Analisa Sistem Manajemen Keamanan Informasi (SMKI) Organisasi Menggunakan Indeks KAMI

Analysis Organization Information Security Management System (ISMS) Using Indeks KAMI

Jeckson Sidabutar[1)], Ahmad Turmudi Zy[2)], Fresly Juliarta[3)]

[1)]*Program Studi Rekayasa Keamanan Siber, Jurusan Keamanan Siber, Politeknik Siber dan Sandi Negara*
Jl. H. Usa, Putat Nutug, Ciseeng, Bogor, Jawa Barat, Indonesia 16120

[2)]*Program Studi Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa*
Jl. Inspeksi Kalimalang No.9, Cibatu, Cikarang Sel., Kabupaten Bekasi, Jawa Barat, Indonesia 17530

[3)]*Program Studi Manajemen, Fakultas Ekonomi dan Bisnis, Universitas Labuhanbatu*
Jl. S.M. Raja, No. 126A, Aek Tapa, Rantauprapat, Labuhanbatu, Sumatera Utara, Indonesia 21411

Riwayat: Copyright ©2024, JITU, Submitted: 14 Agustus 2024; Revised: 4 September 2024; Accepted: 19 September 2024; Published: 30 September 2024
DOI: 10.32938/jitu.v4i2.7747

Abstract - A high amount of data and a low level of security will jeopardize an organization's business processes. The important role of the organization's leaders is justified in managing the situation with the proposed new attitude. Organizational leaders have responsibility and commitment to the Information Security Management System (ISMS) policy, as well as providing knowledge to employees about ISMS "discipline". With good IMS discipline, the organization can systematically protect itself from the dangers and potential losses of computer misuse and cybercrime. This research provides a comprehensive way to apply SMKI Gap Analysis using the KAMI Index. KAMI Index is an evaluation tool that analyzes the level of SMKI readiness in an organization using ISO / IEC 27001: 2022 and COBIT standards. From this study, it is known that the Respondent Identity is at Value 41, which is Strategic. The results of the analysis were obtained based on the evaluation of the KAMI Index, namely the gap in the range of completeness of the Factual Gap security (Meeting the Basic Framework) with the Conformance Gap (Good Enough) with a range of 1 Level. While the Factual Gap gap (Meets the Basic Framework) with the Ideal Gap (Good) with a range of 2 Levels. These results provide an overview of SMKI readiness to organizational leaders in increasing awareness of information security needs and a new attitude toward the "discipline" of SMKI to the organization.

Keywords *- Gap Analysis; Indeks KAMI; Information Security Management System; Organization.*

Abstrak - Jumlah data yang tinggi dan tingkat keamanan yang rendah akan membahayakan proses bisnis dari suatu organisasi.

Peran penting pemimpin organisasi dibenarkan dalam mengelola situasi dengan sikap baru yang diusulkan. Pemimpin organisasi memiliki tangung jawab dan komitmen atas kebijakan Sistem Manajemen Keamanan Informasi (SMKI), serta memberikan pengetahuan kepada karyawan tentang "disiplin" SMKI. Dengan disiplin SMKI yang baik membuat organisasi dapat secara sistematis melindungi dirinya dari bahaya dan potensi kerugian akibat penyalahgunaaan komputer dan kejahatan dunia maya. Penelitian ini memberikan cara yang komprehensif dengan menerapkan Analisa Gap SMKI menggunakan Indeks KAMI. Indeks KAMI merupakan alat evaluasi untuk menganalisa tingkat kesiapan SMKI disuatu organisasi dengan menggunakan standar ISO/IEC 27001:2022 dan COBIT. Dari penelitian ini diketahui Identitas Responden pada Nilai 41 yaitu Strategis. Hasil Analisa yang diperoleh berdasarkan evaluasi Indeks KAMI yaitu kesenjangan rentang kelengkapan pengamanan Gap Faktual (Memenuhi Kerangka Kerja Dasar) dengan Gap Kesesuaian (Cukup Baik) dengan rentang 1 Tingkat. Sedangkan kesenjangan Gap Faktual (Memenuhi Kerangka Kerja Dasar) dengan Gap Ideal (Baik) dengan rentang 2 Tingkat. Hasil ini memberikan gambaran kesiapan SMKI kepada pimpinan organisasi dalam meningkatkan kesadaran mengenai kebutuhan keamanan informasi dan sikap baru dalam "disiplin" SMKI kepada organisasi.

Kata kunci *- Analisa Gap; Indeks KAMI; Organisasi; Sistem Manajemen Keamanan Informasi.*

[*)] Penulis korespondensi (Jeckson Sidabutar)
Email: jeckson.sidabutar@poltekssn.ac.id

I. PENDAHULUAN

Dengan kemajuan teknologi yang pesat, pergeseran lanskap ancaman siber, dan peningkatan digitalisasi, organisasi dapat mengekspos diri mereka pada risiko

keamanan siber yang berpotensi memberikan dampak buruk bagi organisasi dan tujuan bisnis (Cyber Security Agency of Singapore, 2021). Insiden pelanggaran keamanan informasi masih sangat tinggi dalam beberapa tahun terakhir, sehingga meningkatkan perhatian terkait masalah keamanan siber dari regulator, praktisi, dan peneliti akademisi (Bui, Clemons and Wang, 2016). Tingginya jumlah data dan rendahnya tingkat keamanan akan membahayakan proses bisnis dari suatu organisasi (Toapanta et al., 2020). Terlepas dari kemajuan teknologi yang berkelanjutan, membuat pelanggaran keamanan menjadi besar dan informasi tetap menyebar di seluruh dunia (Bui, Clemons and Wang, 2016). Informasi tentang model atau arsitektur keamanan di analisa untuk meminimalkan serangan siber dan mendukung layanan yang terintegrasi (Kementrian Sekretariat Negara, 2022) (Badan Siber dan Sandi Negara, 2021). Masalahnya adalah bahwa model keamanan yang digunakan dalam organisasi publik mengalami ancaman keamanan informasi dikarenakan kerentanan dalam Sistem Manajemen Keamanan Informasi (SMKI) (Toapanta et al., 2020). Ancaman ini mengakibatkan kebocoran data konsumen maupun organisasi, sehingga dapat mengurangi kapabilitas organisasi (Jhony Pranata and Nuruzzaman, 2022). Saat ini pengelolaan data yang baik merupakan asset yang tidak ternilai bagi setiap organisasi. Dalam penanganan data, keamanan dan pelindungan data pribadi sangat penting bagi organisasi yang bertanggung jawab secara hukum atas pemrosesan data pribadi yang diselenggarakan (UUD No. 27, 2022).

Pemimpin organisasi harus memiliki tangung jawab dan komitmen atas kebijakan SMKI, serta memberikan pengetahuan kepada karyawan tentang “disiplin” yang diperlukan dalam proses bisnis (Badan Standarisasi Nasional, 2023). Penerapan SMKI merupakan keputusan yang sangat strategis dari sebuah organisasi dan memberikan kepercayaan kepada pihak yang berkepentigan bahwa risiko telah dikelola secara baik (Badan Standarisasi Nasional, 2023). SMKI dipertimbangkan dari sudut pandang kinerja bisnis organisasi secara keseluruhan, dalam konteks ini fokus praktisnya adalah pada evaluasi dan transformasi kinerja sistematik. SMKI yang baik dapat melindungi informasi yang bersifat rahasia dan ketersedian informasi yang disimpan maupun sedang diolah (WIJATMOKO, 2020). Peran penting pemimpin organisasi dibenarkan dalam mengelola situasi dan sikap baru yang diusulkan. Organisasi dapat secara sistematis melindungi dirinya dari bahaya dan potensi kerugian akibat penyalahgunaaan komputer, kejahatan siber dan dampak perang siber. Organisasi dapat membuat keputusan praktis tentang investasi keamanan informasi pada teknologi dan solusi keamanan yang digunakan untuk meningkatkan keamanan informasi dalam mengelola dan mengendalikan biaya keamanan informasi (Calder and Watkins, 2008).

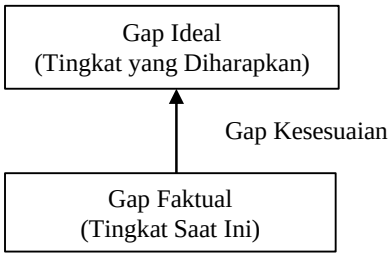
Evaluasi tentang keamanan informasi telah banyak dilakukan, menghasilkan rekomendasi yang dapat memperbaiki SMKI menjadi lebih baik lagi. Pada penelitian K. Pecina, A. Bilbao, dan E. Bilbao menjelaskan perlunya konvergensi manajemen keamanan Fisik dan Logis, serta kesulitan implementasi dikarenakan model organisasi yang berbeda disebagian besar departemen keamanan pada perusahaan atau organisasi (Pecina et al., 2022). Penelitian tersebut mengintegrasikan metodologi standar ISO 31000 untuk keamanan fisik dan standar ISO 27001 untuk keamanan logis, dalam menganalisa informasi dan asset fisik secara bersamaan. Penelitian tentang evaluasi dan manajemen keamanan menjelaskan dalam penangan data, keamanan dan privasi sangat penting bagi administrator dan pengguna (Toapanta et al., 2020). Penelitian tersebut menganalisa evaluasi dan manajemen keamanan basisdata di organisasi publik untuk mengurangi serangan siber berdasarkan proses enkripsi data dalam transaksi. Penelitian T. Weil menggunakan penilaian resiko dalam konteks SMKI untuk platform komputasi awan dengan menggunakan ISO 27001 (Weil, 2019). Sedangkan penelitian M. A. Talib, A. Khelifi, dan T. Ugurlu menggunakan pendekatan baru dalam mengajar dan melibatkan siswa dalam konteks pengalaman nyata yang terkait dengan bidang keamanan informasi menggunakan ISO 27001 (Talib, Khelifi and Ugurlu, 2012).

Pada penelitian ini memberikan cara yang komprehensif dengan banyak sudut pandang yang berbeda dan relevan secara praktis untuk menerapkan SMKI melalui alat evaluasi Indeks Keamanan Informasi (Indeks KAMI). Alat evaluasi ini bertujuan untuk menganalisa tingkat kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan organisasi. Indeks KAMI menggunakan standar ISO/IEC 27001:2022 untuk aspek keamanan kelengkapan kontrol, dan kerangka kerja COBIT untuk tingkat kematangan penerapan pengamanan (BSSN, 2023). Pentingnya Analisa keamanan informasi memberikan Informasi risiko, ancaman, dan kelemahan teknologi yang ditemukan, serta rekomendasi kepada organisasi (Calder and Watkins, 2008).

Indeks KAMI digunakan pada organisasi dengan berbagai tingkatan, ukuran, maupun kepentingan penggunaaan Teknologi Informasi dan Komunikasi. Proses evaluasi menggunakan sejumlah pertanyaan, seperti: kategori sistem elektronik yang digunakan, tata kelola, pengelolaan risiko, kerangka kerja keamanan informasi, pengelolaan asset, teknologi dan keamanan informasi, pelindungan data pribadi, dan pengamanan keterlibatan pihak ketiga (BSSN, 2023). Sehingga memberikan gambaran kondisi kesiapan SMKI sebagai hasil dari program kerja yang dijalankan kepada pimpinan organisasi. Hasil evaluasi ini dapat menjadi sikap baru dalam “disiplin” SMKI dan meningkatkan kesadaran dalam meningkatkan kesiapan mengenai kebutuhan keamanan informasi yang diusulkan kepada organisasi.

II. METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif, bertujuan untuk memahami kejadian yang sedang dialami oleh subjek, seperti tingkah laku manusia, kejadian di lapangan, dan kegiatan lainnya (Prof. Dr. Suryana, 2012). Metode analisa gap digunakan untuk mengetahui kejadian pada subjek. Analisa gap merupakan salah satu proses untuk mengidentifikasi kesenjangan dan perbedaan kondisi saat ini terhadap kondisi yang ingin dicapai organisasi. Penelitian ini menggunakan analisa gap ekspetasi melalui tiga jenis kesenjangan, yaitu: gap faktual, gap kesesuaian, dan gap ideal, seperti Gambar 1 (Kim, Sora and Ji, 2018).



Gambar 1. Analisa Gap Ekspetasi

Melalui analisa gap, organisasi berusaha untuk memperbaiki kondisi saat ini dalam mencapai situasi yang diinginkan. Analisa gap berkontribusi untuk merencanakan implementasi organisasi dan meningkatkan efektifitas organisasi. Analisa gap memiliki empat langkah yaitu, mengidentifikasi kebutuhan utama dari situasi saat ini, menentukan kebutuhan yang ideal atau situasi yang diinginkan organisasi, menyoroti kesenjangan yang ada dan perlu diisi, serta modifikasi dan implementasi rencana organisasi dalam mengisi kesenjangan.

Proses Analisa pada evaluasi Indeks KAMI dilakukan melalui sejumlah pertanyaan di masing-masing area, seperti Tabel 1 (BSSN, 2023).

Tabel 1. Area Evaluasi Indeks KAMI

Area	Penjelasan
Tata Kelola	Evaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan, fungsi, tugas dan tanggung jawab pengelola keamanan
Pengelolaan Risiko	Evaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.
Kerangka Kerja Keamanan Informasi	Evaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.
Pengelolaan Aset	Evaluasi kelengkapan pengamanan asset informasi, termasuk keseluruhan siklus penggunaan asset tersebut.
Teknologi dan Keamanan Informasi	Evaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan asset informasi.
Pelindungan Data Pribadi	Evaluasi kelengkapan, konsistensi dan efektifitas penerapan control keamanan terkait Pelindungan Data Pribadi (PDP).
Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan	Evaluasi kelengkapan, konsistensi dan efektifitas penerapan mekanisme keamanan terkait risiko keterlibatan pihak ketiga eksternal dalam operasional penyelenggaraan layanan instansi/Perusahaan.

Dengan analisa gap ekspetasi pada evaluasi Indeks KAMI memberikan gambaran hasil evaluasi akhir dan tingkat kesiapan pengamanan informasi disuatu organisasi. Sehingga pimpinan dapat melihat kebutuhan dan perbaikan SMKI pada organisasinya

A. Gap Faktual (Tingkat Saat Ini)

Gap Faktual (*Factual*) mengacu pada perbedaan yang dirasakan dalam fakta mengenai keadaan atau kinerja organisasi saat ini. Pada bagian ini merupakan aktivitas awal yang dilakukan untuk mendapatkan informasi kondisi SMKI saat ini, meliputi kegiatan: studi literatur, penyusunan kuesioner, dan pengumpulan umpan balik kuesioner dari responden. Penyusunan kuesioner didasarkan pada kerangka kerja evaluasi Indeks KAMI yang diintegrasikan dengan kerangka kerja ISO/IEC 27001:2022 dan COBIT.

Terdapat 2 tahapan yang dilakukan untuk mengevaluasi kondisi saat ini, yaitu evaluasi tingkat kategori sistem elektronik (SE) dan evaluasi tingkat keamanan informasi organisasi saat ini. Pada evaluasi kategori SE bertujuan untuk mengetahui tingkat atau kategori SE yang digunakan, semakin tinggi nilai yang diperoleh maka semakin tinggi Kategori SE. Sehingga untuk mencapai Status Kesiapan Baik pada Indeks KAMI dibutuhkan nilai akhir tinggi untuk evaluasi tingkat keamanan informasi, seperti pada Tabel 2 (BSSN, 2023).

Tabel 2. Kategori Sistem Elektronik

Rendah		Nilai Akhir		Status Kesiapan
10	15	0	274	Tidak Layak
		248	443	Pemenuhan Kerangka Dasar
		44	760	Cukup Baik
		761	916	Baik
Tinggi		**Nilai Akhir**		**Status Kesiapan**
16	34	0	387	Tidak Layak
		388	646	Pemenuhan Kerangka Dasar
		647	828	Cukup Baik
		829	916	Baik
Strategis		**Nilai Akhir**		**Status Kesiapan**
35	50	0	472	Tidak Layak
		473	760	Pemenuhan Kerangka Dasar
		761	864	Cukup Baik
		865	916	Baik

Berdasarkan Tabel 2, Status kesiapan tingkat Kematangan Indeks KAMI didefinisikan menggunakan pengukuran, seperti pada Gambar 2 (BSSN, 2023).

Gambar 2. Metrik Target Keamanan Informasi

Evaluasi tingkat kematangan keamanan informasi bertujuan untuk mengetahui area-area mana yang memiliki tingkat kematangan yang harus diperhatikan dan diperbaiki. Pertanyaan dikategorikan sesuai dengan kesiapan penerapan pengamanan berdasarkan kelengkapan kontrol dengan standar ISO/IEC27001:2022. Kategori pengamanan diberikan dengan label "1" (kerangka kerja dasar keamanan informasi), label "2" (efektifitas dan konsistensi penerapannya), dan label "3" (selalu meningkatkan kinerja keamanan informasi. Label 3 ini merupakan prasyarat kesiapan minimum pada proses sertifikasi standar ISO/IEC27001:2022, seperti pada Tabel 3 (BSSN, 2023).

Tabel 3. Area Evaluasi Indeks KAMI

Status Pengamanan	Kategori Pengamanan		
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan atau Diterapkan Sebagian	2	4	6
Diterapkan Seluruhnya	3	6	9

B. Gap Kesesuaian

Gap Kesesuaian (*Conformance*) menunjukkan perbedaan antara "kondisi saat ini" dengan apa yang "diinginkan" berdasarkan persepsi organisasi. Hal ini berdasarkan gap antara organisasi anggap sebagai "status yang diinginkan" dalam hal apa yang ingin dicapai organisasi dengan kondisi saat ini (Peciña, Bilbao and Bilbao, 2011). Pada gap kesesuaian dilakukan kegiatan perbandingan antara kondisi saat ini dengan status yang diinginkan organisasi. Kesesuaian ini berdasarkan analisa dan formulasi umpan balik dari kuesioner responden, penentuan target terkait keamanan informasi pada tiap kurun waktu sampai dengan rencana pencapaian Indeks KAMI dan ISO 27001, serta penentuan kerangka kerja keamanan informasi yang disepakati.

C. Gap Ideal (Tingkat yang Diharapkan)

Gap Ideal merupakan perbedaan antara apa yang "diinginkan" organisasi dan apa yang "seharusnya" dilakukan organisasi (Kim, Sora and Ji, 2018). Pada aktivitas ini dilakukan perbandingan antara keinginan organisasi dengan seharusnya yang dilakukan melalui kegiatan evaluasi, konfirmasi, dan klarifikasi (evaluation), serta membaca literatur-literatur tentang keamanan informasi dalam mengetahui yang seharusnya dilakukan organisasi. Kegiatan pada tahap ini antara lain: Diskusi formal maupun informal yang melibatkan personil Pusdatik, Forum Group Discusion (FGD) yang melibatkan audiens lebih besar, dan diskusi menggunakan berbagai media yang bersifat online (Zoom, WA, e-mail, dll).

III. HASIL DAN PEMBAHASAN

A. Gap Faktual

Dari hasil poling responden pimpinan organisasi pada Evaluasi Kategori SE, diperoleh nilai penetapan kategori SE dengan nilai akhir 38, berdasarkan Tabel 2 nilai ini masuk kedalam Kategori Strategis. Sedangkan Evaluasi Tingkat Keamanan Informasi, menghasilkan total nilai nilai 477 dengan tingkat kematangan Pemenuhan Kerangka Kerja Dasar, seperti pada Tabel 4.

Tabel 4. Nilai dan Tingkat Kematangan

No	Area	Nilai	Tingkat Kematangan
1	Tata Kelola	47	I+
2	Pengelolaan Risiko	35	I+
3	Kerangka Kerja Keamanan Informasi	65	I+
4	Pengelolaan Aset	148	II
5	Teknologi dan Keamanan Informasi	125	II
6	Pelindungan Data Pribadi	57	I+
7	Pengamanan Keterlibatan Pihak Ketiga	70%	
	Total	477	Pemenuhan Kerangka Dasar

Berdasarkan Tabel 4 tingkat kematangan pada posisi I+ dan II, maka Gap Faktual Indeks KAMI berada pada kategori Pemenuhan Kerangka Kerja Dasar. Jika evaluasi area target penerapan keamanan informasi berdasarkan kepatuhan ISO 27001, terlihat pada Gambar 3.

Gambar 3. Diagram Indeks KAMI

Pada Gambar 3, Penerapan Operasional hanya pada area Pengelolaan Aset dan Aspek Teknologi, sedangkan Kerangka Kerja, Pengelolaan Risiko, Tata Kelola, dan PDP masih dalam Kerangka Kerja Dasar. Pada area evaluasi Pengamanan Keterlibatan Pihak Ketiga sebesar 70% yang sasaran pencapaian maksimal/objektif.

B. Gap Kesesuaian

Dari hasil Gap faktual dengan Evaluasi Kategori SE masuk kedalam kategori Tinggi, sedangkan tingkat kematangan masuk ke tingkat I+ sampai II dengan rentang kelengkapan pengamanannya masuk ke status pemenuhan kerangka dasar. Penentuan target SMKI berdasarkan persepsi organisasi yaitu: tercapainya kesiapan Indeks KAMI dan Sertifikasi ISO 27001. Jika dilihat pada Gambar 2 untuk mencapai kesiapan sertifikasi ISO 27001 minimal rentang tingkat kematangannya berada pada tingkat 3.5 atau rentang status pengamanannya berada pada status Cukup Baik. Pada Tabel 2 menjelaskan rentang pengamanan dengan status Cukup Baik pada Tingkat 3.5 dengan memiliki status pengamanannya pada setiap area berada "Diterapkan Sebagian" dan "Diterapkan Seluruhnya" sehingga memperoleh minimal nilai 761. Hal ini menunjukkan perbedaan antara "fakta saat ini" dengan "apa yang diinginkan" oleh organisasi, dalam Tabel 5.

Tabel 5. Analisa Kesenjangan Kesesuaian

Area	Gap Faktual		Gap Kesesuaian	
	Status	T	Status	T
Tata Kelola	Dalam Perencanaan, Diterapkan Sebagian	I+	Diterapkan Sebagian, Diterapkan Seluruhnya	III+
Pengelolaan Risiko	Dalam Perencanaan, Diterapkan Sebagian	I+	Diterapkan Sebagian, Diterapkan Seluruhnya	III+
Kerangka Kerja Keamanan Informasi	Dalam Perencanaan, Diterapkan Sebagian	I+	Diterapkan Sebagian, Diterapkan Seluruhnya	III+
Pengelolaan Aset	Diterapkan Sebagian, Diterapkan Seluruhnya	II	Diterapkan Sebagian, Diterapkan Seluruhnya	IV
Teknologi dan Keamanan Informasi	Diterapkan Sebagian, Diterapkan Seluruhnya	II	Diterapkan Sebagian, Diterapkan Seluruhnya	IV
Pelindungan Data Pribadi	Diterapkan Sebagian, Diterapkan Seluruhnya	I+	Diterapkan Sebagian, Diterapkan Seluruhnya	III+
Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan	Dalam Perencanaan	70%	Diterapkan Sebagian, Diterapkan Seluruhnya	85%
Kelengkapan Pengamanan	Pemenuhan Kerangka Kerja Dasar		Cukup Baik	

C. Gap Ideal

Gap Ideal pada Indeks KAMI berada pada tingkat kematangan tertinggi yaitu tingkat V dengan status pengamanan Baik. Dari hasil Gap Kesesuaian yang diinginkan organisasi berada pada tingkat kematangan 3.5 dengan status kelengkapan pengamanan Cukup Baik. Sehingga organisasi dapat mememenuhi kesiapan penilaian Indeks KAMI dan kesiapan sertifikasi ISO 27001. Berdasarkan kegiatan evaluasi, konfirmasi, dan klarifikasi, serta membaca literatur tentang keamanan informasi dengan kategori SE Strategis. Maka didapatkan kesimpulan tingkat pengamanan informasi harus diterapkan seluruhnya pada semua area organisasi yang berarti pada kematangan tingkat V. Hal ini menunjukkan perbedaan antara apa yang "diinginkan" organisasi dan apa yang "seharusnya" dilakukan organisasi, seperti pada Tabel 6.

Tabel 6. Analisa Kesenjangan Ideal

Area	Gap Faktual		Gap Kesesuaian	
	Status	T	Status	T
Tata Kelola	Diterapkan Sebagian, Diterapkan Seluruhnya	III+	Diterapkan Seluruhnya	V
Pengelolaan Risiko	Diterapkan Sebagian, Diterapkan Seluruhnya	III+	Diterapkan Seluruhnya	V
Kerangka Kerja Keamanan Informasi	Diterapkan Sebagian, Diterapkan Seluruhnya	III+	Diterapkan Seluruhnya	V
Pengelolaan Aset	Diterapkan Sebagian, Diterapkan Seluruhnya	IV	Diterapkan Seluruhnya	V
Teknologi dan Keamanan Informasi	Diterapkan Sebagian, Diterapkan Seluruhnya	IV	Diterapkan Seluruhnya	V
Pelindungan Data Pribadi	Diterapkan Sebagian, Diterapkan Seluruhnya	III+	Diterapkan Seluruhnya	V
Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan	Diterapkan Sebagian, Diterapkan Seluruhnya	85%	Diterapkan Seluruhnya	100%
Kelengkapan Pengamanan	Cukup Baik		Baik	

Berdasarkan Tabel 6, organisasi seharusnya menerapkan pengamanan seluruhnya pada semua area. Sehingga evaluasi Indeks KAMI pada organisasi mendapatkan tingkat kematangan V dengan status kesiapan Baik.

D. Hasil Analisa

Hasil Analisa kesenjangan yang diperoleh kesenjangan antara Gap Faktual, Gap Kesesuaian, dan Gap Ideal seperti pada Tabel 7.

Tabel 7. Hasil Analisa

Area	Tingkat Kematangan		
	Faktual	Sesuai	Ideal
Tata Kelola	I+	III+	V
Pengelolaan Risiko	I+	III+	V
Kerangka Kerja Keamanan Informasi	I+	III+	V
Pengelolaan Aset	II	IV	V
Teknologi dan Keamanan Informasi	II	IV	V
Pelindungan Data Pribadi	I+	III+	V
Pengamanan Keterlibatan Pihak Ketiga	70%	85%	100%
Kelengkapan Pengamanan	Pemenuhan Kerangka Dasar	Cukup Baik	Baik

Kesenjangan tingkat kelengkapan pengamanan Gap Faktual yang memenuhi kerangka kerja dasar dengan Gap Kesesuaian Cukup Baik, jaraknya sekitar 2 Tingkat. Sedangkan kesenjangan Gap Faktual yang memenuhi Kerangka Kerja Dasar dengan Gap Ideal hasil Baik sekitar 4 Tingkat, seperti pada Gambar 4.

Gambar 4. Hasil Analisa Gap

Dari Gambar 4 untuk memenuhi kesiapan sertifikasi ISO27001 ISMS minimal rentang Tingkat kematangan di Tingkat 3,5 atau III+, maka Gap Kesesuain yang di pilih di Tingkat 3,5 atau III+. Responden harus melengkapi kesenjangan yang ada sekitar 2 tingkat, sehingga dapat memenuhi target yang ingin di capai yaitu pada Tingkat 3,5 atau III+. Maka Gap ideal dengan nilai kategori SE dengan nilai Strategis tingkat pengamanan informasi harus diterapkan seluruhnya pada semua area organisasi. Hasil Analisa yang diperoleh berdasarkan evaluasi Indeks KAMI yaitu kesenjangan rentang kelengkapan pengamanan Gap Faktual (Memenuhi Kerangka Kerja Dasar) dengan Gap Kesesuaian (Cukup Baik) dengan rentang 2 Tingkat. Sedangkan kesenjangan Gap Faktual (Memenuhi Kerangka Kerja Dasar) dengan Gap Ideal (Baik) dengan rentang 3,5 Tingkat.

IV. KESIMPULAN

Berdasarkan analisa SMKI Organisasi menggunakan Indeks KAMI, diketahui Identitas Responden pada Nilai Kategori SE dengan Nilai 38 yaitu Strategis. Gap faktual didapatkan pada tingkat kelengkapan penerapan standar dengan total nilai 474 dan tingkat kematangan berada pada tingkat I+ sampai II, maka Gap Faktual Indeks KAMI berada pada kategori Pemenuhan Kerangka Dasar. Dari hasil Gap kesesuaian yang diinginkan organisasi berada pada tingkat kematangan III+ dengan status kelengkapan pengamanan Cukup Baik. Organisasi dapat mememenuhi kesiapan penilaian Indeks KAMI dan kesiapan sertifikasi ISO 27001. Hasil dari penelitian ini memberikan gambaran kondisi kesiapan SMKI kepada pimpinan organisasi dalam meningkatkan kesadaran mengenai kebutuhan keamanan informasi dan sikap baru dalam "disiplin" SMKI yang diusulkan kepada organisasi. Sehingga pimpinan organisasi dapat melakukakan pembenahan untuk meningkatkan Nilai pada masing-masing Area Evaluasi dalam memperoleh hasil evaluasi akhir kategori Baik.

DAFTAR PUSTAKA

Badan Siber dan Sandi Negara (2021) *Peraturan BSSN Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE, Badan Siber dan Sandi Negara*. Indonesia.

Badan Standarisasi Nasional (2023) *SNI ISO IEC 27001:2022 Keamanan informasi, keamanan siber, dan proteksi privasi — Sistemmanajemen keamanan informasi — Persyaratan*.

BSSN (2023) *Indeks Keamanan Informasi (Kami)*. Versi 5.0, *Badan Siber dan Sandi Negara (BSSN)*. Versi 5.0. Edited by Tim Indeks KAMI BSSN. Jakarta: Badan Siber dan Sandi Negara. Available at: https://bssn.go.id/indeks-kami/.

Bui, T., Clemons, E. and Wang, D. (2016) 'Introduction to the information security and privacy minitrack', *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2016-March, p. 4792. doi: 10.1109/HICSS.2016.594.

Calder, A. and Watkins, S. (2008) *IT Governance: A Manager's Guide to Data Security and ISO 27001/ISO27002*. 4th edn, *Governance An International Journal Of Policy And Administration*. 4th edn.

Cyber Security Agency of Singapore (2021) 'Guide To Conducting Cybersecurity Risk Assessment for Critical Information Infrastructure', (February). Available at: https://www.csa.gov.sg/-/media/Csa/Documents/Legislation_Supplementary_References/Guide-to-Conducting-Cybersecurity-Risk-Assessment-for-CII---Feb-2021.pdf.

Jhony Pranata, E. and Nuruzzaman, M. T. (2022) 'Optimasi Keamanan Informasi Menggunakan Manajemen Indeks Keamanan Informasi (Kami) Studi Kasus: Ibisa Purworejo', 5(1), pp. 32–45.

Kementrian Sekretariat Negara (2022) *Peraturan Presiden Nomor 132 Tahun 2022 tentang Arsitektur SPBE, Menteri Hukum Dan Hak Asasi Manusia Republik Indonesia*. Indonesia.

Kim, Sora and Ji, Y. (2018) 'Gap Analysis', *Information Security Risk Analysis*, (April), pp. 116–127. doi: 10.1201/ebk1439839560-9.

Pecina, K. *et al.* (2022) 'Physical and Logical Security Management Organization Model Based On ISO 31000 and ISO 27001', *IEEE Xplorer*, (1), pp. 1–5.

Peciña, K., Bilbao, A. and Bilbao, E. (2011) 'Physical and logical Security Risk Analysis model', *Proceedings - International Carnahan Conference on Security Technology*, pp. 1–7. doi: 10.1109/CCST.2011.6095895.

Prof. Dr. Suryana, Ms. (2012) *Metodologi Penelitian :*

Metodologi Penelitian Model Prakatis Penelitian Kuantitatif dan Kualitatif, Universitas Pendidikan Indonesia. doi: 10.1007/s13398-014-0173-7.2.

Talib, M. A., Khelifi, A. and Ugurlu, T. (2012) 'Using ISO 27001 in teaching information security', *IECON Proceedings (Industrial Electronics Conference)*, pp. 3149–3153. doi: 10.1109/IECON.2012.6389395.

Toapanta, S. M. *et al.* (2020) 'Analysis for the evaluation and security management of a database in a public organization to mitigate cyber attacks', *IEEE Access*, 8, pp. 169367–169384. doi: 10.1109/ACCESS.2020.3022746.

UUD No. 27 (2022) *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang RI*. Indonesia.

Weil, T. (2019) 'Risk assessment methods for cloud computing platforms', *Proceedings - International Computer Software and Applications Conference*, 1, pp. 545–547. doi: 10.1109/COMPSAC.2019.00083.

WIJATMOKO, T. E. (2020) 'Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) Pada Kantor Wilayah Kementerian Hukum Dan Ham Diy', *Cyber Security dan Forensik Digital*, 3(1), pp. 1–6. doi: 10.14421/csecurity.2020.3.1.1951.