pada instansi pemerintah daerah. Namun, evaluasi pada versi-versi sebelumnya seringkali belum mencakup aspek-aspek terbaru dari standar internasional ISO/IEC 27001:2022, padahal standarisasi menggunakan kerangka kerja ini sangat krusial bagi sektor perbankan dan keuangan [11].

Untuk menjawab kebutuhan terhadap standar keamanan informasi yang lebih mutakhir, Indeks KAMI Versi 5.0 (2023) hadir dengan penyelarasan terhadap ISO/IEC 27001:2022 dan penambahan khusus untuk Pelindungan Data Pribadi (PDP). Pergeseran fokus ini sangat signifikan karena menuntut organisasi untuk tidak hanya mengamankan infrastruktur, tetapi juga mengelola siklus hidup data pribadi secara ketat. Sebuah studi terbaru oleh [12] pada Satuan Logistik POLRI menemukan bahwa penerapan Indeks KAMI 5.0 mampu memberikan gambaran yang lebih komprehensif mengenai profil risiko sistem elektronik. Meskipun demikian, literatur yang secara spesifik mengkaji penerapan Indeks KAMI 5.0 pada sektor jasa keuangan masih terbatas, padahal sektor ini memiliki kompleksitas keamanan data yang tinggi dan membutuhkan metode penilaian risiko yang komprehensif seperti pada komputasi awan [13].

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Berdasarkan urgensi dan identifikasi celah penelitian tersebut, penelitian ini bertujuan untuk mengevaluasi tingkat kematangan (maturity level) keamanan informasi pada PT X menggunakan Indeks KAMI Versi 5.0. Evaluasi ini mencakup tujuh area utama, yaitu Kategori Sistem Elektronik (SE), Tata Kelola, Pengelolaan Risiko, Kerangka Kerja, Pengelolaan Aset, Teknologi, dan suplemen Pelindungan Data Pribadi (PDP). Penelitian ini tidak hanya bertujuan menilai tingkat kematangan, tetapi juga memberikan kontribusi praktis berupa usulan strategi perbaikan kepatuhan dan keamanan siber berbasis risiko [14] yang dapat direplikasi oleh entitas lain di sektor keuangan. Secara akademis, penelitian ini diharapkan dapat memperkaya literatur mengenai penerapan Indeks KAMI versi terbaru dalam konteks tata kelola keamanan informasi di sektor keuangan negara.

2. TINJAUAN PUSTAKA

2.1. *Penelitian Terdahulu*

Penelitian mengenai evaluasi keamanan informasi pada berbagai sektor industri strategis terus berkembang seiring dengan meningkatnya standar regulasi nasional [15], [16], [17]. Pemetaan penelitian terdahulu ini bertujuan untuk menunjukkan posisi dan kebaruan dari penelitian ini di antara studi-studi yang telah ada. Terkait penggunaan instrumen Indeks KAMI pada sektor publik, [9] melakukan evaluasi di Dinas Komunikasi dan Informatika Kota Bogor menggunakan Indeks KAMI Versi 4.0 dengan hasil tingkat kematangan Level I, yang mengindikasikan perlunya pembenahan dasar. Senada dengan hal tersebut, [10] menekankan pentingnya pemenuhan area tata kelola dan pengelolaan risiko untuk mencapai kepatuhan standar ISO 27001. Namun, studi-studi ini masih menggunakan instrumen versi lama yang belum mencakup kontrol privasi data yang komprehensif.

Dalam konteks sektor keuangan, audit sistem informasi menjadi krusial untuk memastikan keandalan layanan. [18] melakukan kajian literatur terhadap audit sistem informasi pada perusahaan perbankan dan menyoroti bahwa sektor ini memiliki profil risiko yang unik yang membutuhkan kontrol akses ketat. Hal ini diperkuat oleh [11] yang menekankan pentingnya standarisasi manajemen keamanan informasi menggunakan kerangka kerja ISO 27001:2022 di sektor perbankan. Sejalan dengan itu, [2] menyoroti bahwa isu privasi data dan keamanan siber merupakan tantangan terbesar dalam digitalisasi sektor keuangan. Meskipun demikian, evaluasi pada penelitian-penelitian tersebut belum sepenuhnya mengadopsi instrumen Indeks KAMI 5.0 yang telah diselaraskan dengan standar global tersebut.

Pembaruan instrumen menjadi Indeks KAMI Versi 5.0 membawa perubahan signifikan dengan penyelarasan terhadap ISO/IEC 27001:2022. Terkait hal ini, [12] berhasil memetakan profil risiko sistem elektronik dalam kategori "Tinggi" pada Satuan Logistik POLRI. Di sektor swasta, Penelitian oleh [6] menganalisis tingkat kematangan keamanan informasi pada PT XYZ dengan fokus pada stabilitas sistem. Meskipun demikian, belum ada penelitian yang secara spesifik mengkaji institusi sektor investasi yang memiliki tantangan ganda berupa pengelolaan aset publik bernilai tinggi dan kepatuhan terhadap regulasi pasar modal. Di sektor teknologi finansial (fintech), tantangan keamanan menjadi lebih dinamis karena ketergantungan penuh pada infrastruktur digital. Penelitian terkait [19] menyoroti bahwa fintech memerlukan kontrol akses yang lebih granular dibandingkan perbankan konvensional. Sementara itu, analisis terhadap kesiapan UMKM dalam mengadopsi standar keamanan informasi menunjukkan bahwa keterbatasan sumber daya seringkali menjadi hambatan utama dalam pemenuhan standar ISO 27001 [20].

Berdasarkan tinjauan di atas, terlihat adanya kesenjangan (gap) di mana belum ada penelitian yang mengevaluasi keamanan informasi pada PT X menggunakan standar terbaru Indeks KAMI Versi 5.0 yang mencakup suplemen Pelindungan Data Pribadi (PDP). Dengan demikian, penelitian ini berkontribusi untuk memperluas penerapan Indeks KAMI 5.0 dalam konteks institusi sektor keuangan yang memiliki kompleksitas regulasi dan infrastruktur yang tinggi.

2.2. *Landasan Teori*

Keamanan informasi merupakan upaya sistematis dalam melindungi informasi dari berbagai ancaman untuk menjamin kelanjutan proses bisnis dan meminimalkan risiko (ISO/IEC 27000:2018). Prinsip dasar keamanan informasi berpusat pada CIA Triad (Kerahasiaan, Keutuhan, Ketersediaan). Efektivitas penerapan ISO 27001 sangat bergantung pada siklus *Plan-Do-Check-Act* (PDCA) yang memastikan perbaikan berkelanjutan. Studi menunjukkan bahwa organisasi yang mengintegrasikan siklus PDCA secara disiplin memiliki tingkat ketahanan (*resilience*) yang lebih tinggi terhadap serangan siber dibandingkan yang hanya berfokus pada kepatuhan administratif semata [21]. Penelitian [13] menambahkan bahwa penilaian risiko keamanan

p-ISSN : 2803-1507 e-ISSN : 2803-1531

informasi menjadi metode fundamental untuk mengidentifikasi kerentanan sebelum dampak negatif terjadi. Dalam lingkungan industri perbankan dan keuangan, [22] menegaskan bahwa implementasi keamanan siber yang kuat sangat diperlukan untuk menanggulangi ancaman cybercrime yang dapat merusak reputasi institusi dan kepercayaan publik.

Tata kelola keamanan informasi memastikan keselarasan antara strategi keamanan dengan tujuan bisnis. Standar ISO/IEC 27001:2022 menjadi acuan utama dalam penerapan Sistem Manajemen Keamanan Informasi (SMKI). Sebuah artikel penelitian keamanan siber [5] menemukan bukti empiris bahwa tata kelola keamanan siber yang kuat berkontribusi positif terhadap inovasi perusahaan. Penelitian manajemen risiko menambahkan bahwa implementasi ISO 27001:2022 membantu organisasi menyusun kerangka kerja manajemen risiko yang sistematis, yang sangat krusial bagi organisasi yang mengelola data transaksi keuangan masif [23].

Indeks Keamanan Informasi (KAMI) adalah alat evaluasi yang dikembangkan oleh BSSN untuk menganalisis tingkat kesiapan keamanan informasi. Versi 5.0 (2023) telah diselaraskan penuh dengan SNI ISO/IEC 27001:2022. Evaluasi ini mencakup lima area inti (Tata Kelola, Risiko, Kerangka Kerja, Aset, Teknologi) dan satu suplemen (PDP) yang dirancang untuk memotret kondisi kematangan [24]. Indeks KAMI mengukur kinerja keamanan informasi menggunakan skala tingkat kematangan yang diadopsi dari standar CMMI (*Capability Maturity Model Integration)*. Konsep model kematangan ini penting untuk memetakan kemampuan organisasi dalam mengelola keamanan informasi dari tahap reaktif menuju proaktif [4]. Tingkatan tersebut didefinisikan sebagai berikut:

1. Tingkat I (Kondisi Awal): Proses keamanan dilakukan secara ad-hoc dan tidak terencana.
2. Tingkat II (Penerapan Dasar): Proses keamanan dilakukan berulang namun belum terdokumentasi dengan baik.
3. Tingkat III (Terdefinisasi): Proses sudah distandarisasi, didokumentasikan, dan dikomunikasikan.
4. Tingkat IV (Terkelola dan Terukur): Manajemen mengawasi dan mengukur efektivitas proses secara kuantitatif.
5. Tingkat V (Optimal): Fokus pada peningkatan proses berkelanjutan (continuous improvement).

Suplemen PDP dalam Indeks KAMI 5.0 merespons pengesahan UU PDP No. 27 Tahun 2022. Area ini mengevaluasi siklus hidup data pribadi untuk mencegah penyalahgunaan. Regulasi keamanan siber yang ketat terbukti dapat mendorong transformasi digital yang lebih aman dan terpercaya [1]. Oleh karena itu, aspek Pelindungan Data Pribadi (PDP) menjadi elemen integral dalam penilaian kematangan keamanan informasi menggunakan Indeks KAMI 5.0 di PT X.

Evaluasi keamanan informasi pada PT X memerlukan pendekatan sistematis yang mengacu pada standar ISO/IEC 27001:2022. Kerangka pemikiran penelitian ini menempatkan Indeks KAMI Versi 5.0 sebagai instrumen utama untuk memotret kondisi faktual keamanan informasi perusahaan melalui perbandingan kondisi existing terhadap kriteria standar pada tujuh area evaluasi.

Secara operasional, kerangka pemikiran ini mengadopsi pendekatan penilaian kepatuhan berbasis risiko (risk-based compliance assessment) sebagaimana disarankan [14]. Proses diawali dengan identifikasi risiko pada aset informasi perusahaan, dilanjutkan dengan asesmen menggunakan instrumen Indeks KAMI. Hasil asesmen kemudian dianalisis untuk menentukan skor dan tingkat kematangan (*maturity level*) saat ini. Output akhir dari kerangka ini adalah identifikasi kesenjangan (*gap analysis*) yang menjadi landasan bagi perumusan rekomendasi strategis guna meningkatkan status keamanan informasi perusahaan.

3. METODOLOGI PENELITIAN

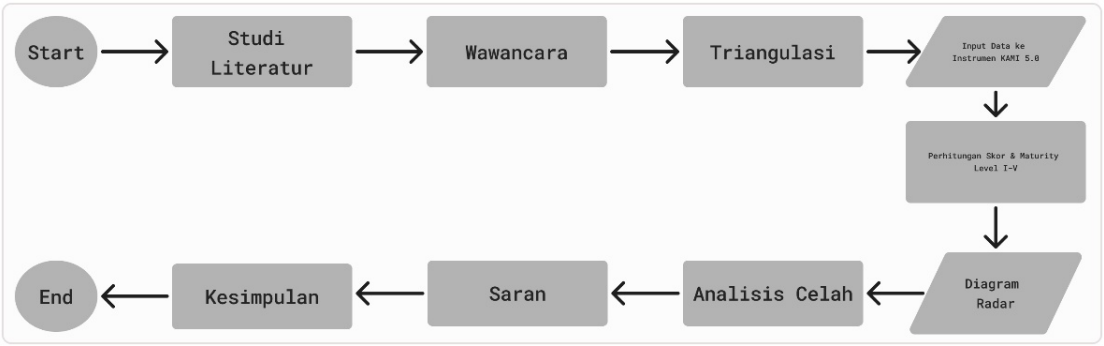
3.1. *Alur Penelitian*

Penelitian ini menerapkan metode penelitian deskriptif dengan pendekatan kuantitatif untuk memberikan gambaran yang akurat, sistematis, dan faktual mengenai profil risiko serta tingkat kematangan keamanan informasi pada PT X. Metode deskriptif dipilih karena penelitian ini bertujuan untuk menyajikan uraian mendalam mengenai karakteristik sistem atau situasi komputasi yang sedang berjalan saat ini sebagaimana adanya, tanpa melakukan percobaan yang mengubah variabel lingkungan [25]. Selanjutnya, prinsip kuantitatif diterapkan karena fokus utama penelitian adalah melakukan pengukuran sistematis menggunakan data numerik untuk menjelaskan fenomena secara objektif [26], yang diimplementasikan melalui penggunaan instrumen standar Indeks KAMI Versi 5.0 untuk menghasilkan skor terukur yang merepresentasikan level kematangan (*maturity level*) sistem elektronik perusahaan. Penggunaan instrumen

p-ISSN : 2803-1507 e-ISSN : 2803-1531

berbasis indeks seperti KAMI 5.0 memungkinkan organisasi untuk melakukan self-assessment yang terukur. Pendekatan evaluasi berbasis maturitas ini dinilai efektif untuk memetakan kesenjangan (gap) antara kondisi aktual dengan kondisi yang diharapkan secara objektif [27]. Selain itu, validasi data melalui wawancara mendalam dengan *stakeholder* (Pemangku kepentingan) yang memiliki peran lebih tinggi sangat disarankan untuk meminimalisir bias subjektivitas dalam pengisian kuesioner mandiri [28].

Seluruh tahapan pelaksanaan disusun secara sistematis mulai dari persiapan, pengumpulan data, asesmen menggunakan instrumen, hingga analisis akhir. Langkah-langkah metodologis ini dirancang untuk memandu jalannya penelitian agar tetap konsisten dengan tujuan evaluasi. Rincian alur kerja penelitian tersebut divisualisasikan secara komprehensif dalam diagram alir (*flowchart*) yang disajikan pada Gambar 1.



Gambar 1. Diagram Alir

Tahapan penelitian disusun secara sistematis untuk memastikan hasil evaluasi yang akurat, alur penelitian meliputi:

1. Studi Literatur: Mempelajari teori manajemen risiko, standar ISO/IEC 27001:2022, serta panduan evaluasi Indeks KAMI 5.0.
2. Pengumpulan Data: Melakukan observasi dokumen dan wawancara dengan pemilik risiko atau unit IT di PT X.
3. Asesmen Risiko & Keamanan (Indeks KAMI): Mengisi instrumen evaluasi untuk memotret kondisi kontrol keamanan saat ini berdasarkan bukti objektif.
4. Analisis & Pelaporan Profil Risiko: Mengolah skor menjadi tingkat kematangan (*maturity level*), memvisualisasikan data, dan mendeskripsikan profil risiko keamanan informasi perusahaan.

3.2. *Lokasi dan Waktu*

Penelitian ini mengambil objek pada PT X yang berkantor pusat di Jakarta Pusat. Proses pengambilan data profil risiko dilaksanakan secara daring (*online*) melalui platform Google Meeting pada 1 November 2025. Kegiatan ini melibatkan Divisi Teknologi Informasi sebagai unit kerja strategis yang bertanggung jawab mengelola infrastruktur kritis perusahaan.

3.3. *Metode Pengumpulan Data*

Untuk memetakan kondisi risiko secara akurat, penelitian ini menggunakan dua metode pengumpulan data utama:

1. Wawancara (*Interview*): Dilakukan dengan narasumber perwakilan dari Divisi Teknologi Informasi. Wawancara bertujuan untuk mengidentifikasi penerapan kontrol risiko di lapangan serta mengklarifikasi jawaban asesmen yang bersifat teknis.
2. Observasi Dokumen: Peneliti meninjau bukti dokumen kebijakan, prosedur manajemen risiko (SOP), dan dokumentasi aset teknologi. Peninjauan ini berfungsi untuk memastikan bahwa jawaban yang diinput ke dalam instrumen didukung oleh bukti objektif.

Validasi data dilakukan melalui teknik triangulasi, yaitu membandingkan hasil wawancara dengan temuan pada dokumen fisik untuk memastikan konsistensi dan keandalan data sebelum dilakukan penilaian skor.

3.4. *Instrumen Penelitian*

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Instrumen utama yang digunakan adalah Indeks Keamanan Informasi (KAMI) Versi 5.0 yang dikembangkan oleh BSSN. Instrumen ini berfungsi sebagai alat Asesmen Risiko (*Risk Assessment Tool*) untuk mengukur sejauh mana kontrol keamanan berbasis ISO/IEC 27001:2022 telah diterapkan. Struktur instrumen mencakup:

1. Bagian I (Profil Risiko Sistem): Kuesioner untuk menentukan klasifikasi Sistem Elektronik (SE) apakah tergolong Rendah, Tinggi, atau Strategis.
2. Bagian II - VI (Area Inti): Kuesioner evaluasi kontrol pada lima area utama: Tata Kelola, Pengelolaan Risiko, Kerangka Kerja, Pengelolaan Aset, dan Teknologi.
3. Bagian VII (Suplemen PDP): Kuesioner evaluasi risiko kepatuhan terhadap Pelindungan Data Pribadi sesuai UU PDP.

Penilaian dilakukan menggunakan skala Likert sederhana sesuai pedoman instrumen:

1. Skor 0 (Tidak Dilakukan).
2. Skor 1 (Dalam Perencanaan).
3. Skor 2 (Diterapkan Sebagian).
4. Skor 3 (Diterapkan Secara Menyeluruh).

3.5. *Metode Analisis Data*

Analisis data dilakukan untuk mengonversi data hasil asesmen menjadi informasi bermakna terkait tingkat kematangan keamanan informasi. Metode deskriptif kuantitatif digunakan untuk menghasilkan Profil Kematangan Keamanan Informasi dengan tahapan sebagai berikut:

1. Penetapan Kategori Sistem Elektronik (SE): Menghitung skor Bagian I untuk menetapkan profil eksposur risiko sistem. Berdasarkan data awal, sistem dikategorikan sebagai "Tinggi" (Skor 21), yang mengindikasikan bahwa sistem memiliki dampak vital bagi operasional dan pelayanan publik jika terjadi insiden.
2. Perhitungan Tingkat Kematangan (*Maturity Level*): Data hasil asesmen pada lima area inti dan suplemen PDP diolah secara otomatis oleh perangkat lunak Indeks KAMI untuk menghasilkan skor akhir. Skor ini dikonversi menjadi *Level* Kematangan (I sampai V) sesuai kriteria kelengkapan kontrol.
3. Visualisasi dan Interpretasi Profil Risiko: Hasil tingkat kematangan divisualisasikan menggunakan diagram radar untuk mempermudah pembacaan profil kekuatan dan kelemahan keamanan. Hasil ini kemudian dideskripsikan untuk menjelaskan status keamanan informasi perusahaan saat ini (misalnya: "Cukup Baik" atau "Perlu Perbaikan"). Analisis ini menjawab seberapa siap PT X dalam menghadapi ancaman siber dan memenuhi kepatuhan regulasi.

4. HASIL DAN PEMBAHASAN

Temuan hasil asesmen keamanan informasi pada PT X menggunakan instrumen Indeks Keamanan Informasi (KAMI) Versi 5.0 yang diselaraskan dengan SNI ISO/IEC 27001:2022. Hasil asesmen mencakup tujuh area evaluasi, yaitu Kategori Sistem Elektronik (SE), Tata Kelola, Pengelolaan Risiko, Kerangka Kerja, Pengelolaan Aset, Teknologi, dan Perlindungan Data Pribadi (PDP). Setiap area dianalisis berdasarkan skor tingkat kematangan (maturity level) dan kesesuaian kontrol keamanan dengan standar.

4.1. *Profil Sistem Elektronik*

Hasil perhitungan pada Bagian I Indeks KAMI menunjukkan bahwa sistem elektronik PT X termasuk dalam kategori Tinggi, dengan Skor Penetapan Kategori Sistem Elektronik sebanyak 21. Klasifikasi ini mengindikasikan bahwa sistem tersebut memiliki tingkat kekritisan dan eksposur risiko yang signifikan, yang apabila terjadi insiden yang dapat menyebabkan kerugian finansial atau dampak operasional yang fatal.

4.2. *Tingkat Kematangan (Maturity Level)*

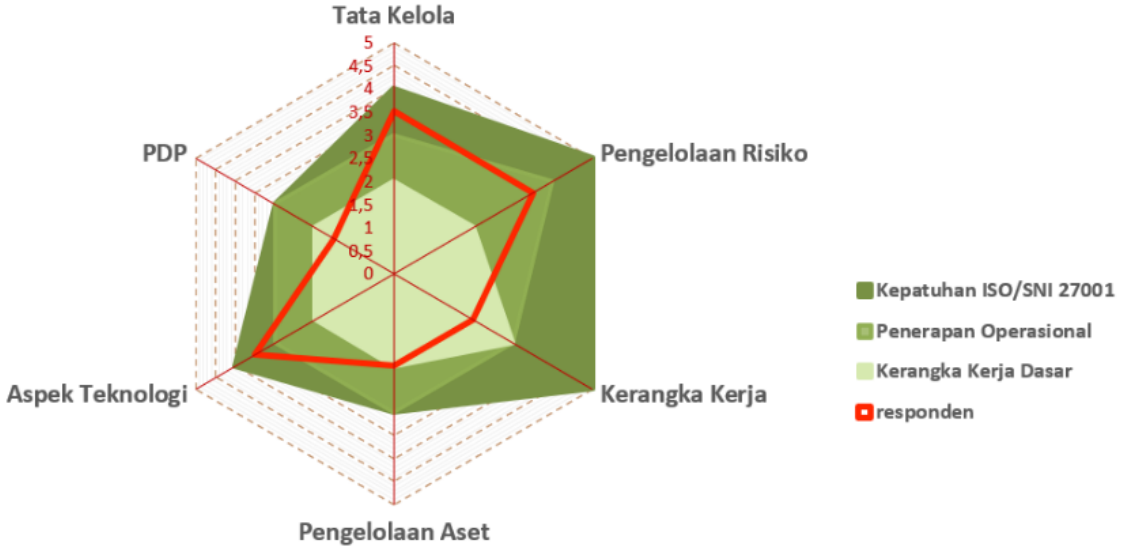
Hasil evaluasi Indeks KAMI 5.0 menunjukkan bahwa secara agregat, status keamanan informasi PT X berada pada predikat "Cukup Baik" dengan Total Skor 730. Capaian ini menunjukkan bahwa kerangka kerja keamanan informasi telah diterapkan, namun masih memerlukan peningkatan konsistensi dan formalisasi dokumentasi. Meskipun status agregat dinilai cukup baik, terdapat variasi tingkat kematangan yang signifikan antar area kontrol. Rincian capaian skor dan tingkat kematangan untuk setiap area disajikan dalam Tabel 1.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Tabel 1. Hasil Evaluasi Tingkat Kematangan Keamanan Informasi

No	Area	Skor	Tingkat Kematangan	Status
1	Tata Kelola	115	III+	Terdefinisi
2	Pengelolaan Risiko	64	III+	Terdefinisi
3	Kerangka Kerja	175	II	Penerapan Dasar
4	Pengelolaan Aset	174	II	Penerapan Dasar
5	Teknologi dan Keamanan Informasi	165	III+	Terdefinisi
6	Pelindungan Data Pribadi (PDP)	37	I+	Kondisi Awal Tinggi

Visualisasi profil kematangan keamanan informasi PT X dapat dilihat melalui diagram radar (radar chart) pada Gambar 2, yang memperlihatkan kesenjangan antara kondisi saat ini dengan target ideal (*Level* IV/V).



Gambar 2. Diagram Radar Profil Kematangan Keamanan Informasi (KAMI)

4.3. *Analisis Celah*

Area Kerangka Kerja masih berada pada *Level* II (Penerapan Dasar), tertinggal dibandingkan Tata Kelola dan Teknologi yang telah mencapai *Level* III+. Kondisi ini menunjukkan fenomena di mana praktik keamanan dijalankan secara rutin (*process performed*), namun belum didukung oleh dokumentasi formal yang memadai. Dokumen krusial seperti Rencana Tanggap Insiden (*Incident Response Plan*) dan prosedur pencadangan data (*backup policy*) belum sepenuhnya disahkan atau disosialisasikan secara sistematis. Hal ini menjadi penghambat utama bagi PT X untuk naik ke *Level* III, yang mensyaratkan adanya standarisasi proses yang terdokumentasi dan terlembaga.

Senada dengan Kerangka Kerja, area Pengelolaan Aset juga tertahan di *Level* II. Kondisi ini menunjukkan adanya ketidakselarasan strategis (strategic misalignment) di mana keamanan informasi di PT X masih sangat bergantung pada kapabilitas individu (*people-dependent*) dan teknologi, bukan pada sistem manajemen yang lebih stabil. Kelemahan mendasar terletak pada absennya proses formal untuk klasifikasi aset informasi yang terintegrasi. Kelemahan ini menciptakan asimetri informasi antara manajemen risiko dan operasional teknis. Tanpa klasifikasi yang jelas, organisasi tidak dapat menerapkan prinsip defense-in-depth secara efisien, yang berimplikasi pada inefisiensi alokasi sumber daya pertahanan. Aset bernilai rendah mungkin diproteksi secara berlebihan (over-secured), sementara aset strategis atau Crown Jewels justru berpotensi terekspos karena diperlakukan sama dengan data umum. Dalam jangka panjang, hal ini melemahkan resiliensi organisasi dalam menghadapi serangan yang menargetkan integritas data finansial. Temuan ini mengonfirmasi urgensi penerapan manajemen aset berbasis risiko sebagaimana hasil saran penelitian sebelumnya [23].

Area ini mencatatkan skor terendah, yaitu Level I+ (Kondisi Awal). Ini merupakan temuan paling kritis mengingat ketatnya regulasi saat ini. Implementasi kebijakan yang diamanatkan oleh UU PDP No. 27 Tahun 2022 masih bersifat inisiatif parsial dan belum terstruktur. Secara spesifik, PT X belum memformalkan fungsi Pejabat Pelindungan Data Pribadi (Data Protection Officer/DPO), serta belum memiliki mekanisme manajemen persetujuan (consent) yang transparan maupun prosedur pemenuhan hak subjek data. Rendahnya

p-ISSN : 2803-1507 e-ISSN : 2803-1531

kematangan di area ini mengekspos perusahaan pada risiko hukum dan sanksi denda administratif yang substansial, sebuah tantangan yang juga disoroti sebagai isu utama dalam transformasi digital yang aman [1]. Rendahnya kematangan pada aspek PDP memiliki implikasi strategis yang melampaui sekadar risiko sanksi administratif. Bagi institusi di sektor jasa keuangan seperti PT X, pelindungan data pribadi merupakan fondasi utama dari Kepercayaan Digital (*Digital Trust*). Kegagalan dalam melembagakan privasi data berisiko mendegradasi reputasi jangka panjang yang jauh lebih sulit dipulihkan dibandingkan kerugian finansial langsung. Oleh karena itu, pemenuhan standar PDP harus dipandang bukan sebagai beban kepatuhan semata, melainkan sebagai investasi strategis untuk menjaga legitimasi operasional perusahaan.

4.4. *Usulan Strategis*

Berdasarkan analisis celah, tiga prioritas utama harus difokuskan pada formalisasi dokumentasi dan peningkatan kepatuhan regulasi data untuk mencapai Tingkat Kematangan minimum Level III dalam waktu dekat. Prioritas paling krusial adalah mengangkat area PDP dari Level I+ ke Level III. Pencapaian ini menuntut PT X untuk segera memformalkan kepatuhan terhadap UU PDP. Strategi utamanya adalah menunjuk dan menetapkan Pejabat Pelindungan Data Pribadi (DPO) yang bertanggung jawab penuh terhadap program PDP. Selanjutnya, organisasi harus menyusun kebijakan siklus hidup data komprehensif (mulai dari perolehan, penyimpanan, pemrosesan, hingga pemusnahan) dan mekanisme penanganan permintaan subjek data yang terstruktur.

Untuk mengatasi defisiensi pada area Kerangka Kerja (Level II), strategi peningkatan harus berfokus pada Standarisasi Dokumen SMKI. PT X diwajibkan untuk menyelesaikan, mengesahkan, dan mensosialisasikan seluruh Kebijakan Keamanan Informasi, Prosedur Operasional Standar (SOP) teknis, dan dokumen struktural penting seperti Rencana Kelangsungan Bisnis (BCP) dan Rencana Tanggap Insiden (IRP).

Area Pengelolaan Aset dari Level II ke Level III harus dilakukan melalui Integrasi Klasifikasi Aset. Strategi ini menuntut PT X untuk memformalisasi proses klasifikasi aset informasi yang mengaitkan tingkat sensitivitas data (contoh: Rahasia, Terbatas, Biasa) dengan kontrol keamanan yang diterapkan dan penunjukan pemilik aset yang bertanggung jawab, dengan menerapkan klasifikasi yang jelas dan kontrol akses (termasuk *role-based access control*).

Implementasi usulan perbaikan di atas ditujukan untuk mengubah paradigma keamanan informasi PT X dari pendekatan reaktif menuju tata kelola berbasis risiko yang adaptif. Dengan memformalisasi kerangka kerja dan manajemen aset, PT X dapat beralih dari sekadar mengejar kepatuhan (*compliance-driven*) menuju pemberdayaan budaya sadar risiko (risk-aware culture). Transformasi ini krusial untuk memastikan bahwa investasi teknologi keamanan yang telah dilakukan selaras dengan tujuan bisnis jangka panjang, serta menjamin bahwa mekanisme pertahanan organisasi mampu berevolusi seiring dengan dinamika ancaman siber.

5. DISKUSI

Hasil evaluasi menunjukkan bahwa Sistem Elektronik PT X berada dalam kategori *Tinggi*, yang merefleksikan tingkat ketergantungan operasional dan eksposur risiko yang signifikan terhadap keberlangsungan layanan. Klasifikasi ini memperlihatkan bahwa kegagalan pengendalian keamanan berpotensi menimbulkan dampak finansial dan reputasional yang besar. Kondisi tersebut sejalan dengan temuan [2] yang menjelaskan bahwa institusi jasa keuangan memiliki profil risiko siber yang lebih kompleks dibandingkan sektor lain akibat sensitivitas data yang dikelola. Dalam konteks ini, pemetaan risiko melalui Indeks KAMI 5.0 memberikan dasar yang relevan untuk memahami posisi keamanan informasi PT X secara objektif.

Variasi tingkat kematangan antar area menunjukkan adanya ketimpangan antara aspek tata kelola dan aspek struktural keamanan informasi. Area Tata Kelola, Pengelolaan Risiko, dan Teknologi yang telah mencapai Level III+ menunjukkan bahwa praktik pengendalian keamanan telah berjalan secara konsisten dan terdefinisi. Pola ini mencerminkan pandangan [11] bahwa penerapan ISO/IEC 27001:2022 mampu memperkuat struktur manajemen keamanan pada organisasi sektor keuangan. Namun, perbedaan capaian ini juga mengindikasikan bahwa keberhasilan kontrol teknis tidak selalu diikuti oleh kematangan dokumentasi dan kerangka kerja organisasi.

Area Kerangka Kerja dan Pengelolaan Aset yang masih berada pada Level II memperlihatkan bahwa praktik keamanan informasi belum sepenuhnya dilembagakan melalui dokumentasi formal. Kondisi ini

p-ISSN : 2803-1507 e-ISSN : 2803-1531

menunjukkan ketergantungan yang tinggi pada individu dan pengalaman praktis dibandingkan sistem manajemen yang terdokumentasi. Fenomena serupa juga diidentifikasi oleh [23] yang menekankan bahwa absennya klasifikasi aset dan kebijakan formal menghambat penerapan manajemen risiko berbasis standar. Dalam konteks PT X, keterbatasan ini berimplikasi pada sulitnya menerapkan kontrol keamanan yang proporsional terhadap nilai dan sensitivitas aset informasi.

Temuan paling kritis terdapat pada area Pelindungan Data Pribadi (PDP) yang masih berada pada Level I+, yang menunjukkan bahwa kepatuhan terhadap UU PDP No. 27 Tahun 2022 masih bersifat awal. Kondisi ini mencerminkan tantangan yang juga disoroti dalam penelitian [1] terkait kesiapan organisasi dalam menyesuaikan regulasi keamanan siber dengan praktik operasional. Bagi institusi jasa keuangan, rendahnya kematangan PDP tidak hanya berkaitan dengan risiko sanksi hukum, tetapi juga dengan kepercayaan publik terhadap pengelolaan data pribadi. Dalam kerangka *digital trust*, pelindungan data pribadi berfungsi sebagai fondasi legitimasi operasional yang memengaruhi keberlanjutan organisasi dalam jangka panjang.

6. KESIMPULAN DAN SARAN

6.1. *Kesimpulan*

Berdasarkan evaluasi keamanan informasi yang dilakukan pada PT X menggunakan instrumen Indeks KAMI Versi 5.0 yang diselaraskan dengan standar ISO/IEC 27001:2022, disimpulkan bahwa Sistem Elektronik (SE) perusahaan tergolong dalam kategori "Tinggi" dengan skor 21, yang mengindikasikan tingginya eksposur risiko dan peran strategis sistem terhadap keberlangsungan operasional. Secara agregat, status keamanan informasi mencapai predikat "Cukup Baik" dengan total skor 730, di mana area Tata Kelola, Pengelolaan Risiko, dan Teknologi telah menunjukkan kematangan yang memadai pada Level III+ (Terdefinisasi). Namun, terdapat ketimpangan signifikan pada area Kerangka Kerja dan Pengelolaan Aset yang masih tertahan di Level II (Penerapan Dasar) akibat kurangnya formalisasi dokumentasi standar operasional (SOP) dan klasifikasi aset, serta temuan paling kritis pada suplemen Pelindungan Data Pribadi (PDP) yang berada di Level I+ (Kondisi Awal). Hal ini menunjukkan bahwa meskipun kontrol teknis dan manajerial telah berjalan, PT X masih menghadapi celah kepatuhan serius terhadap UU PDP No. 27 Tahun 2022 dan membutuhkan penguatan struktur dokumentasi untuk mencapai standar keamanan yang lengkap.

6.2. *Saran*

Sebagai tindak lanjut atas temuan tersebut, manajemen PT X disarankan untuk segera memprioritaskan strategi perbaikan kepatuhan, dimulai dengan menunjuk Pejabat Pelindungan Data Pribadi (DPO) dan menyusun kebijakan siklus hidup data guna meningkatkan area PDP dari Level I+ ke target minimal Level III. Selanjutnya, untuk mengatasi kelemahan pada area Kerangka Kerja dan Pengelolaan Aset, organisasi perlu melakukan formalisasi dokumen Rencana Tanggap Insiden (IRP), mengesahkan seluruh kebijakan keamanan informasi (SMKI), serta menerapkan klasifikasi aset yang terintegrasi dengan kontrol akses berbasis peran. Bagi pengembangan ilmu pengetahuan di masa mendatang, mengingat penelitian ini terbatas pada potret kondisi sesaat (snapshot), peneliti selanjutnya direkomendasikan untuk melakukan studi longitudinal guna mengukur efektivitas pasca-implementasi perbaikan atau memperluas cakupan studi komparatif dengan entitas sektor keuangan lain untuk memvalidasi pola adopsi Indeks KAMI 5.0 di industri serupa.

DAFTAR PUSTAKA

[1] J. Xianglan, C. Huizhu, L. Fengwei, H. Ziqiang, and C. Yonghao, “Does Cybersecurity Regulation Promote Digital Transformation? Evidence from the Cyber Security Law in China,” *Financ. Res. Lett.*, vol. 76, p. 107041, 2025, doi: 10.1016/j.frl.2025.107041.

[2] S. Wang, M. Asif, M. F. Shahzad, and M. Ashfaq, “Data Privacy and Cybersecurity Challenges in the Digital Transformation of the Banking Sector,” *Comput. Secur.*, vol. 147, p. 104051, 2024, doi: 10.1016/j.cose.2024.104051.

[3] Riska and S. M. Sulubara, “Tantangan dan Peluang Otoritas Jasa Keuangan dalam Era Digitalisasi Layanan Keuangan,” *J. Ris. Manaj.*, vol. 2, no. 21, pp. 240–248, 2024, doi: doi.org/10.54066/jurma.v2i4.2712.

[4] M. Zammani, R. Razali, and D. Singh, “Organisational Information Security Management Maturity Model,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 9, pp. 668–678, 2021, doi:

10.14569/ijacsa.2021.0120974.

[5] J. Xu, "Cybersecurity Governance and Corporate Innovation: Evidence from China," *Financ. Res. Lett.*, vol. 82, p. 107619, 2025, doi: 10.1016/j.frl.2025.107619.

[6] T. Hasani, N. O. Reilly, A. Dehghantanha, D. Rezania, and N. Levallet, "Evaluating the Adoption of Cybersecurity and Its Influence on Organizational Performance," *SN Bus. Econ.*, vol. 3, no. 5, pp. 1–38, 2023, doi: 10.1007/s43546-023-00477-6.

[7] T. Hadlington, "The 'Human Factor' in Cybersecurity: Exploring the Accidental Insider," in *Psychological and Behavioral Examinations in Cyber Security*, J. McAlaney, L. A. Frumkin, and V. Benson, Eds., IGI Global, 2021, pp. 46–63, doi: 10.4018/978-1-5225-4053-3.ch003.

[8] S. Perera, X. Jin, A. Maurushat, and D. J. Opoku, "Factors Affecting Reputational Damage to Organisations Due to Cyberattacks," *Informatics*, vol. 9, no. 28, pp. 1–24, 2022, doi: 10.3390/ informatics9010028.

[9] H. A. Pratiwi and L. Wulandari, "Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 4.0 pada Dinas Komunikasi dan Informatika Kota Bogor," *J. Ind. Eng. Manag. Res.*, vol. 2, no. 5, pp. 146–163, 2021, doi: 10.7777/jiemar.v2i5.196.

[10] A. Kornelia and D. Irawan, "Analisis Keamanan Informasi Menggunakan Tools Indeks KAMI ISO 4.1," *J. Pengemb. Sist. Inf. dan Inform.*, vol. 2, no. 2, pp. 78–86, 2021, doi: 10.47747/jpsii.v2i2.548.

[11] K. Ryanto and V. Tundjungsari, "Standardization of Information Security Management in the Banking Sector using the ISO 27001:2022 Framework," *J. La Multiapp*, vol. 05, no. 04, pp. 361–379, 2024, doi: 10.37899/journallamultiapp.v5i4.1399.

[12] Z. S. Nadine, I. Aknuranda, and H. Farisi, "Evaluasi Pengelolaan Keamanan Informasi Berbasis Indeks KAMI 5.0 di Satuan Logistik (SLOG) Polri," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 9, no. 10, pp. 1–12, 2025. [Online]. Available: https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/15393

[13] T. Ali, M. Al-khalidi, and R. Al-zaidi, "Information Security Risk Assessment Methods in Cloud Computing : Comprehensive Review," *J. Comput. Inf. Syst.*, pp. 1–28, 2024, doi: 10.1080/08874417.2024.2329985.

[14] A. Alfaadhel, I. Almomani, and M. Ahmed, "Risk-Based Cybersecurity Compliance Assessment System (RC2AS)," *Appl. Sci.*, vol. 13, no. 10, p. 6145, 2023, doi: 10.3390/ app13106145 Academic.

[15] N. T. Mai and I. Khalid, "Human Error vs. System Security: Evaluating the Weakest Link in Digital Business Information Systems," *J. Manag. Informatics*, vol. 4, no. 3, pp. 981–997, Dec. 2025, doi: 10.51903/jmi.v4i3.305.

[16] S. Arkha, A. Nugroho, and A. Wibowo, "Evaluating Digital Transformation within Integration Limitations using Desk-Based Analytical Case Study," *J. Technol. Informatics Eng.*, vol. 4, no. 2, pp. 289–299, Aug. 2025, doi: 10.51903/jtie.v4i2.365.

[17] M. Izzani, N. Nellatul, A. Ismatul, and A. Hamdani, "Evaluasi Penerapan Kemanan Informasi pada SIAKAD Universitas Ibrahimy Berbasis ISO/IEC 27001:2022," *J. Ilm. Sist. Inf.*, vol. 5, no. 1, pp. 175–185, Jan. 2026, doi: 10.51903/d3bktm29.

[18] J. Angelo, S. Tania, and F. Loren, "Kajian Literatur Terhadap Audit Sistem Informasi pada Perusahaan Perbankan," *JDMIS J. Data Min. Inf. Syst.*, vol. 2, no. 2, pp. 82–89, 2024, doi: 10.54259/jdmis.v2i2.2216.

[19] D. Javaheri, M. Fahmideh, H. Chizari, P. Lalbakhsh, and J. Hur, "Cybersecurity Threats in FinTech: A Systematic Review," *Expert Syst. Appl.*, vol. 241, pp. 1–42, 2023, doi: 10.1016/j.eswa.2023.122697.

[20] D. Javaheri, M. Fahmideh, H. Chizari, P. Lalbakhsh, and J. Hur, "Cybersecurity Threats in FinTech: A Systematic Review," *Expert Syst. Appl.*, vol. 241, pp. 1–42, 2023, doi: 10.1016/j.eswa.2023.122697.

[21] M. Mirtsch, J. Kinne, and K. Blind, "Information Security Management System Standard ISO / IEC 27001 : A Web Mining-Based Analysis," *IEEE Trans. Eng. Manag.*, vol. 68, no. 1, pp. 87–100, 2021,

p-ISSN : 2803-1507 e-ISSN : 2803-1531

doi: 10.1109/tem.2020.2977815.

[22] N. S. Azzahra, A. M. Tambunan, N. N. Aulia, A. Binarsih, and T. H. Saepudin, "Tinjauan Literatur tentang Ancaman Cybercrime dan Implementasi Keamanan Siber di Industri Perbankan," *Humanit. J. Humaniora, Sos. dan Bisnis*, vol. 2, no. 7, pp. 692–700, 2024. https://humanisa.my.id/index.php/hms/article/view/188

[23] F. C. Arumdiya and R. Christ, "Implementasi ISO 27001:2022 dalam Manajemen Risiko Keamanan Informasi," *J. PETISI*, vol. 6, no. 2, pp. 143–155, 2025, doi: 10.36232/jurnalpetisi.v6i2.2012.

[24] Badan Siber dan Sandi Negara (BSSN), *Indeks Keamanan Informasi (KAMI) Versi 5.0: Panduan Evaluasi Keamanan Informasi*, 2023. https://www.bssn.go.id/indeks-kami

[25] A. Ghanad, "An Overview of Quantitative Research Methods," *Int. J. Multidiscip. Res. Anal.*, vol. 06, no. 08, pp. 3794–3803, 2023, doi: 10.47191/ijmra/v6-i8-52.

[26] J. Recker, *Scientific Research in Information Systems: A Beginner's Guide*, Springer International Publishing, 2021, doi: 10.1007/978-3-030-85436-2.

[27] B. Novriyadi, M. Jazman, M. Megawati, and M. Afdal, "Evaluation of Information Security Readiness Using the KAMI Index 5.0 and ISO/IEC 27001:2022," *Progresif J. Ilm. Komput.*, vol. 21, no. 2, pp. 573–585, 2025, doi: 10.35889/progresif.v21i2.2882.

[28] A. Ebekozien, C. O. Aigbavboa, and M. Ramotshela, "A Qualitative Approach to Investigate Stakeholders' Engagement in Construction Projects," *Benchmarking: An Int. J.*, vol. 31, no. 3, pp. 866–883, 2024, doi: 10.1108/bij-11-2021-0663.