NIVEDITA JOURNAL INFORMATICS
ISSN 3089-8366
(Media Online)

Vol. 01, No. 2, Juni 2025

EVALUASI TINGKAT KESIAPAN KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (INDEKS KAMI) VERSI 5.0 PADA DISKOMINFO XYZ

Fedro Ali Handro[1], Alwi Azis Mahendra[2], Megawati[3]

[1,2,3]Prodi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Sultan Syarif Kasim Riau, Indonesia

email: 12150311233@students.uin-suska.ac.id

Abstract

The advancement of information technology encourages organizations, including government institutions, to ensure information security in order to improve operational efficiency and effectiveness. Based on observations and interviews, it was found that DISKOMINFO XYZ has never conducted a comprehensive information security evaluation. The KAMI Index is compiled by BSSN and refers to the international standard ISO/IEC 27001:2013, thus providing a credible and standardized evaluation framework. This study evaluates the level of information security readiness at the XYZ Communication and Informatics Service using the Information Security Index (KAMI Index) Version 5.0 which refers to the international standard ISO/IEC 27001:2013. The evaluation was conducted in seven main areas: governance, risk management, framework, asset management, technology management, electronic system categories, and security supplements. The results show that DISKOMINFO XYZ is at the Basic Framework Fulfillment stage with a total evaluation score of 695, indicating a level of information security maturity that varies between levels I+ to V. These results indicate that DISKOMINFO XYZ already has a basis in implementing information security, but still needs improvement in documentation, procedures, and supporting infrastructure to achieve a more mature level of readiness and meet the ISO/IEC 27001 standard. Recommendations are given to improve the readiness and effectiveness of information security governance, preparing the agency for ISO/IEC 27001 certification.

Keywords: *Information Security, KAMI Index, ISO/IEC 27001:2013, Readiness Evaluation, Diskominfo.*

Abstrak

Kemajuan teknologi informasi mendorong organisasi, termasuk institusi pemerintah, untuk memastikan keamanan informasi guna meningkatkan efisiensi dan efektivitas operasional. Berdasarkan observasi dan wawancara, ditemukan bahwa DISKOMINFO XYZ belum pernah melakukan evaluasi keamanan informasi secara menyeluruh. Indeks KAMI disusun oleh BSSN dan mengacu pada standar internasional ISO/IEC 27001:2013, sehingga memberikan kerangka evaluasi yang kredibel dan terstandar. Penelitian ini mengevaluasi tingkat kesiapan keamanan informasi di Dinas Komunikasi dan Informatika XYZ menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 5.0 yang mengacu pada standar internasional ISO/IEC 27001:2013. Evaluasi dilakukan pada tujuh area utama: tata kelola, manajemen risiko, kerangka kerja, pengelolaan aset, pengelolaan teknologi, kategori sistem elektronik, dan suplemen keamanan. Hasil menunjukkan bahwa DISKOMINFO XYZ berada pada tahap Pemenuhan Kerangka Kerja Dasar dengan total skor evaluasi 695, mengindikasikan tingkat kematangan keamanan informasi yang bervariasi antara level I+ hingga V. Hasil ini menunjukkan bahwa DISKOMINFO XYZ telah memiliki dasar dalam penerapan keamanan informasi, namun masih perlu peningkatan dalam dokumentasi, prosedur, dan infrastruktur pendukung untuk mencapai tingkat kesiapan yang lebih matang dan memenuhi standar ISO/IEC 27001. Rekomendasi diberikan untuk meningkatkan kesiapan dan efektivitas tata kelola keamanan informasi, mempersiapkan instansi menuju sertifikasi ISO/IEC 27001.

Kata kunci: Keamanan Informasi, Indeks KAMI, ISO/IEC 27001:2013, Evaluasi Kesiapan, Diskominfo.

Diajukan:6 Jnnuari 2025; Direvisi: 3 Juni 2025; Diterima: 4 Juni 2025

PENDAHULUAN

Pemanfaatan teknologi informasi dan komunikasi mampu membawa organisasi pada proses bisnis yang efektif dan efisien[1]. Di tingkat daerah, urusan komunikasi dan informatika dikelola oleh Dinas Komunikasi dan Informasi (DISKOMINFO) pemerintah.Diskominfo sangat penting untuk mengelola informasi publik, menyebarkan kebijakan pemerintah, dan membantu orang berkomunikasi dengan

pemerintah. Dalam era digital saat ini, diskominfo sangat penting karena teknologi komunikasi dan informasi berkembang pesat dan sangat penting untuk pembangunan daerah[2].

Dalam menjalankan tugas tersebut, aspek keamanan informasi menjadi elemen krusial yang tidak dapat diabaikan. Sesuai dengan Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016, semua instansi pemerintah diwajibkan untuk menerapkan Sistem Manajemen Keamanan Informasi (SMKI) yang bertujuan melindungi kerahasiaan, integritas, dan ketersediaan informasi yang dikelola[3]. Namun, berdasarkan observasi dan wawancara yang dilakukan, ditemukan bahwa DISKOMINFO XYZ belum melakukan evaluasi keamanan informasi secara menyeluruh. Evaluasi menggunakan Indeks KAMI perlu dilakukan karena DISKOMINFO XYZ belum memiliki sistem pengamanan informasi yang terstandar dan menyeluruh. Selama ini, upaya pengamanan hanya difokuskan pada mitigasi penyadapan, sementara aspek penting lain seperti kerahasiaan dan integritas data belum terkelola dengan baik. Hal ini menimbulkan risiko tinggi terhadap ancaman keamanan informasi yang semakin kompleks. Indeks KAMI Versi 5.0, yang disusun oleh BSSN dan mengacu pada standar ISO/IEC 27001:2013, digunakan sebagai alat evaluasi karena mampu mengukur kesiapan keamanan informasi secara komprehensif dan terstruktur. Melalui evaluasi ini, kelemahan-kelemahan dapat diidentifikasi dan dijadikan dasar untuk menyusun langkah perbaikan menuju sistem keamanan informasi yang lebih matang dan siap menghadapi tantangan digital.Upaya yang telah dilakukan sebatas mitigasi ancaman penyadapan, sementara risiko lain terkait kerahasiaan dan integritas data belum terukur secara optimal. Ketidaksiapan ini dapat menimbulkan kerentanan terhadap ancaman keamanan informasi yang semakin kompleks seiring perkembangan teknologi dan meningkatnya jumlah data yang dikelola[4].

Evaluasi keamanan informasi yang terstandar diperlukan untuk memastikan tata kelola teknologi informasi berjalan secara aman dan efisien[5]. Indeks Keamanan Informasi (Indeks KAMI) versi 5.0 yang disusun oleh Badan Siber dan Sandi Negara (BSSN) merupakan alat bantu yang efektif dalam mengevaluasi tingkat kesiapan dan kematangan keamanan informasi di organisasi pemerintah[6]. Indeks ini dirancang mengacu pada standar internasional ISO/IEC 27001:2013 dengan mencakup enam area utama, meliputi tata kelola, manajemen risiko, kerangka kerja, pengelolaan aset, pengelolaan teknologi, dan suplemen keamanan[7]. Keamanan informasi merupakan aspek krusial dalam pengelolaan teknologi informasi di organisasi modern, khususnya instansi pemerintah. Menurut ISO/IEC 27001:2013, keamanan informasi bertujuan untuk melindungi tiga aspek utama informasi, yaitu kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability). Dengan semakin kompleksnya sistem informasi serta meningkatnya volume dan nilai data yang dikelola, risiko terhadap keamanan informasi pun meningkat. Ancaman seperti peretasan, penyadapan, kehilangan data, hingga penyalahgunaan akses menjadi tantangan utama yang perlu diantisipasi dengan pendekatan sistematis dan berbasis standar internasional .

Penelitian ini bertujuan untuk mengevaluasi tingkat kesiapan dan kematangan keamanan informasi di DISKOMINFO XYZ menggunakan Indeks KAMI versi 5.0, serta memberikan rekomendasi yang dapat mendukung penguatan tata kelola keamanan informasi. Hasil evaluasi diharapkan menjadi dasar dalam menentukan langkah strategis untuk memenuhi standar keamanan informasi dan mempersiapkan instansi menuju sertifikasi keamanan informasi.

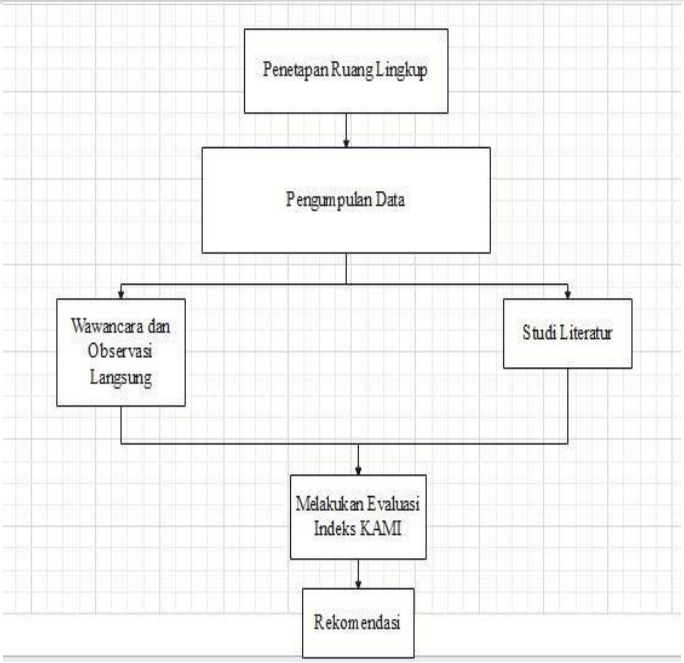
METODE

Dalam Gambar 1 menunjukkan langkah-langkah penelitian yang dilakukan dalam penelitian ini. Kerangka penelitian adalah komponen penting dari proses penelitian agar rangkaian penelitian dapat terarah, teratur, dan sistematis.

Metode penelitian yang digunakan dalam studi ini mengikuti pendekatan evaluatif dengan mengacu pada Indeks Keamanan Informasi (Indeks KAMI) Versi 5.0 sebagai instrumen utama. Alur penelitian dimulai dengan penetapan ruang lingkup, dilanjutkan dengan pengumpulan data, evaluasi menggunakan Indeks KAMI, serta analisis dan penyusunan rekomendasi berdasarkan hasil evaluasi [8].

Penetapan ruang lingkup penelitian dilakukan dengan mendefinisikan batasan penelitian dan penilaian yang sesuai pada tahap penetapan ruang lingkup, peneliti mendefinisikan batasan objek penelitian, yaitu DISKOMINFO XYZ, serta area evaluasi yang mencakup tujuh aspek: kategori sistem elektronik, tata kelola, manajemen risiko, kerangka kerja, pengelolaan aset, teknologi, dan suplemen keamanan.. Data dan dokumen pendukung dikumpulkan melalui wawancara dan studi literatur.

NIVEDITA
JOURNAL INFORMATICS
ISSN 3089-8366
(Media Online)
Vol. 01, No. 2, Juni 2025



Gambar 1. Metodologi penelitian

Wawancara dilakukan secara langsung dengan Kepala Bagian DISKOMINFO XYZ yang memiliki tanggung jawab dalam perencanaan dan pengelolaan sistem informasi di lingkungan instansi tersebut.Model evaluasi yang digunakan adalah Indeks KAMI Versi 5.0 dari Badan Siber dan Sandi Negara, yang sesuai dengan SNI ISO/IEC 27001[9]. Proses evaluasi dilakukan dengan mengisi sejumlah pertanyaan terkait di masing-masing area. Berdasarkan hasil evaluasi, rekomendasi disusun untuk meningkatkan kelengkapan dokumen, ketersediaan prosedur operasional standar, infrastruktur, dan elemen pendukung lainnya. Implementasi rekomendasi ini diharapkan dapat meningkatkan nilai indeks dan kesiapan pengamanan informasi pada DISKOMINFO XYZ pada periode evaluasi berikutnya.[10]

HASIL DAN PEMBAHASAN

Penetapan Ruang Lingkup

DISKOMINFO XYZ menggunakan Indeks KAMI versi 5.0 untuk melakukan evaluasi tingkat kesiapan pengamanan informasi. Terdapat 195 pertanyaan yang dibagi menjadi 7 bagian area evaluasi:

1. Kategori Sistem Elektronik sebanyak 10 pertanyaan
2. Tata Kelola Keamanan Informasi sebanyak 22 pertanyaan.
3. Pengelolaan Risiko Keamanan Informasi dengan 16 pertanyaan
4. Kerangka Kerja Pengelolaan Keamanan Informasi dengan 32 pertanyaan
5. Pengelolaan Aset Informasi dengan 53 pertanyaan
6. Teknologi dan Keamanan Informasi dengan 35 pertanyaan
7. Suplemen dengan 27 pertanyaan.

Pengumpulan Data

Melakukan Wawancara yang dimana mengumpulkan data melalui wawancara dan dokumen seperti Peraturan, SOP, dan data terkait. Dan Studi Literatur yang dimana mengumpulkan teori dari jurnal, buku teks, dan e-book yang relevan dengan keamanan informasi.

Melakukan Evaluasi Indeks KAMI

1. Evaluasi Kategori Sistem Elektronik

Jenis sistem elektronik yang digunakan dibahas dalam bagian ini. Untuk kategori sistem elektronik, penilaian terdiri dari sepuluh pertanyaan, setiap jawaban pertanyaan menunjukkan status institusi yang dinilai saat ini. Menurut penetapan skor dalam Indeks KAMI Versi 5.0, nilai untuk setiap pertanyaan ditetapkan sebagai berikut: jika jawaban sesuai dengan status pada poin A, nilainya adalah 5, jika B nilainya adalah 2, dan jika C nilainya adalah 1. Dari sepuluh pertanyaan yang diberikan, skor dari setiap jawaban dijumlahkan, dan hasilnya adalah skor total. Seperti yang ditunjukkan pada gambar 2, terdapat tiga kategori hasil evaluasi: Rendah, Tinggi, dan Strategis.

Tabel 1. Kategori Sistem Elektronik

Skor	Kategori
10 – 15	Rendah
16 – 34	Tinggi
35 – 50	Strategis

Dalam kategori ini, DISKOMINFO XYZ mendapat skor total 38 seperti yang ditunjukkan pada tabel 2. Berdasarkan tabel 1, skor antara 35 dan 50 termasuk dalam kategori strategis, yang menunjukkan bahwa penggunaan sistem elektronik menjadi bagian penting dari proses kerja yang berjalan.

Tabel 2. Hasil evaluasi Kategori Sistem Elektronik

1.6	**Data pribadi yang dikelola Sistem Elektronik** [A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya [B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha [C] Tidak ada data pribadi	A	5
1.7	**Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyadapan ataupun penerobosan keamanan informasi** [A] Sangat Rahasia [B] Rahasia dan/atau Terbatas [C] Biasa	B	2
1.8	**Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi** [A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik [B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung [C] Proses yang hanya berdampak pada bisnis perusahaan	A	5
1.9	**Dampak dari kegagalan Sistem Elektronik** [A] Membahayakan pertahanan keamanan negara [B] Tidak tersedianya layanan publik berskala nasional atau berdampak pada layanan di sektor lain [C] Tidak tersedianya layanan publik dalam 1 propinsi atau internal 1 instansi/perusahaan	A	5
1.10	**Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme)** [A] Menimbulkan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan mengakibatkan kerugian finansial)	A	5
	Skor penetapan Kategori Sistem Elektronik		38

2. Evaluasi Kelengkapan dan Kematangan Pengamanan Informasi

Evaluasi kelengkapan dan tingkat kematangan pengamanan informasi dilakukan pada 5 area pengamanan informasi, yaitu:

a. Tata Kelola Keamanan Informasi.
b. Pengelolaan Risiko Keamanan Informasi.
c. Kerangka Kerja Pengelolaan Keamanan Informasi.
d. Pengelolaan Aset Informasi.
e. Teknologi dan Keamanan Informasi.

Setiap pertanyaan dijawab sesuai kondisi yang sudah diterapkan dengan skor sesuai dengan kategori pengamanan yang telah didefinsikan dalam Indeks KAMI Versi 5.0 seperti dalam tabel 3.

Tabel 3. Skor Tingkat Kematangan

Status Penerapan	Penetapan Skor		
	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan atau Diterapkan Sebagian	2	4	6
Diterapkan secara Menyeluruh	3	6	9

Hasil evaluasi dari penilaian lima bagian pengamanan data adalah sebagai berikut:

a. Hasil Evaluasi Tata Kelola Keamanan Informasi:
Bagian ini mengevaluasi seberapa siap sistem manajemen keamanan informasi, serta tugas dan tanggung jawab pengelola keamanan informasi, dengan total nilai evaluasi 123.

b. Pengelolaan Risiko Keamanan Informasi:
Bagian ini mengevaluasi seberapa siap strategi keamanan informasi untuk menerapkan pengelolaan risiko keamanan informasi. Nilai evaluasi total untuk wilayah ini adalah 70.

c. Kerangka Kerja Pengelolaan Keamanan Informasi:
Bagian ini menilai kekuatan dan kesiapan kerangka kerja pengelolaan keamanan informasi, serta strategi untuk menerapkannya. Nilai total untuk evaluasi wilayah ini adalah 159

d. Pengelolaan Aset Informasi:
Bagian ini menilai kelengkapan pengamanan aset informasi, termasuk siklus penggunaan aset tersebut. Nilai total evaluasi di bagian ini adalah 139.

e. Teknologi Teknologi dan Keamanan Informasi:
Bagian ini menilai penggunaan teknologi untuk melindungi aset informasi. Nilai total untuk evaluasi wilayah ini adalah 120.

Contoh hasil evaluasi terhadap 5 area pengaman informasi dengan menggunakan Indeks KAMI Versi 5.0 yang telah dilakukan pada DISKOMINFO XYZ dapat dilihat pada tabel 4.

Tabel 4. Hasil Evaluasi Teknologi dan Keamanan Informasi

Bagian IV: Teknologi dan Keamanan Informasi					
Bagian ini mengevaluasi kelengkapan, Konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
6.27	III	2	**Apakah instansi/perusahaan anda sudah menerapkan proses perencanaan pengembangan sistem?** (Dengan mempertimbangkan hasil pemrograman yang tidak baik/kil pada sistem sebelumnya, konfigurasi software/development tool yang aman (secure), kontrol terhadap lingkungan pengembangan, desain arsitektur yang aman)	Dalam Penerapan / Diterapkan Sebagian	4
6.28	III	2	**Apakah instansi/perusahaan anda menerapkan proses source code review** (baik secara manual atau menggunakan piranti lunak) sebelum dilanjutkan ke lingkungan produksi?	Dalam Penerapan / Diterapkan Sebagian	4
6.29	II	1	**Apakah instansi/perusahaan anda memiliki kontrol atas perubahan source code aplikasi** ?	Dalam Penerapan / Diterapkan Sebagian	2
6.30	III	2	**Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/divalidasi pada saat proses pengembangan dan uji coba?**	Dalam Penerapan / Diterapkan Sebagian	4
6.31	III	3	Apakah instansi/perusahaan anda secara rutin menganalisa dan memperbaiki jika ditemukan celah pada sistem (misal adanya laporan kelemahan dan/atau	Dalam Penerapan / Diterapkan Sebagian	6

			teknik eksploit baru) yang berdampak pada keamanan sistem aplikasi?		
6.32	III	3	**Apakah instansi/perusahaan anda menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun?**	Dalam Penerapan / Diterapkan Sebagian	6
6.33	III	3	Apakah instansi/perusahaan anda sudah menerapkan proses atau mekanisme untuk mencegah karyawan/mitra bisnis/perusahaan lain dari perusahaan (misal membatasi/mengamankan lampiran email atau memblokir pengiriman dokumen/data ke luar)?	Dalam Penerapan / Diterapkan Sebagian	6
6.34	IV	3	**Apakah instansi/perusahaan sudah menerapkan teknologi (DLP Data Leakage Prevention) untuk mencegah terungkapnya informasi sensitif ke luar dari perusahaan?**	Dalam Penerapan / Diterapkan Sebagian	6
6.35	IV	3	**Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?**	Tidak Dilakukan	0
			Total Nilai Evaluasi Teknologi dan Keamanan Informasi	**120**	

3. Evaluasi Suplemen

Dalam bagian ini, evaluasi dilakukan untuk menilai kelengkapan, konsistensi, dan efektivitas teknologi yang digunakan untuk melindungi aset informasi. Evaluasi ini membahas aspek kesiapan Pengamanan Keterlibatan Pihak Ketiga, Pengamanan Layanan Infrastrukutur Awan (Cloud Service), dan Perlindungan Data Pribadi dalam konteks atau cakupan saat ini.

Yang membedakan bagian ini dari enam bagian evaluasi lainnya adalah bahwa nilai total evaluasi tidak digunakan; sebaliknya, nilai rata-rata dari semua nilai yang diperoleh dari setiap kelompok pertanyaan dihitung. Tabel 5 menunjukkan hasil evaluasi suplemen yang dilakukan pada DISKOMINFO XYZ dengan menggunakan Indeks KAMI Versi 5.0.

Tabel 5. Hasil Evaluasi Suplemen

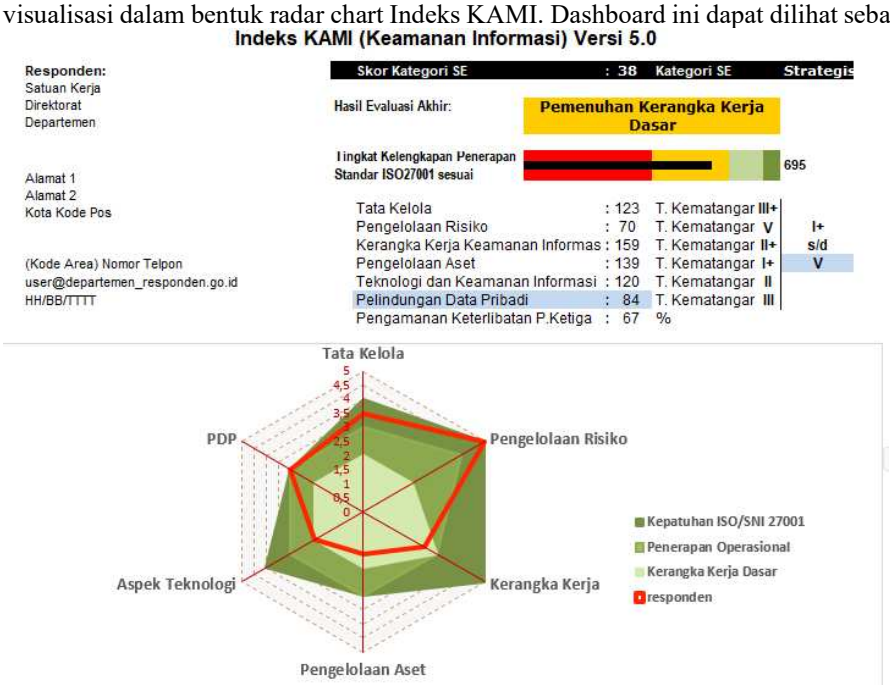
Bagian VIII: Suplemen			
Bagian ini mengevaluasi kelengkapan, Konsistensi dan efektifitas penerapan mekanisme keamanan terkait risiko keterlibatan pihak ketiga eksternal dalam operasional penyelenggaraan layanan instansi/perusahaan			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh		**Status**	Skor
8.1	**Manajemen Risiko dan Pengelolaan Keamanan pihak ketiga**		
8.1.1	**Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerja sama dengan pihak ketiga atau karyawan kontrak?**	Dalam Penerapan / Diterapkan Sebagian	2
8.1.2	Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?	Dalam Penerapan / Diterapkan Sebagian	2
8.1.3	**Apakah instansi/perusahaan mengidentifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipenuhi oleh pihak ketiga?**	Dalam Penerapan / Diterapkan Sebagian	2
8.1.4	Apakah pihak ketiga sudah sepenuhnya memahami persyaratan mitigasi tersebut oleh manajemen pihak ketiga atau karyawan kontrak?	Dalam Penerapan / Diterapkan Sebagian	2
8.1.5	**Apakah instansi/perusahaan telah menerapkan kebijakan keamanan informasi bagi pihak ketiga secara memadai, mencakup persyaratan**	Dalam Penerapan / Diterapkan Sebagian	2

NIVEDITA
JOURNAL INFORMATICS
ISSN 3089-8366
(Media Online)
Vol. 01, No. 2, Juni 2025

	pengendalian akses, pengahncuran informasi, manajemen risiko penyediaan layanan pihak ketiga, dan NDA nagi karyawan pihak ketiga?		
8.1.6	Apakah kebijakan tersebut (7.1.1.5) telah dikomunikasikan kepada pihak ketiga dan mereka menyatakan persetujuannya dalam dokumen kontrak, SLA atau dokumen sejenis lainnya?	Dalam Penerapan / Diterapkan Sebagian	2
8.1.7	Apakah hak audit TI secara berkala ke pihak ketiga/pihak ketiga telah ditetapkan sebagai bagian dan persyaratan kontrak, dikomunikasikan dan disetujui pihak ketiga? Apakah instansi/perusahaan telah mendokumentasikan internal / eksternal tentang kondisi kontrol keamanan informasi pihak ketiga/pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian	2
8.2	**Pengelolaan Sub-Kontraktor/Alih Daya pada Pihak Ketiga**		
8.2.1	Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia pihak ketiga untuk sistem dan layanannya?	Dalam Penerapan / Diterapkan Sebagian	2
8.2.2	Apakah instansi/perusahaan sudah menetapkan pengendalian risiko dalam perjanjian dengan pihak ketiga untuk pengendalian pihak ketiga lainnya?	Dalam Penerapan / Diterapkan Sebagian	2
8.2.3	Apakah instansi/perusahaan melakukan pemantauan dan evaluasi terhadap kepatuhan alih daya, subkontraktor atau penyedia pihak ketiga lainnya terhadap persyaratan keamanan yang ditetapkan?	Dalam Penerapan / Diterapkan Sebagian	2
	Total Nilai Evaluasi Teknologi dan Keamanan Informasi	**120**	

Dashboard Indeks KAMI

Dashboard Indeks KAMI menampilkan hasil penilaian untuk seluruh area penilaian, yang mencakup skor dari tujuh area penilaian dan tingkat kematangan masing-masing. Selain itu, dashboard ini menampilkan hasil akhir terkait status kesiapan pengamanan informasi, tingkat penerapan Standar ISO 27001, dan visualisasi dalam bentuk radar chart Indeks KAMI. Dashboard ini dapat dilihat sebagai berikut:



Gambar 2. Dashboard Penilaian Indeks KAMI pada DISKOMINFO XYZ

Dashboard penilaian yang ada pada gambar 2 dapat dijelaskan seperti di bawah ini :

1. Kategori Sistem Elektronik memiliki skor 38 dan termasuk dalam kategori Strategis, yang ditunjukkan di bagian atas dashboard dengan warna hitam. Menunjukkan bahwa penggunaan sistem elektronik merupakan komponen strategis yang secara signifikan mendukung proses kerja DISKOMINFO XYZ.
2. Skor 123 pada area Tata Kelola Keamanan Informasi yang termasuk dalam tingkat kematangan III+ menunjukkan bahwa DISKOMINFO XYZ sudah memiliki sebagian besar elemen pengelolaan keamanan informasi, namun masih ada beberapa aspek penting yang perlu diperbaiki atau dilengkapi agar sistem tata kelola tersebut benar-benar optimal dan berstandar tinggi. Dengan kata lain, nilai dan tingkat kematangan ini menunjukkan bahwa DISKOMINFO XYZ sudah berada di tahap menengah menuju matang, tetapi belum stabil dan berkelanjutan secara penuh.
3. Skor 70 pada area Pengelolaan Risiko Keamanan Informasi yang berada pada tingkat kematangan V menunjukkan bahwa DISKOMINFO XYZ telah mencapai tingkat tertinggi dalam hal pengelolaan risiko keamanan informasi. Dengan tingkat kematangan V ini, dapat disimpulkan bahwa pengelolaan risiko di DISKOMINFO XYZ sudah sangat baik, menjadi contoh praktik terbaik (best practice), dan mendukung pencapaian tujuan keamanan informasi secara maksimal.
4. Skor 159 pada area Kerangka Kerja Keamanan Informasi yang berada pada tingkat kematangan II+ menunjukkan bahwa DISKOMINFO XYZ baru berada pada tahap awal pengembangan kerangka kerja keamanan informasi, dan pelaksanaannya belum sepenuhnya konsisten atau menyeluruh.
5. Skor 139 pada area Pengelolaan Aset Informasi yang termasuk dalam tingkat kematangan I+ menunjukkan bahwa DISKOMINFO XYZ masih berada pada tahap paling awal dalam mengelola aset informasi, dengan implementasi yang sangat terbatas dan belum terstruktur. Dengan skor ini, dapat disimpulkan bahwa pengelolaan aset informasi di DISKOMINFO XYZ masih sangat lemah, sehingga menjadi prioritas utama untuk ditingkatkan.
6. Skor 120 pada area Teknologi dan Keamanan Informasi yang berada pada tingkat kematangan II menunjukkan bahwa DISKOMINFO XYZ telah mulai menerapkan teknologi keamanan informasi, namun penerapannya masih terbatas, belum konsisten, dan belum terdokumentasi secara formal. dapat disimpulkan penggunaan teknologi di DISKOMINFO XYZ sudah ada, namun masih perlu ditingkatkan dari sisi cakupan, dokumentasi, pengawasan, dan standarisasi agar bisa mencapai tingkat kematangan yang lebih tinggi dan mendukung keamanan informasi secara menyeluruh.
7. Skor Suplemen pada dashboard ditunjukkan dalam bentuk persentase total skor untuk setiap aspek dibandingkan dengan skor maksimal seluruh pertanyaan untuk setiap kelompok. Untuk kelompok perlindungan data pribadi, skor ini mencapai 84%, dan untuk kelompok pengamanan keterlibatan pihak ketiga, skor ini mencapai 67%. Persentase ini membantu menunjukkan tingkat kelengkapan dan efektivitas pengamanan di area tambahan (suplemen) yang mendukung keamanan informasi secara keseluruhan. Meskipun perlindungan data pribadi tergolong baik, pengamanan terhadap keterlibatan pihak ketiga masih perlu ditingkatkan agar tidak menjadi celah keamanan di lingkungan DISKOMINFO XYZ.

Tingkat kelengkapan penerapan standar ISO 27001 berada pada rentang Tingkat I+ hingga V, berdasarkan 695 skor evaluasi dari lima area pengamanan informasi. Ini ditunjukkan dalam dashboard pada gambar 7 sebagai garis horizontal hitam yang mencapai area kuning, yang dimana skor 695 dalam hasil evaluasi menggunakan Indeks KAMI Versi 5.0 merupakan skor kumulatif dari lima area utama pengamanan informasi (tata kelola, manajemen risiko, kerangka kerja, pengelolaan aset, dan teknologi informasi). Skor ini menunjukkan tingkat kesiapan dan kematangan keamanan informasi secara keseluruhan di DISKOMINFO XYZ. Pewarnaan dalam Indeks KAMI menunjukkan tingkat kematangan: merah menunjukkan Tingkat I, kuning menunjukkan Tingkat II, hijau muda menunjukkan Tingkat III, dan hijau tua menunjukkan Tingkat IV.

Secara keseluruhan, hasil akhir evaluasi Indeks KAMI menunjukkan bahwa status kesiapan pengamanan data DISKOMINFO XYZ berada pada tahap Pemenuhan Kerangka Kerja Dasar, dengan skor total 695. Dengan latar berwarna kuning, ditampilkan pada dashboard di bagian atas gambar 7 Skor 695 dan status area kuning tersebut menunjukkan bahwa DISKOMINFO XYZ telah memiliki landasan awal dalam keamanan informasi, tetapi masih berada dalam tahap pengembangan dan penguatan. Evaluasi ini penting sebagai acuan untuk menyusun strategi perbaikan, agar bisa naik ke tingkat kematangan yang lebih tinggi.

KESIMPULAN

Hasil evaluasi Indeks Keamanan Informasi (KAMI) Versi 5.0 terhadap kesiapan dan kematangan keamanan data DISKOMINFO XYZ menunjukkan hal-hal berikut:

1. Kategori Sistem Elektronik:

Hasil evaluasi menunjukkan bahwa kategori sistem elektronik termasuk dalam kategori strategis dengan skor 38. Ini menunjukkan bahwa penggunaan sistem elektronik merupakan komponen strategis yang secara signifikan mendukung proses kerja DISKOMINFO XYZ.

2. Lima Area Pengamanan:

Evaluasi yang dilakukan pada lima area pengamanan menghasilkan skor total 695. Hasilnya menunjukkan bahwa status kesiapan pengamanan informasi berada pada tahap "Pemenuhan Kerangka Kerja Dasar", dengan tingkat kematangan antara I+ dan V.

3. Area Suplemen:

Evaluasi perlindungan data pribadi mencapai 84% dan evaluasi keterlibatan pihak ketiga mencapai 67% di bidang suplemen.

[1] S. Maryati and M. I. Siregar, "Kepemimpinan Digital dalam meningkatkan kinerja organisasi peran Teknologi Informasi dan Komunikasi," *Owner*, vol. 6, no. 4, pp. 3616–3624, Oct. 2022, doi: 10.33395/owner.v6i4.1176.

[2] U. K. Islam Negeri Raden Fatah Jl H Zainal Abidin Fikri, "https://rumah-jurnal.com/index.php/jsaps/index STRATEGI DISKOMINFO KOTA PALEMBANG DALAM MENGELOLA APLIKASI SIDEMANG UNTUK PENINGKATAN PELAYANAN KOMUNIKASI PUBLIK (PALEMBANG CITY DISKOMINFO STRATEGY IN MANAGING THE SIDEMANG WEBSITE TO IMPROVE PUBLIC COMMUNICATION SERVICES) Widya Darma Sasabila," 2024. [Online]. Available: https://rumah-jurnal.com/index.php/jsaps/index

[3] "PERATURAN MENTERI KOMUNIKASI DAN INFORMATIKA REPUBLIK INDONESIA."

[4] A. Kusnandar, A. F. Rochim, and V. Gunawan, "Pengukuran Tingkat Risiko dan Keamanan Informasi Menggunakan Metode FMEA Berbasis ISO/IEC 27001 pada Instansi XYZ untuk Keamanan Sistem Informasi," *Jurnal Sistem Informasi Bisnis*, vol. 14, no. 4, pp. 375–384, Oct. 2024, doi: 10.21456/vol14iss4pp375-384.

[5] D. I. Pembimbing Hanim Maria Astuti and D. I. Pembimbing Bekti Cahyo Hidayanto, "PADA DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) ITS SURABAYA EVALUATING INFORMATION SECURITY MANAGEMENT USING INDEKS KEAMANAN INFORMASI (KAMI) BASED ON ISO/IEC 27001:2013 AT DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) ITS SURABAYA."

[6] 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.

[7] A. Goeritno *et al.*, "UNTUK SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) PADA FAKULTAS TEKNIK UIKA-BOGOR."

[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, doi: 10.7777/jiemar.

[9] Rizkillah Muhammad, "EVALUASI KEAMANAN INFORMASI PERGURUAN TINGGI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) VERSI 5.0," vol. 3, pp. 2835–2842, 2024.

[10] M. Iqbal *et al.*, "Penggunaan Indeks Keamanan Informasi (KAMI) 4.2 Sebagai Metode Evaluasi Kemanan Informasi Pada Dinas Komunikasi Dan Informatika Kota XYZ," *EQUIVA Journal of Mathematics & Information Technology*, vol. 2, no. 1, 2024.