JURNAL ILMIAH SISTEM INFORMASI (JUSI)
VOL 5, No. 1, Januari 2026, pp. 439 - 448
p-ISSN : 2803-1507 (media cetak) | e-ISSN : 2803-1531 (media *online*)
Link Publikasi: https://ejurnal.provisi.ac.id/index.php/JUISI/issue/view/169

Implementation of KAMI Index for IT Risk Management at PT. X

Nur Amalina Sabrina*[1], Keisha Jovie Dermawan[2], Annisa Wulandari[3], Muhammad Hafidz Fadlillah[4], Vicho Yunanda Hidayat[5], Afifah Trista Ayunda[6]
[1,2,3,4,5,6] Fakultas Sains & Teknologi, Universitas Pradita
Jl. Gading Serpong Boulevard No. 1, 15810, Tangerang, Banten, Indonesia
e-mail: nur.amalina@student.pradita.ac.id*[1], keisha.jovie@student.pradita.ac.id[2], annisa.wulandari@student.pradita.ac.id[3], muhammad.hafidz@student.pradita.ac.id[4], vicho.yunanda@student.pradita.ac.id[5], afifah.trista@pradita.ac.id[6]

ARTICLE INFO

Article History:

Received: 11-11-2025
Revised: 12-12-2025
Accepted: 04-01-2026
Published: 21-01-2026

ABSTRACT

Information security has become a critical aspect for organizations that rely heavily on information technology in their business operations. PT. X, as a large-scale shopping center operator, relies on various electronic systems, including membership systems, payment systems, CCTV systems, and parking management systems. This high degree of dependence requires a structured, measurable approach to information security. This study aims to evaluate PT's information security maturity level. X is using the Information Security Index (Indeks KAMI) Version 5.0 developed by BSSN. The research was conducted through literature review and structured interviews with the IT Department Head, and the results were processed using the official KAMI Index assessment worksheet. The evaluation results show that PT. X falls into the High Electronic System category with a total score of 563 and a maturity level of I+ (Basic Framework Fulfillment). The highest score was obtained in the Technology and Information Security area, while the weakest areas were Risk Management and Personal Data Protection. The key gaps include a lack of a defined risk appetite, the absence of formal procedures for the disposal of personal data, limited documentation of security policies, and a lack of a routine patch management process. Recommendations are proposed to address these gaps, including formalizing information security policies, implementing structured patch management, establishing secure data disposal procedures, and defining risk tolerance parameters. The findings are expected to support PT. X in prioritizing information security improvements and contributing to the literature on the application of the KAMI Index in the retail and shopping center sectors.

Keywords: *KAMI Index, Information Security, IT Risk Management, Maturity Level, PT. X.*

Abstrak

Keamanan informasi menjadi aspek yang sangat penting bagi perusahaan yang bergantung pada teknologi informasi dalam operasional bisnisnya. PT. X sebagai pengelola pusat perbelanjaan modern memiliki tingkat

DOI: https://doi.org/10.51903/pkbfwq48

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

ketergantungan tinggi terhadap sistem elektronik seperti *membership*, pembayaran, CCTV, dan perparkiran, sehingga membutuhkan pengelolaan keamanan informasi yang terstruktur. Penelitian ini bertujuan mengevaluasi tingkat kematangan keamanan informasi PT. X menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 5.0 yang dikembangkan oleh BSSN. Metode penelitian dilakukan melalui studi pustaka dan wawancara terstruktur dengan Kepala Departemen IT, kemudian hasilnya diolah menggunakan lembar kerja resmi Indeks KAMI. Hasil penelitian menunjukkan bahwa PT. X berada pada kategori Sistem Elektronik Tinggi dengan skor total 563 dan tingkat kematangan berada pada level I+ (Pemenuhan Kerangka Kerja Dasar). Area dengan skor tertinggi adalah Teknologi dan Keamanan Informasi, sementara kelemahan utama terdapat pada Pengelolaan Risiko dan Pelindungan Data Pribadi. Kesenjangan utama meliputi belum adanya penetapan *risk appetite*, belum tersedianya prosedur pemusnahan data pribadi, minimnya dokumentasi kebijakan keamanan informasi, serta belum diterapkannya *patch management* secara rutin. Rekomendasi perbaikan difokuskan pada penyusunan kebijakan keamanan informasi formal, penerapan *patch management*, penyusunan SOP pemusnahan data, serta penetapan toleransi risiko. Temuan ini diharapkan dapat membantu PT. X dalam menyusun prioritas peningkatan keamanan informasi serta memberikan kontribusi terhadap literatur penerapan Indeks KAMI di sektor retail dan pusat perbelanjaan.

Kata Kunci: *Indeks KAMI, Keamanan Informasi, Manajemen Risiko TI, Maturity level, PT. X.*

1. PENDAHULUAN

Keamanan informasi merupakan aspek yang semakin krusial di era digital, khususnya bagi sektor retail dan pusat perbelanjaan yang sangat bergantung pada teknologi informasi dalam mendukung layanan operasional dan transaksi pelanggan [1]. Peningkatan ancaman siber seperti pencurian data, serangan *ransomware*, dan penyusupan sistem membuktikan bahwa organisasi membutuhkan penerapan keamanan informasi yang kuat untuk menjaga kerahasiaan, integritas, dan ketersediaan aset informasi [2], [3], [4]. Kondisi ini menuntut perusahaan untuk memiliki manajemen risiko IT yang tersusun secara sistematis agar potensi kerugian baik bagi perusahaan maupun pelanggan dapat diminimalkan secara efektif [5], [6].

Selain itu, dengan disahkannya regulasi terkait privasi data di Indonesia, perusahaan yang mengelola data konsumen dalam jumlah besar wajib menjamin kerahasiaan data tersebut untuk menghindari sanksi hukum dan kerugian reputasi [7]. PT. X sebagai perusahaan pengembang properti dan pengelola pusat perbelanjaan skala besar merupakan contoh organisasi yang memiliki ketergantungan tinggi terhadap sistem IT dalam menjalankan operasional bisnisnya. Sistem seperti keanggotaan pelanggan (*membership*), sistem pembayaran, perparkiran, pemantauan CCTV, hingga administrasi internal membutuhkan stabilitas dan keamanan sistem yang optimal agar layanan bisnis tetap berjalan tanpa gangguan. Namun, meskipun pemanfaatan teknologi tinggi, tantangan muncul ketika perusahaan belum memiliki mekanisme evaluasi formal untuk mengukur kesiapan keamanan informasi secara menyeluruh dan terstandarisasi [8]. Hal ini memicu kesenjangan antara kondisi keamanan informasi eksisting dengan standar keamanan yang seharusnya diterapkan.

Untuk mengatasi kesenjangan tersebut, dibutuhkan alat ukur yang mampu mengevaluasi tingkat kematangan keamanan informasi dengan pendekatan yang relevan terhadap kebutuhan organisasi di Indonesia. Indeks Keamanan Informasi (Indeks KAMI) yang dikembangkan oleh Badan Siber dan Sandi Negara (BSSN) dirancang untuk menilai kesiapan keamanan informasi organisasi berdasarkan pedoman keamanan nasional dan kesesuaian terhadap ISO/IEC 27001 [5]. Indeks KAMI bukanlah alat audit teknis, tetapi alat evaluasi manajerial untuk mengukur tingkat kematangan TI dalam lima area utama: Tata kelola, Pengelolaan Risiko, Kerangka Kerja Keamanan Informasi, Pengelolaan Teknologi dan Keamanan, serta Pengelolaan Aset Informasi [9]. Struktur penilaian ini menjadikan Indeks KAMI relevan bagi organisasi non-pemerintahan dan korporasi seperti PT. X.

Secara spesifik, penelitian ini bertujuan untuk mengukur tingkat kematangan keamanan informasi PT. X, mengidentifikasi kesenjangan (*gap*) keamanan informasi berdasarkan hasil evaluasi, serta memberikan rekomendasi perbaikan untuk meningkatkan tata kelola keamanan informasi secara berkelanjutan. Ruang lingkup evaluasi dalam penelitian ini mencakup penilaian pada area Tata Kelola, Pengelolaan Risiko, Kerangka Kerja Keamanan Informasi, Pengelolaan Teknologi dan Keamanan, Pengelolaan Aset Informasi, serta aspek Perlindungan Data Pribadi (PDP) dan Suplemen. Hasil penelitian diharapkan dapat membantu manajemen PT. X dalam menentukan prioritas perbaikan serta memberikan kontribusi akademis mengenai profil risiko TI di sektor pusat perbelanjaan. Penelitian ini tidak mencakup audit teknis mendalam seperti

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

penetration testing maupun *vulnerability assessment* karena fokus penelitian berada pada aspek manajerial dan tata kelola keamanan informasi, bukan aspek investigasi teknis.

2. TINJAUAN PUSTAKA

2.1. *Landasan Teori dan Kerangka Evaluasi*

Berbagai penelitian menunjukkan bahwa penerapan manajemen risiko keamanan informasi berperan penting dalam upaya organisasi melindungi kerahasiaan, integritas, dan ketersediaan aset informasi dari ancaman siber. Berbagai studi menegaskan bahwa pengelolaan risiko yang efektif diperlukan untuk meminimalkan potensi gangguan operasional akibat kegagalan sistem maupun kebocoran data. Dalam konteks nasional Indonesia, evaluasi terhadap efektivitas manajemen keamanan ini dilakukan menggunakan instrumen Indeks Keamanan Informasi (Indeks KAMI) yang dikembangkan oleh Badan Siber dan Sandi Negara (BSSN). Sejumlah studi sebelumnya memanfaatkan Indeks KAMI sebagai kerangka evaluasi untuk menilai tingkat kematangan penerapan keamanan informasi organisasi dengan mengacu pada standar SNI ISO/IEC 27001. Pendekatan Indeks KAMI dalam penelitian-penelitian tersebut umumnya digunakan untuk menilai kesiapan tata kelola dan pengelolaan keamanan informasi dari perspektif manajerial, bukan untuk menguji aspek teknis sistem secara mendalam. Melalui evaluasi ini, pimpinan organisasi dapat memperoleh gambaran utuh mengenai kesiapan tata kelola keamanan mereka, mulai dari aspek risiko, pengelolaan aset, hingga aspek teknologi, guna menentukan strategi perbaikan yang tepat sasaran.

2.2. *Penelitian Terdahulu dan Posisi Penelitian*

Evaluasi kesiapan keamanan informasi menggunakan instrumen Indeks KAMI telah banyak diterapkan di berbagai sektor untuk memetakan kepatuhan terhadap standar ISO/IEC 27001. Peneliti [10] melakukan pengukuran pada Dinas Komunikasi dan Informatika Kota Pontianak dan menemukan bahwa tingkat kematangan berada pada rentang level I+ hingga III+. Studi tersebut menyoroti perlunya perbaikan mendasar pada aspek tata kelola dan pengelolaan aset. Temuan serupa didapatkan oleh Pratiwi & Wulandari [11] yang mengevaluasi Diskominfo Kota Bogor menggunakan Indeks KAMI versi 4.0. Hasilnya menunjukkan area terlemah berada pada pengelolaan risiko dengan skor yang minim, sehingga rekomendasi difokuskan pada pemenuhan level III sesuai standar ISO 27001.

Di sektor pendidikan, [12] mengevaluasi Sistem Informasi Akademik UIN Sunan Kalijaga dan mencatatkan skor pada level Pemenuhan Kerangka Kerja Dasar. Penelitian ini menekankan bahwa meskipun aspek teknologi sudah cukup baik, pengelolaan risiko dan aset seringkali tertinggal. Sementara itu, pada sektor privat khususnya perbankan, [13] menganalisis PT. BPR Jawa Timur menggunakan Indeks KAMI versi 4.1. Hasil studi menunjukkan bahwa meskipun sektor perbankan memiliki kematangan teknologi dan aset yang tinggi (Level III-IV), aspek tata kelola dan manajemen risiko masih berada pada level dasar (Level II). Hal ini mengindikasikan pola umum di mana investasi teknologi seringkali mendahului kematangan kebijakan manajerial.

Penelitian ini memiliki perbedaan signifikan dengan studi-studi sebelumnya. Jika penelitian terdahulu didominasi oleh objek sektor publik dan keuangan, penelitian ini berfokus pada sektor retail dan pusat perbelanjaan yang memiliki dinamika interaksi pelanggan yang tinggi. Selain itu, penggunaan instrumen Indeks KAMI Versi 5.0 dalam penelitian ini memungkinkan evaluasi yang lebih komprehensif, mencakup aspek Perlindungan Data Pribadi (PDP) yang belum banyak dibahas pada versi sebelumnya. Ringkasan perbandingan antara penelitian ini dengan penelitian terdahulu disajikan secara rinci dalam Tabel 1.

Tabel 1. Komparasi Penelitian

No	Peneliti	Tahun	Objek	Metode	Hasil	Gap
1	Rahayu et al.	2021	Diskominfo Pontianak	Deskriptif, Indeks KAMI	Kematangan level I–III, perlu perbaikan tata kelola, risiko, aset	Belum spesifik bahas manajemen risiko TI di sektor bisnis
2	Pratiwi & Wulandari	2021	Diskominfo Bogor	Deskriptif kualitatif, KAMI 4.0	Skor 395 (level I–II), area terlemah pengelolaan risiko (29)	*Gap* risiko hanya diidentifikasi, belum ada *gap analysis* terstruktur
3	Hidayatullah et al.	2025	SIA UIN Sunan Kalijaga	Kuesioner, KAMI 4.0, ISO 27001	Skor 407 (kerangka dasar), risiko dan aset masih rendah	Fokus kesiapan sertifikasi kampus, bukan manajemen risiko TI korporat

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

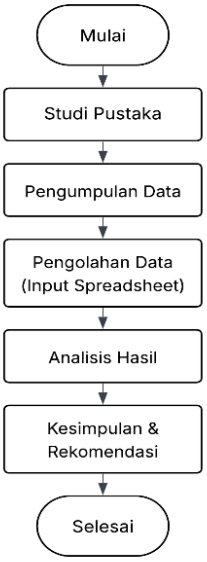
4	Balqis et al.	2023	PT BPR Jatim	Literatur + wawancara, KAMI 4.1/4.2	Skor 549, aset & teknologi tinggi, risiko & tata kelola masih dasar	Tidak mengulas risiko TI di konteks retail/pusat belanja

Melalui Tabel 1, terlihat bahwa kesenjangan utama yang ingin dijawab oleh penelitian ini adalah belum adanya analisis mendalam mengenai manajemen risiko TI menggunakan Indeks KAMI versi terbaru pada model bisnis pusat perbelanjaan, yang memiliki risiko kebocoran data pribadi yang tinggi namun seringkali tidak se-terregulasi sektor perbankan.

3. METODOLOGI PENELITIAN

3.1. *Tahapan dan Instrumen Penelitian*

Penelitian ini dilaksanakan melalui serangkaian langkah terstruktur yang diadaptasi dari prosedur evaluasi standar Indeks KAMI. Tahapan dimulai dengan studi pustaka mengenai standar ISO/IEC 27001 dan pedoman Indeks KAMI Versi 5.0, dilanjutkan dengan pengumpulan data, pengolahan data, analisis hasil, hingga penarikan kesimpulan. Instrumen utama yang digunakan adalah Lembar Kerja Evaluasi (*Spreadsheet*) Indeks KAMI Versi 5.0 yang dikeluarkan oleh BSSN.



Gambar 1. Alur Tahapan Penelitian

Instrumen ini terdiri dari bagian identifikasi Kategori Sistem Elektronik (SE) serta tujuh area pengukuran kematangan, mencakup: Tata Kelola, Pengelolaan Risiko, Kerangka Kerja, Pengelolaan Aset, Teknologi dan Keamanan, Perlindungan Data Pribadi (PDP), dan Suplemen. Alur penelitian divisualisasikan dalam Diagram Alir (*Flowchart*) pada Gambar 1, dengan rincian tahapan sebagai berikut:

1. Studi Pustaka: Penelaahan literatur mengenai standar ISO/IEC 27001 serta pedoman teknis Indeks KAMI versi 5.0 sebagai landasan teori utama.
2. Pengumpulan Data: Melakukan wawancara dengan Kepala Departemen TI (*IT Head*) PT. X mengacu pada daftar kuesioner dalam lembar kerja (*Spreadsheet*) Indeks KAMI.
3. Pengolahan Data: Menginput hasil wawancara ke dalam *Spreadsheet* evaluasi. Formula sistem secara otomatis akan memetakan Kategori Sistem Elektronik (SE) dan menghitung Skor Kematangan pada tujuh area keamanan informasi lainnya.
4. Analisis Hasil: Menganalisis skor akhir dan grafik visual untuk menentukan tingkat kelayakan keamanan informasi perusahaan.
5. Kesimpulan & Rekomendasi: Merumuskan kesimpulan status keamanan saat ini dan menyusun saran perbaikan strategis.

3.2. *Pengumpulan Data dan Analisis Data*

Pengumpulan data dilakukan melalui wawancara terstruktur dengan Kepala Departemen TI (*IT Head*) PT. X. Jawaban narasumber diverifikasi dan diinput ke dalam sistem evaluasi untuk menghasilkan skor kuantitatif.

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

Analisis data dilakukan secara otomatis oleh sistem melalui dua tahap utama. Pertama, penentuan Kategori Sistem Elektronik (SE) berdasarkan tingkat ketergantungan, kerahasiaan, dan dampak kegagalan sistem, yang diklasifikasikan menjadi kategori Rendah, Tinggi, atau Strategis. Kedua, perhitungan skor kematangan pada setiap area keamanan berdasarkan tingkat kelengkapan penerapan prosedur (skala 0 s.d 3). Klasifikasi Sistem Elektronik dan penetapan status kelayakan (Tidak Layak s.d. Baik) dilakukan mengikuti standar rentang skor yang ditetapkan dalam pedoman Indeks KAMI Versi 5.0 [5]. Hasil akhir berupa status kelayakan (misalnya "Pemenuhan Kerangka Kerja Dasar") dan tingkat kematangan (Level I s.d V) digunakan untuk memetakan kekuatan dan kelemahan sistem keamanan informasi perusahaan.

3.3. *Keterbatasan Penelitian*

Penting untuk dicatat bahwa metode penelitian ini memiliki keterbatasan. Evaluasi dilakukan berbasis *self-assessment* yang dipandu melalui wawancara dengan perwakilan manajemen IT tunggal. Meskipun memberikan gambaran manajerial yang cepat dan komprehensif, metode ini memiliki potensi bias subjektivitas dari responden. Oleh karena itu, penelitian ini berfokus pada aspek kelengkapan tata kelola dan kepatuhan administratif, dan tidak mencakup pengujian teknis mendalam seperti *penetration testing* atau audit forensik.

4. HASIL DAN PEMBAHASAN

4.1. *Profil Risiko dan Klasifikasi Elektronik*

PT. X merupakan pengelola pusat perbelanjaan yang memiliki ketergantungan tinggi pada sistem terintegrasi seperti manajemen *membership*, CCTV, dan pembayaran. Berdasarkan evaluasi menggunakan Indeks KAMI yang ditunjukkan pada Tabel 2, Sistem Elektronik (SE) PT. X diklasifikasikan sebagai Kategori Tinggi dengan skor total 19.

Tabel 2. Rincian Penilaian Kategori SE

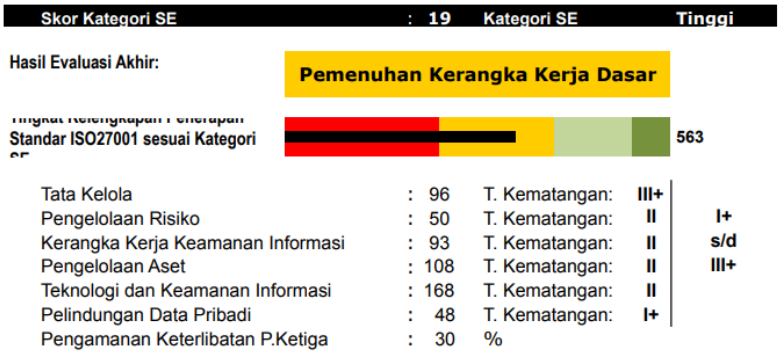
No	Kriteria Penilaian	Kategori Pilihan	Skor
1	Nilai Investasi Sistem Elektronik	C (< Rp 3 Miliar)	1
2	Anggaran Operasional Tahunan	C (< Rp 1 Miliar)	1
3	Kewajiban Kepatuhan (Regulasi)	C (Tidak ada peraturan khusus)	1
4	Penggunaan Kriptografi	C (Tidak ada)	1
5	Jumlah Pengguna Sistem	C (< 1.000 Pengguna)	1
6	Data Pribadi yang Dikelola	A (Data Pribadi terhubung)	5
7	Tingkat Kekritisan Data	A (Sangat Rahasia)	5
8	Tingkat Kekritisan Proses	C (Dampak bisnis perusahaan)	1
9	Dampak Kegagalan Sistem	C (Internal instansi/perusahaan)	1
10	Potensi Kerugian	B (Terbatas kerugian finansial)	2
Total			19
Kategori SE			Tinggi

Klasifikasi "Tinggi" ini memberikan implikasi manajerial yang penting. Meskipun nilai investasi dan anggaran operasional TI perusahaan relatif rendah (Kategori C), tingkat risiko melonjak akibat pengelolaan data pribadi pelanggan yang bersifat masif dan rahasia. Hal ini menegaskan bahwa PT. X tidak bisa lagi mengelola keamanan informasi dengan standar operasional mall konvensional, melainkan harus menerapkan kontrol keamanan setara dengan standar pelindungan data perbankan atau korporasi tingkat tinggi untuk memitigasi risiko kebocoran data yang dapat merusak reputasi bisnis.

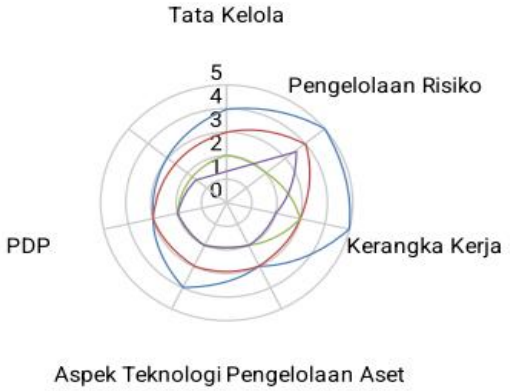
4.2. *Evaluasi Tingkat Kematangan Keamanan Informasi*

Hasil penilaian menyeluruh pada tujuh area Indeks KAMI menunjukkan bahwa PT. X berada pada tingkat kematangan Level I+ (Pemenuhan Kerangka Kerja Dasar) dengan skor total 563. Ringkasan hasil penilaian untuk ketujuh area dapat dilihat pada Gambar 2 dan divisualisasikan melalui grafik jaring laba-laba (*radar chart*) pada Gambar 3.

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



Gambar 2. Ringkasan Penilaian



Gambar 3. Grafik Laba-Laba (Radar chart)

Visualisasi pada Gambar 3 memperlihatkan ketimpangan yang signifikan antar area evaluasi. Area Teknologi dan Keamanan Informasi menjadi domain terkuat dengan skor 168, sementara area Pengelolaan Risiko dan Perlindungan Data Pribadi (PDP) menjadi titik terlemah dengan skor masing-masing 50 dan 48.

Ketimpangan skor antar area mengindikasikan fenomena "keamanan berbasis alat, bukan berbasis sistem". Tingginya skor teknologi (168 poin) menunjukkan bahwa secara teknis, PT. X telah memiliki infrastruktur pertahanan yang baik seperti *firewall* dan enkripsi jaringan. Namun, kecanggihan teknis ini tidak diimbangi dengan tata kelola formal.

1. Kelemahan Tata Kelola dan Manajemen Risiko: Rendahnya skor Pengelolaan Risiko (50 poin) disebabkan oleh belum adanya penetapan *risk appetite* (selera risiko). Dalam perspektif ISO 27001, hal ini merupakan ketidakpatuhan mendasar terhadap klausul perencanaan risiko. Tanpa parameter risiko yang jelas, manajemen akan kesulitan menentukan prioritas mitigasi, sehingga keputusan keamanan cenderung bersifat reaktif alih-alih preventif.
2. Isu Perlindungan Data Pribadi (PDP): Mengingat status Sistem Elektronik Kategori Tinggi, skor PDP yang hanya 48 poin adalah temuan kritis. Celah utama terletak pada ketiadaan prosedur baku pemusnahan data (*secure disposal*). Hal ini berisiko melanggar prinsip *storage limitation* dalam regulasi PDP, di mana data residu pelanggan pada perangkat lama dapat dipulihkan dan disalahgunakan oleh pihak yang tidak berwenang.
3. Konteks Skor Rendah pada Layanan Pihak Ketiga & Cloud: Penting untuk dicatat bahwa skor nol atau rendah pada area layanan awan (*cloud*) dan pengamanan pihak ketiga bukan merupakan kelemahan kontrol, melainkan refleksi dari strategi infrastruktur *on-premise* yang dianut PT. X. Perusahaan memilih mengelola data secara internal untuk meminimalisir risiko serangan rantai pasok (*supply chain attacks*), sebuah strategi yang valid namun menuntut kapasitas pengelolaan internal yang lebih ketat.

Secara agregat, Tabel 3 menunjukkan bahwa PT. X masih berada pada tahap Pemenuhan Kerangka Kerja Dasar (Level I+), yang mengindikasikan bahwa tata kelola keamanan informasi di PT. X baru pada tahap

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

inisiasi dan belum terdokumentasi secara konsisten. Validitas pencapaian level yang lebih tinggi (Level III) terhambat oleh "*bottleneck*" pada area manajemen risiko, meskipun kemampuan teknisnya sudah mumpuni.

Tabel 3. Hasil Akhir Tingkat Kematangan Keamanan Informasi

Komponen Evaluasi	Hasil Penilaian
Total Skor Akhir	563
Status Tingkat Kematangan	Tingkat I+
Kategori Kelayakan	Pemenuhan Kerangka Kerja Dasar
Status Kesiapan ISO 27001	Perlu Perbaikan

4.3. *Rekomendasi Perbaikan*

Berdasarkan analisis kesenjangan di atas, rekomendasi disusun untuk menyeimbangkan aspek teknis dan manajerial guna mencapai kepatuhan ISO 27001:

1. Prioritas Utama (Manajerial): Formalisasi Kebijakan dan Risiko. Manajemen perlu segera menetapkan parameter *risk appetite* dan menuangkannya dalam SK Direksi. Hal ini akan menjadi landasan hukum internal agar evaluasi risiko tidak lagi bersifat subjektif.
2. Prioritas Operasional: Transformasi *Patch Management*. Evaluasi menemukan bahwa pembaruan sistem operasi masih bergantung pada siklus pergantian perangkat keras. Disarankan untuk menerapkan prosedur *patch management* otomatis bulanan untuk menutup celah keamanan (*vulnerability*) pada perangkat yang sedang berjalan.
3. Prioritas Kepatuhan: Prosedur Pemusnahan Data. Untuk mematuhi regulasi PDP, PT. X wajib menyusun SOP Pemusnahan Data Aman untuk memastikan data pada aset yang tidak terpakai dimusnahkan secara permanen, melindungi privasi pelanggan jangka panjang.

5. DISKUSI

Hasil evaluasi menunjukkan bahwa tingkat kematangan keamanan informasi PT. X berada pada Level I+ dengan kategori Pemenuhan Kerangka Kerja Dasar, yang mencerminkan tahap awal penerapan tata kelola keamanan informasi. Kondisi ini menggambarkan bahwa sebagian besar kontrol keamanan telah tersedia, namun belum terdokumentasi dan diterapkan secara konsisten di seluruh area organisasi. Posisi kematangan tersebut berkaitan langsung dengan tujuan penelitian yang berfokus pada pemetaan kesiapan keamanan informasi menggunakan Indeks KAMI Versi 5.0. Temuan ini memberikan konteks bahwa pengelolaan keamanan informasi di sektor pusat perbelanjaan masih berkembang pada ranah manajerial.

Apabila dibandingkan dengan penelitian pada sektor publik seperti Diskominfo Pontianak dan Kota Bogor, pola kelemahan pada aspek pengelolaan risiko juga ditemukan dalam penelitian [6], [13]. Kesamaan tersebut menunjukkan bahwa rendahnya formalitas manajemen risiko merupakan karakteristik umum pada organisasi yang belum menjadikan keamanan informasi sebagai fungsi strategis. Berbeda dengan studi pada sektor perbankan yang menunjukkan kematangan teknologi dan aset lebih tinggi [15], sektor retail memperlihatkan ketimpangan yang lebih besar antara kesiapan teknis dan kebijakan formal. Perbedaan konteks industri ini menjelaskan variasi tingkat kematangan meskipun menggunakan kerangka evaluasi yang sama.

Skor tinggi pada area Teknologi dan Keamanan Informasi, yang tidak diikuti oleh skor seimbang pada Pengelolaan Risiko dan Perlindungan Data Pribadi, menunjukkan dominasi pendekatan *tool-driven security*. Pola serupa juga dijumpai dalam penelitian pada sektor pendidikan, di mana kesiapan infrastruktur tidak selalu sejalan dengan kematangan tata kelola [14]. Rendahnya skor pada penetapan *risk appetite* dan prosedur pemusnahan data dapat dipahami sebagai konsekuensi dari belum terintegrasinya manajemen risiko ke dalam proses pengambilan keputusan organisasi. Kondisi ini memperlihatkan bahwa aspek perlindungan data masih diperlakukan sebagai fungsi operasional, bukan sebagai bagian dari strategi bisnis jangka panjang.

Dari sisi implikasi praktis, temuan penelitian ini memberikan gambaran area kritis yang perlu diperhatikan oleh pengelola pusat perbelanjaan dalam mengelola keamanan informasi. Secara teoretis, hasil evaluasi ini menunjukkan bahwa Indeks KAMI mampu mengidentifikasi ketimpangan antara kesiapan teknis dan kematangan tata kelola pada sektor non-keuangan. Keterbatasan penelitian ini terletak pada penggunaan metode *self-assessment* melalui satu narasumber, yang berpotensi memengaruhi objektivitas penilaian. Selain itu, penelitian ini tidak mencakup pengujian teknis seperti *penetration testing* atau *vulnerability assessment*, sehingga pembahasan difokuskan pada aspek manajerial dan administratif keamanan informasi.

6. KESIMPULAN DAN SARAN

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

6.1. *Kesimpulan*

Penelitian ini bertujuan untuk mengevaluasi tingkat kesiapan dan kematangan keamanan informasi PT. X menggunakan Indeks KAMI Versi 5.0. Berdasarkan hasil penilaian, PT. X dikategorikan sebagai Sistem Elektronik Tinggi dengan skor total 563 dan tingkat kematangan berada pada Level I+ (Pemenuhan Kerangka Kerja Dasar). Hasil ini menunjukkan bahwa penerapan keamanan informasi pada PT. X telah berjalan, namun masih belum terdokumentasi secara formal dan belum diterapkan secara menyeluruh pada setiap area yang dinilai. Area Teknologi dan Keamanan Informasi menjadi komponen terkuat, menandakan bahwa aspek teknis dan pengamanan jaringan telah diterapkan dengan baik. Namun, area Pengelolaan Risiko dan Pelindungan Data Pribadi menjadi titik kelemahan yang signifikan. Beberapa kekurangan yang ditemukan meliputi tidak adanya penetapan *risk appetite*, belum tersedianya prosedur baku untuk pemusnahan data, belum adanya dokumentasi formal atas kebijakan keamanan informasi, serta belum diterapkannya *patch management* secara rutin.

Berdasarkan temuan tersebut, penelitian ini merekomendasikan sejumlah langkah strategis yang perlu diprioritaskan, antara lain penyusunan kebijakan keamanan informasi yang formal, penetapan batas toleransi risiko, penyusunan SOP pemusnahan data pribadi, dan penerapan *patch management*. Implementasi rekomendasi ini diyakini dapat membantu PT. X meningkatkan tingkat kematangan keamanan informasi menuju level yang sesuai dengan standar ISO 27001 serta memperkuat perlindungan data pribadi pelanggan [23].

6.2. *Saran*

Berdasarkan temuan kesenjangan (*gap*) pada penelitian ini, penulis merumuskan saran perbaikan yang ditujukan bagi peneliti selanjutnya:

1. Perluasan Metode Evaluasi: Penelitian selanjutnya disarankan untuk tidak hanya menggunakan asesmen mandiri (*self-assessment*), tetapi juga menggabungkannya dengan metode audit teknis seperti *Vulnerability assessment* untuk memvalidasi temuan pada area teknologi secara lebih mendalam [25].
2. Komparasi *Framework*: Dapat dilakukan penelitian komparatif dengan menggunakan kerangka kerja lain seperti NIST *Cybersecurity Framework* atau COBIT 2019 untuk mendapatkan perspektif tata kelola yang lebih luas pada sektor ritel/pusat perbelanjaan.

DAFTAR PUSTAKA

[1] B. Raharjo, R. Rudjiono, and Y. Fitrianto, “Prediction and Detection of Scam Threats on Digital Platforms for Indonesian Users Using Machine Learning Models,” *Journal of Technology Informatics and Engineering*, vol. 3, no. 3, pp. 350–369, 2024, doi: 10.51903/jtie.v3i3.208.

[2] M. Y. Darus, A. Ramli, Y. M. Yussoff, and B. Azni, “Cybersecurity Resilience — An Integrated Framework for Detection of Threats and Response in the Digital Age,” *Malaysian Journal of Computing*, vol. 10, no. 1, pp. 2099–2116, 2025, doi: 10.24191/mjoc.v10i1.4520.

[3] S. Setiawan, M. Ghufron, and D. Mochtar, “Legal Protection of Consumer Personal Data in E-Commerce Transactions,” *Merdeka Law Journal*, vol. 2, no. 1, pp. 1–15, 2022, doi: 10.26905/mlj.v2i1.5496.

[4] N. T. Mai and I. Khalid, “Human error vs. system security: evaluating the weakest link in digital business information systems,” *Journal of Management and Informatics*, vol. 4, no. 3, pp. 215–234, 2025, doi: 10.51903/jmi.v4i3.305.

[5] Badan Siber dan Sandi Negara, *Pedoman Evaluasi Keamanan Informasi (Indeks KAMI) Versi 5.0*, Jakarta: Badan Siber dan Sandi Negara, 2023. [online]. Available: https://www.bssn.go.id/indeks-kami

[6] S. F. Rahayu, D. Prawira, and I. Rusi, “Pengukuran Tingkat Keamanan Informasi Menggunakan Metode Indeks KAMI,” *Coding: Jurnal Komputer dan Aplikasi*, vol. 9, no. 3, pp. 468–477, 2021, doi: 10.26418/coding.v9i03.51126.

[7] K. Tam, K. Jones, and P. I. P. Security, “Cybersecurity Threats and Defensive Strategies for Small and Medium Firms: A Systematic Mapping Study,” *Administrative Sciences*, vol. 15, no. 12, p. 481, 2025, doi: 10.3390/admsci15120481.

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

[8] T. Dyl, "Cybersecurity Challenges Peak During Shopping Seasons: a Retail Analysis," *Retail Insider*, Oct. 29, 2025. [Online]. Available: https://retail-insider.com/retail-insider/2025/10/cybersecurity-challenges-during-peak-shopping-seasons

[9] M. Tutik, N. Mutiah, and I. Rusi, "Analisis dan Manajemen Risiko Keamanan Informasi Menggunakan Metode Failure Mode and Effects Analysis (FMEA) dan Kontrol ISO/IEC 27001:2013 (Studi Kasus: Dinas Komunikasi dan Informatika Kabupaten Sambas)," *Coding: Jurnal Komputer dan Aplikasi*, vol. 10, no. 02, pp. 249–261, 2022, doi: 10.26418/coding.v10i02.55082.

[10] M. Parlindungan, "Exploration of Security Awareness and Cultural Factors Regarding Information Security of the XYZ District Communication and Information Agency," *The Indonesian Journal of Computer Science*, vol. 13, no. 6, p. 4536, 2024, doi: 10.33022/ijcs.v13i6.4536.

[11] M. P. Firmansyah, M. N. Nashir, N. Rahmeisi, P. S. Augusta, and A. Arfriandi, "A Systematic Literature Review of Artificial Intelligence-Based Anomaly Detection for Network Intrusion in IoT," *Jurnal Ilmiah Sistem Informasi (JUISI)*, vol. 5, no. 1, pp. 71–83, 2026, doi: 10.51903/eqne0j35.

[12] A. Rifmika, M. Akbar, D. L. Jayanto, and J. R. Bu'tu, "Cloud Governance Frameworks: CIA-Based Security and Compliance," *Journal of Embedded Systems, Security and Intelligent Systems*, vol. 6, no. 3, pp. 379–389, 2025, doi: 10.59562/jessi.v6i3.9541.

[13] 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," *Journal of Industrial Engineering & Management Research*, vol. 2, no. 5, pp. 146–163, 2021, doi: 10.7777/jiemar.v2i5.196.

[14] M. H. Z. Hidayatullah, W. Y. Sulistyo, and S. A. Pratiwi, "Evaluasi Tingkat Keamanan Informasi SIA UIN SUKA Berdasarkan Indeks KAMI 4.0," *JITU : Journal Informatic Technology and Communication*, vol. 9, no. 1, pp. 83–91, 2025, doi: 10.36596/jitu.v9i1.1802.

[15] M. Reja Balqis S., M. Andriani Mahadewi, S. A. Imani, and R. Permatasari, "Analisis Kematangan Pengelolaan Keamanan Informasi Berbasis Indeks KAMI di PT. BPR Jawa Timur," *Prosiding Seminar Nasional Teknologi dan Sistem Informasi (SITASI)*, vol. 3, no. 1, pp. 78–86, 2023, doi: 10.33005/sitasi.v3i1.546.

[16] Zainal, Munirul Ula, and Nurdin, "Analisis Kinerja Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 pada Universitas Jabal Ghafur," *JITET : Jurnal Informatika dan Teknik Elektro Terapan*, vol. 13, no. 2, pp. 174–182, 2025, doi: 10.23960/jitet.v13i2.6130.

[17] D. Contieri, A. Annosi, and F. Brunetta, "Forecasting the Diffusion of ISO/IEC 27001: a Grey Model Approach," *The TQM Journal*, vol. 35, no. 9, pp. 123–151, 2023, doi: 10.1108/tqm-07-2022-0220.

[18] H. Faotu, O. N. Asheshemi, and E. T, "Human Vulnerabilities in Cybersecurity: Analyzing Social Engineering Attacks and AI-Driven Machine Learning Countermeasures," *Journal of Science and Technology*, vol. 30, no. 1, pp. 72–84, 2025, doi: 10.20428/jst.v30i1.2597.

[19] I. Made Adi Surya Permana, I. Gede Putu Krisna Juliharta, and I. Gede Juliana Eka Putra, "Analisis Keamanan Sistem Informasi Menggunakan Metode Vulnerability Assesment pada Aplikasi Web Karangasem.go.id," *REMIK: Riset dan E-Jurnal Manajemen Informatika Komputer*, vol. 9, no. 2, pp. 466–473, Apr. 2025, doi: 10.33395/remik.v9i2.14561.

[20] M. Y. K. A. Yaseen, "Patching Vulnerabilities to Improve the Security Posture in the Financial Transactions," *European Journal of Computer Science and Information Technology*, vol. 11, no. 6, pp. 55–61, 2023, doi: 10.37745/ejcsit.2013/vol11n65561.

[21] **1.** N. Dissanayake, A. Jayatilaka, M. Zahedi, and M. A. Babar, "Software Security Patch Management – A Systematic Literature Review of Challenges, Approaches, Tools and Practices," *Information and Software Technology*, vol. 144, p. 106771, 2022, doi: 10.1016/j.infsof.2021.106771.

[22] S. A. Hussien, "A Review on Secure Data Disposal Methods and Compliance Requirements in Information Security," *International Journal of Computer Science and Network Security*, vol. 24, no. 2, pp. 45–56, 2024, doi: 10.12345/ijcsns.v24i2.4589.

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

[23] Lucia Devlina Adventia Jelita, Moh Noor Al Azam, and Aryo Nugroho, "Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks KAMI 5.0 dan ISO/IEC 27001:2022," *Jurnal Saintekom: Sains, Teknologi, Komputer dan Manajemen*, vol. 14, no. 1, p. 623, 2025, doi: 10.33020/saintekom.v14i1.623.

[24] H. Djenna, "Ransomware Trends in 2024: Implications for SME Retailers," *Computers & Security*, vol. 135, p. 103501, 2024, doi:10.1016/j.cose.2024.103501.

[25] M. S. Bahary and B. Sugiantoro, "Evaluasi Tingkat Keamanan Indeks Kami (Studi Kasus: Universitas X) dan Korelasinya dengan Iso 27001:2022," *Cybersecurity: e-Journal UIN Suka*, vol. 7, no. 2, pp. 90–94, 2024, doi:10.14421/csecurity.2024.7.2.4634.