Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 8 Nomor 1, Maret 2024, pp. 72-84
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Evaluasi Keamanan Informasi Menggunakan ISO/IEC 27001: Studi Kasus PT XYZ

Dayyan Fatih[1], Rizal Fathoni Aji[2]
[1,2]Universitas Indonesia, Indonesia
e-mail: [1]dayyanf@gmail.com, [2]rizal@cs.ui.ac.id

Abstract

PT XYZ is one of the government-owned enterprises of the Republic of Indonesia that engaged in agribusiness. PT XYZ already has an information security management system (ISMS), but there are still several obstacles that are found, such as low personnel attention to information security, the need to remain compliant with government regulations, to technical constraints that arise, so PT XYZ wants to improve its information security-related capabilities. This study aims to determine the current condition of the existing ISMS at PT XYZ and provide recommendations for improving the ISMS. This research uses information security controls based on the ISO/IEC 27001: 2022 standard to get the information security condition gap, then divides the information technology (IT) assets owned by the IT division of PT XYZ into several categories using the ISO/IEC 27005: 2018 standard, and conducts a risk assessment using the gap result data, namely the selected information security controls. Then recommendations were made based on the ISO/IEC 27002:2022 standard. The findings of this study were the discovery of 17 ISO/IEC 27001:2022 control activities whose value results were not maximised. These 17 controls are then divided into 3 categories of recommendations based on the urgency, from the results of the risk assessment.

Keywords*: information security, information security management system, evaluation, compliance audit, ISO 27001*

Abstrak

PT XYZ merupakan salah satu Badan Usaha Milik Pemerintah (BUMN) Republik Indonesia yang bergerak pada bidang agribisnis. PT XYZ sudah memiliki sistem manajemen keamanan informasi (SMKI), namun masih ditemukan beberapa kendala seperti atensi personil terhadap keamanan informasi yang rendah, kebutuhan untuk tetap patuh dengan peraturan pemerintah, hingga kendala teknis yang muncul, sehingga PT XYZ ingin meningkatkan kapabilitas terkait keamanan informasi yang mereka miliki. Penelitian ini bertujuan untuk mengetahui kondisi terkini dari SMKI yang ada pada PT XYZ dan memberikan rekomendasi peningkatan SMKI. Penelitian ini menggunakan kontrol keamanan informasi berdasarkan standar ISO/IEC 27001:2022 untuk mendapatkan gap kondisi keamanan informasi, kemudian membagi aset teknologi informasi (TI) yang dimiliki oleh divisi TI PT XYZ menjadi beberapa kategori menggunakan standar ISO/IEC 27005:2018, dan melakukan risk assessment yang memakai data hasil gap yaitu kontrol keamanan informasi yang terpilih. Kemudian dilakukan rekomendasi yang disusun berdasarkan standar ISO/IEC 27002:2022. Temuan dari penelitian ini adalah ditemukannya 17 aktivitas kontrol ISO/IEC 27001:2022 yang hasil nilainya belum maksimal. 17 kontrol ini kemudian dibagi menjadi 3 kategori rekomendasi berdasarkan urgensi peningkatan yang sesuai dari hasil risk assessment.

Kata kunci*: keamanan informasi, sistem manajemen keamanan informasi, evaluasi, audit kepatuhan, ISO 27001*

1. PENDAHULUAN

Teknologi informasi (TI) dan komunikasi telah memberikan dampak yang sangat besar bagi perkembangan berbagai sektor kehidupan, termasuk sektor bisnis dan pemerintahan [1]. Terdapat studi yang menyebutkan bahwa manajemen perusahaan yang menerapkan aspek TI mendapatkan manfaat seperti

produktifitas personil yang meningkat, meningkatkan efisiensi dan penghematan biaya perusahaan, dan juga telah membuka peluang baru bagi terciptanya ekosistem digital yang terintegrasi dan inklusif [1].

Namun, seiring dengan pemanfaatan TI yang semakin berkembang, peluang rawannya keamanan *cyber* serta informasi yang dimiliki organisasi turut meningkat, dimana studi lain mencatut bahwa kecerdasan buatan (AI) dan *machine learning* (20%), adopsi *cloud* (19%), dan kemajuan pengembangan dalam identitas pengguna serta manajemen akses (15%) akan memiliki pengaruh terbesar pada strategi risiko cyber responden selama beberapa tahun ke depan [2]. Temuan lain adalah rencana implementasi teknologi baru akan dilakukan secara kombinasi, yang dengan signifikan meningkatkan kompleksitas lingkungan digital yang perusahaan miliki, dan menyoroti kebutuhan untuk melakukan manajemen risiko digital ketika transformasi digital dilakukan [2]. Suatu perusahaan harus menyeimbangkan nilai dari teknologi baru dan potensi eksposur ruang *cyber* yang yang menyertainya untuk mengelola risiko keamanan digital, teknologi, dan informasi yang dimiliki secara efektif pada beberapa tahun mendatang [2].

Keamanan informasi adalah salah satu aspek penting dalam era digital, di mana informasi memiliki nilai dan peran yang sangat besar bagi semua aspek kehidupan . Aktivitas mitigasi risiko digital, teknologi, dan siber (dimana aspek informasi termasuk dalam bidang ketiganya) merupakan salah satu prioritas tertinggi yang harus dilakukan oleh suatu perusahaan mulai pada tahun 2024 mendatang [3]. Fakta ini tidak terlepas dari serangan siber yang semakin masif dan bervariatif, dimana serangan ini dapat dirangkai dan menjadi kombinasi yang membahayakan perusahaan.

Sektor Badan Usaha Milik Negara (BUMN) tidak terlepas sebagai tempat yang sedang melaksanakan mitigasi risiko. BUMN adalah salah satu pilar penting dalam perekonomian nasional yang memiliki peran strategis dalam menyediakan barang dan jasa publik, mengelola sumber daya alam, serta mendukung pembangunan nasional. Untuk mewujudkan potensi yang dimiliki, BUMN perlu melakukan transformasi digital, yang bertujuan untuk meningkatkan kinerja operasional, meningkatkan kualitas layanan kepada pelanggan dan masyarakat, meningkatkan nilai tambah bagi pemegang saham dan pemangku kepentingan lainnya, serta meningkatkan daya tahan dan adaptabilitas di tengah perubahan lingkungan bisnis yang dinamis [4].

Namun dengan demikian, transformasi digital di BUMN juga membawa tantangan dan risiko baru, khususnya terkait dengan aspek keamanan informasi. Perlu adanya upaya yang sistematis dan terpadu untuk meningkatkan keamanan informasi di BUMN sebagai bagian dari transformasi digital [5]. Keamanan informasi di BUMN juga perlu didukung oleh kebijakan dan regulasi yang jelas dan konsisten, baik dari internal BUMN maupun dari pemerintah sebagai pemegang saham mayoritas [6]. Salah satu upaya yang dapat dilakukan dalam meningkatkan keamanan informasi yang dimiliki adalah dengan mengevaluasi keamanan informasi yang ada pada perusahaan BUMN tersebut.

PT XYZ adalah Badan Usaha Milik Pemerintah (BUMN) Republik Indonesia, yang bergerak pada bidang agribisnis dan menjadi perusahaan induk (*holding*

company). PT XYZ ingin meningkatkan kapabilitas terkait keamanan informasi yang mereka miliki. Berdasarkan wawancara dan analisis yang dilakukan dengan manajemen PT XYZ, terdapat beberapa temuan seperti adanya peraturan terbaru dari pemerintah untuk BUMN [7], yang mewajibkan BUMN menjaga keamanan informasi yang mereka miliki, PT XYZ yang ingin kembali melakukan evaluasi keamanan informasi, masih ditemukannya kendala terkait keamanan informasi yang muncul, hingga atensi personil PT XYZ yang masih belum terlalu memperhatikan keamanan informasi yang sedang berjalan. Berdasarkan masalah yang ditemukan, perlu dilakukan kembali evaluasi keamanan informasi, yang kemudian hasil rekomendasinya akan meningkatkan keamanan informasi yang ada pada PT XYZ.

Setelah menjelaskan latar belakang, maka penelitian ini melakukan evaluasi keamanan informasi Menggunakan ISO/IEC 27001, dimana penelitian ini ditujukan untuk mengkaji kondisi terkini Sistem Manajemen Keamanan Informasi (SMKI) yang ada pada PT XYZ, mengetahui kontrol terkait keamanan informasi yang penerapannya dapat ditingkatkan dalam perusahaan, dan kemudian memberikan rekomendasi peningkatan sistem manajemen keamanan informasi di PT XYZ.

2. METODOLOGI PENELITIAN

Penelitian evaluasi keamanan informasi pada PT XYZ menggunakan metodologi klasifikasi *action research*, karena peneliti bekerja dengan praktisi (dalam hal ini PT XYZ) untuk mendapatkan pemahaman bersama tentang masalah organisasi yang kompleks, melakukan intervensi untuk memperbaiki situasi secara *real time*, dan mengkomunikasikan pengetahuan yang diperoleh setelah investigasi dilakukan [8]. Selain klasifikasi, jenis data yang dikumpulkan bersifat *mixed method* (kuantitatif dan kualitatif), dan proses pengumpulan data pada penelitian dilakukan dengan cara wawancara, penyebaran kuesioner, studi dokumen PT XYZ, serta observasi.

2.1. Alur Penelitian

Alur penelitian disusun berdasarkan langkah evaluasi keamanan informasi menggunakan tahapan PDCA (*Plan, Do, Check, Act*). Tahapan PDCA merupakan model penguraian masalah menggunakan empat langkah iteratif, dimana praktik ini umumnya digunakan dalam bidang pengendalian kualitas [9]. Pada penelitian tahapan PDCA dibatasi pada tahapan *Plan* saja, karena peneliti tidak bekerja pada PT XYZ serta terbatasnya waktu penelitian. Gambar 1 menggambarkan alur penelitian yang dilakukan.

Gambar 1. Alur Penelitian

a) Menetapkan Ruang Lingkup Dan Batasan SMKI
Pada tahap ini peneliti menentukan ruang lingkup dan batasan SMKI. Hasil akhir tahap ini yang didapatkan adalah ruang lingkup SMKI dari PT XYZ, dimana dijelaskan sebagai berikut:
1. Evaluasi keamanan informasi dilakukan hanya pada ruang lingkup PT XYZ saja sebagai perusahaan induk (*holding company*), tidak mencakup anak perusahaan/*subholding* yang dimiliki PT XYZ
2. Pada langkah analisis *gap*, pertanyaan yang disusun menjadi kuesioner hanya berdasarkan pada *Annex A* standar ISO/IEC 27001:2022 saja
3. Terkait identifikasi aset, hanya aset yang terkait dengan divisi TI PT XYZ saja yang disertakan
4. Penilaian risiko yang dilakukan mencakup hasil analisis *gap* kontrol yang bernilai *partial/none*, identifikasi aset kontrol tersebut, probabilitas dan dampak jika risiko terjadi, dan *gap* risiko yang diperoleh

b) Menganalisis *Gap* Keamanan Informasi
Setelah mendapatkan ruang lingkup, kemudian peneliti melakukan analisis *gap* keamanan informasi, untuk mengidentifikasi perbedaan kondisi keamanan informasi yang terdapat sekarang dengan kondisi keamanan yang diharapkan menggunakan domain kontrol yang tercantum pada standar ISO/IEC 27001. Hasil ini didapatkan dari penyusunan kuesioner yang didasarkan pada kontrol ISO/IEC 27001, wawancara, dan observasi, yang kemudian dipetakan ke dalam aspek dan kontrol obyektif ISO. Hasil yang didapatkan adalah penilaian skor SMKI yang ada pada saat ini.

c) Menyusun Identifikasi Aset
Pada tahap ini peneliti mengidentifikasi aset keamanan informasi yang termasuk pada ruang lingkup SMKI yang ada pada PT XYZ. Identifikasi aset ini dibantu dengan standar ISO/IEC 27005. Hasil yang didapatkan adalah klasifikasi aset keamanan informasi yang ada pada PT XYZ.

d) Melakukan *Risk Assessment*
Pada tahap ini dilakukan analisis probabilitas dan dampak risiko pada kegiatan perusahaan, dimana hal yang dianalisis adalah hasil *gap* kontrol informasi yang muncul. Hasil dari tahap ini adalah tingkatan risiko pada kontrol keamanan informasi yang kemudian dapat dipilih dan diprioritaskan.

e) Menetapkan Rekomendasi
Pada tahap ini kemudian ditetapkan rekomendasi sesuai dengan risiko yang sudah ditentukan sebelumnya, dimana penentuan rekomendasi ini menggunakan dokumen standar ISO/IEC 27002 sebagai pedoman.

2.2. Kuesioner

Kuesioner digunakan untuk menganalisis *gap* keamanan informasi yang ada pada PT XYZ dan pada saat penilaian risiko. Kuesioner disusun berdasarkan

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 8 Nomor 1, Maret 2024, pp. 72-84
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

pernyataan dari versi paling terbaru dari standar ISO/IEC 27001 (ISO/IEC 27001:2022). Untuk menilai kuesioner, digunakan skala rating. Skala ini awalnya berbentuk data kuantitatif yang kemudian ditafsirkan menjadi kualitatif, sehingga pada skala ini responden hanya mengetahui secara numerik saja [10]. Penelitian ini menggunakan skala nilai A, B, dan C, dengan definisi masing-masing nilai dijelaskan pada Tabel 1 berikut.

Tabel 1. Definisi Skala Nilai

Skala	Nilai	Keterangan
A	1	Aktivitas sudah seluruhnya dilakukan (*Complete*)
B	0,5	Hanya ada sebagian aktivitas yang sudah dilakukan (*Partial*)
C	0	Aktivitas belum pernah dilakukan sama sekali (*None*)

Standar ISO/IEC 27001:2022		Uraian Pertanyaan	Jawaban Mohon beri tanda '✓' pada kolom yang sesuai: - Kolom A : sudah sepenuhnya dilakukan - Kolom B : hanya sebagian yang dilakukan - Kolom C : sama sekali belum dilakukan			Keterangan (Apabila diperlukan, cantumkanlah keterangan untuk memperjelas suatu perilaku dalam kontrol; dan isilah 'NA' pada kolom ini jika pertanyaan tidak relevan terhadap kondisi perusahaan/*not applicable*)
			A	B	C	
5 - Kontrol Organisasi						
1	**5.1 Kebijakan Untuk Keamanan Informasi**	Apakah kebijakan terkait keamanan informasi sudah didefinisikan dan disetujui manajemen perusahaan?	✓			Sudah terdapat SOP yang mengatur.
		Apakah kebijakan tersebut sudah dipublikasikan dan diterima dengan personel/pihak lain yang relevan?	✓			*Top Level* pada organisasi menerima briefing tentang kondisi keamanan siber terkini lebih dari satu tahun sekali

Gambar 2. Contoh kuesioner pengendalian kontrol ISO 27001:2022

Gambar 2 merupakan contoh kuesioner yang digunakan untuk mengetahui bagaimana analisis *gap* keamanan informasi untuk mendapatkan perbedaan yang ada pada saat ini dengan domain dan kontrol yang tercantum dalam standar ISO/IEC 27001. Kuesioner penilaian ini berisi 118 pertanyaan, dimana setiap pertanyaan didasarkan pada 93 kontrol yang terdapat pada dokumen ISO/IEC 27001:2022 [6]. Jika terdapat kontrol yang memiliki nilai *partial* atau *none*, maka pada kontrol tersebut dilakukan penilaian risiko yang mungkin dapat muncul.

Kemudian dikumpulkan data aset yang dimiliki oleh divisi TI dari PT XYZ, yang kemudian aset tersebut dikategorisasi berdasarkan versi terbaru standar ISO/IEC 27005 (ISO/IEC 27005:2018). Tabel 2 merupakan definisi pengkategorian aset tersebut [11].

Tabel 2. Definisi Kategori Aset Berdasarkan ISO/IEC 27005:2018

No.	Aset Primer
1	Proses dan Aktivitas Bisnis

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 8 Nomor 1, Maret 2024, pp. 72-84
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

No.	Aset Primer
2	Informasi
3	Perangkat Keras (*Hardware*)
4	Perangkat Lunak (*Software*)
5	Jaringan (*Network*)
6	Personel/sumber daya manusia (*Personnel*)
7	Situs (*Site*)
8	Struktur Organisasi (*Organization*)

Setelah itu dilakukan pendefinisian risiko yang mungkin dapat terjadi. Risiko ini dinilai dengan cara mempertimbangkan *probability* (kemungkinan hal terjadi), *impact* (dampak yang dapat diberikan), beserta aset TI PT XYZ yang terkait dengan risiko tersebut. *Probability* dan *impact* dinilai dengan menggunakan rentang skor 1 (satu) sampai 5 (lima), yang dideskripsikan dalam Tabel 3.

Tabel 3. *Probability* dan *Impact* Risiko

Nilai Skor	Keterangan *Probability*	Keterangan *Impact*
1	*Remote* (sangat kecil kemungkinan terjadi)	*None* (tidak ada dampak)
2	*Unlikely* (kecil kemungkinan terjadi)	*Minor* (berdampak kecil)
3	*Possible* (bisa terjadi/sedang kemungkinan terjadi)	*Moderate* (berdampak sedang)
4	*Likely* (besar kemungkinan terjadi)	*Major* (berdampak besar)
5	*Almost Certain* (akan terjadi dalam hampir seluruh situasi)	*Catastrophic* (berdampak fatal)

Setelah dilakukan penentuan nilai *probability* dan *impact*, kemudian dilakukan penentuan nilai dari kedua aspek tersebut dengan cara melakukan perkalian antara nilai *probability* dan *impact*. Hasil perkalian akan menjadi *risk matrix* 5x5 yang nilainya dapat dilihat pada Tabel 4. Sedangkan, nilai kategori penilaian risiko digambarkan dalam Tabel 5.

Tabel 4. *Risk Matrix*

Probability / *Impact*	***Remote***	***Unlikely***	***Possible***	***Likely***	***Almost Certain***
None	1	2	3	4	5
Minor	2	4	6	8	10
Moderate	3	6	9	12	15
Major	4	8	12	16	20
Catastrophic	5	10	15	20	25

Tabel 5. Kategori Penilaian Risiko

Nilai Skor Risiko	Keterangan
1 - 5	*Negligible* (dapat diabaikan)
6 – 10	*Low* (kecil)
11 – 15	*Medium* (menengah)
15 - 20	*High* (tinggi)
21 - 25	*Extreme* (ekstrim)

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 8 Nomor 1, Maret 2024, pp. 72-84
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Salah satu contoh kuesioner penilaian risiko dapat dilihat pada Gambar 3 berikut ini.

Standar ISO/IEC 27001:2022	Risiko	Penyebab Risiko	Aset SMKI Yang Terkena Risiko	Akibat Risiko	Hasil Evaluasi Kontrol Yang Ada Pada Perusahaan	Penilaian Risiko				Skor Batas Aman	*Gap* Risiko
						Probabilitas	Dampak	Total Skor	Level Risiko		
5 - *Organizational Controls*											
5.3 Segregasi Peran	Adanya peluang kecurangan dan kesalahan terkait kontrol keamanan informasi	Tugas/bidang tanggung jawab beberapa jabatan yang saling bertentangan karena belum ada segregasi peran	Aset Pendukung Sumber Daya Manusia dan Organisasi yang terkait dengan peran/tugas suatu personil	Ada kemungkinan kolusi yang terjadi, kemudian kontrol menjaga keamanan informasi yang berkurang jika terjadi kesalahan/kecurangn	0%	3	3	9	*Low*	5	-4
5.7 *Threat Intelligence*	Ancaman keamanan informasi yang meningkat	Tidak adanya aksi *threat intelligence* yang mengumpulkan dan menganalisis ancaman perusahaan terkait KI serta lingkungannya	Seluruh aset primer dan pendukung yang berpotensi terkena risiko keamanan informasi	Peluang terjadinya insiden keamanan informasi semakin meningkat dan tidak adanya respon yang cepat jika terjadi suatu insiden	0%	2	4	8	*Low*	5	-3

Gambar 3. Kuesioner Penilaian Risiko

Setelah kuesioner dilakukan, kemudian dilakukan penentuan rekomendasi, dimana rekomendasi yang dicantumkan pada penelitian ini disusun berdasarkan standar ISO/IEC 27002:2022. Pembagian skala rekomendasi dibagi berdasarkan hasil nilai skor risiko yang diperoleh yang dijelaskan pada Tabel 6.

Tabel 6. Pendefinisian Skala Tingkat Rekomendasi

Nilai Skor Risiko	Keterangan	Rekomendasi
21 - 25	*Extreme* (ekstrim)	Urgensi Tinggi
15 - 20	*High* (tinggi)	
11 – 15	*Medium* (menengah)	Urgensi Menengah
6 – 10	*Low* (kecil)	Urgensi Rendah

3. HASIL DAN PEMBAHASAN

Pada bagian ini menjelaskan hasil evaluasi keamanan informasi yang dilakukan pada PT XYZ, dimana tersusun dari hasil analisis *gap* keadaan saat ini, identifikasi aset TI, penilaian risiko, serta rekomendasi.

3.1. Hasil Analisis Gap

Dari jumlah total 93 kontrol yang terdapat pada *Annex A* ISO/IEC 27001:2022, ditemukan 76 kontrol yang bernilai 1 (*complete*). Sebaliknya, terdapat 17 kontrol yang bernilai 0,5 (*Partial*) dan 0 (*None*). Hasil kontrol yang mendapatkan nilai *Partial* serta *None* dapat dilihat pada Tabel 7.

Tabel 7. Kontrol ISO/IEC 27001:2022 Yang Mendapat Nilai *Partial* dan *None*

Klausa	Kontrol Organisasi	Penilaian	
		Partial	None
Organizational Controls			
5.3	Segregasi Peran		✓

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 8 Nomor 1, Maret 2024, pp. 72-84
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

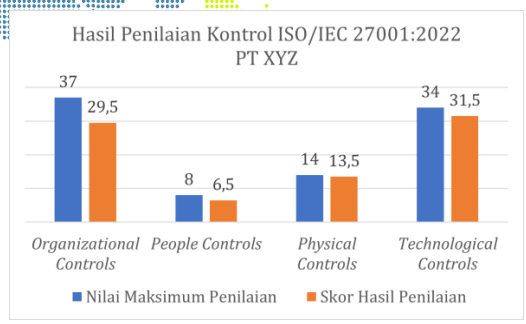
Klausa	Kontrol Organisasi	Penilaian	
		Partial	None
5.7	*Threat Intelligence*		✓
5.8	Keamanan Informasi Dalam Manajemen Proyek		✓
5.12	Klasifikasi Informasi	✓	
5.17	Informasi Autentikasi		✓
5.18	Hak Akses	✓	
5.20	Menangani Keamanan Informasi Dalam Perjanjian Dengan *Supplier*		✓
5.21	Mengelola Keamanan Informasi Dalam *ICT Supply Chain*	✓	
5.26	Respon Dalam Insiden Yang Menyangkut Keamanan Informasi	✓	
5.30	Kesiapan ICT Untuk Kesinambungan Bisnis	✓	
People Controls			
6.3	Kesadaran, Edukasi, dan Pelatihan Terkait Keamanan Informasi	✓	
6.7	*Remote Working*		✓
Physical Controls			
7.7	*Clear Desk* dan *Clear Screen*	✓	
Technological Controls			
8.9	Manajemen Konfigurasi	✓	
8.11	*Data Masking*		✓
8.15	*Logging*	✓	
8.20	Keamanan Jaringan	✓	

Jika dilihat dari sisi grup kontrol, grup *Physical Controls* hampir mendapatkan nilai yang maksimum (persentase penilaian sebesar 96,43%), karena pada kontrol 7.7 *Clear Desk* dan *Clear Screen* hanya sebagian aktivitas yang masih dilakukan sehingga bernilai *Partial*. Begitu juga pada grup *Technological Controls* yang memperoleh persentase penilaian sebesar 92,65%, dimana klausa yang mendapatkan nilai *Partial/None* adalah klausa 8.9 Manajemen Konfigurasi, 8.11 *Data Masking*, 8.15 *Logging*, dan 8.20 Keamanan Jaringan. Selebihnya pada grup *People Controls* mendapatkan persentase nilai 81,25% dan grup *Organizational Controls* mendapatkan persentasi nilai 79,73%. Tabel 8 dan Gambar 4 merupakan deskripsi dari hasil nilai yang didapatkan berdasarkan grup kontrol.

Tabel 8. Hasil Penilaian Per Grup Kontrol

Aspek Penilaian Grup Kontrol Sesuai Standar ISO/IEC 27001:2022	Nilai Maksimum Penilaian	Skor Hasil Penilaian	Persen
Organizational Controls	37	29,5	79,73%
People Controls	8	6,5	81,25%
Physical Controls	14	13,5	96,43%
Technological Controls	34	31,5	92,65%

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 8 Nomor 1, Maret 2024, pp. 72-84
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti



Gambar 4. *Gap* Skor Hasil Penilaian Per Grup Kontrol

3.2. Identifikasi Aset

Kemudian dilakukan pengidentifikasian aset-aset TI yang dimiliki oleh PT XYZ. Berdasarkan kategori yang sudah ditentukan oleh standar ISO/IEC 27005:2018. Contoh daftar aset TI teridentifikasi yang dimiliki oleh PT XYZ dapat dilihat pada Gambar 5.

Kode	**Proses Bisnis (A)/Informasi (B)**					
A1	Pelayanan operasional teknologi informasi (TI)					
B1	Rencana Kerja Dan Anggaran Tahunan					
Perangkat Keras						
Peralatan Pemroses Data	**Peralatan *Portable***	***Fixed Equipment***	***Processing Peripheral***	***Data Medium***	***Electronic Medium***	**Media Lain**
Cloud Based	Laptop	*Server*	*Printer*	*Hard Disk Laptop*	*CD-ROM*	Kertas/ Dokumen
Perangkat Lunak						
Sistem Operasi (OS)	**Software Layanan, Administrasi, dan *Maintenance***		***Package/Standard Software***		***Business Application Software***	
Windows	*Content Management System*		Microsoft Office		DOMO	
Jaringan						
Medium And Support	***Passive or Active Relay***		***Communication Interface***			
Public Switched Telephone Network (PSTN)	*Bridge*		Adaptor Ethernet			
Sumber Daya Manusia						
Decision Maker	***User***		**Operation/ *Maintenance Staff***		***Developer***	
Direktur SDM	Divisi Sekretariat Perusahaan		Sub Divisi Tata Kelola dan Strategi TI		Sub Divisi Program Penyelarasan dan Pengembangan TI	
Situs						
External Environment	***Premises***	***Zone***	***Essential services***	***Communication***	***Utilities***	

Lokasi di Luar Kantor Yang Diizinkan	Gedung Kantor	Ruang Kerja	Semua layanan yang diperlukan agar peralatan perusahaan dapat beroperasi	Jalur Telepon	Listrik
Organisasi					
Pejabat Berwenang	**Pejabat Struktural**	***Project/System Organization***	**Subkontraktor/ *Supplier/ Manufacturer***		
Direktur SDM	Kepala Divisi TI	*Strategic Transformation Office* (STO)	Vendor		

Gambar 5. Contoh Identifikasi Aset TI PT XYZ

3.3. Penilaian Risiko dan Rekomendasi

Selanjutnya dilakukan penilaian risiko menggunakan aspek *probability* dan *impact* dari kontrol *Annex* A ISO/IEC 27001:2022 yang masih mendapatkan nilai *Partial* dan *None*. Tabel 9 merupakan pembagian rekomendasi berdasarkan kontrol ISO/IEC 27001:2022 yang sudah ditentukan nilai skor risikonya.

Tabel 9. Pembagian Rekomendasi Berdasarkan Kontrol ISO/IEC 27001:2022

Klausa	Kontrol Organisasi	Nilai Skor	Rekomendasi		
			Tinggi	Menengah	Rendah
Organizational Controls					
5.3	Segregasi Peran	9			✓
5.7	*Threat Intelligence*	8			✓
5.8	Keamanan Informasi Dalam Manajemen Proyek	9			✓
5.12	Klasifikasi Informasi	12		✓	
5.17	Informasi Autentikasi	9			✓
5.18	Hak Akses	9			✓
5.20	Menangani Keamanan Informasi Dalam Perjanjian Dengan *Supplier*	12		✓	
5.21	Mengelola Keamanan Informasi Dalam *ICT Supply Chain*	12		✓	
5.26	Respon Dalam Insiden Yang Menyangkut Keamanan Informasi	12		✓	
5.30	Kesiapan *ICT* Untuk Kesinambungan Bisnis	12		✓	
People Controls					
6.3	Kesadaran, Edukasi, dan Pelatihan Terkait Keamanan Informasi	9			✓
6.7	*Remote Working*	6			✓
Physical Controls					
7.7	*Clear Desk* dan *Clear Screen*	6			✓
Technological Controls					
8.9	Manajemen Konfigurasi	9			✓
8.11	*Data Masking*	16	✓		

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 8 Nomor 1, Maret 2024, pp. 72-84
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Klausa	Kontrol Organisasi	Nilai Skor	Rekomendasi		
			Tinggi	Menengah	Rendah
8.15	*Logging*	16	✓		
8.20	Keamanan Jaringan	12		✓	

Tabel 10 merupakan rangkuman dari rekomendasi peningkatan kontrol untuk PT XYZ, yang disusun berdasarkan standar dokumen ISO 27002:2022.

Tabel 10. Rekomendasi Peningkatan Kontrol

Klausa	Kontrol	Rekomendasi
Urgensi Tinggi		
8.11	*Data Masking*	Menyembunyikan data sensitif dengan menggunakan teknik seperti penyamaran data, pseudonimisasi, atau anonimisasi.
8.15	*Logging*	Menghubungkan log deteksi *malware* dengan perangkat *anti-malware administrations* dan *event log servers*, serta menyimpan semua *log* personil yang mengakses *URL.*
Urgensi Menengah		
5.12	Klasifikasi Informasi	Karena klasifikasi informasi dan klasifikasi ancaman siber adalah istilah yang terkait, maka klasifikasi ancaman siber dapat didasarkan pada klasifikasi konfidentialitas informasi yang terdapat pada standar ISO/IEC 27002:2022.
5.20	Menangani Keamanan Informasi Dalam Perjanjian Dengan Pemasok	Menambah sejumlah persyaratan terkait keamanan informasi ketika melakukan perjanjian dengan *supplier,* misal deskripsi/klasifikasi informasi, persyaratan legal, dan lain-lain.
5.21	Mengelola Keamanan Informasi Dalam *ICT Supply Chain*	Melakukan sejumlah prosedur untuk dapat melakukan prevensi/mitigasi Ketika terjadi insiden keamanan informasi dalam *ICT Supply Chain.*
5.26	Respon Dalam Insiden Yang Menyangkut Keamanan Informasi	Meningkatkan penanganan insiden keamanan informasi dalam PT XYZ, dapat dilakukan respon yang mencakup hal berikut seperti *containing*, mengoleksi *evidence*, memastikan kegiatan respon tercatat dengan benar, dan sejumlah prosedur lainnya.
5.30	Kesiapan *ICT* Untuk Kesinambungan Bisnis	Perlu dilakukan strategi yang turut membahas mengenai *backup* dan *restoration* dari data pribadi, seperti adanya rencana kontinuitas teknologi informasi.
8.20	Keamanan Jaringan	Perlu mengadopsi bentuk otentikasi terpusat, dan menggunakan *firewall implicit or explicit deny any/any rule* serta *firewall filtering* untuk meningkatkan keamanan jaringan yang dimiliki perusahaan, dan mempertimbangkan hal lain mengacu pada standar ISO/IEC 27002:2022.
Urgensi Rendah		
5.3	Segregasi Peran	Melakukan pemisahan tugas yang bertentangan antara satu personil dengan yang lain seperti mendefinisikan aktivitas mana yang perlu segregasi, dan dapat juga digunakan sistem kontrol akses berbasis peran untuk

Klausa	Kontrol	Rekomendasi
		memastikan personil tidak diberikan peran yang bertentangan.
5.7	*Threat Intelligence*	Dapat membagi *threat intelligence* menjadi tiga lapisan, dan melakukan sejumlah hal seperti menetapkan sasaran, identifikasi sumber informasi yang tepat, melakukan komunikasi tentang *threat intelligence*, dan sejumlah kegiatan lain.
5.8	Keamanan Informasi Dalam Manajemen Proyek	Karena PT XYZ belum mengintegrasi keamanan informasi dengan manajemen proyek, dapat melakukan persyaratan yang ditambahkan seperti contoh adanya penambahan penilaian risiko keamanan informasi pada tahap awal proyek dan adanya persyaratan keamanan informasi serta ditinjau.
5.17	Informasi Autentikasi	Pemastian beberapa prosedur seperti adanya kata sandi otomatis selama pendaftaran, prosedur untuk memverifikasi identitas pengguna, hingga memastikan persyaratan kepada personil PT XYZ terkait penggunaan informasi autentikasi.
5.18	Hak Akses	Terkait hak akses dimana tidak ada pemastian *update* kebijakan hak akses ketika terdapat aturan dan kebijakan yang berubah, jadi PT XYZ perlu melakukan *review* hal tersebut.
6.3	Kesadaran, Edukasi, dan Pelatihan Terkait Keamanan Informasi	Karena kesadaran dan pengetahuan dari personel perusahaan yang rendah terkait insiden keamanan informasi, jadi perlu melakukan program pendidikan dan pelatihan untuk personil.
6.7	*Remote Working*	Tidak ada aturan yang mengatur *remote working*, sehingga perusahaan perlu membuat kebijakan mengenai hal ini.
7.7	*Clear Desk* dan *Clear Screen*	PT XYZ perlu menerapkan prosedur kebijakan seperti penguncian informasi kertas/alat elektronik, adanya proteksi perangkat end-point jika alat tersebut ditinggalkan, hingga informasi papan tulis yang kritis sebaiknya segera dihapus.
8.9	Manajemen Konfigurasi	Membutuhkan *Change Advisory Board* untuk meninjau/menerapkan manajemen konfigurasi, selain itu juga dapat mempertimbangkan catatan konfigurasi yang baik sesuai standar ISO/IEC 27002:2022.

4. SIMPULAN

Berdasarkan hasil yang sudah diperoleh, ditemukan 17 kontrol ISO/IEC 27001:2022 yang tidak memiliki nilai 1 (dalam arti lain PT XYZ belum pernah melaksanakan aktivitas sama sekali/hanya melaksanakan sebagian aktivitas yang sudah ditentukan). Temuan lain yang dapat diidentifikasi dari evaluasi ini adalah definisi aset TI PT XYZ yang digunakan dalam membantu penilaian risiko. Kemudian menggunakan hasil analisis *gap* dan identifikasi aset, dilakukan penilaian risiko pada PT XYZ. Hasil yang didapatkan dalam kegiatan ini adalah nilai skor dari masing-masing 17 kontrol, yang kemudian dibagi berdasarkan urgensi. Terakhir disusun rekomendasi mengacu pada dokumen ISO/IEC 27002:2022, yang harapannya dapat digunakan oleh PT XYZ untuk meningkatkan sistem manajemen

keamanan informasi (SMKI) mereka. Pada penelitian selanjutnya, dapat dilakukan penelitian yang bertujuan mengetahui level maturitas suatu kondisi keamanan informasi (misal menggabungkan kondisi keamanan informasi dan penilaian level maturitas/kapabilitas COBIT 2019). Kemudian untuk memperdalam rekomendasi, kedepannya juga dapat dipertimbangkan pemanfaatan dokumen standar keamanan informasi lain, seperti dokumen SNI ISO/IEC 27003 dan standar *NIST Cybersecurity Framework*.

DAFTAR PUSTAKA

[1] KPMG, "KPMG global tech report 2023," 2023.
[2] WEC, "Global Cybersecurity Outlook 2023," 2023.
[3] PwC, "The C-suite playbook: Putting security at the epicenter of innovation," 2023.
[4] Kementerian BUMN, "KAMI BERTRANSFORMASI - LAPORAN TAHUNAN 2021 ANNUAL REPORT," 2021. [Daring]. Tersedia pada: www.bumn.go.id
[5] Accenture, "State of Cybersecurity Resilience 2023," 2023.
[6] ISO, *SNI ISO/IEC 27001:2022*. 2023. [Daring]. Tersedia pada: www.bsn.go.id
[7] MENTERI BADAN USAHA MILIK NEGARA REPUBLIK INDONESIA, "Pedoman Tata Kelola dan Kegiatan Korporasi Signifikan Badan Usaha Milik Negara." Jakarta, 2023.
[8] J. Recker, *Scientific Research in Information Systems*. Berlin: Springer, 2013. [Daring]. Tersedia pada: http://www.springer.com/series/10440
[9] M. Von Rosing, A.-W. Scheer, dan H. Von Scheel, *The Complete Business Process Handbook*, vol. 1. Elsevier, 2015.
[10] Abuzar Asra, Puguh Bodro Irawan, dan Agus Purwoto, *Metode penelitian survei*. In Media, 2016.
[11] ISO, *ISO/IEC 27005:2018*. 2018.