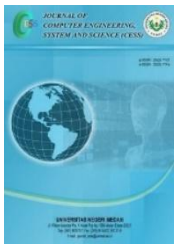
*CESS (Journal of Computer Engineering, System and Science)*
*Vol. 11, No. 1, Januari 2026, pp.113-126*

**CESS**
**(Journal of Computer Engineering, System and Science)**
Available online: https://jurnal.unimed.ac.id/2012/index.php/cess
ISSN: 2502-714x (Print) | ISSN: 2502-7131 (Online)



# Evaluasi Tata Kelola Keamanan Informasi Indeks KAMI 5.0: Studi Kasus PT. XYZ

## *Evaluation of Information Security Governance using Indeks KAMI 5.0: Case Study of PT. XYZ*

**Chelyne[1*], Rido Dwi Kurniawan[2]**

*[1,2]Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Pradita, Indonesia*
*Scientia Business Park, Jl. Gading Serpong Boulevard No.1 Tower 1, Curug Sangereng, Kecamatan Kelapa Dua, Kabupaten Tangerang, Banten 15810*
*Email: [1]chelyne@student.pradita.ac.id, [2]rido.dwi@pradita.ac.id*
**Corresponding Author*

**A B S T R A K**

Transformasi digital menuntut perusahaan teknologi seperti PT. XYZ untuk menjamin keamanan informasi, terutama pada sistem elektronik yang diklasifikasikan sebagai kategori tinggi. Penelitian ini bertujuan mengevaluasi tingkat kematangan keamanan informasi perusahaan menggunakan instrumen Indeks KAMI 5.0 yang selaras dengan standar ISO/IEC 27001:2022. Metode penelitian menggunakan pendekatan deskriptif evaluatif melalui kuesioner asesmen mandiri pada lima area inti. Hasil evaluasi mengungkap adanya disparitas tata kelola yang signifikan: domain Pengelolaan Aset Informasi mencapai skor tertinggi sebesar 190, menunjukkan inventarisasi infrastruktur yang sangat matang. Sebaliknya, domain Pelindungan Data Pribadi (PDP) mencatat skor terendah sebesar 28, mengindikasikan kerentanan serius terhadap risiko privasi dan potensi ketidakpatuhan terhadap regulasi UU PDP. Berdasarkan temuan tersebut, penelitian ini merumuskan rekomendasi strategis untuk meningkatkan kepatuhan PDP dengan memanfaatkan kekuatan manajemen aset yang telah ada sebagai landasan pemetaan data sensitif.

**Kata Kunci**: *Indeks KAMI 5.0; Keamanan Informasi; Pelindungan Data Pribadi; Manajemen Aset; Tata Kelola TI.*

**A B S T R A C T**

Digital transformation requires technology companies like PT. XYZ to ensure information security, especially in electronic systems classified as high category. This study aims to evaluate the company's information security maturity level using the Indeks KAMI 5.0 instrument, aligned with ISO/IEC 27001:2022. The research employs a descriptive evaluative approach through self-assessment questionnaires across five core areas. The evaluation

results reveal a significant governance disparity: the Asset Management domain reached the highest score of 190, indicating a highly mature infrastructure inventory. Conversely, the Personal Data Protection (PDP) domain recorded the lowest score of 28, indicating serious vulnerability to privacy risks and potential non-compliance with PDP regulations. Based on these findings, this study formulates strategic recommendations to improve PDP compliance by leveraging existing asset management strengths as a foundation for sensitive data mapping.

**Keywords**: *Indeks KAMI 5.0; Information Security; Personal Data Protection; Asset Management; IT Governance.*

## 1. PENDAHULUAN

Perkembangan teknologi digital di masa ini mendorong banyaknya perusahaan memasuki fase transformasi digital. Transformasi ini sangat krusial bagi industri maupun sektor pemerintahan yang mengandalkan sistem, strategi, dan sumber daya manusia. Proses ini berfokus pada optimalisasi nilai bisnis melalui pemanfaatan data dan analitik untuk menghadirkan pengalaman baru yang lebih inovatif bagi pelanggan [1]. Selain itu, transformasi digital menuntut organisasi untuk mengikuti perkembangan teknologi agar tetap kompetitif. Implementasinya mampu meningkatkan efisiensi kinerja serta membentuk budaya organisasi yang lebih adaptif [2]. Namun, perubahan ini juga meningkatkan risiko keamanan informasi. Lanskap Keamanan Siber mencatat banyaknya insiden kebocoran data akibat lemahnya sistem perlindungan [3]. Ancaman ini menuntut adanya tata kelola keamanan informasi yang sistematis. Manajemen risiko, seperti kerangka kerja COBIT maupun ISO 31000, menjadi elemen krusial dalam mengidentifikasi dan mengendalikan ancaman siber [4], [5]. Penerapan manajemen risiko memungkinkan organisasi membentuk strategi yang efektif melalui pemanfaatan sumber daya yang tersedia [6]. Sebelum menerapkan standar keamanan, diperlukan evaluasi untuk memetakan tingkat kesiapan keamanan informasi yang dimiliki [7].

Di Indonesia, urgensi keamanan informasi mendapat perhatian serius dari Badan Siber dan Sandi Negara (BSSN) melalui instrumen Indeks Keamanan Informasi (Indeks KAMI). Alat evaluasi ini memberikan gambaran mengenai kondisi kesiapan dan kematangan kerangka kerja keamanan informasi [8]. Versi terbaru, Indeks KAMI 5.0, telah diselaraskan dengan standar ISO/IEC 27001:2022, yang mencakup evaluasi tata kelola, pengelolaan risiko, aset, teknologi, hingga pelindungan data pribadi [9].

Penelitian ini mengambil studi kasus pada PT. XYZ, penyedia perangkat lunak intelijen bisnis dan lokasi di Indonesia yang memanfaatkan *big data* dan *machine learning* untuk analisis prediktif, mencakup pengelolaan aset, logistik, hingga manajemen risiko asuransi [10]. Sebagai perusahaan berbasis teknologi geospasial, PT. XYZ mengelola aset data dalam jumlah besar sehingga dikategorikan sebagai pemilik Sistem Elektronik (SE) Strategis. Namun, observasi awal menunjukkan adanya anomali tata kelola: perusahaan memiliki infrastruktur teknologi yang sangat matang, namun aspek kebijakan pelindungan data pribadi (PDP) belum mendapatkan perhatian yang setara. Ketimpangan ini berisiko tinggi mengingat data lokasi merupakan informasi sensitif.

Pentingnya evaluasi keamanan informasi telah dibuktikan oleh berbagai penelitian terdahulu. Putra (2024) menekankan bahwa manajemen risiko pada pusat data dinas sangat krusial untuk melindungi aset informasi [11]. Hanif et al. (2025) menemukan bahwa evaluasi Indeks KAMI 5.0 di lingkungan pendidikan membantu memetakan kepatuhan standar [12]. Sejalan dengan itu, analisis tingkat kematangan di tingkat desa juga diperlukan untuk menjamin keberlanjutan layanan publik [13]. Di sektor kesehatan, Ramadhan et al. (2025) menunjukkan perlunya perbaikan kebijakan keamanan berbasis ISO 27001 pada sistem rumah sakit [14]. Sementara itu, Fitria et al. (2025) menyimpulkan bahwa digitalisasi layanan publik seperti pajak daerah meningkatkan risiko serangan siber, sehingga evaluasi berkala menjadi mutlak [15].

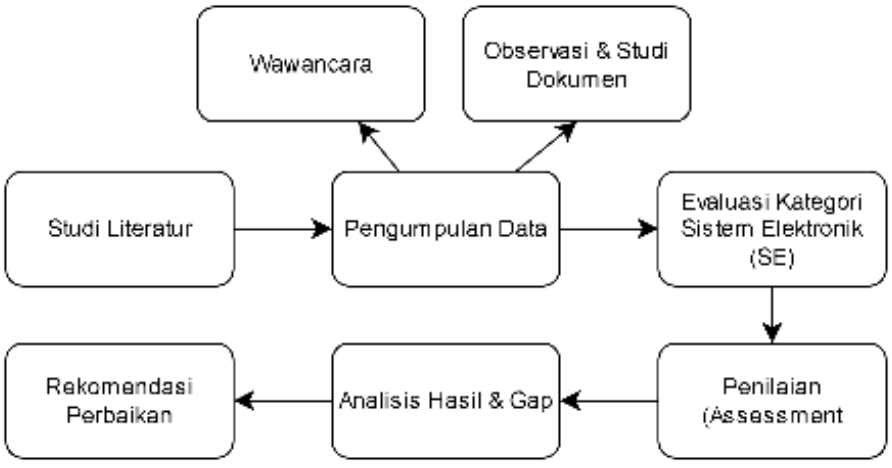
Berdasarkan paparan tersebut, penelitian ini bertujuan untuk mengevaluasi tingkat kematangan keamanan informasi pada PT. XYZ menggunakan *framework* Indeks KAMI 5.0. Kebaruan (*novelty*)' penelitian ini terletak pada analisis kesenjangan (*gap analysis*) antara kematangan pengelolaan aset informasi teknologi dengan kesiapan pelindungan data pribadi perusahaan. Hasil evaluasi diharapkan memberikan rekomendasi strategis untuk menyeimbangkan aspek teknis dan kebijakan sesuai standar ISO/IEC 27001:2022.

## 2. METODE PENELITIAN

Penelitian ini menggunakan metode deskriptif evaluatif dengan pendekatan kuantitatif untuk mengukur tingkat kematangan (*maturity level*) keamanan informasi. Objek penelitian dilakukan pada PT. XYZ. Instrumen utama yang digunakan adalah alat evaluasi Indeks KAMI (Keamanan Informasi) Versi 5.0 yang dikembangkan oleh BSSN dan telah diselaraskan dengan standar internasional ISO/IEC 27001:2022 [3].

### 2.1. Tahapan Penelitian

Prosedur penelitian dilakukan secara sistematis melalui beberapa tahapan untuk memastikan hasil evaluasi yang akurat dan dapat dipertanggungjawabkan. Alur tahapan penelitian dapat dilihat pada Gambar 1.




Gambar 1. Diagram Alur Penelitian

Tahapan penelitian terdiri dari:

1. Studi Literatur: Mempelajari standar ISO/IEC 27001:2022, panduan Indeks KAMI 5.0, serta regulasi terkait seperti UU PDP (Undang-Undang Perlindungan Data Pribadi).
2. Pengumpulan Data:
   a. Wawancara: Dilakukan dengan pihak manajemen TI dan *stakeholder* terkait untuk memahami proses bisnis dan kebijakan yang berlaku.
   b. Observasi & Studi Dokumen: Memeriksa bukti fisik berupa dokumen kebijakan (SOP), topologi jaringan, daftar aset, dan log aktivitas sistem.
3. Evaluasi Kategori Sistem Elektronik (SE): Mengukur tingkat ketergantungan dan dampak kegagalan sistem untuk menentukan kategori SE (Rendah, Tinggi, atau Strategis).
4. Penilaian (*Assessment*): Mengisi kuesioner Indeks KAMI 5.0 yang mencakup lima area utama dan suplemen.
5. Analisis Hasil & *Gap*: Membandingkan skor aktual dengan standar kelulusan sesuai kategori SE, serta menganalisis kesenjangan (*gap*) pada area yang lemah.
6. Rekomendasi Perbaikan: Menyusun strategi perbaikan berdasarkan temuan audit.

**2.2. Instrumen Penelitian**

Instrumen Indeks KAMI 5.0 terdiri dari kuesioner yang dikelompokkan ke dalam area tata kelola keamanan informasi. Penilaian dibagi menjadi dua bagian utama:

a. Evaluasi Kategori Sistem Elektronik (SE) Bagian ini digunakan untuk mengklasifikasikan sistem milik PT. XYZ. Parameter yang dinilai meliputi nilai investasi, total anggaran operasional, kewajiban kepatuhan hukum, dan dampak kegagalan terhadap publik [12].
b. Evaluasi Keamanan Informasi Penilaian dilakukan terhadap lima area inti dan satu suplemen dengan rincian sebagai berikut:
   1. Tata Kelola: Menilai struktur organisasi dan tanggung jawab keamanan.
   2. Pengelolaan Risiko: Menilai identifikasi dan penanganan risiko keamanan.
   3. Kerangka Kerja: Menilai kelengkapan kebijakan dan prosedur (SOP).
   4. Pengelolaan Aset: Menilai manajemen aset informasi dan teknologi.
   5. Teknologi: Menilai keamanan teknis pada jaringan dan sistem.
   6. Suplemen: Menilai aspek khusus seperti Pelindungan Data Pribadi (PDP) dan pengamanan keterlibatan pihak ketiga [14].

**2.3. Teknik Analisis Data**

Data yang diperoleh dari pengisian *tools* Indeks KAMI 5.0 dianalisis secara otomatis oleh sistem pembobotan pada lembar kerja evaluasi. Tingkat kematangan diklasifikasikan ke dalam lima tingkat, yaitu: Tingkat I (Kondisi Awal) hingga Tingkat V (Teroptimalisasi).

Khusus pada penelitian ini, analisis difokuskan pada perbandingan skor antara area dengan nilai tertinggi (*strength*) dan terendah (*weakness*) untuk mengidentifikasi disparitas tata kelola. Hasil akhir akan memetakan posisi PT. XYZ pada *dashboard* evaluasi untuk menentukan status kepatuhan, seperti "Tidak Layak", "Pemenuhan Kerangka Kerja Dasar", atau "Baik" [15].

## 3. HASIL DAN PEMBAHASAN

Evaluasi keamanan informasi pada PT. XYZ dilakukan menggunakan perangkat lunak asesmen mandiri Indeks KAMI versi 5.0. Hasil evaluasi mencakup penentuan kategori sistem elektronik dan pengukuran tingkat kematangan pada lima area inti serta suplemen.

### 3.1. Kategori Sistem Elektronik (SE)

Berdasarkan pengisian kuesioner pada bagian identifikasi sistem, diperoleh skor ketergantungan sebesar 20. Berdasarkan standar BSSN, nilai ini menempatkan sistem elektronik yang dikelola PT. XYZ ke dalam Kategori Tinggi.

Implikasi dari kategori "Tinggi" ini adalah perusahaan diwajibkan untuk menerapkan standar keamanan informasi yang lebih ketat dibandingkan kategori "Rendah". Kegagalan dalam pengamanan sistem pada kategori ini dianggap memiliki dampak yang signifikan terhadap keberlangsungan layanan publik atau tata kelola perusahaan yang strategis [12]. Oleh karena itu, ambang batas (*threshold*) kelulusan untuk setiap area menjadi lebih tinggi.

### 3.2. Tingkat Kematangan Keamanan Informasi

Rekapitulasi hasil penilaian pada lima area inti dan suplemen Indeks KAMI 5.0 menunjukkan adanya variasi tingkat kematangan yang signifikan. Rincian perolehan skor dapat dilihat pada Tabel 1 dan visualisasi diagram radar pada Gambar 2. Untuk memberikan pemahaman yang lebih komprehensif mengenai parameter penilaian yang mendasari hasil tersebut, rincian evaluasi pada dua domain dengan skor ekstrem, yakni Pengelolaan Aset Informasi (skor tertinggi) dan Pelindungan Data Pribadi (skor terendah) disajikan pada Tabel 2 dan Tabel 3. Penyajian ini juga mencakup contoh item kuesioner Indeks KAMI 5.0 guna memperjelas kriteria penilaian yang digunakan.

Tabel 1. Rekapitulasi Skor Indeks KAMI 5.0

| No | Area Indeks KAMI 5.0 | Skor Maksimal | Skor Diperoleh | Tingkat Kematangan |
|---|---|---|---|---|
| I | Tata Kelola | 126 | 61 | II |
| II | Pengelolaan Risiko | 72 | 43 | II |
| III | Kerangka Kerja | 192 | 91 | II |
| IV | Pengelolaan Aset | 258 | 190 | II |
| V | Teknologi | 186 | 141 | II |
| VII | Perlindungan Data Pribadi | 84 | 28 | I+ |
| VIII | Suplemen | | 83% | |
| Total | Skor Akhir | 916 | 554 | V |

Tabel 2. Tabel Pengelolaan Aset Informasi

| Bagian V: Pengelolaan Aset Informasi | |
|---|---|
| Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut. | |
| [Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh | Status |
| # Pengelolaan Aset Informasi | |

| | | | | |
|---|---|---|---|---|
| 5.1 | II | 1 | Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara ? (termasuk kepemilikan aset ) | Diterapkan Secara Menyeluruh |
| 5.2 | II | 1 | Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku? | Diterapkan Secara Menyeluruh |
| 5.3 | II | 1 | Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya? | Diterapkan Secara Menyeluruh |
| 5.4 | II | 1 | Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut | Diterapkan Secara Menyeluruh |
| 5.5 | II | 1 | Apakah tersedia proses untuk mengidentifikasi dan menginventarisir syarat retensi asset informasi sesuai dengan peraturan perundangan yang ada dan menghapusnya jika sudah melewati batas retensi tersebut | Diterapkan Secara Menyeluruh |
| 5.6 | II | 1 | Apakah tersedia proses untuk mengevaluasi kepatuhan terhadap syarat retensi dan menghapus aset informasi jika sudah melewati batas retensi tersebut | Diterapkan Secara Menyeluruh |
| 5.7 | II | 1 | Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten? | Diterapkan Secara Menyeluruh |
| 5.8 | II | 1 | Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten? | Dalam Penerapan / Diterapkan Sebagian |
| 5.9 | II | 1 | Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi? | Dalam Penerapan / Diterapkan Sebagian |
| | | | Apakah instansi/perusahaan anda memiliki dan menerapkan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko? | |
| 5.10 | II | 1 | Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda | Diterapkan Secara Menyeluruh |
| 5.11 | II | 1 | Tata tertib penggunaan komputer, email, internet dan intranet | Diterapkan Secara Menyeluruh |
| 5.12 | II | 1 | Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI | Diterapkan Secara Menyeluruh |
| 5.13 | II | 1 | Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan | Diterapkan Secara Menyeluruh |
| 5.14 | II | 1 | Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi | Dalam Penerapan / Diterapkan Sebagian |
| 5.15 | II | 1 | Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya | Diterapkan Secara Menyeluruh |

| | | | | |
|---|---|---|---|---|
| 5.16 | II | 1 | Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi | Diterapkan Secara Menyeluruh |
| 5.17 | II | 1 | Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data | Diterapkan Secara Menyeluruh |
| 5.18 | II | 1 | Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya | Diterapkan Secara Menyeluruh |
| 5.19 | II | 1 | Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi | Diterapkan Secara Menyeluruh |
| 5.20 | II | 1 | Prosedur *back-up* dan uji coba pengembalian data (*restore*) secara berkala | Diterapkan Secara Menyeluruh |
| 5.21 | II | 2 | Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya | Diterapkan Secara Menyeluruh |
| 5.22 | III | 2 | Proses pengecekan latar belakang SDM | Diterapkan Secara Menyeluruh |
| 5.23 | III | 2 | Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib. | Diterapkan Secara Menyeluruh |
| 5.24 | III | 2 | Proses dan metoda untuk penghancuran informasi yang sudah tidak diperlukan dan sesuai dengan klasifikasi informasi (mis: *secure delete*, jenis/kerapatan *shredder* dll),Termasuk didalamnya laporan bukti penghancuran informasi ? | Diterapkan Secara Menyeluruh |
| 5.25 | III | 2 | Prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya *(user access rights*) berikut langkah pembenahan apabila terjadi ketidaksesuaian (*non-conformity*) terhadap kebijakan yang berlaku | Diterapkan Secara Menyeluruh |
| 5.26 | III | 2 | Prosedur untuk *user* yang mutasi/keluar atau tenaga kontrak/*outsource* yang habis masa kerjanya. | Diterapkan Secara Menyeluruh |
| 5.27 | III | 3 | Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya? | Diterapkan Secara Menyeluruh |
| 5.28 | III | 3 | Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya? | Diterapkan Secara Menyeluruh |
| 5.29 | III | 3 | Apakah telah diterapkan proses dan metoda untuk mengaburkan data (*data masking*) agar hanya dapat dilihat oleh pihak yang mempunyai otoritas sesuai regulasi atau kebijakan? Mis: pengamanan data pribadi, data sensitif | Dalam Penerapan / Diterapkan Sebagian |
| 5.30 | III | 3 | Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/*vendor*) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan? | Dalam Penerapan / Diterapkan Sebagian |
| # | | | Pengamanan Layanan Infrastruktur Awan (*Cloud Service*) | |
| 5.31 | III | 2 | Apakah instansi/perusahaan sudah melakukan kajian risiko terkait penggunaan layanan berbasis *cloud* dan menyesuaikan kebijakan keamanan informasi terkait layanan ini? | Diterapkan Secara Menyeluruh |

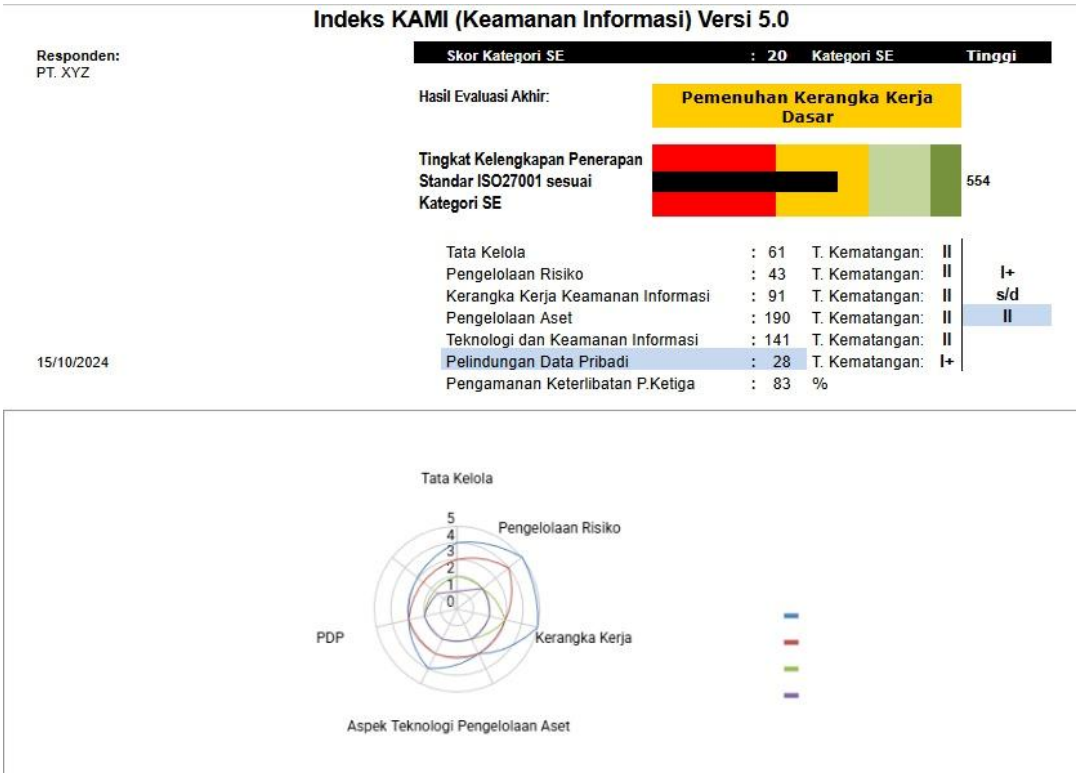
| | | | | |
|---|---|---|---|---|
| 5.32 | III | 2 | Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis *cloud*? | Diterapkan Secara Menyeluruh |
| 5.33 | III | 2 | Apakah instansi/perusahaan sudah menetapkan kebijakan dan menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan *cloud*? | Dalam Penerapan / Diterapkan Sebagian |
| 5.34 | III | 2 | Apakah instansi/perusahaan sudah mengkaji, menetapkan pembagian tanggung jawab keamanan informasi antara perusahaan dan penyelenggara layanan *cloud* ? | Diterapkan Secara Menyeluruh |
| 5.35 | III | 2 | Apakah instansi/perusahaan sudah mengkaji, menetapkan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis *cloud*? | Diterapkan Secara Menyeluruh |
| 5.36 | III | 2 | Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan *cloud* terkait reputasi penyelenggaranya? | Diterapkan Secara Menyeluruh |
| 5.37 | III | 2 | Apakah instansi/perusahaan sudah menetapkan standar keamanan teknis penggunaan layanan *cloud,* termasuk aspek penggunaannya oleh pengguna di internal instansi/perusahaan? | Diterapkan Secara Menyeluruh |
| 5.38 | III | 2 | Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan *cloud* termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001? | Diterapkan Secara Menyeluruh |
| 5.39 | III | 2 | Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan *cloud*? | Diterapkan Secara Menyeluruh |
| 5.40 | III | 3 | Apakah instansi/perusahaan sudah memiliki kebijakan, strategi dan proses untuk mengganti layanan *cloud* atau menyediakan fasilitas pengganti apabila terjadi gangguan sementara pada layanan tersebut? | Diterapkan Secara Menyeluruh |
| 5.41 | III | 3 | Apakah instansi/perusahaan sudah memiliki proses untuk menghentikan layanan *cloud,* termasuk proses pengamanan data yang ada (memindahkan dan menghapus data)? | Diterapkan Secara Menyeluruh |
| # | | | Pengamanan Fisik | |
| 5.42 | II | 1 | Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang? | Diterapkan Secara Menyeluruh |
| 5.43 | II | 1 | Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik? | Diterapkan Secara Menyeluruh |
| 5.44 | II | 1 | Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya? | Diterapkan Secara Menyeluruh |
| 5.45 | II | 1 | Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir? | Diterapkan Secara Menyeluruh |
| 5.46 | II | 1 | Apakah infrastruktur komputasi yang terpasang dapat dipantau melalui CCTV ? | Diterapkan Secara Menyeluruh |

| | | | | |
|---|---|---|---|---|
| 5.47 | II | 1 | Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)? | Diterapkan Secara Menyeluruh |
| 5.48 | II | 1 | Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris)? | Diterapkan Secara Menyeluruh |
| 5.49 | II | 2 | Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai? | Diterapkan Secara Menyeluruh |
| 5.50 | II | 2 | Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting? | Diterapkan Secara Menyeluruh |
| 5.51 | II | 2 | Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga? | Diterapkan Secara Menyeluruh |
| 5.52 | II | 2 | Apakah tersedia 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 telepon genggam di dalam ruang server, menggunakan kamera dll) | Diterapkan Secara Menyeluruh |
| 5.53 | III | 3 | Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan anda? | Diterapkan Secara Menyeluruh |
| | | | Total Nilai Evaluasi Pengelolaan Aset | 190 |

Tabel 3. Tabel Perlindungan Data Pribadi

| Bagian VII: Perlindungan Data Pribadi | | | | |
|---|---|---|---|---|
| Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penerapan kontrol keamanan terkait Pelindungan Data Pribadi (PDP). | | | | |
| [Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh | | | | Status |
| # | | | Perlindungan Data Pribadi | |
| 7.1 | II | 1 | Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal? | Dalam Perencanaan |
| 7.2 | II | 1 | Apakah instansi/perusahaan sudah memetakan alur pemrosesan data di internal dan pertukaran data dengan pihak eksternal, termasuk kapan dan dimana data pribadi tersebut diperoleh? | Dalam Perencanaan |
| 7.3 | II | 1 | Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan? | Dalam Perencanaan |

| | | | | |
|---|---|---|---|---|
| 7.4 | II | 1 | Apakah instansi/perusahaan sudah memiliki kebijakan terkait Pelindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku? | Dalam Perencanaan |
| 7.5 | II | 2 | Apakah instansi/perusahaan sudah menunjuk fungsi/unit Pejabat Pelindung Data Pribadi yang bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Pelindungan Data Pribadi? | Dalam Perencanaan |
| 7.6 | II | 2 | Apakah instansi/perusahaan sudah menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain? | Dalam Perencanaan |
| 7.7 | III | 2 | Apakah kajian risiko keamanan pada instansi/perusahaan sudah memasukkan aspek Pelindungan Data Pribadi? | Dalam Perencanaan |
| 7.8 | III | 2 | Apakah mekanisme pelindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku? | Dalam Perencanaan |
| 7.9 | III | 2 | Apakah instansi/perusahaan sudah menjalankan program peningkatan pemahaman/kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi, termasuk hal-hal terkait Peraturan Perundangan yang berlaku? | Dalam Perencanaan |
| 7.10 | III | 2 | Apakah instansi/perusahaan sudah mendapatkan persetujuan dari pemilik data pribadi saat mengambil data tersebut, termasuk penjelasan hak pemilik data, apa saja yang akan diberlakukan pada data pribadi tersebut dan menyimpan catatan persetujuan tersebut ? | Dalam Perencanaan |
| 7.11 | III | 2 | Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi? | Dalam Perencanaan |
| 7.12 | III | 2 | Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut? | Dalam Perencanaan |
| 7.13 | III | 2 | Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan? | Dalam Perencanaan |
| 7.14 | III | 2 | Apakah instansi/perusahaan sudah menerapkan proses terkait periode penyimpanan data pribadi dan penghapusan/pemusnahannya sesuai dengan peraturan atau perjanjian dengan pemilik data? | Dalam Perencanaan |
| 7.15 | III | 2 | Apakah instansi/perusahaan sudah menerapkan proses terkait penghapusan/pemusnahan data apabila sudah tidak ada keperluan yang sah untuk menyimpan/mengolahnya lebih lanjut atau atas permintaan pemilik data dan menyimpan catatan proses tersebut? | Dalam Perencanaan |
| 7.16 | III | 2 | Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum? | Dalam Perencanaan |
| | | | Total Nilai Evaluasi Pelindungan Data Pribadi | 28 |




Gambar 2. Visualisasi Tingkat Kematangan (Radar Chart)

Berdasarkan Tabel 1 dan Gambar 2, terlihat disparitas yang mencolok antara area teknis operasional dengan area kepatuhan privasi. Area Pengelolaan Aset Informasi menjadi domain terkuat dengan skor 190, sementara area Pelindungan Data Pribadi (PDP) menjadi domain terlemah dengan skor 28.

### 3.3. Analisis Kekuatan: Maturitas Pengelolaan Aset

Tingginya skor pada Area IV (Pengelolaan Aset Informasi) sebesar 190 menunjukkan bahwa PT. XYZ memiliki kontrol yang sangat baik terhadap inventarisasi infrastruktur TI. Sebagai perusahaan berbasis teknologi geospasial, Pengelolaan Aset Informasi memang menjadi tulang punggung operasional.

Hasil evaluasi menunjukkan bahwa perusahaan telah berhasil menerapkan:

1. Inventarisasi aset informasi yang lengkap dan terbarukan.
2. Klasifikasi kepemilikan aset (*asset ownership*) yang jelas.
3. Mekanisme pengendalian perangkat keras dan lunak yang terstandarisasi. Kematangan di sektor ini sejalan dengan prinsip ISO 27001:2022 domain A.5 (*Asset Management*), di mana visibilitas aset menjadi prasyarat utama bagi keamanan siber [3]. Hal ini menjadi modal kapital yang kuat bagi perusahaan, karena pengamanan data tidak mungkin dilakukan tanpa mengetahui di mana data tersebut disimpan.

### 3.4. Analisis Kelemahan: Kritisnya Pelindungan Data Pribadi

Berbanding terbalik dengan pengelolaan aset, skor pada Suplemen Pelindungan Data Pribadi (PDP) hanya mencapai angka 28. Angka ini jauh di bawah ambang batas yang

diharapkan untuk Sistem Elektronik Kategori Tinggi. Rendahnya skor ini mengindikasikan beberapa kelemahan fundamental:

1. Belum adanya kebijakan spesifik terkait daur hidup data pribadi (*data lifecycle*), mulai dari pengumpulan hingga pemusnahan.
2. Absennya peran pejabat atau komite khusus yang menangani pelindungan data (*Data Protection Officer*).
3. Kurangnya mekanisme persetujuan (*consent*) yang eksplisit dari subjek data.

Temuan ini menunjukkan risiko kepatuhan (*compliance risk*) yang tinggi terhadap UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi. Jika terjadi insiden kebocoran data, perusahaan rentan terhadap sanksi hukum maupun reputasi, mengingat status sistemnya yang strategis [11].

### 3.5. Analisis Kesenjangan (*Gap Analysis*)

Ketimpangan antara skor Aset (190) dan PDP (28) menunjukkan fenomena "Teknologi Maju, Kebijakan Tertinggal". Perusahaan sangat mahir dalam mengelola "wadah" (aset server, perangkat, jaringan), namun kurang memberikan perhatian pada "isi" (data pribadi) yang ada di dalam wadah tersebut.

Evaluasi akhir menyimpulkan bahwa meskipun aspek teknis memadai, status kelayakan keamanan informasi PT. XYZ secara keseluruhan masih Belum Memenuhi (*Compliance* Gap) standar Kategori Tinggi, terutama disebabkan oleh jatuhnya nilai pada suplemen PDP yang menjadi syarat mutlak dalam Indeks KAMI versi 5.0.

### 3.6. Rekomendasi Perbaikan Strategis

Untuk meningkatkan tingkat kematangan dan menutup celah keamanan, penelitian ini merekomendasikan strategi berbasis kekuatan aset (*Asset-Driven Improvement*):

1. Pemanfaatan Database Aset untuk Pemetaan Data Pribadi: Menggunakan daftar aset yang sudah lengkap (Skor 190) untuk melakukan *tagging* atau pelabelan aset mana saja yang menyimpan Data Pribadi Spesifik maupun Umum.
2. Penyusunan Kebijakan Privasi: Mengembangkan dokumen kebijakan PDP yang merujuk pada ISO 27701 sebagai ekstensi dari ISO 27001 yang sudah diadopsi sebagian.
3. Implementasi Kontrol Akses Berbasis Aset: Memperketat hak akses logis pada aset-aset kritis yang telah teridentifikasi menyimpan data pelanggan.

## 4. KESIMPULAN

Berdasarkan hasil evaluasi keamanan informasi menggunakan Indeks KAMI 5.0 pada PT. XYZ, dapat disimpulkan bahwa tingkat kematangan keamanan informasi perusahaan masih menghadapi tantangan kepatuhan yang signifikan, terutama mengingat status Sistem Elektronik (SE) yang tergolong Kategori Tinggi.

Penelitian ini menemukan adanya disparitas tata kelola yang tajam antar domain. Di satu sisi, perusahaan menunjukkan kematangan yang sangat baik pada domain Pengelolaan Aset Informasi dengan skor 190, yang mengindikasikan bahwa inventarisasi dan kontrol infrastruktur teknologi telah berjalan optimal. Namun, keunggulan teknis ini belum diimbangi dengan aspek kepatuhan privasi, di mana domain Pelindungan Data Pribadi (PDP) mencatat skor terendah sebesar 28. Hal ini menunjukkan bahwa perusahaan memiliki kerentanan tinggi

terhadap risiko pelanggaran privasi data dan belum sepenuhnya memenuhi standar regulasi UU PDP.

Sebagai rekomendasi perbaikan, penelitian ini menyarankan strategi pembenahan berbasis aset (*asset-based improvement*). Manajemen perusahaan disarankan untuk memanfaatkan kelengkapan data inventaris aset yang sudah ada sebagai landasan untuk memetakan keberadaan data pribadi (data mapping). Dengan mengetahui lokasi penyimpanan data pada aset yang terdata, perusahaan dapat segera menerapkan kebijakan klasifikasi data dan kontrol akses yang lebih ketat untuk meningkatkan skor PDP dan memenuhi standar kelulusan Kategori Tinggi.).

**DAFTAR PUSTAKA**

[1] E. E. W. Tulungen, D. P. E. Saerang, and J. B. Maramis, "Transformasi Digital : Peran Kepemimpinan Digital," *Jurnal EMBA : Jurnal Riset Ekonomi, Manajemen, Bisnis dan Akuntansi*, vol. 10, no. 2, pp. 1116–1123, Apr. 2022, doi: 10.35794/emba.v10i2.41399.

[2] J. K. Ekonomi *et al.*, "Oikos-Nomos: Transformasi Digital dan Strategi Manajemen," *Jurnal Oikos-Nomos*, vol. 16, no. 1, pp. 16-26, Jun. 2023, doi: https://doi.org/10.37479/jkeb.v16i1.20322.

[3] L. D. A. Jelita, M. N. Al Azam, and A. Nugroho, "Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/EIC 27001:2022," *Jurnal SAINTEKOM*, vol. 14, no. 1, pp. 84–94, Mar. 2024, doi: 10.33020/saintekom.v14i1.623.

[4] P. P. Thenu, A. F. Wijaya, C. Rudianto, U. Kristen, and S. Wacana, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan Cobit 5 (Studi Kasus: PT Global Infotech)," *Jurnal Bina Komputer*, vol. 2, no. 1, pp. 1-13, Feb. 2020, doi: https://doi.org/10.33557/binakomputer.v2i1.799

[5] M. Miftakhatun, "Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000," *Journal of Computer Science and Engineering (JCSE)*, vol. 1, no. 2, pp. 128–146, Aug. 2020, doi: 10.36596/jcse.v1i2.76.

[6] V. Patrick, P. Wijaya, and A. D. Manuputty, "Manajemen Risiko Teknologi Informasi Pada BTSI UKSW Menggunakan ISO 31000:2018," *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, vol. 9, no. 2, pp. 1295–1307, Jun. 2022, doi: https://doi.org/10.35957/jatisi.v9i2.2087.

[7] R. Dewantara, B. Sugiantoro, and P. Korespondensi, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Pada Jaringan (Studi Kasus : Uin Sunan Kalijaga Yogyakarta)", *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK),* vol. 8, no. 6, pp. 1137-1148, Dec. 2021, doi: 10.25126/jtiik.202183123.

[8] 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, Oct. 2021, doi: 10.7777/jiemar.

[9] Muhammad Rizkillah, "Evaluasi Keamanan Informasi Perguruan Tinggi Menggunakan Indeks Keamanan Informasi (KAMI) Versi 5.0," *Jurnal Cakrawala Ilmiah*, vol. 3, no, 10, pp. 2835-2842, Jun. 2024, doi: https://www.bajangjournal.com/index.php/JCI/article/view/7988.

[10] "Tentang Perusahaan Bumi Vharta." Accessed: Sep. 26, 2025. [Online]. Available: https://bvarta.com/id/tentang-perusahaan/

[11] R. Putra, "Manajemen Risiko Keamanan Informasi: Studi Kasus Pusat Data Dinas XYZ," *The Indonesian Journal of Computer Science*, vol. 13, no. 4, Aug. 2024, doi: 10.33022/ijcs.v13i4.4129.

[12] A. Hanif Nadanta, H. Farisi, and D. W. Brata, "Analisis Evaluasi Indeks KAMI (Keamanan Informasi) 5.0 dalam Pengelolaan Keamanan Informasi di SMK Telkom Purwokerto," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 9, no. 8, Aug. 2025. Available: http://j-ptiik.ub.ac.id

[13] K. H. R and M. S. Hasibuan, "Analisis Tingkat Kematangan Keamanan Informasi Menggunakan Indeks KAMI pada Tiyuh Pulung Kencana," *Journal of Digital Literacy and Volunteering*, vol. 2, no. 1, pp. 31–37, Jan. 2024, doi: 10.57119/litdig.v2i1.78.

[14] R. Ramadhan, N. Widiyasono, A. Rahmatullah, and S. Artikel, "Evaluasi Keamanan Informasi Sistem Informasi Manajemen RSUD KHZ Musthafa Menggunakan Indeks KAMI 5.0 Berbasis ISO/IEC 27001:2022," *Jurnal Multimedia dan IT, vol. 9, no. 01, pp. 080-086, Jun.* 2025, doi: 10.46961/jommit.v9i1.

[15] Gita Fitria, Dwi Yuniarto, and David Setiadi, "Evaluasi Keamanan Sistem Pajak Daerah Online Kabupaten Sumedang Menggunakan Indeks Keamanan Informasi 5.0," *Jurnal Teknik Mesin, Industri, Elektro dan Informatika*, vol. 4, no. 1, pp. 232–242, Feb. 2025, doi: 10.55606/jtmei.v4i1.4817.