Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)
Volume 6, Nomor 3 Oktober-Desember 2023, Hal 180-190
ISSN 2723- 6129 (media online)
Link Jurnal : https://ejournal.sisfokomtek.org/index.php/jikom

Penilaian Keamanan Informasi Data Center Instansi Yaza untuk Mencegah Ancaman Siber dalam Meningkatkan Pertahanan

Jefferson Benyamin[1*], Much Mualim[2], Editha Praditya Duarte[3]

[1,2,3]Manajemen Pertahanan, Unversitas Pertahanan Republik Indonesia
Email: [1]jeffersonbenyamin@gmail.com, [2]mualimdrt@gmail.com, [3]editha.duarte@yahoo.com
Email Penulis Korespondensi: [1]jeffersonbenyamin@gmail.com

Abstrak− Instansi YAZA merupakan instansi pemerintah yang memiliki tugas dalam bidang keamanan informasi. Dalam menjalankan tugasnya, perlu didukung oleh beberapa layanan publik yang bersifat elektronik serta memanfaatkan aplikasi dengan menggunakan jaringan internet, contohnya: absensi elektronis, email, website, portal, sistem informasi kepegawaian, dan sistem informasi manajemen aset. Keseluruhan data dari aplikasi-aplikasi tersebut dikelola secara terpusat pada data center. Dengan banyaknya aplikasi yang terhubung pada data center tersebut, maka akan berdampak munculnya ancaman pada sistem keamanan informasi seperti pencurian data, perubahan data, dan ancaman dunia maya seperti virus, pembajakan, DoS, dan DDoS yang dapat mengancam Instansi YAZA. Oleh karena itu, perlu dilakukan penilaian atas sistem keamanan informasi pada data center di Instansi YAZA. Tujuan penelitian ini untuk mengevaluasi pengelolaan data center di instansi YAZA dengan memberikan rekomendasi berdasarkan standar SNI ISO/IEC 27001:2013. Penelitian ini menggunakan metode penelitian deskriptif dengan mengkaji aspek teoritis dan aspek legal lalu dilakukan studi literatur, observasi, diskusi narasumber, dan kuesioner. Tingkat ketergantungan penggunaan sistem elektronik sebesar 36 dari total skor 50 dan masuk kedalam kategori Strategis. Hasil perhitungan kelima area sebesar 242 dari 645 dan terletak pada kategori belum optimal.

Kata Kunci: Ancaman**,** Data Center, Instansi YAZA, Keamanan Informasi, Penilaian Keamanan Informasi

Abstract− The YAZA agency is a government agency that has duties in the field of information security. In carrying out its duties, it needs to be supported by several public services that are electronic and utilize applications using the internet network, for example: electronic attendance, email, website, portal, personnel information system, and asset management information system. All data from these applications are managed centrally in the data center. With so many applications connected to the data center, it will have an impact on the emergence of threats to information security systems such as data theft, data changes, and cyber threats such as viruses, piracy, DoS, and DDoS that can threaten YAZA Agencies. Therefore, it is necessary to assess the information security system in the data center at the YAZA Agency. The purpose of this research is to evaluate data center management at the YAZA agency by providing recommendations based on the SNI ISO / IEC 27001: 2013 standard. This research uses descriptive research methods by examining theoretical and legal aspects and then conducting literature studies, observations, resource person discussions, and questionnaires. The level of dependence on the use of electronic systems is 36 out of a total score of 50 and falls into the Strategic category. The results of the calculation of the five areas amounted to 242 out of 645 and are located in the not yet optimal category.

Keywords: Data Center, Information Security, Information Security Assessment, Threats, YAZA Agency

1. PENDAHULUAN

Pada masa globalisasi dikala ini, data ialah aset yang sangat berharga untuk seluruh pihak baik individu maupun kelompok (organisasi). Informasi dianggap sebagai aset yang berharga karena banyak keputusan strategis yang bergantung kepada informasi.[1] Kesadaran akan pentingnya data pada masa saat ini terus semakin berkembang, sehingga menimbulkan bertambahnya data ataupun informasi yang digunakan serta dihasilkan suatu organisasi. Perihal tersebut menimbulkan suatu organisasi tersebut memerlukan media penyimpanan dengan kapasitas yang besar. Tetapi pada masa digital saat ini menaruh informasi ataupun data secara fisik sudah tidak terakomodir serta efektif lagi sehingga bergeser dengan metode elektronik semacam harddisk, cd, dvd, flash memori serta yang lain. Dikala ini mengolah serta mengelola informasi yang besar tentu tidak gampang, sehingga pada suatu institusi buat mengelola informasi dengan jumlah yang banyak bisa menyimpan serta memusatkan informasi pada data center.

Data center ialah sarana yang digunakan buat penempatan beberapa gabungan server serta elemen-elemen terkaitnya, seperti sistem telekomunikasi dan penyimpanan data. Data center menyimpan semua data atau informasi yang diperlukan oleh institusi.[2] Data tersebut didapat, diolah serta disimpan lagi pada data center. Data yang disimpan pada data center ialah data yang mempunyai harga untuk institusi. Proteksi atas data tersebut, bisa dilakukan dengan mempraktikkan manajemen data yang baik. Manajemen data yang baik dibutuhkan untuk seluruh organisasi, terlebih

Submitted: **10/08/2023**; Accepted: **22/08/2023**; Published: **20/11/2023**

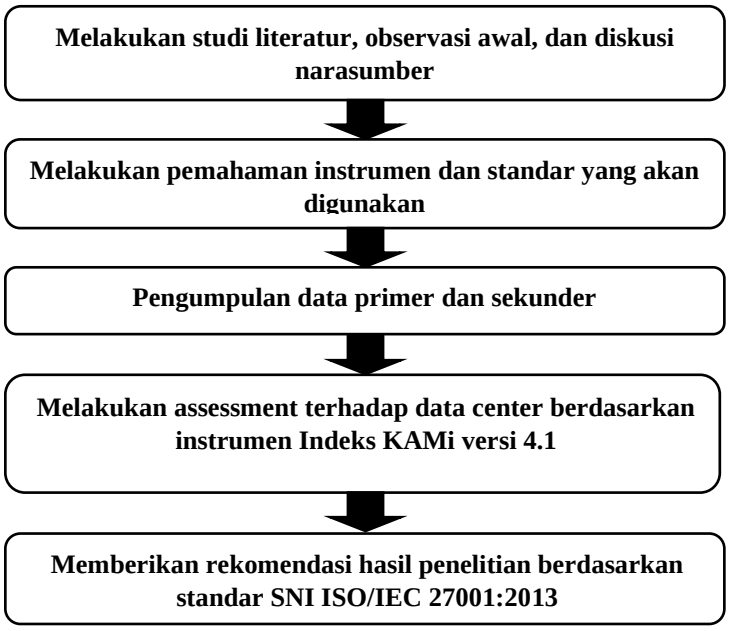
lagi bila organisasi tersebut ialah organisasi yang besar serta banyak berkecimpungan dalam pengolahan data-data yang sensitif/berklasifikasi. Sistem keamanan informasi pada data center harus aman untuk digunakan dalam sistem pertahanan negara. Dimana aman dari segi infrastruktur, jaringan, operasional, dan sumber daya manusia.

Ancaman siber dapat mengakibatkan sistem keamanan pada data center menjadi down sehingga dapat terjadi pencurian data, perubahan data, dan ancaman dunia maya seperti virus, pembajakan, DoS, dan DDoS yang dapat memberikan risiko kepada Instansi secara finansial. Instansi YAZA merupakan instansi pemerintah yang memiliki tugas dalam bidang keamanan informasi. Dimana dalam menjalankan tugasnya, memiliki beberapa layanan publik yang bersifat elektronik serta memanfaatkan aplikasi dengan menggunakan jaringan internet, contohnya: absensi elektronis, email, website, portal, sistem informasi kepegawaian, dan sistem informasi manajemen aset. Keseluruhan data dari aplikasi-aplikasi tersebut dikelola secara terpusat pada data center. Dengan banyaknya aplikasi yang terhubung pada data center tersebut, maka akan berdampak munculnya risiko pada keamanan informasi seperti kebocoran data yang bersifat rahasia sehingga dapat mengancam Instansi YAZA dalam melaksanaan kegiatan operasional.

Berdasarkan uraian diatas, maka pada riset ini perlu dilakukan evaluasi sistem keamanan informasi pada data center di Instansi YAZA buat mengetahui situasi terkini sistem keamanan informasi sesudah itu dilanjutkan dengan membuat rekomendasi pembaruan terhadap sistem keamanan informasi sebagai bahan pertimbangan untuk meningkatkan pertahanan negara dibidang keamanan informasi dan meningkatkan kualitas sistem keamanan informasi pada data center di Instansi YAZA supaya dapat memberikan pelayanan publik yang optimal kepada masyarkat maupun negara.

2. METODOLOGI PENELITIAN

Metode penelitian yang akan digunakan dalam penelitian ini dengan pendekatan kualitatif dan menggunakan metode penelitian deskriptif. Dalam penelitian ini, kerangka pemikiran yang dibuat diawali dengan mengkaji aspek teoritis dan aspek legal lalu dilakukan studi literatur, observasi, diskusi narasumber, dan kuesioner kemudian dilanjutkan dengan menjabarkan proses yang dilakukan berupa teknik pengumpulan dan analisis data yang dilakukan untuk menjawab permasalahan pada penelitian ini.[10] Pada penelitian ini menggunakan instrumen Indeks KAMI untuk mengevaluasi pengelolaan data center di Instansi YAZA, kemudian memberikan rekomendasi berdasarkan standar SNI ISO/IEC 27001. Adapun kerangka pemikiran dalam penelitian ini dapat dilihat pada gambar 1.



Gambar 1. Kerangka Pemikiran

Submitted: **10/08/2023**; Accepted: **22/08/2023**; Published: **20/11/2023**

Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)
Volume 6, Nomor 3 Oktober-Desember 2023, Hal 180-190
ISSN 2723- 6129 (media online)
Link Jurnal : https://ejournal.sisfokomtek.org/index.php/jikom

3. HASIL DAN PEMBAHASAN

a. Mekanisme Pengumpulan Data

Pengumpulan data dilakukan dengan wawancara serta penelaahan dokumen-dokumen mengenai pengelolaan data center yang ada di Instansi YAZA. Kegiatan wawancara dilakukan dengan personil yang memiliki fungsi, wewenang, dan mengampu pengelolaan data center di Instansi YAZA.

b. Data Pengukuran Indeks KAMI pada Data Center di Instansi YAZA

Tahap awal pemanfaatan indeks KAMI ialah dengan menanggapi pertanyaan terkait kesiapan pengamanan informasi, responden dimohon buat mendeskripsikan Peran TIK dalam pengelolaan data center. Tujuan dari langkah ini ialah buat menggolongkan Instansi ke "ukuran" tertentu: Rendah, Tinggi, dan Strategis. Setelah itu dilakukan pengukuran kesiapan keamanan informasi mulai dari tata kelola keamanan informasi, pengelolaan resiko keamanan informasi, pengukuran kerangka kerja keamanan informasi, pengukuran pengelolaan aset informasi, serta pengukuran teknologi dan keamanan informasi.

1) Berikut ialah hasil dari penilaian tingkatan kebutuhan pennggunaan kategori Sistem Elektronik pada data center Instansi YAZA.

Bagian I: Kategori Sistem Elektronik

Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan

	[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis	Status	Skor
#	**Karakteristik Instansi/Perusahaan**		
1.1	Nilai investasi sistem elektronik yang terpasang [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar [C] Kurang dari Rp.3 Miliar	A	5
1.2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik [A] Lebih dari Rp.10 Miliar [B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar [C] Kurang dari Rp.1 Miliar	B	2
1.3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional [C] Tidak ada Peraturan khusus	A	5
1.4	Menggunakan teknik kriptografi khusus untuk keamanan informasi dalam Sistem Elektronik [A] Teknik kriptografi khusus yang disertifikasi oleh Negara [B] Teknik kriptografi sesuai standar industri, tersedia secara publik atau dikembangkan sendiri [C] Tidak ada penggunaan teknik kriptografi	B	2
1.5	Jumlah pengguna Sistem Elektronik [A] Lebih dari 5.000 pengguna [B] 1.000 sampai dengan 5.000 pengguna [C] Kurang dari 1.000 pengguna	C	1
1.6	Data pribadi yang dikelola Sistem Elektronik [A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya [B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha [C] Tidak ada data pribadi	A	5
1.7	Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Sangat Rahasia [B] Rahasia dan/ atau Terbatas [C] Biasa	A	5
1.8	Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik [B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung [C] Proses yang hanya berdampak pada bisnis perusahaan	A	5
1.9	Dampak dari kegagalan Sistem Elektronik [A] Tidak tersedianya layanan publik berskala nasional atau membahayakan pertahanan keamanan negara [B] Tidak tersedianya layanan publik dalam 1 propinsi atau lebih [C] Tidak tersedianya layanan publik dalam 1 kabupaten/kota atau lebih	A	5
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme) [A] Menimbulkan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan mengakibatkan kerugian finansial)	C	1
	Skor penetapan Kategori Sistem Elektronik	**36**	

Gambar 2. Hasil Penilaian Tingkat Kepentingan Penggunaan Kategori Sistem Elektronik

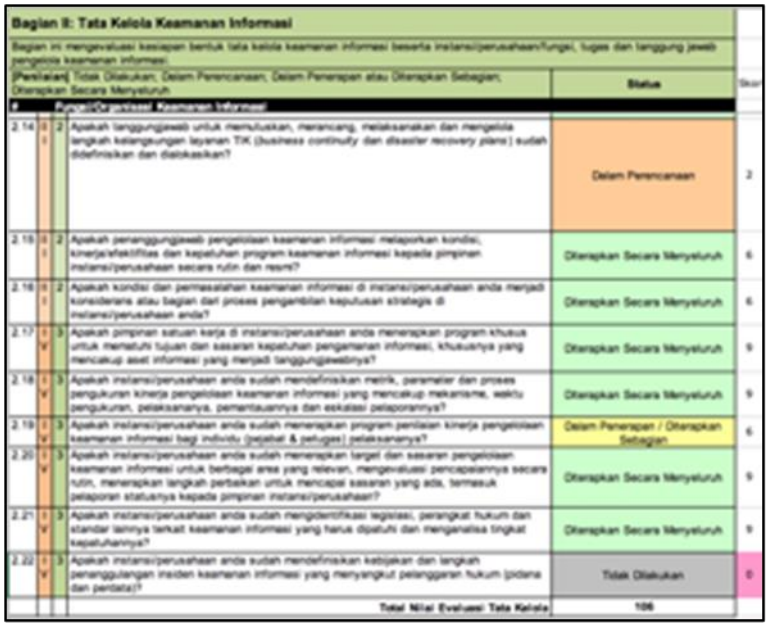
Dari hasil evaluasi tingkatan kebutuhan pemakaian kategori Sistem Elektronik pada data center Instansi YAZA telah diperoleh skor sebesar 36, maka Sistem Elektornik bisa dikategorikan ke dalam tingkatan Tinggi sesuai dengan tabel tingkatan kematangan Indeks KAMI yaitu kategori Strategis karena berkisar antara skor 35 sampai dengan 50.

Submitted: **10/08/2023**; Accepted: **22/08/2023**; Published: **20/11/2023**

Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)
Volume 6, Nomor 3 Oktober-Desember 2023, Hal 180-190
ISSN 2723- 6129 (media online)
Link Jurnal : https://ejournal.sisfokomtek.org/index.php/jikom

2) Selanjutnya yakni hasil dari penilaian Tata Kelola Keamanan Informasi pada data center Instansi YAZA.

Tabel 2. Hasil Penilaian Tata Kelola Keamanan Informasi

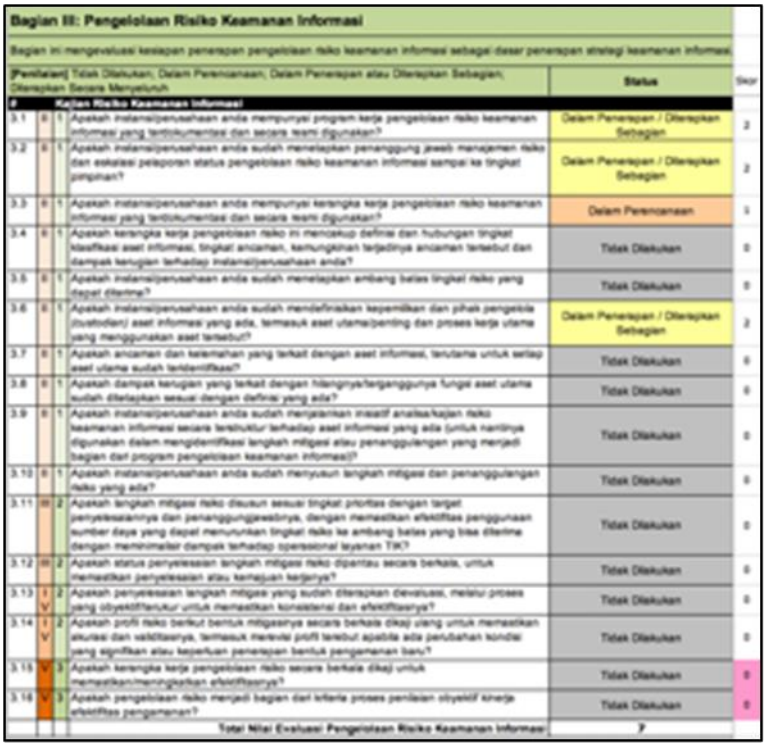


Bagian II: Tata Kelola Keamanan Informasi					
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				Status	Skor
#	Area/Objektif Keamanan Informasi				
2.14	I	2	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity dan disaster recovery plans*) sudah didefinisikan dan dialokasikan?	Dalam Perencanaan	2
2.15	I	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan instansi/perusahaan secara rutin dan resmi?	Diterapkan Secara Menyeluruh	6
2.16	I	2	Apakah kondisi dan permasalahan keamanan informasi di instansi/perusahaan anda menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis di instansi/perusahaan anda?	Diterapkan Secara Menyeluruh	6
2.17	V	3	Apakah pimpinan satuan kerja di instansi/perusahaan anda menerapkan program khusus untuk memastikan tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	Diterapkan Secara Menyeluruh	9
2.18	V	3	Apakah instansi/perusahaan anda sudah mendefinisikan metrik, parameter dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?	Diterapkan Secara Menyeluruh	9
2.19	V	3	Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & pelaksana) pelaksananya?	Dalam Penerapan / Diterapkan Sebagian	6
2.20	V	3	Apakah instansi/perusahaan anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan instansi/perusahaan?	Diterapkan Secara Menyeluruh	9
2.21	V	3	Apakah instansi/perusahaan anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	Diterapkan Secara Menyeluruh	9
2.22	V	3	Apakah instansi/perusahaan anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Tidak Dilakukan	0
			Total Nilai Evaluasi Tata Kelola	106	

Gambar 3. Hasil Penilaian Tata Kelola Keamanan Informasi

Pada gambar 3 diuraikan bahwa kategori kontrol satu dengan pertanyaan yang berjumlah delapan bernilai 22. Pertanyaan tahap dua dengan jumlah delapan bernilai 42. Sedangkan untuk pertanyaan tahap tiga dengan jumlah enam bernilai 42. Dari hasil yang didapat maka jumlah nilai untuk Tahap Penerapan satu, dua dan tiga berjumlah 106.

3) Selanjutnya ialah hasil dari perhitungan Pengelolaan Risiko Keamanan Informasi pada data center Instansi YAZA.



Bagian III: Pengelolaan Risiko Keamanan Informasi					
Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				Status	Skor
#	Kajian Risiko Keamanan Informasi				
3.1	II	1	Apakah instansi/perusahaan anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Dalam Penerapan / Diterapkan Sebagian	2
3.2	II	1	Apakah instansi/perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?	Dalam Penerapan / Diterapkan Sebagian	2
3.3	II	1	Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Dalam Perencanaan	1
3.4	II	1	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap instansi/perusahaan anda?	Tidak Dilakukan	0
3.5	II	1	Apakah instansi/perusahaan anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	Tidak Dilakukan	0
3.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan kepemilikan dan pihak pengelola (*custodian*) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	Dalam Penerapan / Diterapkan Sebagian	2
3.7	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	Tidak Dilakukan	0
3.8	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	Tidak Dilakukan	0
3.9	II	1	Apakah instansi/perusahaan anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?	Tidak Dilakukan	0
3.10	II	1	Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	Tidak Dilakukan	0
3.11	III	2	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?	Tidak Dilakukan	0
3.12	III	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	Tidak Dilakukan	0
3.13	I V	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?	Tidak Dilakukan	0
3.14	I V	2	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil tersebut apabila ada perubahan kondisi yang signifikan atau kepastian penerapan bentuk pengamanan baru?	Tidak Dilakukan	0
3.15	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	Tidak Dilakukan	0
3.16	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	Tidak Dilakukan	0
			Total Nilai Evaluasi Pengelolaan Risiko Keamanan Informasi	7	

Gambar 4. Hasil Penilaian Risiko Keamanan Informasi

Submitted: **10/08/2023**; Accepted: **22/08/2023**; Published: **20/11/2023**

Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)
Volume 6, Nomor 3 Oktober-Desember 2023, Hal 180-190
ISSN 2723- 6129 (media online)
Link Jurnal : https://ejournal.sisfokomtek.org/index.php/jikom

Pada gambar 4 diuraikan bahwa kategori kontrol satu dengan pertanyaan yang berjumlah 10 bernilai 7. Pertanyaan tahap dua dengan jumlah empat bernilai 0. Sedangkan pertanyaan tahap tiga dengan jumlah dua bernilai 0. Dari hasil yang didapat maka jumlah nilai untuk Tahap Penerapan satu, dua dan tiga berjumlah 7.

4) Selanjutnya ialah hasil dari perhitungan Kerangka Kerja Keamanan Informasi pada data center Instansi YAZA.

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi

Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapann

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				Status	Skor
4.23	III	1	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?	Tidak Dilakukan	0
4.24	III	1	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?	Tidak Dilakukan	0
4.25	III	2	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisatif peningkatan kinerja keamanan informasi?	Tidak Dilakukan	0
4.26	III	2	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	Tidak Dilakukan	0
4.27	IV	3	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?	Tidak Dilakukan	0
4.28	V	3	Apakah organisasi anda secara periodik mengaji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif?	Tidak Dilakukan	0
4.29	V	3	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Tidak Dilakukan	0
			Total Nilai Evaluasi Kerangka Kerja	**16**	

Gambar 5. Hasil Perhitungan Kerangka Kerja Keamanan Informasi

Pada gambar 5 diuraikan bahwa kategori kontrol satu dengan pertanyaan yang berjumlah 12 bernilai 10. Pertanyaan tahap dua dengan jumlah 10 bernilai 6. Sedangkan untuk pertanyaan tahap tiga dengan jumlah 7 bernilai 0. Dari hasil yang didapat maka jumlah nilai untuk Tahap Penerapan satu, dua, dan tiga berjumlah 16.

5) Selanjutnya ialah hasil dari perhitungan Pengelolaan Aset Keamanan Informasi pada data center Instansi YAZA.

Bagian V: Pengelolaan Aset Informasi

Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				Status	Skor
5.3 3	II	1	Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris)?	Dalam Penerapan / Diterapkan Sebagian	2
5.3 4	II	2	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?	Diterapkan Secara Menyeluruh	6
5.3 5	II	2	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	Dalam Penerapan / Diterapkan Sebagian	4
5.3 6	II	2	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	Tidak Dilakukan	0
5.3 7	II	2	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)	Tidak Dilakukan	0
5.3 8	III	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan anda?	Dalam Penerapan / Diterapkan Sebagian	0
			Total Nilai Evaluasi Pengelolaan Aset	**53**	

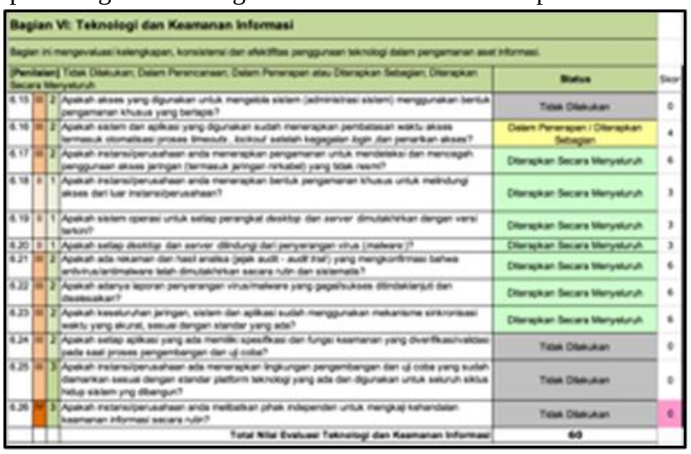
Gambar 6. Hasil Perhitungan Aset Keamanan Informasi

Pada gambar 6 diuraikan bahwa kategori kontrol satu dengan pertanyaan yang berjumlah 24 bernilai 25. Pertanyaan tahap dua dengan jumlah 10 bernilai 26. Sedangkan untuk pertanyaan tahap tiga dengan jumlah 4 bernilai 0. Dari hasil yang didapat maka jumlah nilai untuk Tahap Penerapan satu, dua, dan tiga berjumlah 51.

Submitted: **10/08/2023**; Accepted: **22/08/2023**; Published: **20/11/2023**

Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)
Volume 6, Nomor 3 Oktober-Desember 2023, Hal 180-190
ISSN 2723- 6129 (media online)
Link Jurnal : https://ejournal.sisfokomtek.org/index.php/jikom

6) Berikut ialah hasil dari perhitungan Teknologi dan Keamanan Informasi pada data center Instansi YAZA.



Bagian VI: Teknologi dan Keamanan Informasi

Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.

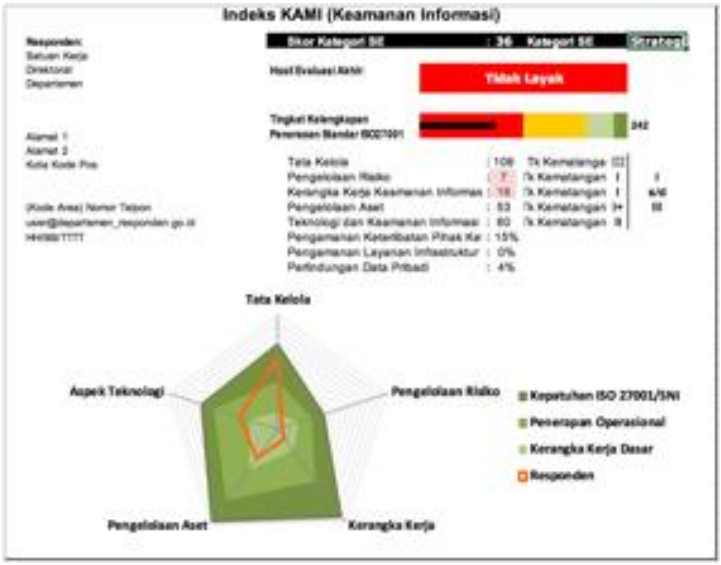
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				Status	Skor
6.15	III	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	Tidak Dilakukan	0
6.16	III	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login dan penarikan akses?	Dalam Penerapan / Diterapkan Sebagian	4
6.17	III	2	Apakah infrastruktur/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	Diterapkan Secara Menyeluruh	6
6.18	II	1	Apakah infrastruktur/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?	Diterapkan Secara Menyeluruh	3
6.19	II	1	Apakah sistem operasi untuk setiap perangkat desktop dan server dimutakhirkan dengan versi terkini?	Diterapkan Secara Menyeluruh	3
6.20	II	1	Apakah setiap desktop dan server dilindungi dari penyerangan virus (malware)?	Diterapkan Secara Menyeluruh	3
6.21	III	2	Apakah ada rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	Diterapkan Secara Menyeluruh	6
6.22	III	2	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	Diterapkan Secara Menyeluruh	6
6.23	III	2	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Diterapkan Secara Menyeluruh	6
6.24	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?	Tidak Dilakukan	0
6.25	III	3	Apakah infrastruktur/perusahaan ada menerapkan lingkungan pengembangan dan uji coba yang sudah disesuaikan dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?	Tidak Dilakukan	0
6.26	III	3	Apakah infrastruktur/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Tidak Dilakukan	0
			Total Nilai Evaluasi Teknologi dan Keamanan Informasi	60	

Gambar 7. Hasil Penilaian Risiko Keamanan Informasi

Pada gambar 7 diuraikan bahwa kategori kontrol satu dengan pertanyaan yang berjumlah 14 bernilai 32. Pertanyaan tahap dua dengan jumlah 10 bernilai 28. Sedangkan untuk pertanyaan tahap tiga dengan jumlah 2 bernilai 0. Dari hasil yang didapat maka jumlah nilai untuk Tahap Penerapan satu, dua, dan tiga berjumlah 60.

c. Hasil Pengukuran Indeks KAMI pada Data Center di Instansi YAZA

Hasil penilaian pada data center di Instansi YAZA terdapat pada tampilan dashboard Indeks KAMI yang dihasilkan sebagai berikut.



Gambar 8. Dashboard Hasil Penilaian Data Center di Instansi YAZA

Dashboard di atas ialah gambaran secara keseluruhan dari penilaian yang telah dilakukan dengan menggunakan Indeks KAMI versi 4.1. Dari dashboard itu, bisa diamati jika ttingkat kematangan keamanan informasi pada Data Center di Perusahaan YAZA masih belum optimal, yakni pada rentang tingkat kematangan I s.d. III dengan nilai sebesar 242. Pada radar chart dashboard itu kalau hampir seluruh area yang dinilai dalam Indeks KAMI masih belum terpenuhi.

Submitted: **10/08/2023**; Accepted: **22/08/2023**; Published: **20/11/2023**

Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)
Volume 6, Nomor 3 Oktober-Desember 2023, Hal 180-190
ISSN 2723- 6129 (media online)
Link Jurnal : https://ejournal.sisfokomtek.org/index.php/jikom

Gambar 9. Hasil Evaluasi Indeks KAMI pada Data Center di Instansi YAZA

Dari gambar 9 terlihat kalau nilai Indeks KAMI yang telah dicapai terkategori belum optimal, yakni hanya mencapai rentang tingkat kematangan I s.d. III. Nilai yang diperoleh masih dikatakan belum optimal karena nilai yang dicapai untuk kepentingan penggunaan sistem elektronik yang digunakan pada data center di Perusahaan YAZA tsudah sesuai, yakni mencapai tingkat Strategis. Namun untuk tingkat kematangan tiap area yang telah dinilai dalam Indeks KAMI versi 4.1 masih ada yang perlu diperbaiki. Berikut ini merupakan uraian dari tingkat kematangan kelima area yang telah dinilai sebelumnya:

	Tata Kelola	Pengelolaan Risiko	Kerangka Kerja	Pengelolaan Aset	Aspek Teknologi
Tingkat II					
Status	II	Tidak	Tidak	I+	II
Tingkat III					
Validitas	Iya	Tidak	Tidak	Tidak	Tidak
Status	III	Tidak	Tidak	Tidak	Tidak
Tingkat IV					
Validitas	Tidak	Tidak	Tidak	Tidak	Tidak
Status	Tidak	Tidak	Tidak	Tidak	Tidak
Tingkat V					
Validitas	Tidak	Tidak	Tidak	Tidak	Tidak
Status	Tidak	Tidak	Tidak	Tidak	Tidak
Status Akhir	III	I	I	I+	II
	5	1	1	2	3

Gambar 10. Tingkatan Kematangan Kelima Area

Urutan tingkat kematangan dari yang terendah hingga yang tertinggi adalah I – V. Batasan minimal yang mesti dicapai supaya bisa melaksanakan sertifikasi ISO 27001 adalah III+. Sementara itu, untuk saat ini tingkat kematangan pada data center di Perusahaan YAZA hanya pada batas I s.d. III. Tingkat kematangan ini memperlihatkan bahwa posisi data center di Perusahaan YAZA sebagai berikut yang ada pada gambar 11.

Tingkatan	Kondisi
I	Kondisi Awal
II	Penerapan Kerangka Kerja Dasar
III	Terdefinisi dan Konsisten
IV	Terkelola dan Terukur
V	Optimal

Gambar 11. Tingkatan Kondisi Data Center di Instansi YAZA

Submitted: **10/08/2023**; Accepted: **22/08/2023**; Published: **20/11/2023**

Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)
Volume 6, Nomor 3 Oktober-Desember 2023, Hal 180-190
ISSN 2723- 6129 (media online)
Link Jurnal : https://ejournal.sisfokomtek.org/index.php/jikom

d. Rekomendasi Keamanan Informasi untuk Data Center di Instansi YAZA

Rekomendasi yang diberikan didasarkan oleh standar SNI ISO/ IEC 27001: 2013 dengan melakukan perbandingan. Perbandingan dilakukan dengan melihat kekurangan apa saja yang terdapat pada tiap area serta membandingkannya dengan kontrol ISO 27001: 2013 yang berkaitan dengan area tersebut. Berikut ini merupakan tabel rekomendasi dari tiap-tiap area serta diurutkan sesuai dengan prioritas berdasarkan dari skor terendah hingga paling tinggi yang diperoleh masing-masing area.

1) Rekomendasi yang diberikan untuk area Tata Kelola keamanan informasi.

Tabel 1. Rekomendasi Tata Kelola Keamanan Informasi

No	Situasi Saat Ini	Rekomendasi	Kontrol ISO
1	Belum mendefinisikan peraturan serta tahap penanggulangan	Mengaplikasikan tanggung jawab serta metode untuk menetapkan reaksi yang cepat, efisien, dan tepat guna	A.16.1.1

2) Rekomendasi yang diberikan untuk area pengelolaan risiko keamanan informasi.

Tabel 2. Rekomendasi Pengelolaan Risiko Keamanan Informasi

No	Situasi Saat Ini	Rekomendasi	Kontrol ISO
1	Belum adanya identifikasi terhadap ancaman serta kelemahan pada aset informasi	Melakukan identifikasi dan pencatatan ancaman dan kelemahan pada aset informasi	A.8.2.3
2	Belum adanya penetapan dan pendefinisian mengenai hilangnya/terganggunya fungsi aset utama	Mengidentifikasi dampak kerugian yang terjadi karena hilangnya/terganggunya fungsi aset utama	A.16.1.6
3	Belum terdapatnya penanggungjawab manajemen risiko	Memastikan serta mengalokasikan kedudukan serta tanggung jawab keamanan informasi	A.6.1.1
4	Belum terdapatnya ambang batasan ancaman	Menerapkan sistem pencatatan dan pelaporan setiap kelemahan keamanan informasi	A.16.1.3
5	Belum adanya inisiatif untuk menganalisa risiko keamanan informasi pada aset informasi	Melaksanakan inisiatif analisa risiko keamanan informasi secara terstruktur pada aset informasi	A.16.1.1
6	Belum adanya langkah mitigasi risiko yang disusun sesuai tingkat prioritas	Menyusun prosedur mitigasi ancaman sesuai tingkatan prioritas dengan sasaran penyelesaiannya serta penanggungjawabnya	A.16.1.7
7	Belum adanya kerangka operasi pengelolaan ancaman yang dikaji secara rutin	Melakukan kajian kerangka operasi pengelolaan ancaman yang dikaji secara rutin	A.16.1.6

Submitted: **10/08/2023**; Accepted: **22/08/2023**; Published: **20/11/2023**

Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)
Volume 6, Nomor 3 Oktober-Desember 2023, Hal 180-190
ISSN 2723- 6129 (media online)
Link Jurnal : https://ejournal.sisfokomtek.org/index.php/jikom

3) Rekomendasi yang diberikan untuk area kerangka kerja pengelolaan keamanan informasi.

Tabel 3. Rekomendasi Kerangka Kerja Pengelolaan Keamanan Informasi

No	Situasi Saat Ini	Rekomendasi	Kontrol ISO
1	Belum tersedianya kebijakan legal buat mengatur suatu dispensasi terhadap penggunaan keamanan informasi	Membuat dan menerapkan kebijakan legal buat mengatur suatu dispensasi terhadap penggunaan keamanan informasi, termasuk cara buat menindaklanjuti konsekwensi	A.18.2.3
2	Belum adanya penerapan proses untuk mengevaluasi risiko	Menjalankan metode buat menilai ancaman terkait konsep pembelian sistem baru serta mengatasi permasalahan yang timbul	A.14.1.1
3	Belum adanya evaluasi mengenai *disaster recovery plan*	Melakukan evaluasi *disaster recovery plan* terhadap layanan TIK untuk menetapkan tindakan perubahan ataupun pengaturan yang dibutuhkan	A.17.1.3
4	Belum adanya peraturan serta metode keamanan informasi yang dievaluasi kelayakannya dengan cara teratur	Membuat dan menyusun peraturan dan metode keamanan informasi serta dievaluasi kelayakannya dengan cara teratur	A.5.1.2
5	Belum adanya pemeriksaan internal serta evaluasi secara berkala	Melakukan pemeriksaan internal serta evaluasi secara berkala	A.12.7.1

4) Rekomendasi yang diberikan untuk area pengelolaan aset informasi.

Tabel 4. Rekomendasi Pengelolaan Aset Informasi

No	Situasi Saat Ini	Rekomendasi	Kontrol ISO
1	Belum terdapat aturan proteksi serta pemanfaatan aset Instansi terkait HAKI	Membuat dan menyusun aturan proteksi serta pemanfaatan aset Instansi terkait HAKI	A.8.1.3
2	Belum ada peraturan pemanfaatan data individu	Membuat dan menyusun peraturan penggunaan data individu yang mewajibkan pemberian ijin tercatat oleh pemilik data individu	A.18.1.4
3	Belum terdapat ketetapan terkait periode penyimpanan buat pengkategorian data yang ada serta ketentuan penghancuran data	Membuat dan menyusun ketetapan terkait periode penyimpanan buat pengkategorian data yang ada serta ketentuan penghancuran data	A.8.3.1
4	Belum terdapat ketetapan pertukaran data dengan pihak eksternal dan pengamanannya	Membuat dan menyusun ketetapan pertukaran data dengan pihak eksternal dan pengamanannya	A.15.2.1

Submitted: **10/08/2023**; Accepted: **22/08/2023**; Published: **20/11/2023**

5	Belum terdapat langkah kajian pemanfaatan akses serta hak aksesnya	Membuat dan menyusun langkah kajian pemanfaatan akses serta hak aksesnya	A.9.2.3

5) Rekomendasi yang diberikan untuk area teknologi dan keamanan informasi.

Tabel 5. Rekomendasi Teknologi dan Keamanan Informasi

No	Situasi Saat Ini	Rekomendasi	Kontrol ISO
1	Belum terdapat analisa terhadap semua log	Melakukan analisa terhadap semua log secara berkala	A.12.4.1
2	Belum terdapat standar enkripsi	Menerapkan standar enkripsi	A.10.1.1
3	Belum adanya penerapan/pengaturan pada sistem aplikasi yang digunakan buat pergantian password	Melakukan penerapan/pengaturan pada sistem aplikasi untuk pergantian *password* secara berkala	A.9.4.3
4	Belum ada pelibatan pihak independen buat menelaah kehandalan keamanan informasi dengan cara teratur	Melakukan mekanisme pelibatan pihak independen buat menelaah kehandalan keamanan informasi dengan cara teratur	A.18.2.1

4. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan pada data center di Instansi YAZA dapat disimpulkan bahwa hasil dari perhitungan tingkatan pemanfaatan Sistem Elektronik ialah 36. Hal ini memperlihatkan kalau Data Center di Instansi YAZA termasuk dalam kategori strategis. Tingkatan kematangan per area hendak dijabarkan sebagai berikut: area Tata Kelola Keamanan Informasi terletak pada tingkatan III, area Pengelolaan Risiko Keamanan Informasi terletak pada tingkatan I, area Kerangka Operasi Pengelolaan Keamanan Informasi terletak pada tingkatan I, area Pengelolaan Aset Informasi terletak pada tingkatan I+, serta area Teknologi dan Keamanan Informasi terletak pada tingkatan II. Nilai paling tinggi yang dihasilkan dari kelima area yaitu pada area Tata Kelola Keamanan Informasi sebesar 106. Sebaliknya nilai paling rendah yang dihasilkan dari kelima area yaitu pada area Pengelolaan Risiko Keamanan Informasi sebesar 7.

Hasil perhitungan kelima area yang menampakkan nilai sebesar 242, dengan hasil nilai tingkatan pemanfaatan sistem elektronik sebesar 36 sehingga data center di Instansi YAZA belum dapat dikatakan matang serta belum sesuai dengan standar ISO 27001 sebab masih belum mencapai tingkatan III+ dimana dalam penerapan keamanan informasi sudah terdefinisi serta konsisten. Data center di Instansi YAZA diberi rekomendasi berlandaskan pada kontrol-kontrol yang terdapat pada standar SNI ISO/ IEC 27001 guna diterapkan pada sistem keamanan informasi, serta dapat mencegah terjadinya ancaman pada sistem keamanan informasi seperti: pencurian data, perubahan data, dan ancaman dunia maya seperti virus, pembajakan, DoS, dan DDoS, serta meningkatkan pertahanan siber di Instansi YAZA.

REFERENSI

[1]. T. Thoyyibah, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) berdasarkan ISO 27001:2013 Pada Pusat Informasi dan Pangkalan Data Perguruan Tinggi X," J. CoreIT J. Has. Penelit. Ilmu Komput. dan Teknol. Inf., vol. 4, no. 2, p. 72, 2018, doi: 10.24014/coreit.v4i2.6292.

[2]. *Facilities Consideration for Data center Network Architecture.* American Power Conversion WhitePaper Solution. 2019.

[3]. Riani, Desta. "Audit Keamanan Sistem Informasi Akademik (SIAKAD) Universitas Lampung Menggunakan Standar ISO/IEC 27001". Fakultas Matematika dan Ilmu Pengetahuan Alam. Universitas Lampung. Lampung. 2018.

Submitted: **10/08/2023**; Accepted: **22/08/2023**; Published: **20/11/2023**

[4]. Musyarofah, S. R., & Bisma, R. Analisis kesenjangan sistem manajemen keamanan informasi (SMKI) sebagai persiapan sertifikasi ISO/IEC 27001: 2013 pada institusi pemerintah. *Teknologi: Jurnal Ilmiah Sistem Informasi*, *11*(1), 1–15. 2021.

[5]. Kurniawan, Endang. "Analisis Tingkat Keamanan Sistem Informasi Akademik Berdasarkan Standard ISO/IEC 27002:2013 Menggunakan SSE CMM". Program Pascasarjana Fakultas Teknologi Industri. Universitas Islam Indonesia. Yogyakarta. 2018.

[6]. B. Panjaitan, L. Abdurrahman, and R. Mulyana, "Pengembangan Implementasi Sistem Manajemen Keamanan Informasi Berbasis Iso 27001 : 2013 Menggunakan Kontrol Annex: Studi Kasus Data Center Pt . Xyz the Development of Information Security Management System Implementation Based on Iso 27001 : 2013 Using a," e-Proceeding Eng., vol. 8, no. 2, pp. 2813–2825, 2021.

[7]. ISO/IEC 27001:2013, Information Technology -- Security Techniques --Information Security Management System -- Requirement, ISO/EC, 2018.

[8].T. Kristanto, M. Sholik, D. Rahmawati, and M. Nasrullah, "Analisis Manajemen Keamanan Informasi Menggunakan Standard ISO 27001:2005 Pada Staff IT Support Di Instansi XYZ," JISA(Jurnal Inform. dan Sains), vol. 2, no. 2, pp. 30–33, 2019, doi: 10.31326/jisa.v2i2.497.

[9]. Sari, I. Y., Muttaqin, M., Jamaludin, J., Simarmata, J., Rahman, M. A., Iskandar, A., Pakpahan, A. F., Abdul Karim, S., Giap, Y. C., & Hazriani, H. *Keamanan Data dan Informasi*. Yayasan Kita Menulis. 2020.

[10]. Sugiyono. *Metode Penelitian Kuantitatif Kualitatif dan R&D.* Bandung: Alfabeta. 2019.

Submitted: **10/08/2023**; Accepted: **22/08/2023**; Published: **20/11/2023**