
Analisis Evaluasi Keamanan Informasi Pada Badan pemerintahan Pemerintahan XYZ Menggunakan Indeks KAMI 4.2

Ahmad Yudistira Fahmi Zaini¹, Bambang Sugiantoro², Yudha Riwanto^{3*}

Universitas Islam Negeri Sunan Kalijaga^{1,2}

Universitas Amikom Yogyakarta^{3*}

Email: ¹ahmadyudistira54@gmail.co.id, ²bambang.sugiantoro@uin-suka.ac.id, ³yudha.riwanto@amikom.ac.id

Abstrak

Badan pemerintahan XYZ merupakan pelaksana otonomi daerah dimana dipimpin oleh seorang kepala instansi, yang berada dibawah Gubernur dan bertanggung jawab kepada Gubernur melalui Sekretaris Daerah. Dalam memenuhi visi dari Badan pemerintahan XYZ masyarakat melalui reformasi kalurahan, pemberdayaan kawasan selatan, serta pengembangan budaya inovasi dan pemanfaatan Teknologi Informasi dimana Badan pemerintahan XYZ telah menggunakan berbagai macam teknologi informasi salah satunya layanan dalam website dengan adanya layanan ini dapat memudahkan masyarakat untuk mendapatkan informasi tentang kegiatan gubernur, kegiatan TI, kegiatan kebudayaan, dan berbagai macam kegiatan lainnya. Kegiatan evaluasi perlu dilakukan untuk memastikan keamanan informasi pada Badan pemerintahan XYZ agar sesuai dengan standar yang berlaku. Evaluasi dilakukan dengan menggunakan indeks KAMI 4.2 pada Badan pemerintahan XYZ dapat mengevaluasi tingkat kematangan kelengkapan penerapan ISO 27001 dan memberikan gambaran tata kelola keamanan informasi pada sebuah organisasi. Selain evaluasi menggunakan indeks KAMI akan dilakukan peninjauan hasil dari evaluasi indeks KAMI 4.2 terhadap ISO 27001 untuk mengetahui apa saja standar keamanan informasi pada Badan pemerintahan XYZ yang sudah sesuai dengan ISO 27001 dan standar apa saja yang belum sesuai lalu harus diberikan rekomendasi. Dari hasil penelitian tentang Tingkat Kematangan Keamanan Informasi pada Badan pemerintahan XYZ menggunakan Indeks KAMI 4.2, dapat diketahui bahwa untuk kategori sistem elektronik tingkat ketergantungan TIK masing-masing tergolong “strategis, tinggi dan tinggi”

Kata kunci : *Evaluasi, Keamanan Informasi, Indeks KAMI 4.2, ISO 27001*

Analysis Information Security Evaluation On Government Agency XYZ Using KAMI Index 4.2

Abstract

Government Agency XYZ is the implementer of regional autonomy which is led by an agency head, who is under the Governor and is responsible to the Governor through the Regional Secretary. In fulfilling the vision of Agency , IT activities, cultural activities, and various other activities. Evaluation activities need to be carried out to ensure that information security at XYZ Agency complies with applicable standards. Evaluations carried out using the KAMI 4.2 index at XYZ Agency can evaluate the maturity level of complete implementation of ISO 27001 and provide an overview of information security governance in an organization. In addition to the evaluation using the KAMI index, a review of the results of the KAMI 4.2 index evaluation against ISO 27001 will be carried out to find out what information security standards at XYZ Agency are in accordance with ISO 27001 and what standards are not appropriate and then recommendations must be given. From the results of research on Information Security Maturity Levels at XYZ Agency using the KAMI 4.2 index, it can be seen that for the electronic systems category the level of ICT dependency is classified as strategic, high and high, respectively.

Keywords: *Evaluation, Information Security, KAMI Index 4.2, ISO 27001*

1. PENDAHULUAN

Dewasa ini, dampak perkembangan teknologi informasi semakin nyata. Perkembangan ini mempengaruhi semua jenis bisnis dan organisasi. Sebagai hasil dari evolusi ini, semua bisnis dan

organisasi harus terus beradaptasi dengan teknologi informasi baru. Informasi diolah dan disimpan melalui teknologi yang terus berkembang. Nilai informasi paling besar ketika digunakan dalam proses pengambilan keputusan. Informasi didefinisikan sebagai data yang dapat diklasifikasikan atau

diinterpretasikan untuk digunakan dalam proses pengambilan keputusan. Manajemen informasi yang kuat akan meningkatkan kualitas, pendapatan, dan daya saing perusahaan.

Suatu lembaga atau usaha yang telah mengadopsi teknologi informasi yaitu Badan pemerintahan XYZ yang bertugas menyelenggarakan otonomi daerah dan dijalankan oleh seorang kepala Badan pemerintahan yang melapor kepada gubernur melalui sekretaris daerah. Melalui pemberdayaan Wilayah Selatan, pelaksanaan Reformasi Kalurahan, penanaman budaya inovatif, dan pemanfaatan teknologi informasi, Badan pemerintahan XYZ berharap dapat mewujudkan misinya. Layanan dalam website yang dapat mempermudah masyarakat untuk mengetahui kegiatan Gubernur, kegiatan IT, kegiatan budaya, dan beberapa kegiatan lainnya, merupakan salah satu perangkat teknologi informasi yang digunakan oleh Badan pemerintahan XYZ. Semua layanan dan peralatan TI yang digunakan oleh Badan pemerintahan XYZ ditempatkan di pusat data yang selalu diperbarui. Karena data di pusat data ini sangat penting dan berharga, peraturan tertentu harus diikuti untuk memastikan kerahasiaannya.

Informasi merupakan aset yang sangat penting, dan jika dikelola dengan baik akan meningkatkan kemampuan manajerial dan pelayanan publik pada Badan pemerintahan XYZ. Oleh karena itu, diperlukan suatu sistem keamanan informasi yang dapat menangani semua informasi agar tetap aman dan rahasia. Setiap penyelenggara sistem elektronik wajib menerapkan pengamanan informasi untuk kepentingan masyarakat umum, pelayanan publik, operasi pemerintahan yang efisien, atau pertahanan dan keamanan negara, sesuai dengan peraturan perundang-undangan Republik Indonesia Nomor 4 Tahun 2006 tentang sistem pengelolaan pengamanan informasi. (Kementerian Kominfo, 2016), Undang-undang ini memperjelas bahwa Menteri Komunikasi dan Informatika Republik Indonesia mewajibkan pengamanan informasi segera dilaksanakan. Kajian ISO 27001 sebagai acuan dan pengukuran atas kekurangan atau lubang keamanan informasi Badan pemerintahan XYZ diperlukan untuk menilai kesiapan sertifikasi sistem manajemen keamanan informasi.

Untuk menjamin keamanan informasi Badan pemerintahan XYZ sesuai dengan standar yang berlaku, maka harus dilakukan kegiatan evaluasi. Indeks KAMI digunakan untuk evaluasi pada Badan pemerintahan XYZ karena dapat menilai tingkat kematangan suatu organisasi, kelengkapan penerapan ISO 27001, dan tata kelola keamanan informasi di dalam perusahaan tersebut. Kajian hasil evaluasi indeks KAMI terhadap ISO 27001 akan dilakukan selain memanfaatkan indeks KAMI untuk menentukan standar keamanan informasi di Badan pemerintahan XYZ mana yang sesuai dengan ISO 27001 dan standar mana yang belum memadai serta memerlukan rekomendasi.

Berdasarkan permasalahan yang telah dijabarkan maka peneliti mengajukan penelitian dengan judul Analisis Evaluasi Keamanan Informasi pada Badan pemerintahan XYZ menggunakan Indeks KAMI 4.2. Dengan menggunakan judul tersebut peneliti bermaksud untuk mengevaluasi kewanamanan informasi pada Badan pemerintahan XYZ serta ditinjau berdasarkan ISO 27001.

2. TINJAUAN PUSTAKA

2.1. Tren Keamanan Data

Dalam laporan Cost of Data Breach Report 2023, Ponemon Institute menyatakan bahwa serangan ransomware tidak hanya mengenkripsi data, tetapi juga sering mengancam untuk mempublikasikan data sensitif sebagai "double extortion." Hal ini mendorong organisasi untuk meningkatkan kebijakan keamanan internal agar siap menghadapi serangan yang dapat merusak citra perusahaan dan berdampak pada biaya pemulihan data dan keamanan siber yang signifikan. (Anon., 2024)

Menurut laporan Top Cybersecurity Trends 2023 dari Gartner Research, perpindahan data ke cloud telah membawa risiko baru bagi perusahaan, terutama melalui kesalahan konfigurasi dan pencurian kredensial pengguna. Gartner mencatat banyak organisasi belum siap hadapi tantangan ini, dan mengalami kebocoran data. Oleh karena itu, langkah-langkah keamanan cloud seperti enkripsi end-to-end dan autentikasi multi-faktor penting. Arsitektur Zero Trust: Menurut model Zero Trust Maturity dari CISA, Zero Trust tidak percaya pengguna atau perangkat secara otomatis, baik dari dalam maupun luar jaringan. Model ini menyarankan autentikasi yang kuat dan validasi akses setiap kali pengguna atau perangkat mencoba mengakses sistem, bahkan jika mereka berada dalam jaringan perusahaan. CISA mengatakan bahwa cara ini penting untuk melawan ancaman dari orang dalam yang tidak terdeteksi oleh metode keamanan biasa. (Anon., n.d.)

Menurut laporan Internet Security Threat Report 2023 dari Symantec, perangkat IoT rentan terhadap serangan karena kelemahan keamanan seperti kurangnya autentikasi yang kuat dan enkripsi yang memadai. Laporan tersebut menyatakan bahwa perangkat IoT yang tidak aman dapat memberikan akses kepada penjahat siber ke jaringan perusahaan melalui perangkat yang tidak dilindungi. Hal ini dapat digunakan sebagai pintu gerbang untuk serangan lebih besar. (Rafy and Rafy, 2024)

Indeks Keamanan dan Ketahanan Informasi (KAMI) telah dikembangkan oleh Kementerian Komunikasi dan Informatika Republik Indonesia sebagai alat pengukuran untuk menilai kesiapan keamanan informasi. Indeks ini menilai banyak hal seperti kebijakan keamanan, pengelolaan SDM, infrastruktur teknologi, manajemen risiko, dan kesiapan menghadapi krisis. Menurut laporan Indeks KAMI tahun 2022, indeks tersebut dapat membantu

organisasi melihat kelemahan dalam sistem keamanan informasi mereka dan membuat rencana perbaikan untuk menghadapi ancaman yang mungkin terjadi. Perbandingan tren keamanan terbaru dengan Indeks KAMI menunjukkan bahwa indeks tersebut merupakan panduan dasar untuk mencapai kesiapan keamanan informasi. Namun, untuk melawan ancaman yang terus berkembang, organisasi perlu mengintegrasikan tren keamanan terkini seperti keamanan IoT, teknologi deteksi ancaman berbasis AI, dan pendekatan Zero Trust secara lebih mendalam. Integrasi ini bisa dilakukan dengan menambahkan parameter khusus yang sesuai dengan perkembangan teknologi, seperti sistem deteksi berbasis AI atau panduan spesifik untuk melindungi perangkat IoT dalam kerangka kerja Indeks KAMI. (Anon., n.d.)

Dalam 2023 Internet Security Threat Report, Symantec mengungkapkan bahwa perangkat IoT rentan terhadap serangan karena lemahnya keamanan yang melekat pada perangkat ini, seperti kurangnya autentikasi yang kuat dan enkripsi yang memadai. Laporan tersebut menekankan bahwa perangkat IoT yang tidak aman membuka jalan bagi penjahat siber untuk mengakses jaringan perusahaan melalui perangkat yang tidak dilindungi, yang dapat dimanfaatkan sebagai titik masuk dalam serangan yang lebih besar.

Peneliti (Prasetyowati et al., 2019) melakukan penelitian tentang “Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Politeknik Ilmu Pelayaran Semarang” dengan tujuan melakukan evaluasi terhadap tingkat keamanan informasi yang terdapat di PIP menggunakan metode wawancara yang menghasilkan sistem elektronik dengan score 20, tingkat kelengkapan informasi sebesar 238.

Peneliti (Thoyyibah, 2018) melakukan penelitian tentang “Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Pusat Informasi dan Pangkalan Data Perguruan Tinggi X” dengan tujuan seberapa baik tingkat keamanan informasi yang ada menggunakan metode Kuesioner yang menghasilkan keamanan sistem informasi pada sistem akademik PT. X berada pada tingkatan “cukup” dengan jumlah score 577.

Peneliti (Husin, Wowor and Karouw, 2017) melakukan penelitian tentang “Implementasi Indeks KAMI di Universitas Sam Ratulangi” dengan tujuan untuk mendapatkan gambaran kondisi kesiapan dan kematangan keamanan informasi menggunakan metode Kuesioner yang menghasilkan score akhir Indeks KAMI di Universitas Sam Ratulangi adalah 191 dari 588 skor maksimum 32.48% dengan skor ini universitas Sam Ratulangi tergolong tidak cukup untuk mencapai standar keamanan yang baik.

Peneliti (Kornelia and Irawan, 2021) melakukan penelitian tentang “Analisis Keamanan Informasi Menggunakan Tools Indeks KAMI” dengan tujuan untuk memastikan kesiapan / kematangan keamanan

informasi di Universitas Bina Darma menggunakan metode Wawancara yang menghasilkan tingkat kelengkapan dan kematangan keamanan informasi di Universitas Bina Darma saat ini masih ada dalam posisi TK II+ atau telah mencapai tingkat kematangan III dimana masih berstatus “Cukup Baik” untuk melaksanakan sertifikasi ISO/IEC 27001:2013.

Peneliti (Ferdiansyah, Subektiningsih and Indrayani, 2019) melakukan penelitian tentang “Evaluasi Tingkat Kesiapan Keamanan Informasi pada Lembaga Pendidikan Menggunakan Indeks KAMI 4.0” dengan tujuan mendapatkan informasi terkait tingkat kematangan dan kesiapan keamanan informasi menggunakan metode observasi yang menghasilkan kebutuhan sistem elektronik sebesar 20, sedangkan tingkat kelengkapan informasi mendapatkan skor 245 yang artinya tingkat keamanan informasi masih sangat rendah dan diperlukan perbaikan pada sistem keamanan informasi.

Peneliti (Puspita and Artina, 2017) melakukan penelitian tentang “Analisis Pengendalian Internal terhadap Sistem Informasi Akuntansi Persediaan pada PT Sriwijaya Baja Sakti” dengan tujuan menganalisis prosedur sistem informasi akuntansi dan pelaksanaan pengendalian internal pada perusahaan serta merancang usulan dan menerapkan sistem informasi akuntansi yang baik untuk perusahaan menggunakan metode Fifo (First-In First-Out) yang menghasilkan sistem informasi akuntansi masih memiliki kelemahan dalam prosedurnya yaitu adanya selisih antara pencatatan persediaan dengan stok fisik persediaan yang berada di Gudang.

Peneliti (Imtikhan Azmi et al., 2024) melakukan penelitian tentang “Evaluasi Tingkat Kesiapan Keamanan Informasi Pada SMK XYZ Menggunakan Indeks KAMI Versi 4.2” untuk melakukan evaluasi penyelenggaraan layanan TI menggunakan Indeks KAMI pada SMK XYZ agar mengetahui gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi yang ada di SMK XYZ kemudian dapat menjadi perhatian bagi penyelenggara TI yang ada agar memperbaiki dan meningkatkan keamanan informasi pada area-area yang telah dievaluasi sesuai dengan standar ISO/IEC 27001:2013. Menggunakan metode wawancara dan observasi menghasilkan skor Kategori SE 14 yang masuk ke dalam Kategori SE Rendah

Peneliti (Hafizuddin and Sugiantoro, 2024) melakukan penelitian tentang “Evaluasi Keamanan Sistem Informasi Pada Penyedia Layanan Cloud Dan Perlindungan Data Pribadi Berdasarkan Index Kami Versi 4.2 (Studi Kasus : PTIPD UIN Sunan Kalijaga Yogyakarta)” dengan tujuan menghasilkan sebuah rekomendasi terkait dengan pengamanan informasi terkait keterlibatan pihak eksternal penyedia layanan cloud dan perlindungan data pribadi pengguna. Menggunakan metode penelitian kualitatif menghasilkan pengamanan keterlibatan pihak ketiga mendapatkan presentase 49%, pengamanan

layanan infrastruktur awan (cloud) sebesar 33% dan untuk pengamanan perlindungan data pribadi mendapatkan presentase 67%. Hal ini menunjukkan bahwa Pusat teknologi informasi dan pangkalan data (PTIPD) UIN Sunan Kalijaga masih memiliki banyak kekurangan dan perlu adanya perbaikan dan mitigasi risiko keamanan informasi.

Peneliti (Anis et al., n.d.) melakukan penelitian tentang “Analisis Keamanan Sistem Informasi Perguruan Tinggi Berbasis Indeks KAMI” dengan tujuan mengevaluasi kesiapan keamanan teknologi informasi pada kedua Perguruan Tinggi serta memberikan kritik dan saran terhadap Perguruan Tinggi dari hasil kuesioner menggunakan metode penelitian survei yang menghasilkan 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.

3. METODOLOGI

Pada penelitian ini kami menggunakan metodologi yang bersifat kualitatif deskriptif dimana pada penelitian ini diharapkan bisa mendapatkan hasil evaluasi terkait tingkat kematangan di Badan pemerintahan XYZ dalam menjalankan sistem keamanan informasi yang ada.

Indeks KAMI adalah alat yang sesuai dan bermanfaat untuk meningkatkan keamanan dalam e-government Indonesia. Ini mencakup aspek kebijakan, sumber daya manusia, dan ketahanan operasional. Namun, agar Indeks KAMI lebih tepat dan efektif, perlu ditambahkan kontrol teknis dan strategi deteksi ancaman dengan teknologi digital terbaru. Pembaharuan ini akan mendukung e-government dalam memberikan layanan digital yang aman, andal, dan sesuai dengan standar keamanan global.

Tabel 1 menjabarkan perbedaan penggunaan indeks KAMI dengan beberapa standar framework keamanan lainnya yang digunakan secara internasional.

Tabel 1 Studi Komparasi Framework Keamanan

Aspek	Indeks KAMI	NIST CSF	ISO/IEC 27001	CIS Controls
Cakupan Geografis	Indonesia	Internasional, banyak digunakan di AS	Internasional	Internasional
Tujuan	Kesiapan dan ketahanan organisasi terhadap ancaman	Siklus hidup keamanan siber	Sistem manajemen keamanan informasi	Kontrol teknis yang mudah diimplementasikan
Pendekatan	Berbasis kebijakan dan sumber daya manusia	Berbasis siklus ancaman	Berbasis manajemen risiko	Berbasis kontrol teknis
Area Fokus	Kebijakan, SDM, teknologi, proteksi,	Identifikasi, proteksi,	Keamanan informasi melalui	Perlindungan

Aspek	Indeks KAMI	NIST CSF	ISO/IEC 27001	CIS Controls
	manajemen risiko	deteksi, respon, pemulihan	manajemen terstruktur	infrastruktur teknis
Standar Kepatuhan	Belum sertifikasi	Belum sertifikasi	Sertifikasi formal (ISMS)	Tidak bersertifikasi
Pemakaian Umum	Organisasi Indonesia	Organisasi dengan kebutuhan keamanan kritis	Berbagai industri yang ingin sertifikasi keamanan	Tim IT, organisasi kecil hingga besar

4. PEMBAHASAN

4.1 Tingkat Kematangan Sistem Elektronik

Pada tingkat ini peneliti memberikan hasil analisis data pada setiap kategori berdasarkan indeks KAMI 4.2 untuk hasil evaluasi tingkat kematangan keamanan teknologi informasi Badan pemerintahan XYZ dalam kategori sistem elektronik. Adapun analisis data yang dilakukan yaitu dengan cara mengumpulkan hasil skor dari setiap Badan pemerintahan yang menjadi responden penelitian, lalu dilakukan rekapitulasi data hasil penilaian kuesioner menggunakan indeks KAMI 4.2 lalu peneliti melakukan analisis data dengan cara mencari skor nilai rata-rata dari setiap Badan pemerintahan yang menjadi responden penelitian. Adapun status klasifikasi penilaian skor yang dilakukan mengacu pada standarisasi nilai yang sudah ada dalam tools indeks KAMI 4.2. Adapun klasifikasi status skor pada kategori sistem elektronik dapat dicermati pada gambar 1.

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

Gambar 1 Klasifikasi Skor Indeks KAMI 4.2

Hasil rekapitulasi data skor penilaian indeks KAMI 4.2 ditunjukkan pada tabel 2.

Tabel 2. Analisis Data Kategori Sistem Elektronik

No	Nama Badan pemerintahan	Quisisioner	Klasifikasi jawaban			Skor Akhir	Satuan Kasifikasi KAMI
			A	B	C		
1	X	10	7	3	0	41	Strategis
2	Y	10	4	3	3	29	Tinggi
3	Z	10	2	4	4	22	Tinggi
Hasil Nilai Rata-rata						30	

4.2 Tingkat Kematangan Tata Kelola

Pada kategori ini, peneliti memberikan hasil analisis evaluasi tingkat kematangan keamanan teknologi informasi Badan pemerintahan XYZ untuk kategori tata kelola keamanan informasi. Adapun hasil rekapitulasi data skor penilaian indeks KAMI 4.2 kategori tata kelola keamanan informasi diperlihatkan pada table 3:

Tabel 3 Analisis Data Kategori Pengelolaan Resiko

N o	Nama Badan pemerintahan	Quisio n	Nilai	Klasifikasi Tingkat Kematangan	Satuan Kasifikas i KAMI
1	X	22	120	III+	3,5
2	Y	22	120	III+	3,5
3	Z	22	120	I+	1,5
Hasil Nilai Rata-rata				II	2

4.3 Tingkat Kematangan Pengelolaan Resiko

Pada kategori ini, peneliti memberikan hasil analisis evaluasi pada kategori tingkat kematangan pengelolaan resiko keamaan informasi pada Badan pemerintahan XYZ. Adapun hasil rekapitulasi data skor penilaian indeks KAMI 4.2 untuk kategori pengelolaan resiko keamanan informasi ditunjukkan pada tabel 4:

Tabel 4 Analisis Data Kategori Pengelolaan Resiko

N o	Nama Badan pemerintahan	Quisio n	Nilai	Klasifikasi Tingkat Kematangan	Satuan Kasifikas i KAMI
1	X	16	64	III+	3,5
2	Y	16	64	III+	3,5
3	Z	16	0	I+	1,5
Hasil Nilai Rata-rata				II	2

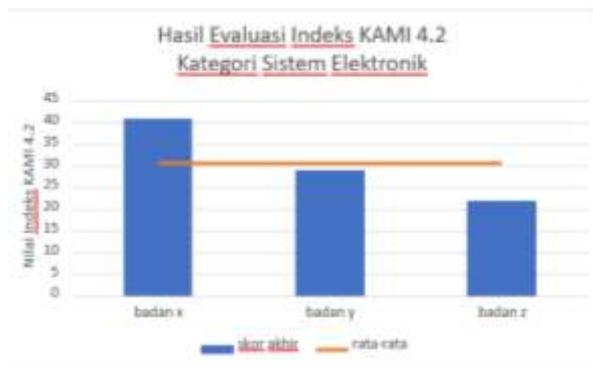
4.4 Tingkat Kematangan Kerangka Kerja

Pada kategori ini peneliti memberikan hasil evaluasi pada kategori tingkat kematangan kerangka kerja keamanan informasi pada Badan pemerintahan XYZ berdasarkan kategori yang ada pada standar indeks KAMI 4.2. Adapun hasil rekapitulasi data skor menggunakan tools penilaian indeks KAMI 4.2 pada kategori kerangka kerja keamanan informasi guna memperoleh hasil nilai rata-rata Badan pemerintahan XYZ sebagai responden penelitian, hasil rekapitulasi data ditunjukkan pada tabel 5:

Tabel .5 Analisis Data Kategori Kerangka Kerja

N o	Nama Badan pemerintahan	Quisio n	Nilai	Klasifikasi Tingkat Kematangan	Satuan Kasifikas i KAMI
1	X	29	155	V	5
2	Y	29	143	III+	3,5
3	Z	29	6	I+	1,5
Hasil Nilai Rata-rata				II	2

4.5 Rata-rata Kategori Sistem Elektronik



Gambar 2 Grafik Rata-rata Sistem Elektronik

Analisis data yang diperoleh menunjukkan bahwa sistem elektronik pada Badan pemerintahan XYZ memiliki status tingkat kematangan tinggi, hal ini dibuktikan dengan nilai rata-rata yang didapatkan oleh setiap Badan pemerintahan yang menjadi responden penelitian berada pada skor 30 seperti yang terlihat pada gambar 2. Oleh karena itu sistem elektronik Badan pemerintahan XYZ perlu dilakukan perbaikan oleh pengelolan dan bisa menjadi pertimbangan bagi pihak terkait seperti pemerintah agar dapat memberikan kebijakan yang dapat mendukung dan membantu perbaikan sistem elektronik.

4.6 Nilai Rata-rata Kategori Tata Kelola



Gambar 3. Nilai Rata-rata kategori Tata Kelola

Analisis data yang diperoleh menunjukkan bahwa nilai rata-rata tata kelola keamanan informasi pada Badan pemerintahan XYZ memiliki status tingkat kematangan II yang artinya masih berada pada tahapan penerapan kerangka kerja dasar seperti yang terlihat pada gambar 3. Oleh karena itu tata kelola keamanan informasi pada Badan pemerintahan XYZ perlu dilakukannya evaluasi perbaikan dan peningkatan status tata kelola keamanan informasi oleh pengelola.

4.7 Nilai Rata-rata Pengelolaan Resiko



Gambar 4 Nilai Rata-rata Pengelolaan Resiko

Analisis data yang diperoleh menunjukkan bahwa nilai rata-rata kategori pengelolaan resiko keamanan informasi Badan pemerintahan XYZ memiliki status tingkat kematangan I+ yang artinya masih pada kondisi awal seperti yang terlihat pada gambar 4. Oleh karena itu pengelolaan resiko keamanan informasi harus segera diberlakukan evaluasi dan peningkatan status dalam kategori pengelolaan resiko keamanan informasi oleh pengelola dan pihak pemerintah untuk mendukung serta membantu jalannya perbaikan dalam pengelolaan resiko keamanan informasi di Badan pemerintahan XYZ.

4.8 Tingkat Kematangan Kerangka Kerja



Gambar 5 Grafik Nilai Rata-rata Kerangka Kerja

Analisis data yang diperoleh menunjukkan bahwa nilai rata-rata pada kategori kerangka kerja keamanan informasi Badan pemerintahan XYZ memiliki status tingkat kematangan II yang artinya masih berada pada tahap penerapan kerangka kerja dasar seperti yang terlihat pada gambar 5. Oleh sebab itu kerangka kerja keamanan informasi perlu dilakukan evaluasi dan peningkatan status dalam kategori kerangka kerja keamanan informasi oleh pengelola Badan pemerintahan XYZ.

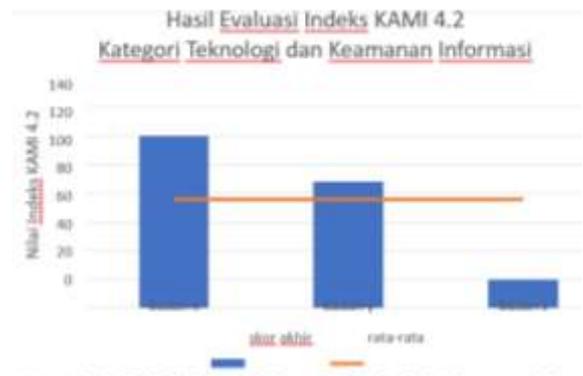
4.9 Tingkat Kematangan Pengelolaan Aset



Gambar 6 Grafik Nilai Rata-rata Kategori Pengelolaan Aset

Analisis data yang diperoleh menunjukkan bahwa nilai rata-rata pada kategori pengelolaan aset keamanan informasi pada Badan pemerintahan XYZ memiliki status tingkat kematangan II yang artinya masih berada pada tahap penerapan kerangka kerja dasar seperti yang terlihat pada gambar 6. Oleh sebab itu pengelolaan aset keamanan informasi harus segera dilakukan evaluasi serta peningkatan status dalam kategori pengelolaan aset keamanan informasi oleh pengelola Badan pemerintahan XYZ.

4.10 Tingkat Kematangan Teknologi dan Keamanan Informasi



Gambar 7
Nilai Rata-rata Kategori Teknologi dan Keamanan Informasi

Analisis data yang diperoleh menunjukkan bahwa nilai rata-rata pada kategori teknologi dan keamanan informasi Badan pemerintahan XYZ memiliki status tingkat kematangan II yang artinya masih berada pada tahap penerapan kerangka kerja dasar seperti yang terlihat pada gambar 7. Oleh sebab itu pengelolaan teknologi dan keamanan informasi harus dilakukan evaluasi dan peningkatan status kematangan dalam kategori ini oleh pengelola Badan pemerintahan XYZ.

4.11 Tingkat Kematangan Suplemen



Gambar 8 Grafik Rata-rata Area Pengamanan Pihak Ketiga

Pesatnya teknologi yang saat ini berkembang dan pola bisnis yang dinamis menyebabkan timbulnya resiko keamanan informasi baru. Keterlibatan pihak ketiga layanan Badan pemerintahan XYZ menimbulkan resiko terkait keberadaan pihak eksternal tersebut seperti yang terlihat pada gambar 8. Analisis nilai presentase rata-rata yang diperoleh pada area pengamanan keterlibatan pihak ketiga sebesar 57%. Nilai persentase ini harus ditingkatkan secara berkala kedepannya agar nilai kesiapan pengamanan keterlibatan pihak ketiga berdasarkan indeks KAMI 4.2 mampu dievaluasi secara berkelanjutan guna terciptanya jaminan keamanan informasi pada Badan pemerintahan XYZ.

4.12 Nilai Rata-rata Hasil Evaluasi Akhir

Adapun grafik nilai rata-rata skor untuk hasil evaluasi akhir dapat di saksikan pada gambar 4.12 berikut:



Gambar 9 Nilai Rata-rata Hasil Evaluasi Akhir

Analisis data yang diperoleh menunjukkan bahwa nilai rata-rata skor evaluasi akhir tingkat kematangan teknologi keamanan informasi pada Badan pemerintahan XYZ memiliki status kesiapan pada level Cukup Baik dengan nilai rata-rata sebesar 426 seperti yang terlihat pada gambar 9.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

1. Nilai kelengkapan tingkat keamanan informasi yang diperoleh di Badan pemerintahan XYZ berada pada Tingkat Kelengkapan Penerapan Standar masing-masing dengan nilai sebesar “626, 531, dan

122” mendapatkan predikat masing masing “Baik, Cukup Baik, dan Tidak Layak”.

2. Hasil evaluasi tingkat kelengkapan dan kematangan keamanan informasi pada Badan pemerintahan XYZ berdasarkan indeks KAMI 4.2 dibagi menjadi 7 kategori diantaranya : kategori sistem elektronik dengan nilai rata-rata 30 yang berarti tinggi, kategori tata kelola dengan status rata-rata tingkat kematangan II, kategori pengelolaan resiko dengan status tingkat kematangan I+, kategori kerangka kerja dengan status rata-rata tingkat kematangan II, kategori pengelolaan aset dengan status rata-rata tingkat kematangan II, kategori teknologi dan keamanan informasi dengan status rata-rata tingkat kematangan II, sedangkan pada kategori suplemen dibagi menjadi 3 area diantaranya untuk area pengamanan pihak ketiga dengan nilai rata-rata sebesar 57%, pengamanan layanan infrastruktur awan sebesar 33%, dan perlindungan data pribadi sebesar 33%.
3. Dari hasil penelitian tentang Tingkat Kematangan Keamanan Informasi pada Badan pemerintahan XYZ menggunakan Indeks KAMI, dapat diketahui bahwa untuk kategori sistem elektronik tingkat ketergantungan TIK masing-masing tergolong “strategis, tinggi dan tinggi” perlu adanya peningkatan yang dilakukan pada Badan pemerintahan X kedepannya yaitu pada area suplemen khususnya bagian keamanan layanan infrastruktur cloud dan perlindungan data. Untuk Badan pemerintahan Y guna menaikkan level yang saat ini berada pada predikat cukup baik ke level baik yaitu perlu adanya peningkatan pada area pengelolaan resiko, pengelolaan aset dan teknologi keamanan informasi. Pada Badan pemerintahan Z hampir semua area masih dalam kategori rendah sehingga perlu ada nya perbaikan khususnya pada area tata kelola, pengelolaan resiko, kerangka kerja, pengelolaan aset dan suplemen agar kedepannya hasil evaluasi akhir meningkat ke level cukup baik.
4. Penerapan keamanan informasi pada Badan pemerintahan XYZ berdasarkan tingkat kelengkapan terbaik berada pada area Teknologi dan Keamanan Informasi, hal ini didukung dengan hasil evaluasi dari Tingkat kelengkapan area teknologi dan keamanan informasi yang mendapatkan nilai paling mendekati untuk memenuhi kepatuhan standar dari ISO27001, sedangkan area lainnya masih perlu perbaikan untuk memenuhi kerangka kerja dasar terutama pada area suplemen khususnya pengamanan keterlibatan pihak ketiga penyedia layanan.

5. Untuk penelitian yang akan datang evaluasi selanjutnya bisa menggunakan standarisasi lainnya selain Indeks KAMI, seperti COBIT5, TOGAF 9, ISO 15500 dan tools lainnya.

5.2 Saran

Berdasarkan kesimpulan diatas maka peneliti dapat memberikan saran - saran sebagai berikut pada Badan pemerintahan X perlu dibentuknya kesadaran baik pimpinan maupun staff terkait tingkat keamanan informasi dengan diberlakukannya kebijakan guna terlaksananya perlindungan data pribadi dan mengamankan layanan infrastruktur cloud. Untuk Badan pemerintahan Y perlu adanya peningkatan khususnya pada kajian resiko keamanan informasi selanjutnya pada Badan pemerintahan XYZ memperbaiki semua aspek terkait keamanan informasi sehingga terciptanya perlindungan serta lancarnya kinerja yang baik. Untuk evaluasi selanjutnya dapat menggunakan standarisasi lainnya seperti COBIT 5, ISO 15500, TOGAF 9, dan berbagai macam tools lainnya.

DAFTAR PUSTAKA

- Anis, F., Ningrum, S., Riwanto, Y., Yanuar, I., Pratiwi, R. and Fikri, M.A., n.d. JIP (Jurnal Informatika Polinema) ANALISIS KEAMANAN SISTEM INFORMASI PERGURUAN TINGGI BERBASIS INDEKS KAMI.
- Anon. 2024. *Highlights IBM Guardium*.
- Anon. n.d. <https://www.cisa.gov/zero-trust>.
- Anon. n.d. <https://www.komdigi.go.id/berita/pengumuman/detail/indeks-keamanan-informasi-kami>.
- Ferdiansyah, P., Subektiningsih, S. and Indrayani, R., 2019. Evaluasi Tingkat Kesiapan Keamanan Informasi Pada Lembaga Pendidikan Menggunakan Indeks Kami 4.0. *Mobile and Forensics*, 1(2), pp.53–62. <https://doi.org/10.12928/mf.v1i2.1001>.
- Hafizuddin, F.A. and Sugiantoro, B., 2024. *Evaluasi Keamanan Sistem Informasi Pada Penyedia Layanan Cloud Dan Perlindungan Data Pribadi Berdasarkan Index Kami Versi 4.2 (Studi Kasus : PTIPD UIN Sunan Kalijaga Yogyakarta)*.
- Husin, M.F., Wowor, Hans.F. and Karouw, S.D.S., 2017. Implementasi Indeks Kami Di Universitas Sam Ratulangi. *Jurnal Teknik Informatika*, 12(1).
- Intikhan Azmi, H., Tulus Akbar, M., Tasya Kumala Dewi, B., Sugiantoro, B., Studi Magister Informatika, P., Sains dan Teknologi, F. and Sunan Kalijaga, U., 2024. *Evaluasi Tingkat Kesiapan Keamanan Informasi Pada SMK XYZ Menggunakan Indeks KAMI Versi 4.2*.
- Kementerian Kominfo, 2016. *Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi*. [online] Available at: <https://jdih.kominfo.go.id/produk_hukum/view/id/532/t/peraturan+menteri+komunikasi+dan+informatika+nomor+4+tahun+2016+tanggal+11+april+2016>.
- Kornelia, A. and Irawan, D., 2021. Analisis Keamanan Informasi Menggunakan Tools Indeks Kami ISO 4.1. *Jurnal Pengembangan Sistem Informasi dan Informatika*, 2(2), pp.78–86. <https://doi.org/10.47747/jpsii.v2i2.548>.
- Prasetyowati, D.D., Gamayanto, I., Wibowo, S. and Suharnawi, S., 2019. Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Politeknik Ilmu Pelayaran Semarang. *JOINS (Journal of Information System)*, 4(1), pp.65–75. <https://doi.org/10.33633/joins.v4i1.2429>.
- Puspita, B. and Artina, N., 2017. Analisis Pengendalian Internal Terhadap Pada Pt Sriwijaya Baja Sakti. *Stmik Gi Mdp*, pp.1–16.
- Rafy, M.F. and Rafy, F., 2024. Artificial Intelligence in Cyber Security. [online] <https://doi.org/10.13140/RG.2.2.19552.66561>.
- Thoyyibah, T., 2018. Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) berdasarkan ISO 27001:2013 Pada Pusat Informasi dan Pangkalan Data Perguruan Tinggi X. *Jurnal CoreIT: Jurnal Hasil Penelitian Ilmu Komputer dan Teknologi Informasi*, 4(2), p.72. <https://doi.org/10.24014/coreit.v4i2.6292>.