Informatics for Educators And Professionals : Journal of Informatics
Vol. 9, No. 2, Desember 2024, 126 - 134
E-ISSN: 2548-3412
Terakreditasi **SINTA Peringkat 5**
Surat Keputusan Direktur Jenderal Pendidikan Tinggi, Riset, dan Teknologi, Nomor: 230/E/KPT/2022
masa berlaku mulai Volume 5 Nomor 1 Tahun 2020 sampai Volume 9 Nomor 2 Tahun 2024

Perencanaan Keamanan Sistem Informasi Menggunakan ISO/IEC 27001:2005

Dede Hendrik[1,*]

[1]Teknik Informatika; Universitas Sehati Indonesia; Jl. Jl. Raya Kosambi - Telagasari Dusun Kawali, Pancawati, Kec. Klari, Karawang, Jawa Barat 41371; e-mail: dede.hendrik@usindo.co.id

* Korespondensi: e-mail: dede.hendrik@usindo.co.id

Diterima: 11 November 2024 ; Review: 19 November; Disetujui: 6 Desember 2024

Cara sitasi: Hendrik D. 2024. Perencanaan Keamanan Sistem Informasi Menggunakan ISO/IEC 27001:2005. Informatics for Educators and Professionals : Journal of Informatics. Vol.9 (2): 126 – 136.

Abstrak : Sistem Manajemen Kemanan Informasi (SMKI) merupakan sebuah framework untuk membangun suatu kemanan sistem jaringan komputer atau sistem informasi. Dalam hal ini Sistem Informasi Terpadu (SITU) merupakan sistem informasi yang akan dijadikan pokok bahasan penelitian. SITU Merupakan sistem informasi pada suatu kampus yang menangani transaksi akademik baik mahasiswa, dosen dan alumni. Setelah di implementasikan ternyata SITU memiliki beberapa ancaman yang diperkirakan akan menghambat layanan publik untuk akes ke SITU tersebut, misalnya: terjadi bencana alam, kerusakan bangunan, kesalahan manusia, ulah orang yang tidak bertanggung jawab (*Hacker*) dll. Maka kami anggap itu semua dapat merugikan Perguruan tinggi. Dengan adanya kemungkinan terjadi ancaman atau kelemahan tersebut, penulis mencoba menganalisis, mempelajari dan merencanakan untuk meminimalisir kemungkinan terjadinya hal tersebut, dengan cara membuat Perencanaan Keamanan Informasi Sistem Informasi Terpadu (SITU) Perguruan tinggi. Dengan standar ISO/IEC 27001:2005.

Kata kunci: ISO ISMS 27001, keamanan, SITU, SMKI

Abstrack *: Information Security Management System (SMKI) is a framework for building a computer network security system or information system. In this case, the Integrated Information System (SITU) is the information system that will be the subject of research. SITU is an information system on a campus that handles academic transactions for students, lecturers and alumni. After being implemented, it turned out that SITU had several threats which were expected to hamper public health services to SITU, for example: natural disasters, building damage, human error, the actions of irresponsible people (hackers), etc. So we consider that all of this can be detrimental to universities. With the possibility of these threats or weaknesses occurring, the author tries to analyze, study and plan to minimize the possibility of this happening, by creating a Higher Education Integrated Information System Security Plan (SITU). With ISO/IEC 27001:2005 standards*.

Keywords: ISO ISMS 27001, Security, SITU, SMKI

1. Pendahuluan

Peran teknologi informasi saat ini telah menjadi hal yang strategis, makan semua sektor sudah bergeser cara kerjanya menjadi berbasis komputerisasi, yang mana komputerisasi akan berhungungan langusung dengan pengguna. Ketika semua hal sudan terkomputerisasi maka keamanan sistem menjadi hal yang tidak kalah penting, karena transaksi yang tinggi pada suatu sistem semakin tinggi pula ancaman dan kemungkinan-kemungkinan terjadinya gangguan pada sistem tersebut. Untuk mengantisipasi hal tersebut maka perlunya diterapkan kemanan untuk

sistem yang digunakan, dalam hal ini metode yang digunakan adalah ISO ISMS 27001 yang dapat mengantisipasi terjadinya gangguan berupa, peretasan, gangguan bencana alam, keslahan pengguna dan lain sebagainya.

2. Metode Penelitian

ISO/IEC 27001 adalah Komisi Elektroteknik Internasional (IEC) dan Organisasi Internasional untuk Standardisasi (ISO) merilis standar keamanan informasi pada bulan Oktober 2005. Menurut ISO 27001 (2005), standar ini telah menggantikan BS-77992:2002.

Organisasi dari berbagai kalangan, mulai dari bisnis nirlaba hingga entitas sektor publik, dipersilakan untuk tunduk pada ISO/IEC 27001: 2005. ISO/IEC 27001:2005 menjabarkan aturan untuk Sistem Manajemen Keamanan Informasi (SMKI), yang juga dikenal sebagai SMKI, dalam kaitannya dengan total risiko bisnis yang dihadapi oleh organisasi. Aturan-aturan ini termasuk mengembangkan, meluncurkan, menjalankan, memantau, menganalisis, dan mendokumentasikan sistem. Standar SMKI, yang didasarkan pada kelompok ISO/IEC 27001, akan dijelaskan di bawah ini.

Tabel 1. ISO/IEC 27000

27000 Fundamental & Vocabulary		
27005: Risk Management	27001: ISMS	
	27002: Code of practices for ISMS	
	27003: Implementastion guidance	
	27004: Matric & Measuremen	
27006: Guidelines on ISMS Acreditation		
27007: Guidelines for ISMS Auditing		

Sumber: [6]

ISO/IEC 27001 mendefinisikan kebutuhan ISMS (Sistem Manajemen Keamanan Informasi). Dengan penerapan IMS ini, Anda dapat yakin bahwa operasi bisnis Anda akan kembali berjalan dalam waktu singkat jika terjadi gangguan pada operasi Anda yang disebabkan oleh bencana alam, peristiwa bencana, atau pelanggaran besar dalam keamanan sistem informasi Anda.

Informasi standar keamanan disusun dalam skema bernomor oleh Organisasi Standar Internasional (ISO), seperti yang terlihat pada grafik di atas. Seri ini disebut ISO 27000. Berikut ini adalah penjelasan ringkas tentang elemen-elemen bernomor pada gambar tersebut:
ISO 27000, dokumen definisi-definisi Keamanan Informasi yang digunakan sebagai istilah dasar dalam serial ISO 27000.
ISO 27001, berisi persyaratan standar yang harus dipenuhi untuk membangun SMKI.
ISO 27002, terkait dengan dokumen ISO 27001, namun dalam dokumen ini berisi panduan praktis (code of practice) teknik keamanan informasi.
ISO 27003, berisi panduan implementasi SMKI perusahaan.
ISO 27004, berisi matriks dan metode pengukuran keberhasilan implementasi SMKI.
ISO 27005, dokuman panduan pelaksanaan manajemen resiko.
ISO 27006, dokumen panduan untuk sertifikasi SMKI perushaan.
ISO 27007, dokumen panduan audit SMKI Perusahaan.

3. Hasil dan Pembahasan

3.1 Perbedaan Standar ISO/IEC 27001 dengan Keamanan SITU:
Seperti yang telah diuraikan terkait standar ISO/IEC 27001 dari segi fisik dan komunikasi dan keamanan SITU, maka didapat perbandingan seperti pada tabel dibawah ini:

Tabel 2. Perbandingan standar ISO/IEC 27001 dengan keamanan SITU

	Standar ISO	Keamanan SITU
ISO/IEC 27001:2005	Physical and environmental security	Tidak ada
	Comunication and oprations management	Ada dan tidak lengkap

Sumber: [6]

Keterangan Tabel:
Ada dan lengkap: Dimaksudkan bahwa standar yang bersangkutan telah ada sesuai dengan standar ISO 27001 dan telah diterapkan secara keseluruhan

Ada dan tidak lengkap: Dimaksudkan bahwa standar yang bersangkutan ada tetapi tidak sepenuhnya ada dan lengkap seperti yang dimaksudka dalam standar ISO 27001 dan belum keseluruhan untuk diterapkan.
Tidak ada: Dimaksudkan bahwa standar yang bersangkutan belum ada dan belum diterapkan seperti yang ada dalam ISO 27001.

3.2 Keamanan yang bersifat fisik (*physical security*)

Hal tersebut mencakup ketersediaan fasilitas, alat, dan media yang digunakan oleh individu. Dahulu kala, ada pencuri komputer (cracker) tertentu yang sering mencari file di tempat sampah untuk mencari file yang mungkin berisi informasi terkait keamanan. Sebagai contoh, ada beberapa kasus ketika kata sandi yang dicoret-coret atau instruksi yang dibuang ditemukan. Materi-materi ini tidak dihancurkan. Keamanan fisik ini juga bisa mencakup masalah seperti penyadapan atau mendapatkan akses ke kabel atau komputer yang sedang digunakan.

Tabel 3. Tabel hasil survei perbandingan ISO dengan SITU

No	ISO/IEC 27001:2005	Artinya	SITU			Penanggung jawab
1	**Daerah Aman**	Menempatkan semua aset di tempat yang aman dan tidak memicu hal-hal yang akan merugikan instansi terkait, misalnya: menyimpan perangkat tidak di sembarang tempat, penempatan mesin seperti server dan perangkat lain di area yang aman dari pencurian dan kesalahan manusia serta mudah di pantau.				
	Perimeter keamanan fisik	Waspada terhadap area berbahaya, seperti selalu memantau ruangan atau area yang kritis terhadap ancaman, misalnya:	**Ada**	**Ada dan tidak lengkap**	**Tidak ada**	
		• Ruang server ancamannya dari pencuri dan hacker, binatang dan bencana alam. Apakah ada prosedur untuk penanganan ancaman tersebut?			√	Pengelola infrastruktur teknologi
		• Perangkat seperti akses poin, kabel LAN yang tersebar di area umum pengguna. Apakah ada pengamanan seperti rak akses poin, kunci gembok untk akses poin dan pengaman kabel?			√	Pengelola infrastruktur teknologi
	Kontrol entri fisik (mengawasi aktivitas ruangan)	• Memastikan bahwa semua pengunjung ke ruangan server di awasi. Apakah ada prosedur yang mengatur hal tersebut?		√		Pengelola infrastruktur teknologi
		• Tersedianya buku tamu untuk pengunjung untuk mencatat identitas dan keperluan pengunjung serta waktu masuk sampai pengunjung keluar			√	Pengelola infrastruktur teknologi
		dari area ruangan server. Sudah adakah buku tamu untuk pengunjung ruang server?			√	Pengelola infrastruktur teknologi
		• Memeriksa terlebih dahulu barang bawaan pengunjung dan di pastikan tidak membara barang apapun tanpa seizin petugas penanggung jawab ruangan server. Apakah ada prosedur yang mengatur hal tersebut?			√	Pengelola infrastruktur teknologi
		• Mendampingi pengunjung selama di area ruangan server. Adakah petugas khusus yang mendampingi pengunjung selama di dalam ruang server?		√		Pengelola infrastruktur teknologi
	Mengamankan kantor, ruangan dan fasilitas.	Pengamanan ini biasanya dilakukan oleh petugas keamanan seperti satpam yang dapat mengawasi kantor dengan di bantu fasilitas seperti CCTV. Apakah ada fasilitas CCTV untuk membantu pengamanan tersebut?	√			Pengelola infrastruktur teknologi

No	ISO/IEC 27001:2005	Artinya	SITU			Penanggung jawab
2	**Peralatan keamanan**	Tersedianya peralatan yang dapat membantu pengamanan area ruangan server seperti:				Pengelola infrastruktur teknologi
		• Rak server	√			------- " "--------
		• Kunci pintu	√			------- " "--------
		• Kunci rak server	√			Pengelola infrastruktur teknologi
		• CCTV	√			
	Penempatan peralatan untuk mengamankan aset					
		Menyimpan peralatan secara teratur serta aman dari bahaya dan ancaman seperti:				
		• Kebakaran			√	
		• Kebocoran gedung			√	
		• Binatang			√	
		• Pencurian			√	
	Melengkapi utilitas (peralatan keamanan seperti obeng, tang, baud, mur dll)	Melengkapi semua kebutuhan utilitas bertujuan untuk memudahkan penanganan kerusakan. Adakah perlengkapan untuk mendukung utilitas tersebut?	√			Pengelola infrastruktur teknologi
	Keamanan kabel	Melindungi kabel dari kesalahan manusia, binatang maupun dari faktor bangunan. Sudah adakah pelindung kabel untuk mendukung keamanan ini?	√			
	Mengamankan area pembuangan (sampah)	Menghancurkan kertas sisa coret-coretan yang penting dan tidak akan di gunakan kembali karena sudah ada back up, menghancurkan jenis-jenis konektor yang sudah tidak di pakai atau rusak.				
		• Adakah alat penghancur untuk kebutuhan mendukung hal tersebut?			√	Pengelola infrastruktur teknologi
		• Sudah adakah prosedur yang mengatur hal ini?			√	
		Total	**7**	**2**	**10**	

Sumber: Hasil Penelitian (2024)

Penjelasan: dilihat dari hasil survei bahwa prosedur yang mengatur tentang keamanan SITU sesuai dengan standar ISO/IEC 27001:2005 dari segi fisik adalah seperti pada table, artinya bahwa SITU belum memenuhi syarat ISO baik dari sisi *fhisical security,* karena jumlah dari kategori **Tidak Ada** masih cukup banyak yang belum ada dan belum diterapkan terhadap SITU.

3.3 Keamanan dari data dan media serta teknik komunikasi (*communications security*)

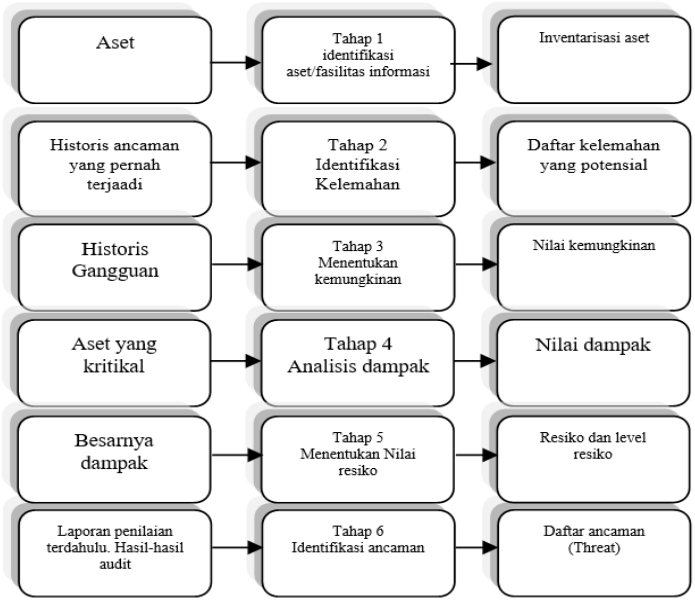
Penjelasan: dilihat dari hasil survei bahwa prosedur yang mengatur tentang keamanan SITU sesuai dengan standar ISO/IEC 27001:2005 dari segi komunikasi adalah seperti pada table, artinya bahwa SITU belum memenuhi syarat ISO baik dari sisi *Comunication security,* karena jumlah dari kategori **Ada Dan Tidak Lengkap** masih cukup banyak yang belum terpenuhi dan belum diterapkan terhadap SITU.

Penilaian Resiko (*Risk Assesment*)

Penilaian resiko *(Risk Assesment)* adalah mengelola risiko dimulai dengan langkah ini. Untuk menentukan ancaman eksternal apa saja yang ada dan kelemahan apa saja yang ada pada keamanan informasi organisasi, penilaian risiko dilakukan. Metode penilaian resiko terdiri dari 6 (enam) tahapan yaitu:

1. Identifikasi aset
2. Identifikasi kelemahan *(vulnerability)*
3. Menentukan kemungkinan keamanan *(probability)*
4. Analisa dampak *(impact analysis)*
5. Menentukan nilai resiko
6. Identifikasi ancaman *(threat)*

Berikut adalah gambar tahapan penilaian resiko dari mulai input, tahapan dan output.



Sumber: [6]

Gambar 1. Tahapan Penilaian Resiko

Analisa dampak *(impact analysis)*

Analisa dampak adalah analisis dampak bisnis, kadang-kadang disingkat menjadi BIA, adalah proses menilai potensi efek negatif dari suatu risiko, seperti kelemahan atau bahaya, pada operasi organisasi atau proses internal. Yang relevan dengan nilai risiko adalah kriteria dampak yang mengevaluasi pengaruhnya terhadap perusahaan. Lihatlah contoh nilai dampak ini.

Tabel 4. Analisis nilai dampak

Resiko	Nilai BIA	Keterangan	Range
LOW	Minor Critical	Tidak mengganggu jalanya proses bisnis, nilai kerugian kecil	< 0.3 %
MEDIUM	Critical	Menggangu jalanya proses bisnis, nilai kerugian besar	> 0.4%
HIGH	Mayor Critical	Proses bisnis terhenti, nilai kerugian sangat besar	> 0.7%

Sumber: Hasil Penelitian (2024)

Ket: presentase di ukur dari maksimal biaya kerugian dan nilai maksimal adalah 1.0 %

Menentukan nilai resiko *(Risk Value)*

Nilai resiko *(risk value)* adalah gambaran dari seberapa besar akibat yang akan diterima organisasi jika ancamana *(threat)* yang mengakibatkan kegagalan keamanan informasi terjadi. Nilai resiko dapat ditentukan dengan dua metode, antara lain:

a) Metode kualitatif

Dilakukan dengan membuat perkiraan terhadap biaya yang akan ditanggung atau dikeluarkan oleh organisasi akibat resiko yang diterima. Nilai resikonya bisnisnya ditentukan dengan range:

- LOW RISK (Resiko yang diterima kecil)
- MEDIUM RISK (Resiko yang diterima sedang)
- HIGH RISK (Resiko yang diterima tinggi)

b) Metode kuantitatif

Metode kuantitatif adalah metode penilaian resiko dengan pendekatan matematis. Dengan metode ini nilai resiko dapa dihitung dengan menggunakan rumus sebagai berikut:

Perhitungan nilai resiko dengan pendekatan matematis:

Risk value = NA x BIA xNT

Dimana:

Nilai aset (Asset value): NA

Analisa dampak bisnis: BIA

Nilai ancaman: NT

Identifikasi Ancaman *(Threat Identification)*

Threat atau ancaman itu adalah potensi yang muncul dalam jalannya proses bisnis organisasi karena insiden yang tidak diinginkan. Tujuan dari mengidentifikasi kegagalan sistem adalah untuk memastikan bahwa kegagalan sistem yang mungkin terjadi dapat dipahami dan diatasi di dalam organisasi. Tiga sumber bahaya tersebut adalah bumi (alam), laut (lingkungan), dan manusia (ancaman manusia). Beberapa penjelasan diberikan di bawah ini.

Tabel 5. Kemungkinan Gangguan Keamanan Terhadap Komunikasi

Gangguan	Jenis	Probabilitas	Jumlah Probabilitas
Pemantauan Log (petugas yang bertugas untuk mengawasi aktivitas pengakses SITU secara rutin)	Threat	High	0,9
Jumlah Ancaman = 5	**Jumlah rata-rata Probabilitas**		**2,8**

Sumber: Hasil Penelitian (2024)

Nilai Jumlah probabilitas dihasilkan dari klasifikasi probabilitas dengan rentang nilai yang dapat didefinisikan sebagai berikut:

- Low : Nilai rata-rata probabilitas 0,1-0,3
- Medium : Nilai rata-rata probabilitas 0,4-0,6
- High : Nilai rata-rata probabilitas 0,7-1,0

Berdasarkan tabel diatas dapat dihitung nilai ancaman dari suatu aset yang dihitung dengan rumus:
Nilai ancaman (NT) = ∑PO x ∑ Ancaman
Dimana:
∑PO: Jumlah probabilitas
∑ Ancaman: Jumlah ancaman terhadap informasi
Setelah diperoleh data ancaman dari sisi fisik dan komunikasi terhadap SITU adalah:

Tabel 6. Probabilitas Ancaman Yang Terjadi Terhadap Fisik

Gangguan	Jenis	Probabilitas	Jumlah Probabilitas
Daerah Aman (Pengamanan area yang berhubungan dengan penempatan perangkat)	Vulnerability	High	0,9
Peralatan Keamanan (peralatan yang dapat membantu pengamanan area ruangan)	Vulnerability	High	0,9
Jumlah Ancaman = 2	**Jumlah rata-rata Probabilitas**		**1,8**

Sumber: Hasil Penelitian (2024)

Dari data tersebut dapat dihitung nilai ancaman (NT) terhadap fisik :
NT (fisik) = ∑PO / ∑ Ancaman
= 1,8 / 2 = **0,9 (High)**

Maka dapat kita simpulkan bahwa nilai ancaman terhadap fisik adalah 0,9 dimana 0,9 ini termasuk kategori ancaman **(High)** sesuai dengan rentang yang terdapat pada klasifikasi ancaman.

Tabel 7. Probabilitas Kemungkinan Ancaman Keamanan Terhadap Komunikasi

Gangguan	Jenis	Probabilitas	Jumlah Probabilitas
Prosedur Oprasional (prosedur yang mengatur tentang penggunaan SITU)	Vulnerability	Low	0,2
Perlindungan terhadap kode berbahaya (Pengawasan log)	Threat	High	0,9
Back up informasi (pemindahan data dari server ke tempat yang dianggap lebih aman untuk penyimpanan)	Vulnerability	Medium	0,4
Keamanan jaringan (Pemenliharaan keberlangsungan koneksi jaringan utama)	Threat	Medium	0,4
Pemantauan Log (petugas yang bertugas untuk mengawasi aktivitas pengakses SITU secara rutin)	Threat	High	0,9
Jumlah Ancaman = 5	**Jumlah rata-rata Probabilitas**		**2,8**

Sumber: Hasil Penelitian (2024)

Dari data tersebut dapat dihitung nilai ancaman (NT) terhadap aset komunikasi adalah:
NT (komunikasi) = ∑PO / ∑ Ancaman
= 2,8 / 5 = **0,56 (Medium)**
Maka dapat kita simpulkan bahwa nilai ancaman terhadap komunikasi adalah 2,8 dimana 2,8 ini termasuk kategori ancaman **(Medium)** sesuai dengan rentang yang terdapat pada klasifikasi ancaman.

3. Hasil dan Pembahasan

Berdasarkan hasil dari analisis yang telah di laksanakan maka dapat menghasilkan beberapa kebijakan yang telah di buat dengan mengacu terhadap klausul 9 dan 10 yaitu klausul 9 mengenai keamanan fisik dan lingkungan dan kalusul 10 mengenai keamanan komunikasi dan oprasi, untuk di terapkan kedalam SITU.

Tabel 8. Hasil Rancangan Kalusul 9

Klausul: 9 Keamanan Fisik dan lingkungan								
9.1 Daerah aman		Objek	Kontrol	Pelaku	Dasar	Status		
9.1.1	Perimeter keamanan fisik	Ruangan Server	Dipastikan batas area ruangan server yang ada di lantai 6 gedung jalak harupat berukuran 3 x 4 meter, ini adalah area yang harus di lindungi dari ancaman atau kelemahan dari ancaman bahaya hacker, kerusakan bangunan, pencurian maupun binatag.	Pengelola server	Ruangan server adalah tempat penyimpanan server SITU, dimana di dalam server Terdapat data-data dan informasi penting akademik dan itu merupakan aset	ST	SP	BT
9.1.1	Perimeter keamanan fisik	Ruangan Server	Harus terdapat beberapa lapis pengamanan untuk area ruang server seperti: - Tralis pada jendela dan pintu	Pengelola server	Lapisan keamanan akan memperlambat penyusup masuk ke	ST	SP	BT

Sumber: Hasil Penelitian (2024)

Ket:
ST = Sudah Terlaksana (artinya kebijakan itu sudah ada dan dijalankan)
SP = Sedang Proses (artinya kebijakan itu masih dalam proses penerapan)
BT = Belum Terlaksana (artinya kebijakan itu belum ada dan belum dijalankan serta belum ada proses pengadaan)

Tabel 9. Hasil Rancangan Kalusul 10

Klausul: 10 Keamanan komunikasi dan oprasi								
10.1 Prosedur oprasional		Objek	Kontrol	Pelaku	Dasar	Status		
10.1.1	Prosedur oprasi	SITU	Harus ada prosedur penanganan error ketika terjadi problem terhadap SITU, misalnya terkena virus dan mengakibatkan SITU tidak dapat diakases, terkena oleh serangan *hacker* yang merusak data didalam aplikasi	Pengelola SITU	Mempercepat proses penanganan error, memudahkan pengelola SITU dalam penanganan	ST	SP	BT
10.1.1	Prosedur oprasi	SITU	Kontak petugas yang dapat menangani problem terhadap SITU harus dimiliki oleh bagian pengelola SITU.	Pengelola SITU	Mempercepat proses penanganan error, memudahkan pengelola SITU dalam penanganan	ST	SP	BT

Sumber: Hasil Penelitian (2024)

Ket:
ST = Sudah Terlaksana (artinya kebijakan itu sudah ada dan dijalankan)

SP = Sedang Proses (artinya kebijakan itu masih dalam proses penerapan)
BT = Belum Terlaksana (artinya kebijakan itu belum ada dan belum dijalankan serta belum ada proses pengadaan)
Kesimpulan:
Bahwa setelah di terapkannya standarisasi dari ISO/IEC 27001:2005 ini dapat meminimalisir gangguan yang kemungkinan akan terjadi ancaman terhadap SITU, bahwa probabilitas ancaman adalah:
NT (komunikasi) = ∑PO / ∑ Ancaman
Eksisting:
= 1,8 / 2 = **0,9 (High) Fisik**
= 2,8 / 5 = **0,56 (Medium) Komunikasi**
Setelah di terapkan Kebijakan:
= 0,6 / 2 = **0,3 (Low) Fisik**
= 1,5 / 5 = **0,3 (Low) Komunikasi**

dengan menerapkan standar ini dapat kita lihar perubahan yang terjadi setelah di terapkanya standar ISO/IEC 27001:2005 tersebut.

Tabel 10. Kesimpulan Tabel Hasil Survei.

Kategori	Ada	Ada dan Tidak Lengkap	Tidak ada	Probabilitas Ancaman
Fhisical	19	0	0	Low
Comunication	9	0	0	Low

Sumber: Hasil Penelitian (2024)

4. Kesimpulan

Dari hasil penelitian tersebut dapat kita simpulkan bahwa keamanan Sistem Informasi Terpadu (SITU) adalah Hasil analisis menemukan bahwa SITU masih dikategorikan rentan terhadap ancaman kemanan data, karena masih ditemukan celah-celah yang bersifat LOW (lemah) terhadap ancaman-ancaman data dari segi fisik dan komunikasi data.

Tempat penyimpanan server masih sangat rentan karena belum maksimalnya backup data ketika terjadi bencana alam dan kerusakan bangunan pada tempat penyimpanan server.

Saran, perlunya di terapkan SMKI dengan Standar ISO ISMS 27001 agar dapat mencegah terjadinya ancaman-ancaman yang mungkin terjadi kapanpun.

Referensi

[1] Yuwono St, Pratama N, Afifah V, Minggu P, Selatan J. Re-Assessment Konsistensi Dokumen Kontrol Sertifikasi Iso 27001:2013 (Isms) Di Bagian Komunikasi Satelit Monitoring Pt. Bank Bri, Tbk. 2020.
[2] Risna R, Amaliah Y, Yunita S. Implementasi Kriptografi Pada Pengamanan Data Pembayaran Piutang Pelanggan Menggunakan Vigener Cipher. Sebatik 2022; 26:525–34. Https://Doi.Org/10.46984/Sebatik.V26i2.2061.
[3] Nasiri A. Evaluasi Tingkat Kapabilitas Keamanan Sistem Informasi Menggunakan Kerangka Kerja Cobit 2019 2023; 9:34–41.
[4] Glavan Af, Gheorghica D, Croitoru V. Multi-Access Edge Computing Analysis Of Risks And Security Measures. Vol. 68. 2023.
[5] Syani M, Mahestro Tresna R, Firdaus Ea, Faisal Nugraha F, Bandung Pt. Penerapan Network Access Control Autentikasi Internal Network Security Protokol 802.1 X. Nuansa Informatika 2022;16.
[6] Budhiningtias Winanti M, Dzulhan I. Audit Keamanan Sistem Informasi Akademik Dengan Kerangka Kerja Iso 27001 Di Program Studi Sistem Informasi Unikom. 2020.
[7] Watkins Sg. Iso/Iec 27001:2022. It Governance Publishing; 2022. Https://Doi.Org/10.2307/J.Ctv30qq13d.
[8] Iso/Iec 27001:2022. Information Security, Cybersecurity And Privacy Protection-Information Security Management Systems-Requirements. 2022.

[9] Syarif Ra, Nugroho A. Analisis Tingkat Kematangan Sistem Manajemen Keamanan Informasi Direktorat Jenderal Perbendaharaan Diukur Dengan Menggunakan Indeks Keamanan Informasi (Studi Kasus: Aplikasi Span) 1) 2). 2020.
[10] Hidaya N, Jatnika I. Perancangan Sistem Manajemen Keamanan Informasi Data Center Standart Sni Isoiec 27001 2013. Jurnal Sistem Informasi Musirawas 2022.
[11] Kurniasih S, Masitoh S. Audit Sistem Informasi Human Resource Information System (Hris) Pada Bagian Human Resource (Hr) Menggunakan Framework Cobit 5 Domain Dss01. Nuansa Informatika 2021;15.
[12] Parama Yoga T, Maharani V, Maulana Nd. Audit Keamanan Sistem Informasi Puskesmas Dengan Standar Iso/Iec 27001:2013 Dan Framework Cobit 5. Nuansa Informatika 2024; 18:2614–5405.
[13] Djebbar F, Nordstrom K. A Comparative Analysis Of Industrial Cybersecurity Standards. Ieee Access 2023; 11:85315–32. Https://Doi.Org/10.1109/Access.2023.3303205.
[14] Algi A, S Reksoprodjo Ah, Agus Gultom Rg. Analisis Standar Iso/Iec 27001: 2013 Sebagai Strategi Keamanan Informasi Di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia. 2020.
[15] Kurii Y, Opirskyy I. Iso 27001: Analysis Of Changes And Compliance Features Of The New Version Of The Standard. Cybersecurity: Education, Science, Technique 2023;3:46–55. Https://Doi.Org/10.28925/2663-4023.2023.19.4655.
[16] Barraza De La Paz Jv, Rodríguez-Picón La, Morales-Rocha V, Torres-Argüelles Sv. A Systematic Review Of Risk Management Methodologies For Complex Organizations In Industry 4.0 An