ANALISIS KEAMANAN SISTEM INFORMASI PERGURUAN TINGGI BERBASIS INDEKS KAMI

Fauzia Anis Sekar Ningrum[1], Yudha Riwanto[2], Inggrid Yanuar Risca Pratiwi[3], Muhammad Ainul Fikri[4]

[1,2,3,4] Teknik Informatika, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta, Indonesia
[1]fauzianingrum@amikom.ac.id, [2]yudha.riwanto@amikom.ac.id,
[3]inggridyrp@amikom.ac.id, [4]fikri.ma@amikom.ac.id

Abstrak

Keamanan informasi merupakan hal yang penting dalam lingkungan Perguruan Tinggi, baik swasta maupun negeri untuk melindungi data sensitif dan menjaga integritas serta kerahasiaan informasi. Dalam paper ini, dilakukan perbandingan manajemen keamanan informasi antara dua Perguruan Tinggi Swasta yang berada di daerah Kabupaten Banyuwangi, yaitu Perguruan Tinggi A dan Perguruan Tinggi B untuk mengukur menggunakan Indeks Keamanan Informasi (Indeks KAMI) versi 5.0. Metode penelitian yang digunakan melibatkan pengumpulan data dari kedua Perguruan Tinggi melalui survey dengan Indeks KAMI. Setelah itu, data tersebut dianalisis dan perbandingan dilakukan berdasarkan elemen-elemen KAMI yang berstandar SNI ISO 27001, meliputi Tata Kelola Keamanan Informasi, Pengelolaan Risiko Keamanan Informasi, Kerangka Kerja Keamanan Informasi, Pengelolaan Aset informasi, Teknologi dan Keamanan Informasi dan Peran TIK. Hasil penelitian menunjukkan perbedaan signifikan antara dua Perguruan Tinggi Swasta yang telah dilakukan survey. Pada Perguruan Tinggi A menunjukkan tingkat keamanan informasi dengan nilai 713 yang menunjukan indikator standar Cukup Baik yang meliputi Tata Kelola yang baik, Perlindungan Data Pribadi yang kuat, dan mengedepankan Aspek Teknologi. Sedangkan pada Perguruan Tinggi B menunjukan tingkat keamanan informasi dengan nilai 321 yang menunjukan indikator Tidak Layak standar ISO, dengan elemen yang paling kuat dalam Perguruan Tinggi B adalah kontrol keamanan Perlindungan Data Pribadi.

Kata kunci: indeks KAMI, ISO 27001, keamanan informasi, manajemen keamanan informasi, perguruan tinggi swasta

1. Pendahuluan

Era digital yang semakin mendunia, keamanan informasi menjadi prioritas utama bagi organisasi, individu, dan pemerintah di seluruh dunia. Dibalik segala kemudahan dan kemungkinan yang menyertai teknologi, terdapat pendekatan serius terhadap teknologi. Ada beberapa faktor yang perlu dipertimbangkan ketika mengelola teknologi informasi untuk memastikan bahwa hal itu tidak menimbulkan dampak yang tidak diinginkan (Manuhutu et al., 2021). Salah satu faktor yang menimbulkan kekhawatiran dan menimbulkan risiko adalah faktor keamanan informasi. Sebab, jika informasi yang menjadi sasaran utama teknologi informasi dan komunikasi mempunyai permasalahan keamanan informasi, maka dapat terjadi kerancuan dan permasalahan dalam teknologi informasi dan komunikasi (Sari et al., 2021).

Tantangan keamanan informasi terus berkembang seiring dengan perkembangan teknologi, dan serangan cyber menjadi semakin canggih dan merugikan (Susanto et al., 2023). Ancaman ini dapat berasal dari berbagai sumber, termasuk peretas yang bertujuan mencuri data sensitif, serangan malware yang merusak sistem, dan ancaman insider yang melibatkan individu di dalam organisasi (Pardosi et al., 2024). Keamanan informasi yang dimaksud yaitu tentang kerahasiaan, integritas, dan ketersediaan. Untuk melindungi informasi, sistem informasi harus melakukan penilaian keamanan informasi untuk mengidentifikasi kesenjangan dan kekurangan keamanan informasi (Setiyowati & Sri Siswanti, 2021). Keamanan informasi terdiri dari empat bidang: organisasi, orang, proses, dan teknologi (Nurul et al., 2022).

Pada penelitian sebelumnya, penelitian Evaluasi Tingkat Kesiapan Keamanan Informasi telah dilakukan di Dinas Komunikasi dan Informatika Kota Bogor (Pratiwi & Wulandari, 2021). Pada penelitian tersebut membahas tingkat kesiapan pengelolaan keamanan informasi pada Dinas Komunikasi dan Informatika Kota Bogor dengan menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 4.0 sesuai dengan aspek-aspek keamanan yang telah didefinisikan oleh standar ISO/IEC 27001:2013 yang dibuat oleh Badan Siber dan Sandi Negara (BSSN). hasil dari penelitian tersebut yaitu mendapatkan hasil evaluasi terhadap Kategori Sistem Elektronik memperoleh nilai 35 dan termasuk dalam Kategori Strategis. Penelitian kedua tentang keamanan informasi yaitu Evaluasi

Manajemen Keamanan Informasi pada Jaringan (Studi Kasus: UIN Sunan Kalijaga Yogyakarta) (Dewantara & Sugiantoro, 2021). Penelitian tersebut dilakukan untuk mengoptimalkan proses keamanan informasi agar berjalan sesuai standar indeks KAMI. Metode penelitian yang digunakan antara lain tinjauan pustaka, melakukan penilaian awal terhadap Indeks KAMI, mengimplementasikan infrastruktur OSSIM (Open Source SIEM), memantau metrik keamanan informasi menggunakan teknologi OSSIM, dan membandingkan kondisi jaringan sebelum dan sesudah melakukan penilaian pasca Indeks KAMI termasuk. Implementasi dari OSSIM di jaringan. Penelitian tersebut menghasilkan dengan peningkatan indeks KAMI membantu menaikan nilai pada aspek tata kelola, pengelolaan asset dan teknologi, namun tingkat kelayakan keamanan informasi masih di level I+ sampai dengan II+ sehingga keamanan informasi pada jaringan tidak layak dan butuh perbaikan. Penelitian selanjutnya yaitu Analisis Keamanan Informasi Menggunakan Aplikasi Indeks KAMI Pada Sekretariat DPRD Kabupaten Jombang (Faradhiya Aulia Rahma et al., 2023). Penelitian tersebut bertujuan untuk mengukur sejauh mana aplikasi Indeks KAMI (Kerangka Audit Manajemen Informasi) efektif dalam mengamankan keamanan informasi di Sekretariat DPRD Kabupaten Jombang dan dihasilkan kesimpulan bahwa status keamanan informasi Sekretariat DPRD Kabupaten Jombang telah berada pada area "Kuning", menandakan bahwa sistem telah memenuhi kerangka dasar penerapan ISO-27001 untuk kategori sistem elektronik. Skor keseluruhan mencapai 283, yang merupakan hasil penjumlahan dari rata-rata skor di masing-masing area evaluasi keamanan informasi.

Seiring dengan tuntutan akan kepatuhan terhadap standar keamanan yang semakin ketat, pembaruan Indeks KAMI ver 5.0 bertujuan untuk memberikan panduan yang lebih komprehensif dan relevan bagi organisasi dalam memperkuat perlindungan terhadap aset informasi mereka. Data dari Lanskap Keamanan Siber Indonesia 2022 mengungkapkan bahwa terdapat 311 insiden kebocoran data yang terjadi di Indonesia. Terdapat beragam instrumen yang tersedia untuk mengevaluasi keamanan informasi, dimana salah satunya adalah Indeks Keamanan Informasi (ISI). KAMI digunakan sebagai alat untuk menilai sejauh mana sebuah organisasi telah mempersiapkan keamanan informasinya sesuai dengan standar SNI ISO/IEC 27001. Dalam paper berikutnya berjudul "Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/IEC 27001:2022" dilakukan di sebuah perusahaan berbentuk hukum yang menggunakan teknologi informasi dalam operasional sehari-harinya. Dengan demikian, peneliti melakukan evaluasi terhadap keamanan teknologi informasi untuk memeriksa kondisi keamanan informasi dan meningkatkannya. Evaluasi ini dilakukan melalui observasi dan wawancara di perusahaan tersebut. Data yang telah diperoleh kemudian akan dinilai sesuai dengan Indeks KAMI. Hasil penilaian dari Indeks KAMI menunjukkan bahwa skor kategori sistem elektronik yang diperoleh adalah 19, yang masuk dalam kategori tinggi. Sementara itu, hasil evaluasi akhir menunjukkan bahwa penilaian keseluruhan adalah "Cukup Baik" dengan skor akhir 674. Tingkat kelengkapan implementasi standar ISO 27001 berada dalam rentang level II sampai IV. (Jelita, Al Azam, & Nugroho, 2024)

Perguruan tinggi adalah salah satu organisasi yang memiliki aliran informasi sangat vital. Informasi terkait dengan akademik, administratif, dan pribadi beredar secara luas di organisasi ini. Namun, dengan meningkatnya keterhubungan digital di area Perguruan Tinggi modern, keamanan informasi ini harus menjadi perhatian utama. Tantangan keamanan informasi di lingkup perguruan tinggi sangat kompleks. Selain mempertahankan keamanan sistem informasi internal, perguruan tinggi juga harus mengelola keamanan data mahasiswa dan staf, serta melindungi kekayaan intelektual yang dihasilkan oleh penelitian dan pengembangan di Perguruan Tinggi. Ancaman tersebut dapat berasal dari berbagai pihak, termasuk peretas eksternal, serangan malware, kebocoran data akibat kesalahan manusia, dan bahkan ancaman insider. Keamanan informasi pada lingkup perguruan tinggi tidak hanya infrastruktur namun meliputi pengembangan kebijakan, prosedur, dan kesadaran yang memadai di antara seluruh civitas akademika Perguruan Tinggi. Dalam upaya untuk mengatasi tantangan tersebut, penelitian-penelitian seperti yang dilakukan oleh Wati, Budiyono, & Fauzia (2019) telah mengadopsi pendekatan dengan menggunakan Indeks Keamanan Informasi (KAMI) untuk mengevaluasi dan meningkatkan tingkat keamanan sistem informasi di Direktorat Sistem Informasi Universitas Telkom. Begitu juga, penelitian oleh Kornelia & Irawan (2021) mengaplikasikan metode serupa untuk mengukur tingkat kematangan keamanan informasi di Universitas Bina Darma. Hal ini menegaskan pentingnya penggunaan standar evaluasi seperti KAMI dalam mendukung upaya meningkatkan keamanan informasi di lingkup perguruan tinggi.

Penelitian ini dilakukan sebuah evaluasi tentang keamanan informasi pada 2 Perguruan Tinggi Swasta di Kabupaten Banyuwangi, yaitu Perguruan Tinggi A dan Perguruan Tinggi B. Peneliti menyebar kuesioner yang diisi oleh pihak berwenang masing-masing Perguruan Tinggi untuk menilai keamanan informasinya. Kuesioner ini telah sesuai dengan aspek penilaian dari Badan Siber dan Sandi Negara (ISO/SNI 27001) yaitu Indeks Keamanan Informasi (KAMI) versi 5.0. Penelitian ini bertujuan untuk mengevaluasi kesiapan keamanan teknologi informasi pada kedua Perguruan Tinggi di atas serta

memberikan kritik dan saran terhadap Perguruan Tinggi dari hasil kuesioner.

2. Metodologi

a. Keamanan Informasi

Perlindungan informasi adalah proses yang bertujuan untuk menjaga keamanan aset informasi dari berbagai ancaman yang mungkin terjadi secara sengaja atau tidak, khususnya seiring dengan meningkatnya insiden yang terkait dengan penggunaan Teknologi Informasi dan Komunikasi (TIK). Ancaman tersebut memiliki potensi untuk mengancam kerahasiaan, integritas, dan ketersediaan layanan. Perlindungan ini semakin penting mengingat dampak yang mungkin ditimbulkan oleh gangguan atau kebocoran informasi yang dapat berdampak serius bagi organisasi. (Gala, Sengkey, & Punusingon, 2021).

Keamanan Informasi tidak hanya berfokus pada melindungi informasi dari akses yang tidak sah. Intinya, Keamanan Informasi adalah praktek yang bertujuan untuk mencegah akses, penggunaan, pengungkapan, gangguan, modifikasi, inspeksi, pencatatan, atau penghancuran informasi yang tidak sah, baik itu dalam bentuk fisik maupun digital. Informasi dapat berupa berbagai hal, mulai dari detail pribadi hingga profil media sosial, data di perangkat seluler, hingga data biometrik. Oleh karena itu, ruang lingkup Keamanan Informasi mencakup banyak bidang penelitian seperti Kriptografi (Taliasih & Afrianto, 2020), Forensik Siber (Syamsudin, 2023), Media Sosial Online (Yel & K. M. Nasution, 2022), dan masih banyak bidang lainnya.

Keamanan informasi menjadi landasan penting dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi, baik dalam bentuk digital maupun fisik seperti dokumen kertas. Beberapa alasannya adalah sebagai proteksi terhadap informasi sensitif (data pribadi, informasi finansial, rahasia dagang bahkan rahasia militer dan pemerintah) dan pengurangan resiko ancaman siber. (Pramono, Fahrianto, & Arini, 2019).

b. Indeks KAMI versi 5.0

Indeks Keamanan Informasi (KAMI) adalah perangkat yang difungsikan sebagai sarana penunjang untuk menilai dan mengevaluasi sejauh mana sebuah organisasi telah mempersiapkan dan menerapkan keamanan informasi, dengan merujuk pada standar SNI ISO/IEC 27001. Proses evaluasi dilakukan melalui sejumlah pertanyaan di beberapa area berikut: (1) Kategori Sistem Elektronik yang digunakan, (2) Tata Kelola Keamanan Informasi, (3) Pengelolaan Risiko Keamanan Informasi, (4) Kerangka Kerja Keamanan Informasi, (5) Pengelolaan Aset Informasi, (6) Teknologi dan Keamanan Informasi Suplemen. (BSSN (Badan Siber dan Sandi Negara), 2024).

Standar SNI ISO/IEC 27001 mengalami penyegaran dengan peluncuran SNI ISO/IEC 27001:2022 pada tahun 2022. Sebagai sebuah Sistem Manajemen Keamanan Informasi (SMKI), SNI ISO/IEC 27001 menunjukkan sifat dinamisnya dengan menyesuaikan diri terhadap kemajuan teknologi. Hal ini penting agar standar keamanan informasi tetap relevan dengan kondisi saat ini. Terjadi perubahan dalam judul antara kedua versi ini. Pada versi 2013, judulnya adalah “Information Technology – Security Techniques – Information Security Management System”, sedangkan pada versi 2022 berubah menjadi “Information Security, Cybersecurity and Privacy Protection – Information Security Management System”. Perubahan pada SNI ISO/IEC 27001:2022 secara rinci mencakup restrukturisasi kategori, penambahan 11 kontrol baru, dan pembaruan pada pengendalian. Dengan adanya pembaruan pada SNI ISO/IEC 27001:2022, terjadi revisi pada Indeks Keamanan Informasi (KAMI) dan pembaruan dari Indeks KAMI versi 4.2 menjadi Indeks KAMI versi 5.0 dengan penambahan sesuai kontrol baru pada SNI ISO/IEC 27001:2022. (BSSN (Badan Siber dan Sandi Negara), 2024).

c. ISO 27001

ISO/IEC 27001 memberikan dasar yang komprehensif untuk menetapkan persyaratan dalam mengembangkan, menerapkan, mengawasi, dan meningkatkan manajemen sumber daya manusia, proses operasional, dan teknologi informasi di berbagai jenis organisasi, termasuk yang berukuran kecil, menengah, atau besar. Pendekatan yang digunakan dalam kerangka kerja ini tidak bergantung pada produk teknologi informasi tertentu, melainkan pada penggunaan metode manajemen yang berbasis risiko untuk memastikan keamanan aset informasi dari berbagai ancaman dan memberikan keyakinan akan keamanan kepada semua pihak yang terlibat. (Pradipta, Rahardja, & Sitokdana, 2019)

Struktur organisasi ISO/IEC 27001 terdiri dari dua bagian utama. Pertama, klausul (proses yang wajib dipatuhi) menetapkan persyaratan yang harus dipatuhi oleh organisasi yang menerapkan Sistem Manajemen Keamanan Informasi berdasarkan kerangka kerja ISO/IEC 27001. Kedua, Annex A (kontrol keamanan) adalah dokumen referensi yang memberikan panduan tentang kontrol keamanan yang harus diterapkan dalam Sistem Manajemen Keamanan Informasi. (Pradipta, Rahardja, & Sitokdana, 2019).

Standar ISO/IEC 27001:2022 telah resmi diterbitkan pada bulan Oktober 2022. Meskipun standar sebelumnya, yaitu ISO 27001:2013, masih dapat digunakan selama periode transisi hingga Oktober 2025, organisasi disarankan untuk mulai beradaptasi dengan standar yang baru ini (Sinaga, 2023). Standar ini memberikan pedoman yang jelas dan terstruktur untuk mengidentifikasi, mengevaluasi, dan mengurangi risiko keamanan informasi dalam suatu organisasi. ISO/27001:2022 memiliki beberapa perbedaan dengan versi

terdahulunya, yaitu ISO/27001:2005 dan ISO/27001:2013. Beberapa perbedaan tersebut yaitu (Sinaga, 2023):

1. ISO/27001:2022 menyediakan kerangka kerja yang lebih komprehensif untuk menerapkan SMKI.
2. ISO/27001:2022 menekankan pada penilaian dan pengelolaan risiko keamanan informasi.
3. ISO/27001:2022 mengharuskan organisasi untuk mempertimbangkan aspek lingkungan dalam penerapan SMKI.

3. Hasil dan Pembahasan

Penelitian ini menggunakan Indeks KAMI, sebuah aplikasi berbasis Microsoft Excel yang dikembangkan oleh Badan Siber dan Sandi Negara (BSSN) Republik Indonesia. Indeks KAMI dirancang untuk mengukur tingkat kesiapan dan asesmen terhadap kelengkapan dan kematangan penerapan keamanan informasi berdasarkan kriteria SNI ISO/IEC 27001. Versi terbaru yang digunakan dalam penelitian ini adalah versi 5.0, yang terakhir diperbarui pada 16 Agustus 2023. Indeks KAMI mengidentifikasi tujuh area evaluasi yang mencakup berbagai aspek keamanan informasi. Tiap area evaluasi dianalisis menggunakan kategorisasi lima tingkat kematangan penerapan pengamanan, yang merujuk pada kerangka kerja COBIT atau CMMI.

Penelitian dilakukan terhadap dua Perguruan Tinggi Pendidikan tinggi di daerah Jawa Timur, yaitu Perguruan Tinggi A dan Perguruan Tinggi B. Pemilihan sampel ini didasarkan pada pertimbangan representativitas serta ketersediaan akses dan kerjasama dari kedua Perguruan Tinggi tersebut. Proses pengumpulan data dimulai dengan mewawancarai dan memberikan penjelasan terkait tujuan penelitian kepada tim perwakilan partisipan dari masing-masing perguruan tinggi. Setelah itu, tim perwakilan diminta untuk mengisi Indeks KAMI yang telah dikirimkan. Indeks ini terdiri dari 11 kategori sektor, dengan masing-masing kategori memiliki 15-20 pertanyaan yang dapat dijawab langsung oleh tim perwakilan. Untuk memudahkan pengisian, tersedia dropdown jawaban dengan empat opsi: Tidak Dilakukan, Dalam Perencanaan, Dalam Penerapan/Diterapkan Sebagian, dan Diterapkan Secara Menyeluruh.

Hasil pengisian Indeks KAMI oleh tim perwakilan partisipan akan dievaluasi untuk menentukan tingkat kesiapan keamanan informasi di masing-masing perguruan tinggi. Berdasarkan hasil evaluasi ini, akan diberikan saran perbaikan yang spesifik untuk meningkatkan keamanan informasi di setiap Perguruan Tinggi.

Validitas dan reliabilitas Indeks KAMI telah terbukti melalui penggunaannya dalam berbagai konteks penelitian sebelumnya. Langkah-langkah yang diambil untuk memastikan keakuratan dan konsistensi hasil meliputi verifikasi data, analisis reliabilitas instrumen, dan konsultasi dengan pakar keamanan informasi.

a. Tingkat Kematangan Sistem Elektronik

Pada tahap ini peneliti memberikan hasil analisis data untuk setiap kategori berdasarkan indeks KAMI 5.0. Status klasifikasi penilaian skor yang dilakukan berkaitan dengan standarisasi nilai yang ada pada alat indeks KAMI 5.0. Rincian skor untuk kategori sistem elektronik dapat dilihat pada tabel 1.

Tabel 1. Rincian Skor Kategori

Rendah		**Skor akhir**		**Status Kesiapan**
10	15	0	174	Tidak Layak
		175	312	Pemenuhan Kerangka Dasar
		313	435	Cukup Baik
		436	645	Baik
Tinggi		**Skor akhir**		**Status Kesiapan**
16	34	0	272	Tidak Layak
		273	455	Pemenuhan Kerangka Dasar
		456	583	Cukup Baik
		584	645	Baik
Strategis		**Skor akhir**		**Status Kesiapan**
35	50	0	333	Tidak Layak
		334	535	Pemenuhan Kerangka Dasar
		536	609	Cukup Baik
		610	645	Baik

Hasil analisis data yang terlihat dalam tabel 2 dengan jelas menggambarkan bahwa sistem informasi di Perguruan Tinggi A telah mencapai tingkat kematangan Tinggi, menandakan pencapaian yang baik dalam pengelolaan sistem tersebut, sementara Perguruan Tinggi B masih memperlihatkan status Rendah, menunjukkan adanya ruang untuk peningkatan lebih lanjut dalam upaya menuju kematangan sistem yang lebih baik.

Tabel 2. Hasil Penilaian Indeks KAMI 5.0

No	Nama Per-guruan Tinggi	Jumlah Kue-sioner	Hasil Jawaban			Hasil Skor Akhir	Status
			A	B	C		
1	A	10	2	2	6	20	Tinggi
2	B	10	1	0	9	14	Rendah

b. Tingkat Kematangan Tata Kelola

Pada kategori ini peneliti memberikan hasil analisis penilaian kematangan keamanan sistem informasi Perguruan Tinggi A dan Perguruan Tinggi B terhadap kategori tata kelola keamanan informasi

klasifikasi kategori kematangan tata kelola keamanan informasi mengacu secara khusus pada standarisasi indeks KAMI 5.0 (tabel 3): Tingkat I (Kondisi Awal), Tingkat II (Penerapan Kerangka Kerja Dasar), Tingkat III (Terdefinisi dan Konsisten), Tingkat IV (Terkelola dan Terukur), Tingkat V (Optimal), untuk membantu memberikan uraian yang lebih detail, tingkatan ini ditambah dengan tingkatan diantaranya I+, II+, III+ dan IV+, sehingga total terdapat 9 tingkat kematangan. Adapun pemetaan skor hasil jawaban kuesioner disajikan pada gambar dibawah ini:

Tabel 3. Pemetaan Skor Hasil Jawaban Kuesioner

Status Pengamanan	Kategori Pengamanan		
	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

Adapun hasil penilaian indeks KAMI 5.0 untuk kategori tata kelola keamanan informasi dapat dilihat pada tabel 4.

Tabel 4. Hasil Penilaian Indeks KAMI Kategori Tata Kelola Keamanan Informasi

No	Nama Perguruan Tinggi	Jumlah Kuesioner	Skor	Tingkat Kematangan	Status Nilai
1	A	22	91	III	3
2	B	22	47	I+	1,5

Data yang diperoleh menunjukkan bahwa Kematangan Tata Kelola pada Perguruan Tinggi A memiliki tingkat kematangan dengan golongan III sedangkan Perguruan Tinggi B memiliki tingkat kematangan dengan golongan I+ dimana masih berada pada tahapan penerapan kerangka kerja dasar.

c. Tingkat Kematangan Pengelolaan Risiko

Pada kategori ini peneliti memberikan hasil analisis penilaian kategori kematangan manajemen risiko keamanan informasi pada Perguruan Tinggi A dan Perguruan Tinggi B. Spesifikasi Kategori Maturitas Manajemen Risiko Keamanan Informasi mengacu pada Standarisasi Indeks KAMI 5.0 yang merangkum data evaluasi di kategori Manajemen Risiko Keamanan Informasi yang dapat dilihat pada tabel 5.

Tabel 5. Hasil Penilaian Indeks KAMI Kategori Manajemen Risiko Keamanan Informasi

No	Nama Perguruan Tinggi	Jumlah Kuesioner	Skor	Tingkat Kematangan	Status Nilai
1	A	16	26	I+	1,5
2	B	16	19	I	1

Pada tabel diatas menunjukkan bahwa Kematangan Tata Kelola pada Perguruan Tinggi A memiliki tingkat kematangan dengan golongan I+ yang sedikit lebih baik dari Perguruan Tinggi B namun keduanya masih berada pada kategori tahap awal.

d. Tingkat Kematangan Kerangka Kerja

Pada kategori ini, peneliti memberikan hasil evaluasi pada tingkat kematangan kerangka kerja keamanan informasi di Perguruan Tinggi. Hasil evaluasi ini dapat dilihat pada tabel 6.

Tabel 6. Hasil Penilaian Indeks KAMI Kategori Kematangan Kerangka Kerja

No	Nama Perguruan Tinggi	Jumlah Kuesioner	Skor	Tingkat Kematangan	Status Nilai
1	A	16	136	II	2
2	B	16	52	I+	1,5

Data yang diperoleh menunjukkan bahwa Kematangan Kerangka pada Perguruan Tinggi A memiliki tingkat kematangan dengan golongan II yaitu pada tahapan penerapan kerangka kerja dasar sedangkan B memiliki tingkat kematangan dengan golongan I+ dimana berada pada tahapan kondisi awal.

e. Tingkat Kematangan Pengelolaan Aset

Pada kategori ini peneliti memberikan hasil evaluasi pada kategori tingkat kematangan Pengelolaan Aset pada Perguruan Tinggi A dan B. Tabel 7 berisikan paparan status nilai dari masing-masing perguruan tinggi.

Tabel 7. Hasil Penilaian Indeks KAMI Kategori Kematangan Pengelolaan Aset

No	Nama Perguruan Tinggi	Jumlah Kuesioner	Skor	Tingkat Kematangan	Status Nilai
1	A	32	190	II	2
2	B	32	110	I+	1,5

Dari hasil tabel tersebut menunjukan bahwa Kematangan Tata Kelola pada Perguruan Tinggi A memiliki tingkat kematangan dengan golongan II yaitu pada tahapan penerapan kerangka kerja dasar sedangkan Perguruan Tinggi B memiliki tingkat kematangan dengan golongan I+ dimana berada pada tahapan kondisi awal.

f. Tingkat Kematangan Teknologi dan Keamanan Informasi

Pada kategori ini peneliti memberikan hasil evaluasi pada kategori tingkat kematangan Teknologi dan Keamanan Informasi pada Perguruan Tinggi A dan Perguruan Tinggi B. Nilainya dapat dilihat pada tabel 8.

Tabel 8. Tabel Hasil Penilaian Indeks KAMI Kategori Kematangan Teknologi dan Keamanan Informasi

No	Nama Perguruan Tinggi	Jumlah Kuesioner	Skor	Tingkat Kematangan	Status Nilai
1	A	53	186	IV	4
2	B	53	152	I	1

Data yang diperoleh menunjukkan bahwa Kematangan Kerangka pada Perguruan Tinggi A memiliki tingkat kematangan dengan golongan IV yaitu pada tahapan penerapan Terkelola dan terukur sedangkan Perguruan Tinggi B memiliki tingkat kematangan dengan golongan I dimana berada pada tahapan kondisi awal.

g. Tingkat Kematangan Perlindungan Data Pribadi

Pada kategori ini peneliti memberikan hasil evaluasi pada kategori tingkat kematangan Perlindungan Data Pribadi pada Perguruan Tinggi A dan Perguruan Tinggi B. Secara komprehensif hasilnya dapat dilihat pada tabel 9.

Tabel 9. Tabel Hasil Penilaian Indeks KAMI Kategori Kematangan Perlindungan Data Pribadi

No	Nama Perguruan Tinggi	Jumlah Quisioner	Skor	Tingkat Kematangan	Status Nilai
1	A	16	84	III	3
2	B	16	41	II	1,5

Dari tabel di atas menunjukan bahwa Kematangan Kerangka pada Perguruan Tinggi A memiliki tingkat kematangan dengan golongan III yaitu pada tahapan Terdefinisi dan Konsisten sedangkan Perguruan Tinggi B memiliki tingkat kematangan dengan golongan II dimana berada pada tahapan penerapan kerangka kerja dasar.

h. Tingkat Kematangan Suplemen

Pada kategori ini peneliti memberikan hasil evaluasi pada kategori tingkat kematangan Perlindungan Data Pribadi pada Perguruan Tinggi A dan Perguruan Tinggi B. Perbedaan antara dua subjek penelitian ini terpapar dalam tabel 10.

Tabel 10. Hasil Penilaian Indeks KAMI Kategori Kematangan Suplemen

No	Nama Perguruan Tinggi	Jumlah Kuesioner	Keterlibatan Pihak Ketiga
1	A	27	100%
2	B	27	60%

Keterlibatan pihak ketiga layanan Perguruan Tinggi A sebesar 100 % menimbulkan resiko ketergantungan terkait keberadaan pihak eksternal tersebut, sedangkan pada Perguruan Tinggi B hanya 70% ketergantungan terhadap pihak ketiga.

i. Rekomendasi

Dari hasil perhitungan yang dilakukan, didapatkan beberapa kesimpulan sebagai rekomendasi perbaikan terhadap keamanan sistem informasi, rekomendasi terbanyak ada pada Perguruan Tinggi B di mana di seluruh sektor terdapat rekomendasi yang harus dijalani agar dapat mencapai standarisasi SNI ISO/IEC 27001 diantaranya:

1. Tata Kelola:
   a. Mengembangkan kebijakan keamanan informasi dan persyaratan keamanan informasi internal.
   b. Mewajibkan seluruh pegawai untuk mengikuti pedoman penerapan keamanan informasi.
   c. Membuat kontrak untuk transfer informasi.
   d. Merespon situasi sesuai protokol yang telah ditetapkan .
   e. Perlunya perguruan tinggi menerapkan kesinambungan keamanan informasi.
   f. Perguruan tinggi harus menerapkan perlindungan informasi terkait privasi dan identifikasi pribadi.
2. Manajemen Risiko:
   a. Membuat manual book terkait resiko yang mungkin terjadi.
   b. Menerapkan SMK3 pada setiap bagian dari sistem informasi.
   c. Perguruan tinggi harus mencatat dan melaporkan semua kerentanan keamanan informasi secara berkala.
3. Kerangka Kerja:
   a. Menetapkan kebijakan keamanan informasi.
   b. Peninjauan terhadap kebijakan keamanan informasi yang telah ditetapkan.
   c. Penetapan persyaratan dan pengendalian prosedur audit yang dilakukan.
   d. Penetapan pedoman pengembangan perangkat lunak yang aman.
   e. Pengambilan keputusan dan penilaian mengenai masalah keamanan informasi.
   f. Mengembangkan rencana untuk keamanan informasi berkelanjutan.
   g. Menentukan undang-undang, peraturan, dan persyaratan kontrak yang relevan.
4. Pengelolaan Aset:
   a. Penyusunan daftar aset yang berkaitan dengan aset yang dikelola oleh Otoritas.
   b. Penyusunan pedoman penanganan aset.
   c. Penerapan pengendalian registrasi.
   d. Penerapan prosedur pemeliharaan peralatan.
   e. Keamanan di luar lokasi aset dan peralatan.
   f. Pengaturan pembagian informasi.
   g. Menanggapi insiden keamanan informasi yang terjadi dengan menggunakan prosedur terdokumentasi.
   h. Menetapkan prosedur yang mematuhi hak kekayaan intelektual

5. Teknologi:
   a. Membuat kebijakan kontrol akses untuk konfigurasi keamanan sistem tertentu.
   b. Melakukan manajemen kata sandi.
   c. Membuat kebijakan untuk penggunaan kontrol kriptografi.
   d. Melakukan manajemen kunci.
   e. Melakukan kontrol malware Eksekusi.
   f. Pencatatan peristiwa mencatat kegiatan pelaksanaan.
   g. Melakukan sinkronisasi waktu.
   h. Melakukan analisis dan spesifikasi kebutuhan keamanan informasi.
   i. Menyediakan lingkungan pengembangan yang aman.
   j. Melakukan audit kepatuhan teknis Penambahan

j. Evaluasi

Perguruan Tinggi A terdapat beberapa catatan evaluasi diantaranya:

1. Manajemen Risiko
   a. Menetapkan kebijakan risiko keamanan
   b. Menetapkan SOP tanggung jawab keamanan informasi
   c. Perguruan tinggi wajib memiliki catatan yang akan dapat menimbulkan kerentanan dalam keamanan sistem informasi

2. Suplemen
   a. Menerapkan manajemen risiko dan pengendalian keamanan untuk pihak ketiga
   b. Menerapkan pengendalian layanan dan keamanan untuk pihak ketiga
   c. Penerapan Layanan Infrastruktur Cloud
   d. Soroti Kebijakan Perlindungan Data Pribadi.
   e. Mengidentifikasi tugas dan peran yang terkait dengan audit keamanan informasi pihak ketiga.
   f. Pertemuan rutin diadakan untuk menilai apakah tujuan tingkat layanan dan langkah-langkah keamanan tercapai.

4. Kesimpulan dan Saran

Adapun kesimpulan dari penelitian ini yaitu: terdapat perbedaan signifikan dalam nilai integritas tingkat keamanan informasi antara perguruan A dan perguruan B, dengan perguruan A memperoleh skor sebesar 713 dan perguruan B hanya mencapai 321 saat diperhitungkan menggunakan KAMI. Secara khusus, pada Klasifikasi Indeks KAMI versi 5.0, perguruan tinggi A dikategorikan sebagai "Tinggi", sementara perguruan tinggi B dikategorikan sebagai "Rendah". Evaluasi ini berfokus pada kelengkapan keamanan dan tingkat kematangan informasi di perguruan tinggi, dan hasilnya menunjukkan bahwa perguruan tinggi A masuk dalam kategori II+ yang menunjukkan penerapan kerangka dasar yang lebih baik. Di sisi lain, perguruan tinggi B hanya mencapai kategori I+, menunjukkan bahwa keamanan sistem informasinya masih pada tahap awal.

Berdasarkan data yang diperoleh melalui metode KAMI versi 5.0, perguruan tinggi A dianggap "LAYAK" untuk mengajukan sertifikasi kelayakan ISO/IEC 27001, meskipun masih memerlukan beberapa perbaikan terutama dalam manajemen risikonya. Namun, pada perguruan tinggi B, statusnya masih "BELUM LAYAK" untuk mengajukan sertifikasi tersebut, mengingat tingkat keamanan informasi yang masih dalam tahap awal. Oleh karena itu, sementara perguruan tinggi A mungkin lebih siap untuk menghadapi tantangan keamanan informasi lebih lanjut, perguruan tinggi B perlu meningkatkan upayanya dalam memperkuat keamanan sistem informasinya untuk mencapai tingkat kelayakan yang diperlukan untuk sertifikasi ISO/IEC 27001.

Adapun saran dari hasil penelitian ini yaitu diperlukan data sebagai pembanding dari indeks KAMI 5.0 dapat menggunakan standarisasi lainnya seperti ISO 15500, COBIT 5 ataupun tools lainnya.

Daftar Pustaka:

BSSN (Badan Siber dan Sandi Negara). (2024, 04 30). Retrieved from Konsultasi dan Assessment Indeks KAMI: https://www.bssn.go.id/indeks-kami/

Dewantara, R., & Sugiantoro, B. (2021). Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Jaringan (Studi Kasus: UIN Sunan Kalijaga Yogyakarta). Jurnal Teknologi Informasi Dan Ilmu Komputer, 8(6), 1137. https://doi.org/10.25126/jtiik.2021863123

Faradhiya Aulia Rahma, Najwa Hamidah Erwin, Bintang Nuari Atno Nichada, & Reisa Permatasari. (2023). Analisis Keamanan Informasi Menggunakan Aplikasi Indeks Kami Pada Sekretariat Dprd Kabupaten Jombang. Prosiding Seminar Nasional Teknologi Dan Sistem Informasi, 3(1), 279–288. https://doi.org/10.33005/sitasi.v3i1.396

Gala, R. P., Sengkey, R., & Punusingon, C. (2021). Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI. Jurnal Teknik Informatika, 15(3), 189-198.

Jelita, L. D., Al Azam, M. N., & Nugroho, A. (2024). Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/EIC 27001:2022. Jurnal Saintekom : Sains, Teknologi, Komputer dan Manajemen, 84-94

Kornelia, A., & Irawan, D. (2021). Analisis Keamanan Informasi Menggunakan Tools Indeks KAMI ISO 4.1. Jurnal Pengembangan Sistem Informasi dan Informatika , 78-86.

Manuhutu, M. A., Muttaqin, M., Irmayani, D., Tamara, T., Gustiana, Z., Hazriani, H., ... &

Karim, A. (2021). Pengantar Forensik Teknologi Informasi. Yayasan Kita Menulis.

Nurul, S., Shynta Anggrainy, & Siska Aprelyani. (2022). Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim). Jurnal Ekonomi Manajemen Sistem Informasi, 3(5), 564–573. https://doi.org/10.31933/jemsi.v3i5.992

Pardosi, V. B. A., Kom, S., Karim, A., TI, M., Ilham, R., Kom, M., ... & Wijaya, A. (2024). SISTEM KEAMANAN KOMPUTER. CV Rey Media Grafika.

Pradipta, Y. C., Rahardja, Y., & Sitokdana, M. N. (2019). Audit Sistem Manajemen Keamanan Informasi Pusat Teknologi Informasi dan Komunikasi Penerbangan Dan Antariksa (PUSTIKPAN) Menggunakan SNI ISO/IEC 27001: 2013. Sebatik, 23(2), 352-358.

Pramono, P. P., Fahrianto, F., & Arini. (2019). Pendeteksian Dini Tingkat Keamanan Informasi Berbasis ISO 27001: 2013 Menggunakan Metode AHP (Analytical Hierarchy Process). CyberSecurity dan Forensik Digital, 2(2), 57-64.

Pratiwi, H. A., & Wulandari, L. (2021). 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, 2(5), 146–163.

Sari, I. Y., Muttaqin, Jamaludin, Simarmata, J., Rahman, M. A., Iskandar, A., Pakpahan, A. F., Karim, A., Sugianto, Giap, Y. C., Hazriani, Yendrianof, D., & Manullang, S. O. (2021). Keamanan Data dan Informasi.

Setiyowati, & Sri Siswanti. (2021). Penilaian Kematangan Proses Keamanan Sistem Informasi Pendaftaran Pasien Menggunakan Framework Cobit 4.1. SATIN - Sains Dan Teknologi Informasi, 7(1), 123–133. https://doi.org/10.33372/stn.v7i1.694

Sinaga, R. (2023). Pengembangan Model Penilaian Kepatuhan Salah Satu Perguruan Tinggi Terhadap Standar ISO 27001: 2022. Jurnal Teknik Informatika dan Sistem Informasi, 9(3), 381-394.

Susanto, E., Antira, L., Kevin, K., Stanzah, E., & Majid, A. A. (2023). Manajemen Keamanan Cyber di Era Digital. Journal of Business And Entrepreneurship, 11(1), 23-33.

Syamsudin, I. (2023). Keamanan Komputer dan Forensik

Taliasih, N., & Afrianto, I. (2020). Sistem Keamanan Basis Data Klien PT Infokes Menggunakan Kriptografi Kombinasi RC4 Dan Base64. Jurnal Nasional Teknologi dan Sistem Informasi, 009-018.

Wati, D. A., Budiyono, A., & Fauzia, R. (2019). Analisis dan Perancangan Manajemen Keamanan Informasi Direktorat Sistem Informasi Univ. Telkom Dengan Menggunakan Indeks Keamanan Informasi (KAMI) Pada Area Pengelolaan Aset Informasi, Teknologi dan Keamanan Informasi. e-Proceedings of Engineering, (pp. 7758-7766).

Yel, M. B., & K. M. Nasution, M. (2022). Keamanan Informasi Data Pribadi Pada Media Sosial. Jurnal Informatika Kaputama (JIK), 92-101.