Journal of Applied Informatics and Computing (JAIC)
Vol.pusat data X, No.pusat data X, Juli 201pusat data X, pp. pusat data Xpusat data X~pusat data Xpusat data X
e-ISSN: 2548-6861

Evaluasi Penerapan Standar ISO 27001 di Pusat Data pusat data X

Ayu Sopia Lajuba [1]*, Andy Triwinarko [2]**
* *Teknik Informatika, Politeknik Negeri Batam*
** Rekayasa Keamanan Siber, Politeknik Negeri Batam
ayusopialajuba9@gmail.com[1], andy@polibatam.ac.id[2]

Article Info

Article history:

Received …
Revised …
Accepted …

Keyword:

ISO 27001, pusat data, keamanan informasi.

ABSTRACT

pusat data X data center is an important part of Telkom Indonesia (Persero) and TelkomGroup's plan to make Indonesia a global digital hub. The data center plays an important role in storing and managing sensitive data to support the development of Indonesia's digital ecosystem. However, the challenge faced by pusat data X is to ensure that information security runs well in its operations. This assessment is crucial to evaluate the degree to which pusat data X has implemented necessary security practices to safeguard sensitive data and ensure operational reliability. The aim of this study is to determine the level of information security maturity at pusat data X and offer recommendations based on the assessment. Analysis of the current maturity level reveals that the detection aspect of information security has attained the highest level of maturity, scoring 4.75. However, there was the lowest score on the identification aspect, specifically on the sub-aspects of asset management, risk management, and reporting, which achieved a score of 4.61. The overall average maturity is 4.67. In addition, gaps between actual conditions and the ISO/IEC 27001:2022 standard were identified, and recommendations have been provided to improve alignment. By comprehending the degree of adherence to the ISO 27001 standard, strategies for enhancement and advancement can be formulated to bolster information security at pusat data X, thus aiding Indonesia's endeavors to materialize its vision as a globally recognized digital hub with a robust and fortified infrastructure.

I. PENDAHULUAN

Keamanan informasi adalah bagian penting dalam dunia digital saat ini, terutama bagi organisasi seperti pusat data yang bertanggung jawab menangani data sensitif. Standar ISO 27001 adalah kerangka kerja referensi yang diakui secara internasional untuk manajemen keamanan informasi [1]. Standar ini memberikan panduan komprehensif untuk mengidentifikasi, mengelola, dan memitigasi risiko keamanan informasi [2]. Kontrol keamanan berdasarkan ISO/IEC 27001:2022 terdiri dari 4 klausul kontrol keamanan dan 93 implementasi kontrol keamanan dalam standar ISO 27001[3].

Standar internasional ISO 27001 telah menjadi standar utama untuk menjaga keamanan informasi di berbagai organisasi dan industri [4]. Pusat data X ini juga bagian penting dari strategi Telkom Indonesia (Persero) dan TelkomGroup untuk menjadikan Indonesia sebagai hub digital global [5]. pusat data X berperan penting dalam mendukung infrastruktur teknologi penting untuk ekosistem digital Indonesia yang sedang berkembang. Dalam konteks ini, penting untuk mengevaluasi penerapan ISO 27001 di pusat data X. Dengan melakukan evaluasi ini, pusat data X dapat memastikan bahwa praktik-praktik keamanan informasi diterapkan selaras dengan standar internasional dan dapat memberikan perlindungan yang optimal terhadap data sensitif yang dikelolanya. Tujuan dari penelitian ini adalah untuk menilai atau mengukur tingkat kematangan keamanan informasi, Mendapatkan pemahaman tentang status keamanan informasi yang sedang berlangsung serta memberikan rekomendasi pada pusat data X berdasarkan evaluasi tersebut [6].

e-ISSN: 2548-6861

II. DASAR TEORI

Bagian ini merangkum kerangka teoritis yang mendukung penyelesaian tugas akhir dengan menyajikan konsep-konsep dan prinsip-prinsip yang relevan dalam konteks penelitian yang dilakukan.

A. Keamanan Informasi

Keamanan informasi adalah langkah-langkah dan prosedur-prosedur yang diterapkan untuk melindungi segala jenis sumber daya informasi dari akses yang tidak sah atau penyalahgunaan oleh pihak yang tidak berwenang. Ini melibatkan usaha untuk mempertahankan kerahasiaan, integritas, dan ketersediaan informasi yang krusial bagi perusahaan [7].

B. Evaluasi

Evaluasi adalah sebuah Prosedur yang dilakukan untuk menilai nilai atau mutu suatu hal atau objek dengan mengacu pada standar atau kriteria tertentu. Tujuan dari proses evaluasi ini adalah untuk memahami sejauh mana hal atau objek ini sesuai dengan tujuan yang telah ditetapkan sebelumnya. Evaluasi seringkali melibatkan pengumpulan data, analisis, dan penilaian berdasarkan sebuah kriteria atau indikator yang telah ditetapkan sebelumnya. Hasil dari evaluasi ini dapat digunakan untuk membuat keputusan, melakukan perbaikan, atau mengidentifikasi peluang perbaikan yang dapat meningkatkan kualitas atau kinerja dari hal atau objek yang dievaluasi. Dengan demikian, evaluasi memiliki peran yang penting dalam membantu mencapai tujuan yang diinginkan [8].

C. ISO/IEC 27001

ISO/IEC 27001 adalah standar internasional yang memberikan panduan komprehensif untuk mengidentifikasi, menilai, dan mengelola risiko keamanan informasi dalam sebuah organisasi. Standar ini tidak hanya fokus pada aspek teknis, tetapi juga mencakup pengelolaan orang, proses, dan kebijakan terkait dengan keamanan informasi. Dengan demikian, implementasi ISO 27001 tidak hanya melibatkan pengaturan infrastruktur teknologi yang aman, tetapi juga mengharuskan organisasi untuk memiliki prosedur yang jelas dalam manajemen sumber daya manusia yang Terlibat dalam bidang keamanan informasi [9].

Struktur organisasi ISO 27001 dibagi menjadi dua bagian utama,yaitu :

1. Klausul (proses yang wajib) adalah persyaratan yang harus ditaati oleh organisasi dalam menerapkan Sistem Manajemen Keamanan Informasi (SMKI) menggunakan standar ISO 27001. Klausul ini bertujuan untuk memberikan kerangka kerja yang komprehensif dan terstruktur bagi organisasi dalam mengelola dan menjaga keamanan informasi secara efektif.

2. AnneX A (Kontrol Keamanan) adalah dokumen referensi yang tersedia dan dapat digunakan sebagai panduan untuk menentukan jenis kontrol keamanan yang perlu diimplementasikan dalam Sistem Manajemen Keamanan.

III. METODE

Pada Gambar 1, dapat ditemukan metode yang digunakan dalam menjalankan audit keamanan informasi [10].

GAMBAR 1. ALUR PENELITIAAN

A. Identifikasi Proses Bisnis

Menganalisis proses bisnis yang tengah berlangsung serta teknologi informasi yang telah diterapkan di pusat data X melalui peninjauan umum dan evaluasi audit keamanan sebelumnya, seperti rencana penanganan risiko, kebijakan, prosedur, dan peraturan. Dari analisis ini, dapat dipahami lebih lanjut tentang kelebihan dan kekurangan sistem keamanan informasi yang ada di pusat data X. Keadaan ini menjadi dasar untuk memberikan rekomendasi dan langkah-langkah perbaikan yang diperlukan guna meningkatkan keamanan informasi dan memastikan bahwa pusat data X mematuhi standar keamanan yang relevan.

B. Menetapkan Lingkup dan Tujuan Audit

Penjelasan tentang ruang lingkup dari penelitian ini mencakup tiga pendekatan utama, yaitu kuesioner, wawancara mendalam, studi lapangan, dan tinjauan literatur.

Ketiga metode ini digunakan untuk mendapatkan pemahaman yang *holistik* dan mendalam terhadap subjek penelitian. Dalam implementasi lingkup penelitian ini, acuan utama adalah standar ISO 27001:2022 yang menjadi landasan bagi praktik keamanan informasi. Hal ini mencakup penerapan Aspek-Aspek kunci yang tercantum dalam standar tersebut, yang menjadi fokus utama evaluasi dan analisis.

Tabel 1 memberikan pemetaan yang jelas antara klausul-klausul yang terdapat dalam ISO 27001:2022 dan hasil tinjauan literatur yang telah dilakukan [11].

TABEL 1
PEMETAAN KLAUSUL DAR ISO 27001

Klausul	Deskripsi
5	Pengendaliaan Operasional *(Operational Controls)*
6	Orang *(People Controls)*
7	Teknologi *(Physical Controls)*
8	Fisik *(Technologi Controls)*

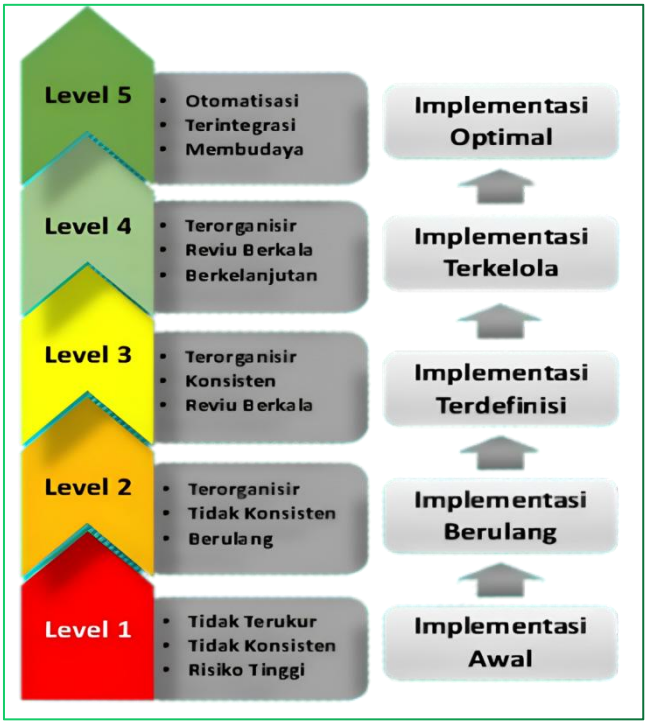
C. Melaksanakan Audit Kepatuhan

Proses audit ini melibatkan tahapan-tahapan penting yang dimulai dengan pembuatan kuesioner yang akan diberikan kepada responden [12]. Kuesioner dirancang secara teliti untuk mencakup segala aspek yang relevan dan memberikan data yang diperlukan dalam penilaian keamanan informasi. Setelah kuesioner disebar dan data terkumpul, langkah selanjutnya adalah pengumpulan data dari berbagai sumber yang telah diidentifikasi. Data yang terkumpul kemudian dianalisis secara terstruktur dan sistematis. Dengan demikian, proses audit ini tidak hanya mencakup pembuatan kuesioner dan pengumpulan data, tetapi juga meliputi analisis data secara mendalam untuk memperoleh pemahaman yang komprehensif tentang status keamanan informasi di pusat data X. Analisis yang terstruktur ini menjadi landasan untuk menyusun rekomendasi dan strategi perbaikan yang dapat meningkatkan keamanan informasi secara efektif.

D. Menentukan Maturity level

Langkah selanjutnya adalah mengembangkan *Maturity level*, yang merupakan proses pengelolaan dan pengendalian tingkat kematangan keamanan informasi. Tingkat kematangan ini didasarkan pada metode evaluasi organisasi yang memungkinkan evaluasi dimulai Mulai dari level 1 (Implementasi Awal) hingga level 5 (Implementasi Optimal).

Gambar 2 Menggambarkan urutan tingkat kematangan keamanan informasi yang mencerminkan perkembangan organisasi dalam meningkatkan keamanan informasi dari tahap awal hingga tahap optimal. Dalam mengelola *Maturity level*, organisasi fokus pada implementasi strategi, kebijakan, dan praktik terbaik untuk meningkatkan tingkat kematangan. Setiap level *Maturity level* mewakili tahap tertentu dalam perjalanan meningkatkan keamanan informasi, mulai dari tahap awal hingga tahap optimal di mana organisasi telah mencapai tingkat kematangan yang maksimal dalam manajemen keamanan informasi. Dengan demikian, pengelolaan dan pengendalian *Maturity level* menjadi kunci dalam upaya pusat data X untuk meningkatkan keamanan informasi, memastikan sistem keamanan informasi mencapai tingkat kematangan yang diinginkan, dan berkelanjutan dalam menjaga keamanan informasi secara efektif.



Gambar 2. Urutan Tingkatan *Maturity Level*
Sumber : BSSN, 2023 (Laporan Kinerja Tahunan)

TABEL 2
SKOR *MATURITY* KEAMANAN SIBER PADA CSM
(*CYBER SECURITY MATURITY*)

e-ISSN: 2548-6861

Tingkat Kematangan	Skor
Level I	0,00 - 1,50
Level II	1,51 - 2,49
Level III	2,50 - 3,49
Level IV	3,50 - 4,49
Level V	4,50 - 5,00

Sumber : BSSN, 2023 (Laporan Kinerja Tahunan 2023)

IV. HASIL DAN PEMBAHASAN

Data yang digunakan dalam penelitian ini diperoleh melalui tiga metode utama pengumpulan informasi, yaitu kuisioner, wawancara, dan observasi. Setelah semua data dari berbagai sumber terkumpul, tahap analisis pun dilakukan secara terstruktur untuk mengurai hasil dari respons kuisioner serta informasi yang terungkap melalui proses wawancara dan observasi.

Hasil dari audit yang dilakukan secara menyeluruh menunjukkan gambaran yang komprehensif terhadap tingkat kematangan sistem keamanan informasi dalam konteks yang diteliti. Hal ini mengarah pada pemahaman yang lebih mendalam mengenai aspek mana yang telah mencapai tingkat kematangan tertinggi dan di mana terdapat potensi untuk perbaikan lebih lanjut.

A. Hasil Keseluruhan Maturity level

Standar ISO 27001:2022 yang digunakan melibatkan beberapa Kontrol Keamanan. terdiri dari 4 klausul, Dari empat klausul tersebut, terdapat 93 kontrol keamanan yang diuraikan dalam standar ISO 27001:2022. Kontrol keamanan ini dirancang untuk membantu organisasi melindungi informasi secara efektif melalui penerapan langkah-langkah yang sesuai dengan kebutuhan dan risiko yang dihadapi oleh organisasi tersebut. Dari 93 kontrol keamanan yang ada dalam standar ISO 27001:2022, dapat dikonversi menjadi serangkaian pertanyaan assessment yang lebih mendalam. Pertanyaan-pertanyaan ini kemudian dapat dikelompokkan ke dalam beberapa aspek utama, seperti yang di tunjukkan pada Tabel 2. Hal ini memungkinkan untuk melakukan evaluasi yang lebih *holistik* terhadap implementasi keamanan informasi dalam suatu organisasi, serta memberikan pemahaman yang lebih mendalam mengenai sejauh mana organisasi telah mematuhi standar ISO 27001:2022.

TABLE 2. PENGELOMPOKAN ASPEK PADA KONTROL KEAMANAN

Aspek	Deskripsi
Tata Kelola	Aspek tata kelola terdiri dari sub aspek kesadaran, audit, kontrol, pemenuhan, kebijakan, dan proses
Identifikasi	Aspek identifikasi terdiri dari sub aspek manajemen aset, inventaris, manajemen risiko, prioritas, pelaporan, dan klasifikasi.
Proteksi	Aspek proteksi terdiri dari sub aspek jaringan, aplikasi, pengguna, manajemen identitas dan akses, cloud, dan data.
Deteksi	Aspek deteksi terdiri dari sub aspek perubahan, monitor, peringatan, pemberitahuan, intelijen, dan pelaporan.
Respon	Aspek respon terdiri dari penahanan, penanggulangan, pemulihan, Kegiatan Paska Insiden, dan pelaporan.

Dari hasil nilai rata-rata respon dari responden pada berbagai aspek ISO 27001, diperoleh nilai tingkat kematangan (*Maturity level*) yang mencerminkan seberapa matang atau berkembangnya sistem keamanan informasi dalam *pusat data X*. Proses ini melibatkan analisis mendalam terhadap respons yang diberikan oleh responden terhadap setiap pertanyaan dalam kuesioner terkait keamanan informasi. Tabel *3* kemudian digunakan sebagai representasi visual dari hasil perhitungan kuesioner tersebut. Tabel tersebut mencakup data-data yang signifikan dalam mengevaluasi kesiapan dan efektivitas sistem keamanan informasi, yang menjadi landasan dalam menetapkan langkah-langkah perbaikan atau pengembangan lebih lanjut untuk mencapai tingkat kematangan yang lebih tinggi dalam hal keamanan informasi.

TABLE 3. LEVEL KEMATANGAN
(*MATURITY LEVEL)*

Tata Kelola		Identifikasi		Proteksi		Deteksi		Respon	
4,66		4,61		4,62		4,75		4,72	
Kesadaran	4,71	Manajemen Aset	4,25	Jaringan	4,43	Perubahan	5,00	Penahanan	4,50
Audit	4,33	Inventaris	4,60	Aplikasi	4,70	Monitor	4,79	Penanggulangan	4,80
Kontrol	4,70	Manajemen Risiko	4,46	Pengguna	4,56	Peringatan	4,50	Pemulihan	5,00
Pemenuhan	5,00	Prioritas	5,00	Manajemen Identitas dan Aset	4,77	Pemberitahuan	5,00	Kegiatan Paska Insiden	4,75
Kebijakan	4,70	Pelaporan	4,33	Cloud	4,43	Intelijen	5,00	Pelaporan	4,57
Proses	4,50	Klasifikasi	5,00	Data	4,86	Pelaporan	4,20		

Gambar : BSSN, 2023

LEVEL MATURITY **4.67**

Maturity level terkini yang diperoleh memberikan gambaran bahwa tingkat kematangan tertinggi terdapat pada Aspek Deteksi dalam Keamanan Informasi, yang mencapai nilai 4.75. Di sisi lain, nilai terendah tercatat pada Aspek Identifikasi dengan sub aspek Manajemen Aset, Manajemen Risiko, dan Pelaporan, yang mencapai nilai 4.61. Dari analisis ini, ditemukan bahwa rata-rata keseluruhan mencapai 4.67, mengindikasikan bahwa organisasi telah

mencapai tingkat kematangan yang baik secara keseluruhan, meskipun masih terdapat ruang untuk perbaikan khususnya pada aspek-aspek yang mencatat nilai lebih rendah.

B. Uji One Way Anova

Uji One Way Anova dilakukan dalam tiga tahap:

1.Melakukan Uji Normalitas menggunakan metode *Shapiro wilk*

2.Melakukan Uji *Homogenitas varians*

3.Melakukan Uji One Way Anova

Kriteria pengambilan keputusan dalam uji normalitas::

1.Jika nilai signifikansi (Sig.) > 0,05, maka data dianggap berdistribusi normal.

2.Jika nilai signifikansi (Sig.) < 0,05, maka data berdistribusi tidak normal.

TABLE 4. *TESTS OF NORMALITY*

Tests of Normality

		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Aspek	Statistic	df	Sig.	Statistic	df	Sig.
Nilai	Tata Kelola	,243	6	,200*	,938	6	,642
	Identifikasi	,219	6	,200*	,872	6	,232
	Proteksi	,194	6	,200*	,911	6	,441
	Deteksi	,275	6	,174	,818	6	,085
	Respon	,182	5	,200*	,961	5	,815

*. This is a lower bound of the true significance.
a. Lilliefors Significance Correction

Interpretasi Output Uji Anova One Way Anova

1. Mengamati Perbedaan Rata-Rata Nilai dari Kelima Aspek

Berdasarkan output SPSS *"Descriptives",* kita dapat mengamati perbedaan rata-rata nilai dari kelima aspek keamanan informasi dengan rincian sebagai berikut:

1). Aspek Tata Kelola memiliki rata-rata nilai sebesar 4,6567.
2). Aspek Identifikasi memiliki rata-rata nilai sebesar 4,6067.
3). Aspek Proteksi memiliki rata-rata nilai sebesar 4,6250.

4). Aspek Deteksi memiliki rata-rata nilai sebesar 4,7483.

5). Aspek Respon memiliki rata-rata nilai sebesar 4,7240.

Oleh karena itu, secara deskriptif dapat disimpulkan bahwa aspek Deteksi memiliki rata-rata nilai tertinggi, yaitu sebesar 4,7483.

TABLE 5. *DESCRIPTIVES*

Descriptives

Nilai

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean Lower Bound	95% Confidence Interval for Mean Upper Bound	Minimum	Maximum
Tata Kelola	6	4,6567	,22616	,09233	4,4193	4,8940	4,33	5,00
Identifikasi	6	4,6067	,32703	,13351	4,2635	4,9499	4,25	5,00
Proteksi	6	4,6250	,18008	,07352	4,4360	4,8140	4,43	4,86
Deteksi	6	4,7483	,33289	,13590	4,3990	5,0977	4,20	5,00
Respon	5	4,7240	,19781	,08846	4,4784	4,9696	4,50	5,00
Total	29	4,6703	,25014	,04645	4,5752	4,7655	4,20	5,00

2. Menguji Kesamaan Varian (Uji Homogenitas)

Berdasarkan output SPSS "Test Homogeneity of Variance", diperoleh nilai signifikansi (sig) sebesar 0,389. Karena nilai sinifikansi 0,389 > 0,05, maka dapat disimpulkan bahwa varian kelima nilai dari aspek yang dibandingkan tersebut adalah sama atau homogen. Sehingga asumsi homogenitas dalam uji one way anova terpenuhi.

TABLE 6. *TESTS OF HOMOGENEITY OF VARIANCES*

Tests of Homogeneity of Variances

		Levene Statistic	df1	df2	Sig.
Nilai	Based on Mean	1,202	4	24	,336
	Based on Median	,718	4	24	,588
	Based on Median and with adjusted df	,718	4	16,419	,592
	Based on trimmed mean	1,078	4	24	,389

3.Melakukan uji Anova untuk menentukan apakah terdapat perbedaan signifikan antara rata-rata kelima sampel.

Dasar pengambilan keputusan dalam analisis Anova adalah sebagai berikut:

1).Jika nilai signifikansi (sig) > 0,05, maka dapat disimpulkan bahwa rata-rata tidak berbeda secara signifikan antara kelompok-kelompok yang dibandingkan.

2).Jika nilai signifikansi (sig) < 0,05, maka dapat disimpulkan bahwa terdapat perbedaan rata-rata yang signifikan antara kelompok-kelompok yang dibandingkan.

Berdasarkan output Anova tersebut, dengan nilai signifikansi (sig) sebesar 0,862 yang lebih besar dari 0,05, dapat disimpulkan bahwa rata-rata dari keempat nilai aspek keamanan informasi tersebut tidak berbeda secara signifikan.

e-ISSN: 2548-6861

TABLE 7. ANOVA

ANOVA

Nilai

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	,089	4	,022	,320	,862
Within Groups	1,663	24	,069		
Total	1,752	28			

4. Melakukan uji Post-Hoc untuk menentukan kelompok mana yang memiliki rata-rata nilai yang sama dan yang tidak sama.

Pengujian Tukey HSD adalah metode untuk melakukan perbandingan antar kelompok dalam analisis varians guna menentukan apakah rata-rata nilai kelompok tersebut berbeda secara signifikan. Dalam konteks ini, kita membandingkan rata-rata nilai antara aspek tata kelola dan aspek identifikasi. Perbedaan rata-rata antara kedua aspek tersebut adalah 0,050. Angka ini dihitung dengan cara mengurangi rata-rata nilai aspek tata kelola (4,656) dengan rata-rata nilai aspek identifikasi (4,6067), seperti yang tercantum dalam output deskriptif. Sementara itu, perbedaan antara rata-rata nilai dari Dalam kasus ini, untuk menguji apakah terdapat perbedaan signifikan antara rata-rata nilai dari dua aspek, kita melihat interval kepercayaan 95% untuk perbedaan rata-rata antara kedua aspek tersebut, yaitu dari -0,3978 *(Lower Bound)* hingga 0,4978 *(Upper Bound).* Kemudian, berdasarkan hasil output uji Multiple Comparisons dari SPSS, diperoleh nilai signifikansi (sig) sebesar 0,997, yang lebih besar dari nilai alpha yang umumnya digunakan (0,05).

Dengan demikian, dapat disimpulkan bahwa rata-rata nilai antara aspek tata kelola dan aspek identifikasi tidak berbeda secara signifikan. Artinya, perbedaan rata-rata nilai secara deskriptif antara kedua aspek keamanan informasi tersebut tidaklah signifikan.

TABLE 8. Post Hoc Tests

Multiple Comparisons

Dependent Variable: Nilai

Tukey HSD

(I) Aspek	(J) Aspek	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
Tata Kelola	Identifikasi	,05000	,15199	,997	-,3978	,4978
	Proteksi	,03167	,15199	1,000	-,4161	,4794
	Deteksi	-,09167	,15199	,973	-,5394	,3561
	Respon	-,06733	,15941	,993	-,5369	,4023
Identifikasi	Tata Kelola	-,05000	,15199	,997	-,4978	,3978
	Proteksi	-,01833	,15199	1,000	-,4661	,4294
	Deteksi	-,14167	,15199	,882	-,5894	,3061
	Respon	-,11733	,15941	,946	-,5869	,3523
Proteksi	Tata Kelola	-,03167	,15199	1,000	-,4794	,4161
	Identifikasi	,01833	,15199	1,000	-,4294	,4661
	Deteksi	-,12333	,15199	,925	-,5711	,3244
	Respon	-,09900	,15941	,970	-,5686	,3706
Deteksi	Tata Kelola	,09167	,15199	,973	-,3561	,5394
	Identifikasi	,14167	,15199	,882	-,3061	,5894
	Proteksi	,12333	,15199	,925	-,3244	,5711
	Respon	,02433	,15941	1,000	-,4453	,4939
Respon	Tata Kelola	,06733	,15941	,993	-,4023	,5369
	Identifikasi	,11733	,15941	,946	-,3523	,5869
	Proteksi	,09900	,15941	,970	-,3706	,5686
	Deteksi	-,02433	,15941	1,000	-,4939	,4453

5. Melihat Kesamaan Rata-Rata Nilai dari Kelima Aspek Keamanan Informasi

Untuk menilai kesamaan rata-rata, kita akan menggunakan output Tukey HSD. Pada subset ini terdapat data nilai dari aspek identifikasi, proteksi, tata kelola, respon, dan deteksi. Dengan demikian, dapat disimpulkan bahwa rata-rata nilai kelima aspek keamanan informasi tersebut tidak menunjukkan perbedaan signifikan. Secara lebih lanjut, hal ini mengindikasikan bahwa rata-rata nilai antara aspek identifikasi, proteksi, tata kelola, respon, dan deteksi adalah sama.

TABLE 9. *Homogeneous Subsets*

Nilai

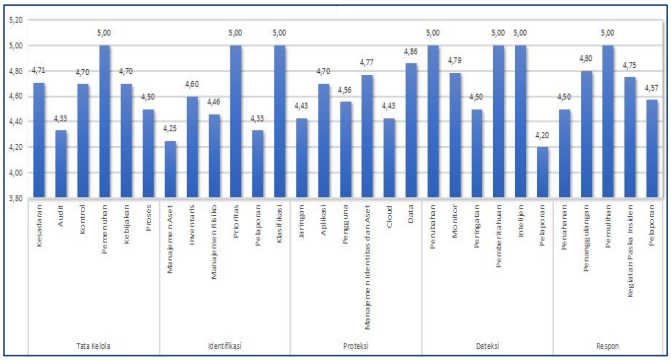
Tukey HSD[a,b]

Aspek	N	Subset for alpha = 0.05 1
Identifikasi	6	4,6067
Proteksi	6	4,6250
Tata Kelola	6	4,6567
Respon	5	4,7240
Deteksi	6	4,7483
Sig.		,889

Means for groups in homogeneous subsets are displayed.
a. Uses Harmonic Mean Sample Size = 5,769.
b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

C. *Analisis GAP*

Grafik pada Gambar 3 memvisualisasikan Perbandingan antara tingkat kematangan yang ada saat ini dengan tingkat kematangan yang diinginkan atau diharapkan dalam konteks keamanan informasi di pusat data X. Grafik tersebut memberikan gambaran yang jelas tentang seberapa jauh organisasi telah mencapai tujuan dalam meningkatkan keamanan informasi, serta seberapa mendekati atau jauhnya dari tingkat kematangan yang diharapkan atau diinginkan. Dengan visualisasi ini, manajemen dan pihak terkait dapat dengan mudah melihat gap antara kenyataan Saat ini dan tujuan yang ingin dicapai dalam hal keamanan informasi. Hal ini menjadi dasar yang kuat untuk mengevaluasi keberhasilan implementasi strategi dan langkah-langkah yang telah diambil, serta merencanakan tindakan perbaikan yang diperlukan untuk mencapai tingkat kematangan yang diharapkan.



Gambar. 3 Perbandingan Nilai *Maturity level* saat ini dengan Nilai *Maturity level* yang diharapkan

Gambar : BSSN, 2023

Menurut hasil penghitungan tingkat kematangan, ditemukan bahwa tingkat kematangan keamanan informasi di berbagai aspek pada umumnya berada di Level 4 (Implementasi Terkelola). Meskipun demikian, temuan ini menyoroti kebutuhan akan peningkatan keamanan informasi dan pengembangan lebih lanjut menuju tahap yang lebih optimal. Tujuannya adalah untuk mencapai tingkat kematangan yang lebih tinggi, yaitu Level 5 (Implementasi Optimal). Dengan mengetahui bahwa organisasi telah mencapai tingkat kematangan yang dikelola dengan baik, namun masih memiliki potensi untuk meningkatkan keamanan informasi ke tingkat yang optimal, ini memberikan arah dan motivasi untuk mengembangkan strategi dan tindakan perbaikan yang diperlukan. Langkah-langkah ini dapat mencakup peningkatan kebijakan keamanan, penguatan infrastruktur teknologi informasi, pelatihan lebih lanjut kepada personel, dan implementasi praktik terbaik dalam manajemen risiko. Dengan fokus pada pengembangan ke tahap yang lebih baik, organisasi pusat data X akan dapat mengoptimalkan keamanan informasi mereka, meningkatkan ketahanan terhadap ancaman keamanan, dan memastikan perlindungan yang lebih efektif terhadap data dan informasi sensitif.

D. *Rekomendasi*

Dari analisis tingkat kematangan pusat data X, terdeteksi variasi yang menciptakan kesenjangan antara data-data yang diamati. Berdasarkan temuan dan kesenjangan yang teridentifikasi, peneliti mengembangkan solusi perbaikan khusus yang ditujukan untuk berbagai sub Aspek di pusat data X. Sub aspek ini mencakup Jaringan, Cloud, Audit, Manajemen Asset, Manajemen Risiko, Pelaporan Identifikasi, Pelaporan deteksi. Tabel yang disajikan menjelaskan rekomendasi-rekomendasi tersebut dengan rinci. Rekomendasi ini disusun berdasarkan analisis mendalam terhadap setiap sub aspek keamanan informasi, dengan tujuan meningkatkan tingkat kematangan pusat data X secara *holistik*. Setiap rekomendasi disesuaikan dengan kebutuhan dan tantangan spesifik yang dihadapi oleh pusat

e-ISSN: 2548-6861

data X dalam aspek keamanan informasi. Dengan menerapkan rekomendasi ini, diharapkan pusat data X dapat mengatasi kesenjangan yang ada, meningkatkan sistem keamanan informasinya, dan mencapai tingkat kematangan yang lebih tinggi sesuai dengan standar keamanan yang diinginkan.

Berikut adalah tabel yang menjelaskan rekomendasi - rekomendasi tersebut.

TABLE 10. REKOMENDASI

NO	SUB ASPEK	REKOMENDASI
1.	Jaringan	Untuk keamanan yang optimal, disarankan agar outbound network traffic hanya mengizinkan lalu lintas yang diperlukan oleh organisasi. ini penting untuk mencegah kebocoran data, serangan malware, dan memastikan bahwa hanya komunikasi yang sah dan diperlukan yang diperbolehkan keluar dari jaringan organisasi
2.	Cloud	Pentingnya melakukan pengujian integritas data secara rutin setiap bulan terhadap data yang telah di-backup sangatlah vital. Hal ini dilakukan dengan melakukan proses restore data untuk memastikan bahwa backup data dapat dipulihkan dengan sukses dan tidak terjadi kerusakan atau kehilangan informasi yang penting.
3.	Audit	Sebaiknya organisasi mempunyai kebijakan yang mewajibkan implementasi perlindungan data pribadi dan melakukan evaluasi secara berkala untuk memastikan kepatuhan terhadap kebijakan tersebut.
4	Manajemen Asset	Sebaiknya Pemantauan kapasitas dilakukan secara teratur untuk memastikan bahwa semua perangkat dan aplikasi sesuai dengan kebutuhan. Hal ini penting agar organisasi dapat mengidentifikasi kebutuhan kapasitas yang tepat, menghindari over-provisioning, serta memastikan ketersediaan dan kinerja optimal dari infrastruktur IT.
5	Manajemen Risiko	Sebaiknya organisasi menerapkan monitoring secara berkala untuk memastikan kepatuhan Terhadap kebijakan yang membatasi penggunaan aset organisasi untuk keperluan pribadi. Hal ini penting untuk memastikan bahwa sumber daya organisasi digunakan secara efisien dan sesuai dengan tujuan bisnis, serta mengurangi risiko terkait penggunaan yang tidak sah atau tidak sesuai kebijakan.
6.	Pelaporan Identifikasi	Untuk memastikan keamanan sistem secara menyeluruh, sebaiknya aspek keamanan mempertimbangkan kapasitas server danperangkat jaringan secara menyeluruh. Hal ini penting karena kapasitas yang memadai memungkinkan sistem untuk mengelola beban kerja dengan baik, mengurangi risiko kegagalan atau kinerja rendah yang dapat dimanfaatkan oleh pihak yang tidak bertanggungjawab.
7.	Pelaporan Deteksi	Disarankan agar pusat data X melakukan peninjauan metrik keamanan peristiwa setiap minggu untuk memastikan pemantauan yang lebih efektif dan respons yang cepat terhadap potensi ancaman keamanan.

V. KESIMPULAN

Dari temuan dalam penelitian yang menggunakan ISO 27001, dapat disimpulkan bahwa:

1. Hasil perhitungan *Maturity level* menunjukkan bahwa tingkat kematangan di pusat data X adalah 4,67, yang berada pada level 5, yaitu tingkat implementasi optimal. Mengindikasikan bahwa pusat data X telah mencapai tingkat kematangan yang baik secara keseluruhan, namun masih terdapat ruang untuk perbaikan pada sub aspek yg rendah.

2. Dari temuan dalam penelitian yang menggunakan ISO 27001:2022, bisa disimpulkan bahwa penerapan standar tersebut secara signifikan meningkatkan keamanan informasi di organisasi. Temuan ini menunjukkan bahwa ISO 27001 memberikan kerangka kerja yang kokoh dan terstruktur untuk manajemen keamanan informasi, sehingga membantu organisasi dalam mengidentifikasi, mengelola, dan mengurangi risiko keamanan secara efektif. Selain itu, penerapan standar ini juga berkontribusi pada peningkatan kesadaran dan kepatuhan terhadap kebijakan keamanan informasi di seluruh organisasi.

3. Hasil dari evaluasi ini dapat digunakan untuk membuat keputusan, melakukan perbaikan, atau mengidentifikasi peluang perbaikan yang dapat meningkatkan kualitas atau kinerja dari hal atau objek yang dievaluasi.

4. Dengan penilaian tingkat kematangan (M*aturity level*) keamanan informasi pusat data X, organisasi dapat mengetahui seberapa jauh mereka telah mencapai tujuan dalam meningkatkan keamanan informasi serta seberapa dekat mereka dengan tingkat kematangan yang diharapkan.

UCAPAN TERIMA KASIH

Penulis ingin mengucapkan terima kasih kepada pusat data X atas bantuan dan pembelajaran yang berharga. Juga, terima kasih tak terhingga kepada para pembimbing magang di Perusahaan atas dedikasi luar biasa mereka dan bimbingan yang telah memberikan ilmu yang sangat berharga. Khususnya, penulis ingin menyampaikan banyak terimakasih kepada Bapak Andy Triwinarko sebagai pembimbing dan penasihat, yang telah memberikan pengajaran dan bimbingan yang sangat berarti selama proses penelitian ini. Semoga ungkapan terima kasih ini mencerminkan ketulusan kepada semua pihak yang telah berperan penting dalam kesuksesan penelitian ini.

DAFTAR PUSTAKA

[1.] Pradipta. Y. C, Rahardja, dan Sitokdana M. N. N., "Audit Sistem Manajemen Keamanan Informasi Pusat Teknologi Informasi Dan Komunikasi Penerbangan Dan Antariksa (Pustikpan) Menggunakan Sni Iso/Iec 27001:2013," Sebatik, vol. 23, no. 2, hal. 352–358, 2019, doi: 10.46984/sebatik.v23i2.782.

[2.] A, Irfansyah. (2023). ISO 27001 dan CIA Triad, Apa Hubngannya dalam Keamanan Informasi. edupart. https://eduparpusat data X.id/blog/insight/hubungan-iso-27001-dan-cia-triad-dalam-keamanan-informasi/#:~:tepusat data Xt=ISO 27001 adalah standar internasional,dan mengurangi risiko keamanan informasi.

[3.] Admin QMS. (2023). Menilik Perbedaan ISO 27001:2022 dengan ISO 27001:2013. QMS. https://qms-consulting.id/menilik-perbedaan-iso-270012022-dengan-iso-270012013/

[4.] B, Kara. (2022). Sistem Manajemen Keamanan Informasi ISO 27001. Mutu Internasional. https://mutucertification.com/iso-27001-adalah-keamanan-informasi/

[5.] Telkom Indonesia. (2022). Memahami Apa Itu pusat data X dan Fungsinya.MyCarier.https://mycarrier.telkom.co.id/id/article/memahami-apa-itu-pusat data X-dan-fungsinya

[6.] Riadi, I. (2016). Analisis Keamanan Informasi Berdasarkan Kebutuhan Teknikal Dan Operasional Mengkombinasikan Standar ISO 27001 : 2005 Dengan *Maturity level* (Studi Kasus Kantor Biro Teknologi Informasi PT . pusat data XYZ). *Seminar Nasional Teknologi Informasi Dan Multimedia 2016*, *4*(1), 1–2.

[7.] S. Kom, "Analisis Implementasi Keamanan Sistem Informasi pada Perusahaan Perakitan Elektronik," vol. 01, no. 01, 2020.

[8.] Haqqi, D. P., Ghozali, K., & Hari, V. (2022). Evaluasi Tata Kelola Keamanan Informasi Berdasarkan Standar ISO / IEC 27001 : 2013 dengan Menggunakan Model SSE-CMM (System Security Engineering Capability Maturity Model) pada Perusahaan Daerah Air Minum Surya Sembada Kota Surabaya. 11(2).

[9.] Informasi, A. T., Manajemen, M., & Its, T. (2015). Audit Teknologi Informasi – Magister Manajemen Teknologi ITS Surabaya 2015. 2013–2016.

[10.] T. Kristanto, M. Sholik, D. Rahmawati, dan M. Nasrullah, "Analisis Manajemen Keamanan Informasi Menggunakan Standard ISO 27001 : 2005 Pada Staff IT Support Di Instansi pusat data XYZ," vol. 02, no. 02, hal. 30–33, 2019.

[11.] Center for Internet Security, "Policy Template Guide," 2015, [Daring]. Tersedia pada: https://www.cisecurity.org/-/jssmedia/Project/cisecurity/cisecurity/data/media/img/uploads/2021/11/NIST-Cybersecurity-Framework-Policy-Template Guide-v2111Online.pdf

[12.] Komputer, J. S. (2020). Audit Keamanan Sistem Informasi Pada Data Center Menggunakan Standar SNI-ISO 27001. 4(September), 581–587.