EVALUASI SISTEM MANAJEMEN KEAMANAN INFORMASI BERDASARKAN PENILAIAN INDEKS KAMI v.4.2 PADA DINAS XYZ PROVINSI JAWA TENGAH

Arfan Bakhtiar*[1], Faizah Salsabila Hidayat[2]

[1,2]Departemen Teknik Industri, Fakultas Teknik, Universitas Diponegoro,
Jl. Prof. Soedarto, SH, Kampus Undip Tembalang, Semarang, Indonesia 50275

Abstrak

Revolusi industri dan digitalisasi membawa dampak negatif dengan munculnya kejahatan siber yang mengancam data dan informasi penting yang dimiliki oleh organisasi. Penting untuk menerapkan sistem manajemen keamanan informasi untuk melindungi data dan informasi yang dikelola. Penelitian ini bertujuan untuk mengukur level kesiapan dan kematangan sistem manajemen keamanan informasi yang diterapkan oleh Dinas XYZ Provinsi Jawa Tengah menggunakan alat evaluasi Indeks KAMI v.4.2. Penelitian mengadopsi metode penelitian deskriptif kuantitatif dan pengumpulan data penelitian dengan metode wawancara, observasi, dan dokumentasi. Hasil penelitian menunjukkan bahwa kategori Sistem Elektronik yang digunakan oleh instansi tergolong "Tinggi" dengan skor 26. Penilaian terhadap kesiapan area keamanan Tata Kelola Keamanan Informasi, Kerangka Kerja Keamanan Informasi, dan Pengelolaan Aset berada pada tingkat kematangan I+. Area Pengelolaan Risiko memperoleh tingkat kematangan II. Sementara area Teknologi dan Keamanan Informasi memperoleh tingkat kematangan I. Penilaian secara keseluruhan memperoleh total skor 225 yang tergolong dalam "Tidak Layak". Penilaian kesiapan pada area Suplemen diperoleh persentase 36% pada Pengamanan Keterlibatan Pihak Ketiga, 33% pada Pengamanan Layanan Infrastruktur Awan, dan 38% pada Perlindungan Data Pribadi. Tentunya diperlukan rekomendasi perbaikan untuk meningkatkan keamanan data.

Kata kunci*: Indeks KAMI; kejahatan siber; sistem elektronik; sistem manajemen keamanan informasi*

Abstract

The industrial revolution and digitalization have had a negative impact with the emergence of cybercrime that threatens important data and information owned by organizations. It is important to implement an information security management system to protect data and managed information. This study aims to measure the level of readiness and maturity of the information security management system implemented by Dinas XYZ of Central Java Province using the KAMI Index v.4.2 evaluation tool. The study adopts quantitative descriptive research methods and research data collection with interview, observation, and documentation methods. The results showed that the Electronic System category used by the agency was classified as "High" with a score of 26. Assessment of the security area readiness of Information Security Governance, Information Security Framework and Asset Management is at maturity level I+. The Risk Management area has achieved maturity level II. Meanwhile, the Information Technology and Security area obtained maturity level I. The overall assessment received a total score of 225 which was classified as "Not Feasible". The readiness assessment in the Supplement area obtained a percentage of 36% in Securing Third Party Involvement, 33% in Securing Cloud Infrastructure Services, and 38% in Personal Data Protection. Of course, recommendations for improvements are needed to increase data security.

Keywords*: Cybercrime; Indeks KAMI; electronic systems; Information Security Management System*

*Penulis Korespondensi.
E-mail: arfanbakhtiar@lecturer.undip.ac.id

1. Pendahuluan

Dorongan kuat pada teknologi jaringan komputer menyebabkan akses informasi semakin cepat dan seluruh pengguna dapat terhubung hingga belahan dunia dengan

sangat singkat (Juliharta et al., 2020). Perkembangan digitalisasi ini menyebabkan efek negatif berupa kemunculan kejahatan siber yang berupaya mengakses data dan informasi penting , sehingga diperlukan evaluasi terhadap keamanan informasi yang dapat memberikan gambaran kesiapan dari penerapan keamanan informasi yang diterapkan dan untuk mencapai tata kelola teknologi informasi yang semakin baik (Rochmadi & Pasa, 2021). Tata kelola teknologi informasi ini berfungsi mengatur dan memastikan bahwa penggunaan teknologi informasi sesuai dengan harapan organisasi. Tujuannya guna melindungi aset-aset berharga yang menjadi kepemilikan organisasi (Riswaya et al., 2020).

Keamanan informasi yaitu upaya perlindungan terhadap aset dari berbagai ancaman yang dapat menggangu kerahasiaan, keutuhan dan ketersediaan layanan data (Gala et al., 2020). Keamanan informasi tidak hanya sekedar menjaga kerahasiaan dari data dan informasi saja, melainkan juga menjaga kebutuhan dan ketersediaan informasi yang ada. Hal ini sesuai dengan tiga prinsip utama keamanan informasi yang disebut dengan unsur CIA, *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Avaibility* (ketersediaan). Akan tetapi, menurut (Mantra et al., 2020) keamanan informasi meluas sebagai pemeliharaan, integritas, kerahasiaan, ketersediaan, akuntabilitas, ketidakpatuhan, dan keandalan informasi. Mengingat dampak dari epidemi covid-19 sangat berpengaruh signifikan terhadap penggunaan teknologi informasi dan komputer untuk menunjang segala aktivitas. Selain itu, meningkatnya organisasi yang beroperasi dari jarak jauh membuat kerentanan data juga semakin meningkat, sehingga kompleksitas dari manajemen data semakin meningkat yang menuntut kepastian dari keamanan data tersebut (Alexei, 2021).

Tantangan berkelanjutan dari kompleksitas manajemen data dan kepastian keamanan data sudah terjawab melalui sertifikasi yang didasarkan pada standar keamanan informasi internasional yang berisi prosedur, metode, dan alat evaluasi yang mampu memastikan keamanan data. Regulasi dari kesiapan organisasi dalam mengimplementasikan keamanan informasi sudah diatur dalam Peraturan Menteri Komunikasi dan Informatika No. 4 tahun 2016 tentang Sistem Manajemen Keamanan Informasi, sedangkan untuk skala internasional diatur melalui penerbitan sertifikat ISO/IEC 27001 oleh *International Organization for Standardization (ISO)*. Standar ISO/IEC 27001 dirancang dan diterbitkan oleh *International Organization for Standardization (ISO)* dan *the International Electrotechnical Commission* (IEC) pada tahun 2005 dan merupakan evolusi dari BS7799 yang menetapkan persyaratan untuk menerapkan, memelihara, dan meningkatkan Sistem Manajemen Keamanan Informasi (Culot et al., 2021). Sertifikasi ISO/IEC 27001 memberikan kerangka manajemen praktik terbaik untuk menerapkan dan memelihara keamanan, sekaligus memberikan dasar untuk bekerja, baik untuk menunjukkan kepatuhan atau untuk sertifikasi eksternal terhadap standar (Sharma & Dash, 2012).

Dinas XYZ Provinsi Jawa Tengah merupakan salah satu instansi pemerintah yang memanfaatkan penggunaan Sistem Elektronik untuk menjalankan kewajiban pelayanan publik. Beberapa Sistem Elektronik berbasis web yang dikelola oleh instansi tersebut adalah Lakon-e Pandu, Web Dinas XYZ, SIAP JATENG, CJIP Investasi dan OSS. Secara tidak langsung dengan penggunaan Sistem Elektronik berbasis web tersebut instansi akan mengelola data dan informasi masyarakat baik yang bersifat publik ataupun non publik.

Sistem Elektronik yang digunakan oleh Dinas XYZ Provinsi Jawa Tengah untuk melaksanakan tugas pelayanan publik tergolong “Tinggi”. Berbagai ancaman dan risiko tentu saja akan mengikuti di setiap aktivitas elektroniknya. Hal ini karena semakin banyak informasi yang disimpan, dikelola, dan dikirimkan, maka semakin besar juga risiko terjadinya gangguan (Wijatmoko, 2020). Berdasarkan observasi awal dan wawancara singkat dengan staf di bagian sistem informasi diketahui bahwa beberapa permasalahan terkait penyelenggaraan Sistem Elektronik yang sudah terjadi diantaranya adalah terjadinya peretasan *website*, permasalahan *domain*, *server down*, permasalahan terkait API yang digunakan, pencurian dan modifikasi data secara ilegal. Permasalahan-permasalahan yang sudah terjadi tersebut tentu saja berdampak buruk dan merugikan, selain dari sisi keamanan data yang dikelola juga akan menghambat tugas pelayanan publik untuk masyarakat. Bagi Dinas XYZ Provinsi Jawa Tengah ancaman tersebut dapat berdampak pada kredibilatasnya sebagai instansi pemerintahan yang menangani masalah perizinan dan investasi. Sedangkan bagi masyarakat pengguna layanan yakni investor maupun pelaku usaha, permasalahan tersebut dapat berdampak terhambatnya pengurusan izin, kebocoran data yang mengakibatkan pemanfaatan tidak semestinya oleh oknum dan dimanfaatkan untuk penipuan serta pemerasan yang dapat berdampak finansial. Oleh sebab itu, untuk menjamin keamanan data dan informasi yang dikelola, sangat penting menerapkan Sistem Manajemen Keamanan Informasi yang sesuai dengan standar dan aturan yang berlaku.

Sesuai dengan Permen Kominfo RI No. 4 tahun 2016 Tentang Sistem Manajemen Pengamanan Informasi menyebutkan bahwa Penyelenggara Sistem Elektronik (PSE) dalam kategori strategis dan tinggi wajib memiliki sertifikat Sistem Manajemen Pengamanan Informasi dan wajib menerapkan standar SNI ISO/IEC 27001 yang berlaku secara mandiri terhadap Sistem Elektronik yang menjadi kepemilikan instansi bersangkutan. Kementerian Komunikasi dan Informatika bersama dengan Badan Siber dan Sandi Negara (BSSN) telah merancang alat evaluasi berupa Indeks Keamanan Informasi (Indeks

KAMI) yang dapat digunakan untuk mempersiapkan sertifikasi ISO/IEC 27001.

Indeks Keamanan Informasi (Indeks KAMI) merupakan media evaluasi yang dapat memberikan gambaran kondisi kesiapan dari manajemen keamanan informasi suatu organisasi, tetapi hasil penilaian tidak dapat dijadikan sebagai pedoman untuk menganalisis kelayakan dari bentuk pengamanan informasi yang diterapkan (Purwanto & Huda, 2019). Penggunaan alat evaluasi Indeks KAMI mampu menciptakan alur komunikasi antar pengelola keamanan informasi di sektor pemerintah, sehingga semua pihak yang terlibat dapat memperoleh *lesson learned* (Kementerian Komunikasi dan Informatika, 2017)

Beberapa penelitian yang telah mengadopsi Indeks Keamanan Informasi (Indeks KAMI) untuk mengkaji tingkat kesiapan keamanan informasi diantaranya yaitu penelitian (Wijatmoko, 2020) di Kantor Wilayah Kementerian Hukum dan HAM DIY. Hasilnya menunjukkan tingkat ketergantungan tinggi terhadap Sistem Elektronik dengan skor 32, dan skor total 314 dalam kategori Pemenuhan Kerangka Kerja Dasar. Penelitian (Riswaya et al., 2020) STMIK Mardira Indonesia menemukan hasil ketergantungan tinggi terhadap Sistem Elektronik dengan skor 21, tetapi tingkat kesiapan keamanan berada pada kategori tidak layak dengan total skor 117. Penelitian (Yunella et al., 2019) juga menemukan hasil yang sama bahwa Diskominfo Kota Malang dengan ketergantungan Sistem Elektronik yang tinggi (skor 21) tetapi tingkat kelengkapan masih belum layak (skor 246) dan tingkat kematangan berada di level 1+.

Berdasarkan penelitian-penelitian yang sebelumnya telah dilakukan, diketahui bahwa banyak organisasi dengan tingkat ketergantungan terhadap Sistem Elektronik yang tinggi belum melakukan pengamanan informasi dengak layak dan memadai. Penelitian ini bertujuan untuk mengetahui dan mengukur tingkat kesiapan sistem manajemen keamanan informasi yang dilakukan oleh Dinas XYZ Provinsi Jawa Tengah menggunkan Indeks KAMI v4.2 sebelum melakukan sertifikasi ISO/IEC 27001.

2. Metode Penelitian

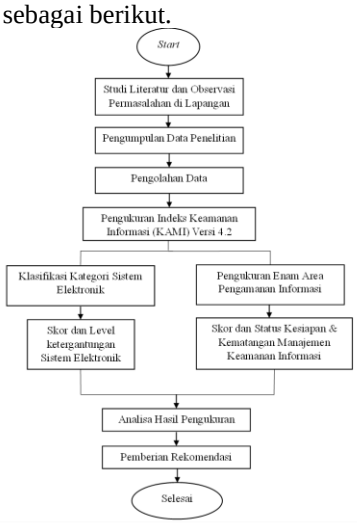
Penelitian mengadopsi pendekatan penelitian deskriptif kuantitatif mempertimbangkan bagaimana pendekatan ini tidak melihat, tidak berupaya menemukan, dan tidak membandingkan dua variabel untuk melihat sebab dan akibat dari suatu fenomena (Yusuf, 2017). Pendekatan kualitatif juga dilakukan guna menggali faktor penyebab buruknya sistem manajemen informasi yang diterapkan.

Responden penelitian terdiri dari dua orang dengan latar belakang pekerjaan dari divisi Sub Koordinator Pengembangan Sistem Informasi yang bertanggung jawab atas keamanan informasi pada Sistem Elektronik di Dinas XYZ Provinsi Jawa Tengah.

Data penelitian dikumpulkan dengan menggunakan metode wawancara untuk mendapatkan informasi penerapan SMKI yang sudah dijalankan . Penlitian juga menggunakan kuesioner Indeks KAMI versi 4.2 sebagai *tools self assesment*. Sedangkan untuk memperoleh bukti dari penerapan SMKI yang telah dijalankan dilakukan menggunakan metode observasi lapangan dan dokumentasi.

Data yang telah dikumpulkan akan dilakukan validasi guna memastikan bahwa data penelitian yang terkumpul bersifat valid dan sesuai dengan keadaan di lapangan. Validasi diterapkan untuk jawaban kuesioner dengan penilaian "Dalam Penerapan/Diterapkan Sebagian" dan penilaian "Diterapkan Menyeluruh". Apabila kedua penilaian tersebut tidak disertai dengan bukti yang sesuai, maka penilaian akan turun menjadi "Dalam Perencanaan"(Khamil et al., 2022).

Adapun alur penelitian dari awal hingga tahap pemberian rekomendasi dan dinyatakan selesai digambarkan sebagai berikut.



Gambar 1. Diagram Alir Penelitian

Analisis data dilakukan melalui dua tahapan, yaitu tahap pengklasifikasian kategori Sistem Elektronik dan tahap pengukuran tingkat kesiapan SMKI pada enam area yang lainnya. Penggolongan kategori Sistem Elektronik dibedakan menjadi tiga kategori dengan rentang skor seperti pada Tabel 1. Kategori Sistem Elektronik:

Tabel 1. Kategori Sistem Elektronik

Kategori Sistem Elektronik	Skor
Rendah	10-15
Tinggi	16-34
Strategis	35-50

Penilaian tingkat kesiapan dan kelengkapan penerapan Sistem Manajemen Keamanan Informasi pada area Tata Kelola Keamanan Informasi hingga area

Teknologi dan Keamanan Informasi terbagi menjadi tiga tahap penerapan, yaitu:
Penerapan tahap 1: kerangka kerja dasar keamanan informasi
Penerapan tahap 2: efektivitas dan konsistensi dari penerapan keamanan informasi
Penerapan tahap 3: kemampuan meningkatkan kinerja keamanan informasi

Status penilaian pada area Tata Kelola Keamanan Informasi hingga area Suplemen terbagi menjadi empat kategori sebagai berikut:

Tabel 2. Skor Penerapan sesuai Kategori Pengamanan

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

Pertanyaan pada penerapan tahap 3 dapat diisi ketika pertanyaan pada penerapan tahap 1 dan 2 sudah terisi dengan minimal status "Diterapkan sebagian". Selain itu, penilaian terhadap area Suplemen dapat dilakukan apabila organisasi mengalami permasalahan terkait pengelolaan data pribadi, seperti akses ilegal dan sebagainya.

Sesudah semua area keamanan dinilai, *output* akhir yang diperoleh berupa total skor status kesiapan dengan rentang pada Tabel 3. Skor Akhir dan Status Kesiapan:

Tabel 3. Skor Akhir dan Status Kesiapan

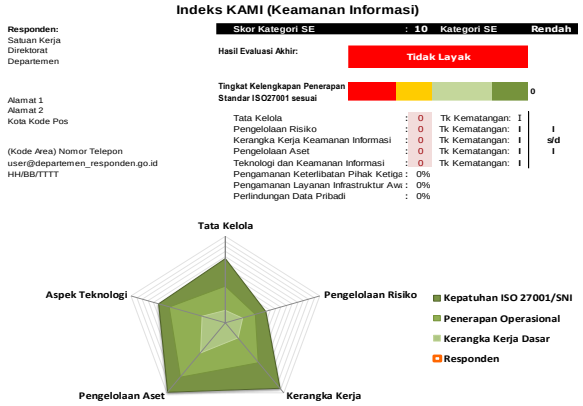
KATEGORI SISTEM ELEKTRONIK				
Rendah		**Skor Akhir**		**Status Kesiapan**
10	15	0	174	Tidak Layak
		175	312	Perlu Perbaikan
		313	535	Cukup
		536	645	Baik
Tinggi		**Skor Akhir**		**Status Kesiapan**
16	34	0	272	Tidak Layak
		273	455	Perlu Perbaikan
		456	583	Cukup
		584	645	Baik
Strategis		**Skor Akhir**		**Status Kesiapan**
35	50	0	333	Tidak Layak
		334	535	Perlu Perbaikan
		536	609	Cukup
		610	645	Baik

Penilaian terhadap tingkat kematangan penerapan Sistem Manajemen Keamanan Informasi dikelompokkan sesuatu aturan *the Control Objectives for Information and related Technology* (COBIT) pada Tabel 4. Tingkat Kematangan SMKI:

Tabel 4. Tingkat Kematangan SMKI

Tingkat	Keterangan
Tingkat I/I+	Kondisi Awal
Tingkat II/II+	Penerapan Kerangka Kerja Dasar
Tingkat III/III+	Terdefinisi dan Konsisten
Tingkat IV/VI+	Terkelola dan Terukur
Tingkat V	Optimal

Untuk padanan dengan standar ISO/IEC 27001, tingkat kematangan yang diharapkan untuk ambang batas minimum kesiapan sertifikasi adalah tingkat III+ (Kementerian Komunikasi dan Informatika, 2017).Semua *output* dari penilaian Indeks KAMI v 4.2 akan ditampilkan seperti Gambar 2. *Dashboard* Penilaian Indeks KAMI:



Gambar 2. *Dashboard* Penilaian Indeks KAMI

3. Hasil dan Pembahasan

A. Kategori Sistem Elektronik

Dinas XYZ Provinsi Jawa Tengah merupakan salah satu Penyelenggara Sistem Elektronik (PSE) yang ditujukan untuk kepentingan pelayanan publik dan sebagai Penyelenggara Sistem Elektronik (PSE), Dinas XYZ harus menerapkan manajemen pengamanan informasi berdasarkan asas risiko sesuai dengan peraturan Sistem Manajemen Keamanan Informasi (SMKI) yang berlaku.

Berdasarkan hasil penilaian diperoleh skor 26 berada di kategori "Tinggi". Hasil ini berarti instansi memiliki ketergantungan tinggi terhadap Sistem Elektronik. Sesuai dengan Permen Kominfo RI No.4 tahun 2016 tentang Sistem Manajemen Pengamanan Informasi Pasal 4 ayat (3) menyebutkan bahwa *"Sistem Elektronik Tinggi merupakan Sistem Elektronik yang berdampak terbatas pada kepentingan sektor dan/atau daerah tertentu"*, dan dan pasal 10 ayat (1) bahwa "*Penyelenggara Sistem*

Elektronik strategis dan Penyelenggara Sistem Elektronik tinggi wajib memiliki Sertifikat Sistem Manajemen Keamanan Informasi". Jadi, sebagai penyelenggara Sistem Elektronik tinggi, Dinas XYZ wajib menerapkan standar SNI ISO/IEC 27001 untuk dapat melaksanakan sertifikasi SMKI.

B. Tata Kelola Keamanan Informasi

Tata kelola keamanan informasi berhubungan dengan prosedur untuk memastikan penggunaan teknologi informasi sesuai dengan tujuan organisasi (Riswaya et al., 2020). Organisasi yang menggunakan teknologi informasi harus menerapkan dan memperhatikan dengan serius.

Penilaian terhadap tingkat kesiapan dan kematangan SMKI pada area Tata Kelola Keamanan Informasi ditujukan guna mengevaluasi bentuk tata kelola keamanan informasi beserta fungsi, tugas, dan tanggung jawab pengelola keamanan informasi. Penilaian pada area ini dilakukan dengan 22 pertanyaan yang terbagi menjadi 3 tahap penerapan. Berdasarkan hasil penilaian, keamanan informasi pada area Tata Kelola Keamanan Informasi yang telah diimplementasikan oleh Dinas XYZ Provinsi Jawa Tengah berada pada tahap 1 dan 2. Hal ini disebabkan karena total skor penerapan tahap 1 dan 2 kurang dari batas skor minimal tahap penerapan 3, sehingga penerapan keamanan informasi pada area Tata Kelola Keamanan Informasi masih belum mengupayakan tindakan peningkatan keamanan informasi. Skor penerapan tahap 1, 2 dan 3 diperoleh skor 43.

Penilaian tingkat kematangan area Tata Kelola Keamanan Informasi diperoleh skor tingkat kematangan II sebesar 33, sedangkan ditetapkan skor minimum tingkat kematangan II adalah 12 dan skor pencapaian tingkat kematangan II 36. Hal ini berarti skor tingkat kematangan II kurang dari skor pencapaian tingkat kematangan II, sehingga diperoleh level kematangan I+ dengan skor ambang batas 43,2 (80% dari total skor kematangan II). Untuk naik di tingkat kematangan III, maka harus memperoleh validitas tingkat kematangan II "Yes" dan skor kematangan II lebih dari skor ambang batas kematangan II. Berdasarkan analisa, skor kematangan tingkat II kurang dari skor ambang batas kematangan tingkat II, sehingga diperoleh validitas "No" untuk kematangan III dan level kematangan tetap berada pada level I+.

Terdapat beberapa kendala yang dialami sehingga banyak syarat yang tidak dapat dipenuhi seperti instansi sulit mengintegrasikan persyaratan keamanan informasi karena masih menggunakan kerangka kerja lama yang sudah digunakan sejak dahulu sehingga diperlukan perombakan, kemudian untuk koordinasi pengelolaan aset baik internal maupun eksternal belum memiliki panduan khusus dan hanya dilakukan seadanya, yang terakhir yakni belum adanya program khusus untuk mematuhi tujuan dan sasaran kepatuhan keamanan informasi.

C. Pengelolaan Risiko Keamanan

Penggunaan teknologi informasi yang semakin meningkat, sangat membutuhkan manajemen risiko keamanan informasi. Akan tetapi, masih banyak entitas yang belum memiliki acuan terkait aturan standar keamanan informasi yang harus diterapkan. Belum terpenuhinya syarat terkait aturan tersebut berdampak pada informasi menjadi tidak terjamin kerahasiaan, integritas, dan ketersediaannya (Sari et al., 2022). Manajemen risiko pada umumnya dimulai dari tahap analisis atau penilaian risiko, penyusunan tindakan mitigasi, dan tahap kontrol pelaksanaan dari strategi mitigasi yang direncanakan (Benyamin et al., 2023). Tujuannya adalah untuk mengetahui dampak dari risiko yang timbul apabila sistem keamanan informasi mengalami kegagalan. Prosedur manajemen risiko keamanan informasi sudah dirancang dalam ISO/IEC 27005 untuk membantu penerapan keamanan informasi dengan pendekatan manajemen risiko sekaligus mendukung konsep umum yang didefinisikan ISO/IEC 27001.

Penilaian terhadap tingkat kesiapan dan kematangan SMKI pada area Pengelolaan Risiko Keamanan Informasi ditujukan guna mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi informasi. Penilaian pada area ini dilakukan dengan 16 pertanyaan yang terbagi menjadi 3 tahap penerapan. Berdasarkan hasil penilaian, keamanan informasi pada area Pengelolaan Aset Informasi yang telah diimplementasikan oleh Dinas XYZ Provinsi Jawa Tengah berada pada tahap 1 dan 2. Hal ini disebabkan karena total skor penerapan tahap 1 dan 2 kurang dari batas skor minimal tahap penerapan 3, sehingga penerapan keamanan informasi pada area Pengelolaan Aset Informasi masih belum mengupayakan tindakan peningkatan keamanan informasi. Skor penerapan tahap 1 dan 2 diperoleh sebesar 34.

Penilaian tingkat kematangan area Tata Kelola Keamanan Informasi diperoleh skor tingkat kematangan II sebesar 20, sedangkan ditetapkan skor minimum tingkat kematangan II adalah 14 dan skor pencapaian tingkat kematangan II 20. Hal ini berarti skor tingkat kematangan II sama dengan skor pencapaian tingkat kematangan II, sehingga diperoleh level kematangan II dengan skor ambang batas 24 (80% dari total skor kematangan II). Untuk naik di tingkat kematangan III, maka harus memperoleh validitas tingkat kematangan II "Yes" dan skor kematangan II lebih dari skor ambang batas kematangan II. Berdasarkan analisa, skor kematangan tingkat II kurang dari skor ambang batas kematangan tingkat II, sehingga diperoleh validitas "No" untuk

kematangan III dan level kematangan tetap berada pada level II.

Terdapat beberapa kendala yang dialami sehingga banyak syarat yang tidak dapat dipenuhi seperti instansi belum secara spesifik mengindentifikasi ancaman dan kelemahan terkait aspek informasi sehingga dampaknya kurang dapat diidentifikasi, selain itu kerangka kerja pengelolaan risiko belum menjadi prioritas instansi.

D. Kerangka Kerja Keamanan Informasi

ISO/IEC 27001 merupakan kerangka kerja atau standar Sistem Manajemen Keamanan Informasi yang harus diterapkan oleh sebuah organisasi untuk mengelola risiko yang mengancam keamanan informasi. Standar yang disusun oleh *the International Electrotechnical Commission (IEC)* pada tahun 2005 ini menjamin bahwa semua informasi dengan berbagai bentuk bersifat aman, dan sistem manajemen keamanan informasi melindungi semua bentuk informasi yang diambil mulai dari pengangkutan, pemrosesan, hingga penyimpanan baik secara fisik maupun dalam bentuk *cloud* dengan tetap mempertimbangkan segi keamanannya (Alexei, 2021). Standar ISO/IEC 27001 berisi muatan persyaratan yang wajib dipenuhi dalam menerapkan konsep keamanan informasi oleh sebuah entitas atau organisasi. ISO/IEC 27001 ini berlaku dalam skala internasional, atau berlaku untuk semua entitas di seluruh dunia.

ISO/IEC 27001 adalah metode standarisasi keamanan informasi yang telah diakui oleh dunia dan memiliki kriteria keamanan (kontrol) yang telah disusun guna diterapkan oleh organisasi atau entitas lainnya dalam membangun sistem manajemen keamanan informasi yang andal (Yunella et al., 2019). Jadi, standar ISO/IEC 27001 dijadikan kerangka kerja yang praktis oleh sebuah organisasi termasuk instansi pemerintahan untuk membantu instansi meningkatkan keamanan informasi yang dimiliki.

Penilaian terhadap tingkat kesiapan dan kematangan SMKI pada area Pengelolaan Aset Informasi ditujukan guna mengevaluasi kelengkapan dan kesiapan kerangka kerja termasuk kebijakan dan prosedur pengelolaan keamanan dan strategi penerapannya. Penilaian pada area ini dilakukan dengan 29 pertanyaan yang terbagi menjadi 3 tahap penerapan. Berdasarkan hasil penilaian, keamanan informasi pada area Pengelolaan Aset Informasi yang telah diimplementasikan oleh Dinas XYZ Provinsi Jawa Tengah berada pada tahap 1 dan 2. Hal ini disebabkan karena total skor penerapan tahap 1 dan 2 kurang dari batas skor minimal tahap penerapan 3, sehingga penerapan keamanan informasi pada area Pengelolaan Aset Informasi masih belum mengupayakan tindakan peningkatan keamanan informasi. Skor penerapan tahap 1 dan 2 diperoleh sebesar 44.

Penilaian tingkat kematangan area Pengelolaan Aset Informasi diperoleh skor tingkat kematangan II sebesar 16, sedangkan ditetapkan skor minimum tingkat kematangan II adalah 15 dan skor pencapaian tingkat kematangan II 24. Hal ini berarti skor tingkat kematangan II kurang dari skor pencapaian, sehingga diperoleh level kematangan I+ dengan skor ambang batas 33,6 (80% dari total skor kematangan II). Untuk naik di tingkat kematangan III, maka harus memperoleh validitas tingkat kematangan II "Yes" dan skor kematangan II lebih dari skor ambang batas kematangan II. Berdasarkan analisa, skor kematangan tingkat II kurang dari skor ambang batas kematangan tingkat II, sehingga diperoleh validitas "No" untuk kematangan III dan level kematangan tetap berada pada level I+.

Terdapat beberapa kendala yang dialami sehingga banyak syarat yang tidak dapat dipenuhi seperti sulitnya mengomunikasikan kebijakan keamanan informasi yang mencakup pelaksanaan, mekanisme, jadwal, materi, dan sasaran ke dalam proses bisnis, selain itu pihak instansi belum melakukan kegiatan audit internal rutin untuk cakupan keseluruhan aset informasi sehingga belum memiliki rencana dan program peningkatan keamanan informasi.

E. Pengelolaan Aset Informasi

Aset informasi dapat berupa *software*, *hardware*, informasi, dan sumber daya manusia yang mengelola dan menjalankan aset informasi tersebut. Pentingnya aset informasi yang dimiliki oleh setiap instansi membutuhkan perlindungan dari risiko-risiko keamanan yang berasal dari dalam ataupun luar lingkungan instansi tersebut (Supradono, 2009). Keamanan informasi yang diimplementasikan terhadap aset informasi tidak hanya berpusat di teknologinya saja melainkan harus diikuti dengan peningkatan pemahaman sumber daya manusianya juga.

Penilaian terhadap tingkat kesiapan dan kematangan SMKI pada area Pengelolaan Aset Informasi ditujukan guna mengevaluasi kelengkapan dari pengamanan aset informasi yang dimiliki oleh organisasi, termasuk proses keseluruhan dari siklus penggunaan aset informasi. Penilaian pada area ini dilakukan dengan 38 pertanyaan yang terbagi menjadi 3 tahap penerapan. Berdasarkan hasil penilaian, keamanan informasi pada area Pengelolaan Aset Informasi yang telah diimplementasikan oleh Dinas XYZ Provinsi Jawa Tengah berada pada tahap 1 dan 2. Hal ini disebabkan karena total skor penerapan tahap 1 dan 2 kurang dari batas skor minimal tahap penerapan 3, sehingga penerapan keamanan informasi pada area Pengelolaan Aset Informasi masih belum

mengupayakan tindakan peningkatan keamanan informasi. Skor penerapan tahap 1 dan 2 diperoleh sebesar 51.

Penilaian tingkat kematangan area Pengelolaan Aset Informasi diperoleh skor tingkat kematangan II sebesar 41, sedangkan ditetapkan skor minimum tingkat kematangan II adalah 25 dan skor pencapaian tingkat kematangan II 62. Hal ini berarti skor tingkat kematangan II kurang dari skor pencapaian, sehingga diperoleh level kematangan I+ dengan skor ambang batas 84 (80% dari total skor kematangan II). Untuk naik di tingkat kematangan III, maka harus memperoleh validitas tingkat kematangan II "Yes" dan skor kematangan II lebih dari skor ambang batas kematangan II. Berdasarkan analisa, skor kematangan tingkat II kurang dari skor ambang batas kematangan tingkat II, sehingga diperoleh validitas "No" untuk kematangan III dan level kematangan tetap berada pada level I+.

Terdapat beberapa kendala yang dialami sehingga banyak syarat yang tidak dapat dipenuhi seperti dalam rencana kerjanya instansi belum memiliki peraturan-peraturan khusus mengenai penggunaan piranti, pengelolaan akses infromasi, maupun memikirkan izin tertulis dari pemilik data. Sehingga dalam instansi tersebut hanya menjalankan segala proses ala kadarnya. Instansi juga belum memiliki pengamanan fisik atas aset informasi dari gangguan listrik, bencana alam, maupun kebakaran karena dianggap bukan priotas dan tidak tercantum dalam anggaran pemeliharaan.

F. Teknologi dan Keamanan Informasi

Keamanan informasi merupakan usaha untuk melakukan perlindungan terhadap informasi dan sistem informasi dari akses, penggunaan, pengungkapan, pengoperasian, modifikasi, atau penghancuran oleh pihak-pihak luar yang tidak memiliki kewenangan atau pihak yang tidak bertanggungjawab (Nurul et al., 2022). Keamanan informasi berpengaruh terhadap keamanan sistem informasi, hal ini didasarkan atas indikator dari keamanan informasi yang mengupayakan keamanan pada aset informasi terhadap berbagai risiko dan ancaman yang muncul. Sedangkan teknologi informasi berpengaruh terhadap keamanan sistem informasi, karena ketika sebuah informasi dapat disalahgunakan oleh pihak yang tidak bertanggung jawab, maka informasi tersebut dianggap tidak akurat, sehingga tidak lagi memenuhi unsur kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) dalam menerapkan keamanan informasi.

Tujuan penilaian area Teknologi dan Keamanan Informasi guna mengevaluasi kelengkapan, konsistensi, dan efektivitas dari penggunaan teknologi dalam pengamanan aset informasi yang dimiliki oleh instansi terkait. Penilaian terhadap area Teknologi dan Keamanan Informasi diukur dengan 26 pertanyaan yang terbagi menjadi tiga tahap penerapan. Tingkat penerapan pada area ini pada tahap 1 dan 2, sebab pada tahap 3 dianggap tidak valid. Hal ini disebabkan karena total skor penerapan tahap 1 dan 2 kurang dari batas skor minimal tahap penerapan 3, sehingga penerapan keamanan informasi pada area Teknologi dan Keamanan Informasi masih belum mengupayakan tindakan peningkatan keamanan informasi. Skor penerapan tahap 1 dan 2 diperoleh sebesar 50.

Penilaian tingkat kematangan area Teknologi dan Keamanan informasi diperoleh skor tingkat kematangan II sebesar 16, sedangkan ditetapkan skor minimum 18 dan skor pencapaian 28. Hal ini berarti skor tingkat kematangan II kurang dari skor pencapaian, sehingga diperoleh level kematangan I+ dengan skor ambang batas 33,6 (80% dari total skor kematangan II). Untuk naik di tingkat kematangan III, maka harus memperoleh validitas tingkat kematangan II "Yes" dan skor kematangan II lebih dari skor ambang batas kematangan II. Berdasarkan analisa, skor kematangan tingkat II kurang dari skor ambang batas kematangan tingkat II, sehingga diperoleh validitas "No" untuk kematangan III dan level kematangan tetap berada pada level I+.

Terdapat beberapa kendala yang dialami sehingga banyak syarat yang tidak dapat dipenuhi seperti pengelola belum memiliki pemahaman yang cukup terkait proteksi dan juga enkripsi data untuk melindungi keamanannya, selain itu beberapa piranti yang digunakan juga tidak dimutakhirkan karena tidak termasuk dalam anggaran tahunan sehingga masih menggunakan versi lama.

G. Suplemen

Menurut (Kementerian Komunikasi dan Informatika, 2017) risiko terhadap sistem keamanan informasi salah satunya diakibatkan karena adanya keterlibatan dari pihak ketiga dalam rantai suplai layanan di suatu organisasi. Langkah penanggulangan tercepat, efisien, dan efektif harus terancang dengan baik sebagai bentuk mitigasi risiko yang dilakukan.

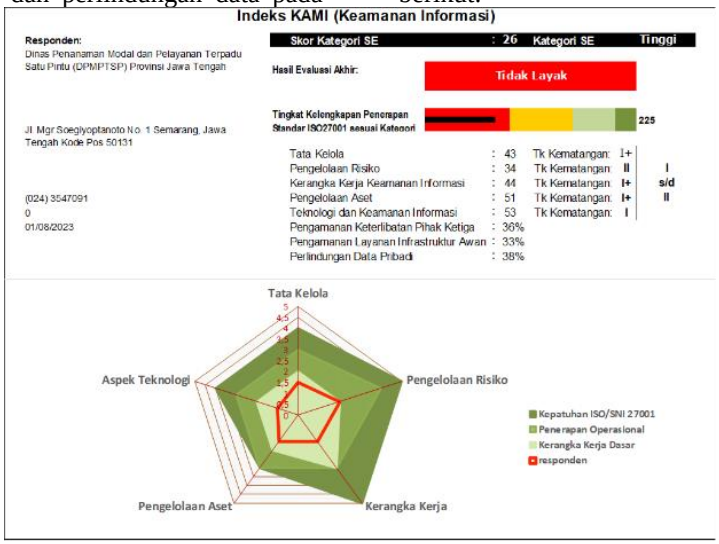
Pihak ketiga dalam rantai suplai layanan salah satunya menyediakan layanan infrastruktur awan karena layanan ini memiliki peluang efisiensi dan peningkatan signifikan terhadap kinerja instansi. Meskipun peluang itu sangat menjanjikan, risiko keamanan data juga harus dipikirkan karena data akan dikendalikan oleh penyelenggara layanan. Area Suplemen pada penilaian Indeks KAMI v.4.2 meliputi tiga area pengamanan, yaitu pengamanan keterlibatan pihak ketiga penyedia layanan, pengamanan layanan infrastruktur awan, dan perlindungan data pribadi. Aspek pengamanan keterlibatan pihak ketiga penyedia layanan yang terdiri dari (a) manajemen

risiko dan pengelolaan keamanan pihak ketiga, (b) pengelolaan sub-kontraktor/ alih daya pada pihak ketiga, (c) pengelolaan layanan dan keamanan pihak ketiga, (d) pengelolaan perubahan layanan dan kebijakan pihak ketiga, (e) penanganan aset, (f) pengelolaan insiden oleh pihak ketiga, dan (g) rencana kelangsungan layanan pihak ketiga.

Penilaian dilakukan dengan 53 pertanyaan dan hasil akhir dari evaluasi tingkat kesiapan dalam bentuk persentase (%) secara objektif. Hasil evaluasi tingkat kesiapan dari aspek suplemen disampaikan dalam bentuk persentase (%) secara objektif. Hasil penilaian menunjukkan bahwa pengamanan terhadap keterlibatan pihak ketiga penyedia layanan sudah diterapkan 36%, pengamanan terhadap layanan infrastruktur awan diterapkan 33%, dan pengamanan terhadap perlindungan data pribadi sudah diterapkan sebesar 38% dati total keseluruhan 100% untuk masing-masing aspek pengamanan. Persentase pengamanan pada area Suplemen masih jauh dari 100% dan dapat diartikan bahwa sistem pengamanan pada area ini masih sangat lemah, sehingga harus ditingkat agar instansi terkait tidak mudah terpapar risiko terhadap ketiga aspek pengaman ini dan untuk menjamin kerahasiaan dan perlindungan data pada pihak ketiga. Mengingat sudah beberapa kali terjadi peretasan data yang sifatnya sangat rentan, maka pengamanan pada Suplemen sangat penting untuk dilakukan agar ancaman tersebut tidak terjadi berulang.

Terdapat beberapa kendala yang dialami sehingga banyak syarat yang tidak dapat dipenuhi seperti dalam kaitan dengan pihak ketiga, instansi hanya melakukan perjanjian di awal dan tidak diperinci terkait persyaratan pengendalian akses, penghancuran informasi, maupun manajemen keamanan risiko. Untuk aspek pengamanan infrastruktur awan, instansi kesulitan mengevaluasi kelayakannya karena belum memiliki parameter, selain itu instansi belum meneukan layanan awan pengganti bila terjadi sesuatu. Kemudian untuk aspek perlindungan data pribadi instansi masih kesulitan mendokumentasikan terkait penyimpanan, pengolahan, dan pertukaran data pribadi.

Berdasarkan hasil penilaian tingkat kesiapan dan kematangan penerapan Sistem Manajemen Keamanan Informasi (SMKI) yang telah dilakukan, seluruh *output* dari penilaian digambarkan melalui *dashboard* penilaian berikut:



Gambar 4. Hasil Penilaian Indeks KAMI v.4.2

Total skor penilaian kesiapan dan kelengkapan penerapan Sistem Manajemen Keamanan Informasi (SMKI) diperoleh sebesar 225 dan dikategorikan dalam "Tidak Layak". Hal ini berarti sangat dibutuhkan pemenuhan kelengkapan segala persyaratan penerapan SMKI agar hasil penilaian semakin baik dan celah ancaman terhadap keamanan data dapat teratasi dengan baik.

Berdasarkan tingkat kematangan penerapan SMKI, dari area Tata Kelola Keamanan Informasi hingga area Teknologi dan Keamanan Informasi masih belum memenuhi standar ambang batas minimal level tingkat kesiapan sertifikasi ISO/IEC 27001.

H. Rekomendasi

Rekomendasi diberikan sebagai pertimbangan untuk langkah perbaikan dan peningkatan kesiapan, kelengkapan dan kematangan penerapan Sistem Manajemen Keamanan Informasi di Dinas XYZ Provinsi Jawa Tengah. Rekomendasi diberikan oleh pihak internal yang mewakili instansi dan pihak eksternal yang mewakili tenaga ahli SMKI. Beberapa rekomendasi yang diberikan diantaranya:

1) Meningkatkan perlindungan terhadap data pribadi yang bersifat sangat rahasia, dimulai dengan mengevaluasi kebutuhan perlindungan data pribadi, pengklasifikasian data sesuai tingkat kerahasiaan, penggunaan enkripsi data, menerapkan kontrol akses yang ketat, melakukan audit dan pemantauan secara berkala, meningkatkan pemahaman pentingnya perlindungan data melalui pelatihan, merancang tanggap darurat untuk menangani insiden keamanan, memastikan sistem dan perangkat lunak terbarui dengan *patch* terbaru, memanfaatkan penyimpanan fisik dan digital, melakukan kerja sama dengan vendor, menguji kelayakan sistem, meninjau dan memperbarui keamanan data, dan memantau kinerja sistem.
2) Mengintegrasikan persyaratan keamanan dalam seluruh aktivitas kerja dengan cara menetapkan kebijakan keamanan informasi, mengedukasi dan memberi pelatihan terhadap staf, membentuk tim keamanan informasi, melakukan penilaian risiko, menerapkan pengendalian akses, mengawasi aktivitas jaringan dan sistem, menerapkan prosedur penanganan insiden, memperbarui sistem dan perangkat lunak, mengaudit dan memantau kepatuhan, menyelaraskan kebijakan dan praktik keamanan dengan proses bisnis, menyiapkan rencana darurat pemulihan insiden keamanan, dan mengevaluasi secara berkala.
3) Memperbarui sistem perekrutan staf sesuai dengan kebutuhan yang dimulai dengan evaluasi dan merancang rencana kebutuhan SDM, merekrut personel dengan keahlian dan pengalaman yang relevan, memberikan pelatihan dan sertifikasi untuk staf, melakukan audit kompetensi internal, mempertimbangkan bekerja sama dengan mitra, menyediakan jalur pengembangan karir yang jelas untuk staf, menetapkan indikator kinerja (KPI) dan melakukan evaluasi rutin.
4) Merancang regulasi parameter pengukuran kinerja pengelolaan keamanan informasi melalui *Key Performance Indicators* (KPI) dan ambang batas tingkat risiko melalui *Key Risk Indicators* (KRI) yang diikuti dengan pengukuran secara teratur, evaluasi dan pemantauan, serta pembaruan
5) Menetapkan standarisasi efektivitas dan efisiensi dari mitigasi risiko yang dilakukan melalui *Key Performance Indicators* KPI) disertai dengan evaluasi berkala, pengembangan rencana mitigasi yang terinci, pemantauan dan pembaruan teratur.
6) Merancang pengembangan dan peningkatan keamanan informasi untuk jangka pendek, jangka menengah, dan jangka panjang sesuai dengan tujuan. Kemudian lakukan audit informasi, pembentukan tim, penyusunan dan prosedur keamanan informasi, penilaian risiko dan pemantauan teratur disertai bukti pelaporan.
7) Memperbaiki rancangan nota kesepakatan (MOU) dengan pihak ketiga agar lebih jelas dan terperinci, termasuk penilaian kepatuhan, komitmen manajemen, dan kinerja vendor.
8) Menetapkan pembatasan waktu akses Sistem Elektronik untuk pihak eksternal guna meminimalisir akses ilegal diikuti dengan penggunaan autentikasi multi faktor (MFA), penggunaan VPN, dan *firewall* yang kuat.
9) Merevisi perjanjian kerja dengan staf yang telah selesai kontrak terkait pemusnahan data dan informasi yang sudah tidak relevan. Jika dibutuhkan konsultasi dengan ahli hukum terkait perjanjian dan kebijakan privasi dan perlindungan data yang berlaku
10) Menyediakan layanan *cloud* cadangan untuk menggantikan *cloud* utama ketika mengalami kendala

4. Kesimpulan

Berdasarkan hasil penelitian ditemukan bahwa kategori sistem elektronik yang diselenggarakan oleh Dinas XYZ Provinsi Jawa Tengah tergolong "Tinggi" dengan skor 26. Sesuai regulasi yang berlaku, penyelenggara Sistem Elektronik strategis dan tinggi harus memiliki sertifikat Sistem Manajemen Keamanan Informasi (SMKI) dan menerapkan standar SNI ISO/IEC 27001. Penilaian terhadap tingkat kesiapan penerapan pada area Tata Kelola Keamanan Informasi diperoleh skor 43 dengan tingkat kematangan I+, area Pengelolaan Risiko Keamanan diperoleh skor 34 dengan tingkat kematangan II, area Kerangka Kerja Keamanan Informasi diperoleh skor 44 dengan tingkat kematangan I+, area Pengelolaan aset dengan skor 51 dan tingkat kematangan I+, dan area Teknologi dan Keamanan Informasi diperoleh skor 53 dengan kematangan I. Tingkat kematangan masing-masing area masih belum memenuhi batas ambang level kematangan minimum untuk kesiapan sertifikasi ISO/IEC 27001. Penilaian secara keseluruhan memperoleh total skor 225 yang tergolong dalam "Tidak Layak". Penilaian kesiapan pada area Suplemen diperoleh persentase 36% pada Pengamanan Keterlibatan Pihak Ketiga, 33% pada Pengamanan Layanan Infrastruktur Awan, dan 38% pada Perlindungan Data Pribadi. Tidak terpenuhinya persyaratan untuk melakukan sertifikasi ISO/IEC 27001 tentu saja akan berdampak pada risiko keamanan data yang dikelola, sehingga perbaikan harus segera dilakukan. Rekomendasi perbaikan dan langkah konkret untuk meningkatkan keamanan data sudah diberikan sesuai dengan celah ancaman yang ada.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada pihak-pihak yang sudah membantu terlaksananya penelitian ini dengan lancar.

Daftar Pustaka

Alexei, A. (2021). Ensuring Information Security In Public Organizations In The Republic Of Moldova Through The ISO 27001 Standard. *Journal of Social Sciences*, *IV*(1). https://doi.org/10.52326/jss.utm.2021.4(1).11

Benyamin, J., Mualim, M., & Duarte, E. P. (2023). Information Security Risk Management In Minimizing Cyber Threats At The Data Center And Communication Information Technology Of The National Cyber And Crypto Agency To Improve Cyber Defense And Security. *Jurnal Manajemen Pertahanan*, *9*(1), 40–54.

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. In *TQM Journal* (Vol. 33, Issue 7, pp. 76–105). Emerald Group Holdings Ltd. https://doi.org/10.1108/TQM-09-2020-0202

Gala, A. P. P., Sengkey, R., & Punusingon, C. (2020). Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI. *Jurnal Teknik Informatika*, *15*(3), 189–198.

Juliharta, I. G. P. K., Komang, T. W., & Astawa, N. L. P. N. S. P. (2020). Penilaian Keamanan Informasi E-Government Menggunakan Index Keamanan Informasi (KAMI) 4.0. *Jurnal Teknologi Informasi Dan Komputer*, *6*(2), 238–244. https://bssn.go.id/mengenali-serangan-siber-

Kementerian Komunikasi dan Informatika. (2017). *Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks Keamanan Informasi (Indeks KAMI)*. Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika.

Khamil, D. I., Sasmita, G. M. A., & Susila, A. A. N. H. (2022). Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Kami 4.2 Dan ISO/IEC 27001:2013 (Studi Kasus: Diskominfo Kabupaten Gianyar). *Jurnal Teknik Informatika Dan Sistem Informasi*, *9*(3), 1948–1960. http://jurnal.mdp.ac.id

Mantra, I., Rahman, A. A., & Saragih, H. (2020). Maturity Framework Analysis ISO 27001: 2013 on Indonesian Higher Education. *International Journal of Engineering & Technology*, *9*(2), 429–436. www.sciencepubco.com/index.php/IJET

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

Purwanto, F. H., & Huda, M. (2019). Pengukuran Tingkat Keamanan Informasi Perguruan Tinggi XYZ Menggunakan Indeks Keamanan Informasi (KAMI) Berbasis ISO/IEC 27001:2013. *Jurnal VOI (Voice of Informatics)*, *8*(2), 31–40.

Riswaya, A. R., Sasongko, A., & Maulana, A. (2020). Evaluasi Tata Kelola Keamanan Teknologi Informasi Menggunakan Indeks KAMI Untuk Persiapan Standar SNI ISO/IEC 27001 (Studi Kasus: STMIK Mardira Indonesia). *Jurnal Computech & Bisnis*, *14*(1), 10–18.

Rochmadi, T., & Pasa, I. Y. (2021). Measurement Of Risk And Evaluation Of Information Security Using The Information Security Index In BKD XYZ Based On ISO 27001 / SNI. *CyberSecurity Dan Forensik DIgital*, *4*(1), 38–43.

Sari, M. K., Saintika, Y., & Prabowo, W. A. (2022). Penyusunan Manajemen Risiko Keamanan Informasi Dengan Standar ISO 27001 Studi Kasus Institut Teknologi Telkom Purwokerto. *Jurnal Sistem Dan Teknologi Informasi (JustIN)*, *10*(4), 423–427. https://doi.org/10.26418/justin.v10i4.48977

Sharma, N. K., & Dash, P. K. (2012). Effectiveness Of ISO 27001, As An Information Security Management System: An Analytical Study Of Financial Aspects. *Far East Journal of Psychology and Business*, *9*(3). www.fareastjournals.com

Supradono, B. (2009). Manajemen Risiko Keamanan Informasi Dengan Menggunakan Metode Octave (Operationally Critical Threat, Asset, And Vulnerability Evaluation). *Media Elektrika*, *2*(1), 4–8. http://jurnal.unimus.ac.id

Wijatmoko, T. E. (2020). *Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Pada Kantor Wilayah Kementerian Hukum Dan HAM DIY* (Vol. 3, Issue 1).

Yunella, M., Dwi Herlambang, A., Hayuhardhika, W., & Putra, N. (2019). Evaluasi Tata Kelola Keamanan Informasi Pada Dinas Komunikasi Dan Informatika Kota Malang Menggunakan Indeks KAMI. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *3*(10), 9552–9559. http://j-ptiik.ub.ac.id

Yusuf, A. M. (2017). *Metode Penelitian Kuantitatif, Kualitatif & Penelitian Gabungan*. Kencana.