P-ISSN: 2548-1932
e-ISSN: 2549-7758

PENILAIAN SISTEM KEAMANAN INFORMASI DATA CENTER PADA INSTANSI YAZA UNTUK MENCEGAH ANCAMAN SIBER DALAM MENINGKATKAN PERTAHANAN NEGARA

Jefferson Benyamin[1], Hikmat Zakky Almubaroq[2]

[1,2] Program Studi Manajemen Pertahanan, Universitas Pertahanan Republik Indonesia
[1]jeffersonbenyamin@gmail.com, [2]zakkyauri94@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. Penelitian ini menggunakan metode penelitian deskriptif dengan mengkaji aspek teoritis dan aspek legal lalu dilakukan studi literatur, observasi, diskusi narasumber, dan kuesioner. Hasil dari penelitian ini adalah tingkat ketergantungan penggunaan sistem elektronik sebesar 36 termasuk dalam kategori Strategis. Hasil perhitungan kelima area sebesar 242 dan terletak pada kategori belum optimal.

Kata Kunci : *Instansi YAZA; Data Center; Keamanan Informasi; Penilaian Sistem Keamanan Informasi*

I. 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 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

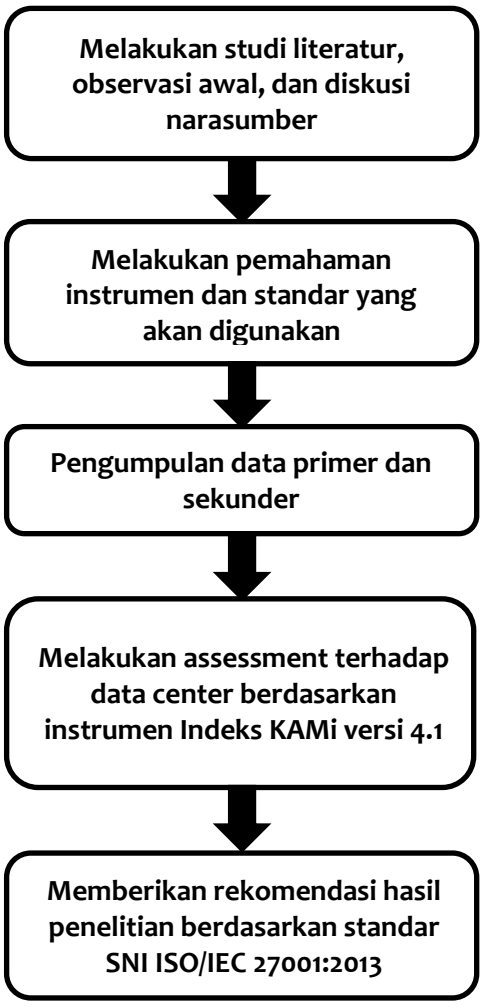
P-ISSN: 2548-1932
e-ISSN: 2549-7758

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 melaksanakan 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 masyarakat maupun negara.

II. METODE 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

III. 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 risiko 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 penggunaan kategori Sistem Elektronik pada data center Instansi YAZA.

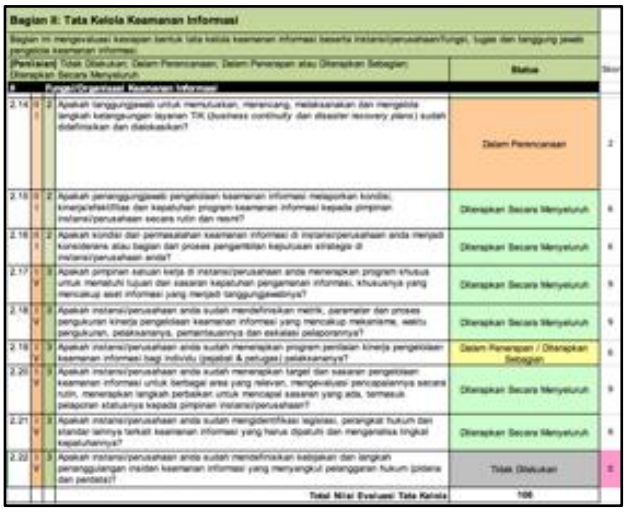
Tabel 1. Hasil Penilaian Tingkat Kepentingan Penggunaan Kategori Sistem Elektronik

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**	

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

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 kerangka 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
#				**Fungsi/Organisasi Keamanan Informasi**		
2.14	II	2	I	Apakah tanggungjawab untuk memutuskan, merencang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (business continuity dan disaster recovery plans) sudah didefinisikan dan dialokasikan?	Dalam Perencanaan	2
2.15	II	2	II	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	4
2.16	II	2	III	Apakah kondisi dan permasalahan keamanan informasi di instansi/perusahaan anda menjadi konsiderans atau bagian dari proses pengambilan kepulusan strategis di instansi/perusahaan anda?	Diterapkan Secara Menyeluruh	4
2.17	II	2	IV	Apakah pimpinan satuan kerja di instansi/perusahaan anda menerapkan program khusus untuk meningkatkan tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	Diterapkan Secara Menyeluruh	4
2.18	II	2	V	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	5
2.19	II	3	I	Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Dalam Penerapan / Diterapkan Sebagian	3
2.20	II	3	II	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	5
2.21	II	3	III	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	5
2.22	II	3	IV	Apakah instansi/perusahaan anda sudah mendefinisikan kebijakan dan langkan penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Tidak Dilakukan	0
				Total Nilai Evaluasi Tata Kelola	**100**	

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

Tabel 3. Hasil Penilaian Risiko Keamanan Informasi

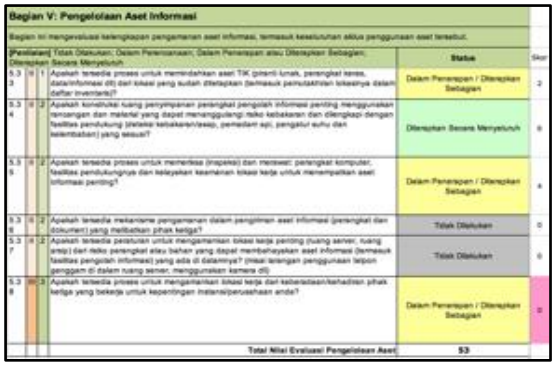
Bagian III: Pengelolaan Risiko Keamanan Informasi					
Bagian ini mengevaluasi kerangka penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara 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 aset 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 menganalisa insiden 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 memperkirakan 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	II V	3	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?	Tidak Dilakukan	0
3.14	II V	3	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 keputusan 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	**0**	

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

Tabel 4. Hasil Perhitungan Kerangka Kerja Keamanan Informasi

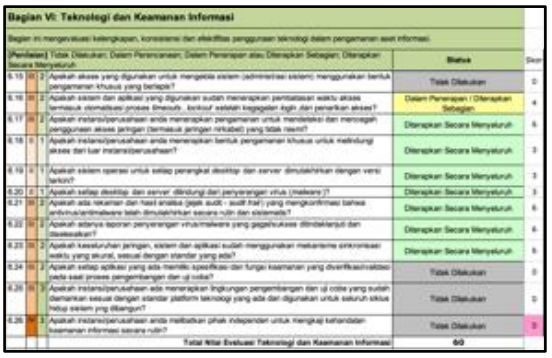
5) Selanjutnya ialah hasil dari perhitungan Pengelolaan Aset Keamanan Informasi pada data center Instansi YAZA.

Tabel 5. Hasil Perhitungan Aset Keamanan Informasi



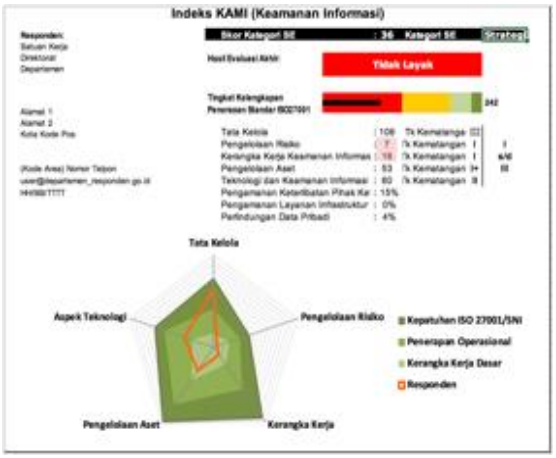
6) Berikut ialah hasil dari perhitungan Teknologi dan Keamanan Informasi pada data center Instansi YAZA.

Tabel 6. Hasil Penilaian Risiko Keamanan Informasi



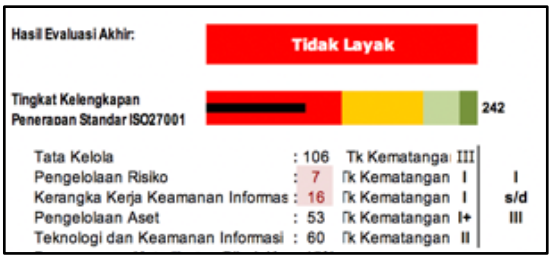
c. Hasil Pengukuran Indeks KAMI pada Data Center di Instansi YAZA

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



Gambar 2. Dashboard Hasil Penilaian Data Center di Instansi YAZA

Dari dashboard diatas, bisa diamati jika tingkatan kematangan keamanan informasi pada data center di Instansi YAZA masih belum optimal, yakni pada rentang tingkatan kematangan I s.d. III dengan nilai sebesar 242.



Gambar 3. Hasil Evaluasi Indeks KAMI pada Data Center di Instansi YAZA

Dari Gambar 3 terlihat kalau nilai Indeks KAMI yang telah dicapai terkategori belum optimal karena tingkatan kematangan tiap area masih ada yang perlu diperbaiki, sehingga dari hasil evaluasi hanya mencapai rentang tingkatan kematangan I s.d. III.

Tabel 7. Tingkatan Kematangan Kelima Area

	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**

Urutan tingkatan kematangan dari yang terendah sampai yang tertinggi adalah I – V. Batasan minimal yang harus dijangkau biar dapat melangsungkan sertifikasi ISO 27001 adalah III+. Sementara itu, untuk saat ini tingkatan kematangan pada data center di Instansi YAZA hanya pada batas I s.d. III. Tingkat kematangan ini memperlihatkan bahwa posisi data center di Instansi YAZA sebagai berikut yang ada pada tabel 8.

Tabel 8. Tingkatan Kondisi Data Center di Instansi YAZA

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

d. Rekomendasi Keamanan Informasi untuk Data Center di Instansi YAZA

Tabel rekomendasi dari tiap-tiap area serta diurutkan sesuai dengan prioritas berlandaskan dari poin terendah sampai tertinggi yang dihasilkan masing-masing area.

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

Tabel 9. 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 10. 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	A.6.1.1

No	Situasi Saat Ini	Rekomendasi	Kontrol ISO
		keamanan informasi	
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 penanggung jawabnya	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

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

Tabel 11. 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 konsekuensi	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	Membuat dan menyusun peraturan dan metode keamanan informasi serta dievaluasi kelayakannya	A.5.1.2

No	Situasi Saat Ini	Rekomendasi	Kontrol ISO
	dievaluasi kelayakannya dengan cara teratur	dengan cara teratur	
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 12. 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 izin tercatat oleh pemilik data individu	A.18.1.4
3	Belum terdapat ketetapan terkait periode penyimpanan buat pengkategorian data yang ada	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 pengamannya	Membuat dan menyusun ketetapan pertukaran data dengan pihak eksternal dan pengamannya	A.15.2.1
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 13. Rekomendasi Teknologi dan Keamanan Informasi

No	Situasi Saat Ini	Rekomendasi	Kontrol ISO
1	Belum terdapat analisis 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	Melakukan penerapan/pengaturan pada sistem aplikasi untuk pergantian *password* secara berkala	A.9.4.3

No	Situasi Saat Ini	Rekomendasi	Kontrol ISO
	buat pergantian password		
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

IV. PENUTUP

4.1 Kesimpulan

Berdasarkan hasil penelitian yang dilakukan pada data center di Instansi YAZA dapat disimpulkan bahwa:

1. Hasil dari perhitungan tingkatan pemanfaatan Sistem Elektronik ialah 36. Hal ini memperlihatkan kalau Data Center di Instansi YAZA termasuk dalam kategori strategis.
2. 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.
3. 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.
4. 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.
5. 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.

DAFTAR PUSTAKA

[1] Kadir, Abdul. *Pengenalan Sistem Informasi*. Yogyakarta: Penerbit ANDI. 2003.
[2] Corso, Dick., Reddy, In., *Data center Tour*, Cisco. 2004.
[3] *Facilities Consideration for Data center Network Architecture.* American Power Conversion WhitePaper Solution. 2005.
[4] M. Whitman dan H. Mattord, Principles of Information Security Fifth Edition, Boston: Cengage Learning, 2018.
[5] C. Chazar, "Standar Manajemen Keamanan Informasi Berbasis ISO/IEC 27001: 2005," *J. Inf.*, vol. VII, no. 2, pp. 48–57, 2015.
[6] Direktorat Keamanan Informasi Kemenkominfo. *Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik*: Jakarta. 2011.
[7] ISO/IEC 27001:2013, Information Technology -- Security Techniques -- Information Security Management System -- Requirement, ISO/EC, 2013.
[8] Standar Nasional Indonesia – ISO (*International of Standard Organization*)/IEC 27001. 2013.
[9] Justanieah, M. *Information Security Management Sistem an* ISO 27001 *introduction*. Jeddah: ISACA. 2009.
[10] Sugiyono. *Metode Penelitian Kuantitatif Kualitatif dan R&D.* Bandung: Alfabeta. 2011.