AUDIT SISTEM INFORMASI DALAM MENGUKUR KEPATUHAN ISO 27002

Rila Marzan Laili[1], Riska Nuriyanti[2], Martinus Damenta Ginting[3]

Sistem Informasi, STMIK KAPUTAMA[1,2,3]

Email: [1]*rilamarzanlaili@gmail.com*, [2]*riskanurianti656@gmail.com*, [3]*gintingmartinus667@gmail.com*

ABSTRAK- Penelitian ini bertujuan untuk mengevaluasi tingkat kepatuhan PT Jaya Sawit Langkat (PT JSL) terhadap standar ISO 27002 dalam konteks keamanan informasi. pada era digital saat ini, perusahaan menghadapi ancaman serius terhadap kerahasiaan, integritas, serta ketersediaan data. Meskipun pentingnya keamanan informasi diakui, banyak perusahaan, termasuk PT JSL, sering kali mengabaikan implementasinya.Metode penelitian yang dipergunakan meliputi studi literatur, observasi, dan wawancara menggunakan pegawai untuk memahami praktik keamanan yang ada dan tantangan yang dihadapi. hasil audit menunjukkan bahwa tingkat kematangan implementasi kontrol keamanan informasi di PT JSL berada pada kategori menengah dengan nilai rata-rata 2.49. Hal ini mengindikasikan bahwa meskipun perusahaan telah memulai penerapan kontrol sesuai ISO 27002, masih ada banyak area yang memerlukan perbaikan. Rekomendasi utama mencakup peningkatan pelatihan bagi karyawan tentang keamanan informasi dan pelaksanaan audit berkala untuk mengidentifikasi dan memperbaiki kelemahan pada sistem keamanan yang ada. dengan langkah-langkah tersebut, diharapkan PT JSL dapat menaikkan keamanan data dan kepercayaan pelanggan.

Kata Kunci: Audit Sistem Informasi ,ISO 27002

ABSTRACT *- This study aims to evaluate the level of compliance of PT Jaya Sawit Langkat (PT JSL) with the ISO 27002 standard in the context of information security. In today's digital era, companies face serious threats to data confidentiality, integrity, and availability. Although the importance of information security is recognized, many companies, including PT JSL, often overlook its implementation. The research methods used include literature studies, observations, and interviews using employees to understand existing security practices and the challenges faced. The audit results show that the maturity level of information security control implementation at PT JSL is in the medium category with an average score of 2.49. This indicates that although the company has started implementing controls in accordance with ISO 27002, there are still many areas that need improvement. Key recommendations include increased training for employees on information security and the implementation of periodic audits to identify and fix weaknesses in existing security systems. With these measures, it is hoped that PT JSL can increase data security and customer trust.*

Keywords: *Information System Audit, ISO 27002.*

PENDAHULUAN

Banyaknya bisnis bergantung pada teknologi dan informasi untuk beroperasi, keamanan informasi menjadi lebih penting dalam lingkungan bisnis saat ini. Sebagai perusahaan perkebunan, PT.JSL (Jaya Sawit Langkat) menghadapi ancaman kerahasiaan, integritas, dan ketersediaan data. Data dan informasi yang dikumpulkan, diolah, dan digunakan disimpan oleh perusahaan sebagai aset strategis yang signifikan.

Meskipun setiap perusahaan mempertimbangkan pentingnya keamanan informasi, banyak yang sering mengabaikannya atau tidak memberi perhatian yang cukup terhadap masalah tersebut. Kurang pengetahuan dan kesadaran tentang keamanan informasi serta kurangnya pelatihan karyawan dalam manajemen teknologi dan informasi adalah beberapa penyebabnya.Dalam era digital saat ini, di mana ancaman terhadap keamanan informasi meningkat, bisnis dapat menjadi rentan terhadap serangan siber dan kebocoran data jika mereka tidak menerima pelatihan dan kesadaran yang cukup tentang keamanan informasi mereka.

PT.JSL belum menganalisis sumber masalah tersebut dan tidak tahu tingkat keamanan data yang dimilikinya. Oleh karena itu, PT.JSL perlu melakukan evaluasi keamanan sistem informasi untuk memastikan bahwa data center, tempat semua informasi pelanggan disimpan, aman. Standar internasional ISO 27002 dapat digunakan untuk melakukan evaluasi keamanan informasi saat membangun dan mengelola SMKI (system manajemen keamanan informasi). Tujuan keamanan informasi adalah untuk memastikan bahwa aspek kerahasiaan (kerahasiaan), integritas (keturunan), dan ketersediaan (ketersediaan) dari informasi dipertahankan (ISO/IEC 27002).Standar internasional ISO 27002 menyediakan kerangka kerja yang lengkap untuk membangun dan mengelola SMKI. Standar ini menyediakan seperangkat kontrol keamanan yang dapat disesuaikan dengan kebutuhan perusahaan. Meskipun demikian, banyak perusahaan, termasuk perusahaan perkebunan, masih menghadapi kesulitan dalam menerapkan dan mempertahankan kepatuhan terhadap standar ini. Pemilihan standar ditentukan oleh direktur perusahaan. PT.JSL memilih ISO 27002 karena sangat fleksibel untuk

disesuaikan dengan kebutuhan, tujuan, persyaratan keamanan, proses bisnis, jumlah karyawan, dan ukuran struktur organisasi. Faktor tambahan adalah ISO 27002 memberikan sertifikasi implementasi Sistem Manajemen Keamanan Informasi (SMKI), yang diakui secara internasional dan dikenal sebagai sertifikasi Manajemen Keamanan Sistem Informasi (ISMS) (Sarno dan Iffano, 2009: 59-60).

Tujuan dari penelitian ini adalah untuk menilai tingkat kepatuhan organisasi terhadap ISO 27002, menemukan masalah dan hambatan dalam menerapkan standar tersebut, dan membuat saran untuk meningkatkan keamanan sistem informasi.Salah satu cara yang efektif untuk mengukur tingkat kepatuhan suatu organisasi terhadap standar ISO 27002 adalah melakukan audit sistem informasi. Audit membantu menemukan celah keamanan dan peluang perbaikan. Hasil audit dapat digunakan untuk meningkatkan efisiensi SMKI dan mengurangi risiko yang berkaitan dengan keamanan data.

METODE PENELITIAN

A. Studi Literatur

Studi literatur ialah langkah awal yang penting pada penelitian ini, di mana peneliti mengumpulkan dan menganalisis informasi yang relevan terkait keamanan informasi serta penerapan standar ISO 27002. Beberapa sumber yang digunakan pada studi literatur ini,peneliti melakukan kajian terhadap berbagai buku serta artikel ilmiah yang didapat dari google scholar,jurnal nasional terakreditasi maupun jurnal internasional yang membahas tentang keamanan informasi, sistem manajemen keamanan informasi (SMKI), serta khususnya standar ISO 27002.

Studi literatur berkontribusi pada pemahaman solusi yang diusulkan dalam beberapa cara:

1) Pemahaman Konsep Keamanan informasi:Studi literatur membantu peneliti memahami konsep keamanan informasi secara lebih mendalam, termasuk definisi, tujuan, dan prinsip-prinsip dasar keamanan informasi. dengan memahami konsep keamanan informasi, peneliti bisa mengidentifikasi kebutuhan keamanan informasi yang spesifik pada konteks perusahaan.

2) Pemahaman standar ISO 27002: Studi literatur membantu peneliti memahami standar ISO 27002 secara lebih mendalam, termasuk struktur, kontrol, dan proses yang dibutuhkan buat menerapkan standar ini. dengan memahami standar ISO 27002, peneliti bisa mengidentifikasi kontrol yang diperlukan untuk menerapkan standar ini dalam konteks perusahaan.

3) Pemahaman Penerapan standar ISO 27002: Studi literatur membantu peneliti memahami bagaimana standar ISO 27002 bisa diterapkan pada konteks perusahaan. dengan memahami penerapan standar ISO 27002, peneliti dapat mengidentifikasi langkah-langkah yang diharapkan untuk menerapkan standar ini pada konteks perusahaan.

4) Pemahaman Tantangan dan Kesulitan:Studi literatur membantu peneliti memahami tantangan serta kesulitan yang mungkin dihadapi pada menerapkan standar ISO 27002. dengan memahami tantangan dan kesulitan, peneliti dapat mengidentifikasi langkah-langkah yang diharapkan untuk mengatasi tantangan serta kesulitan tersebut.

B. ISO

ISO 27002: 2005 berisi pedoman yang menjelaskan contoh penerapan keamanan berita dengan menggunakan bentuk-bentuk kontroleksklusif agar mencapai sasaran kontrol yang ditetapkan.Bentuk-bentuk kontrol yang disajikan seluruhnya menyangkut 11 area pengamanan sebagaimana ditetapkan di dalam ISO/IEC 27001.Sarno dan Iffano (2009: 187) berkata kontrol keamanan sesuai ISO/IEC 27001 terdiri dari11 klausul kontrol keamanan (security control clauses), 39 objektif kontrol 4 (control objectives) serta 133 kontrol keamanan/ kontrol (controls)

C. Teknik Pengumpulan Data

Penelitian ini menggunakan dua teknik pengumpulan data utama sebagai berikut:

1) Observasi*:* Peneliti melakukan observasi eksklusif terhadap praktik keamanan yang diterapkan di PT JSL. Observasi ini meliputi peninjauan sistem keamanan data,prosedur pengelolaan isu, serta software kebijakan keamanan yang ada.Tujuan dari observasi ini adalah untuk menilai secara langsung kondisi dan efektivitas

langkah-langkah keamanan yang diterapkan, serta untuk mengidentifikasi celah atau ketidaksesuaian di penerapan standar ISO 27002.

Hasil dari observasi ini memberikan wawasan yang berharga perihal efektivitas langkah-langkah keamanan yang diterapkan pada PT JSL. Temuan dari observasi berkontribusi pada rekomendasi yang diberikan, seperti perlunya peningkatan pelatihan bagi karyawan tentang prosedur keamanan serta peninjauan kembali kebijakan yang terdapat untuk memastikan bahwa mereka sesuai dengan praktik terbaik yang diakui.

2) Wawancara: Wawancara dilakukan dengan pegawai PT JSL, termasuk manajer IT, staf keamanan informasi, serta karyawan lainnya yang terlibat pada pengelolaan data. Wawancara ini bertujuan untuk menerima pemahaman yang lebih mendalam perihal praktik keamanan informasi yang ada, tingkat kesadaran karyawan terhadap keamanan informasi, dan tantangan yang dihadapi pada penerapan standar ISO 27002. Wawancara semi-terstruktur digunakan untuk memberikan fleksibilitas dalam menggali informasi, di mana peneliti menyiapkan daftar pertanyaan namun juga membiarkan diskusi mengalir sesuai dengan respons narasumber.

Hasil dari wawancara ini membantu dalam mengevaluasi tingkat kesadaran karyawan terhadap keamanan informasi. penemuan dari wawancara menunjukkan area di mana karyawan merasa kurang teredukasi atau tidak konfiden tentang prosedur keamanan yang harus diikuti.Ini berkontribusi pada rekomendasi untuk meningkatkan acara pelatihan dan kesadaran keamanan informasi pada perusahaan, sebagai akibatnya karyawan bisa lebih tahu pentingnya keamanan informasi serta peran mereka pada menjaga data perusahaan.

D. Proses Audit

Proses audit keamanan informasi dilakukan untuk mengevaluasi efektivitas langkah-langkah keamanan yang diterapkan di PT Jaya Sawit Langkat (PT JSL). Proses audit ini dilakukan di tiga level, yaitu level organisasi, level teknologi, dan level operasional.

Level Organisasipada level organisasi, proses audit dilakukan untuk mengevaluasi kebijakan dan prosedur keamanan informasi yang diterapkan pada PT JSL. Langkah-langkah yang diambil adalah sebagai berikut:

1.Pengumpulan Dokumen: Peneliti mengumpulkan dokumen-dokumen yang terkait dengan kebijakan dan mekanisme keamanan informasi, seperti kebijakan keamanan informasi, prosedur pengelolaan akses, dan prosedur penanganan data sensitif.

2.Analisis Dokumen:Peneliti menganalisis dokumen-dokumen yang terkumpul untuk mengevaluasi apakah kebijakan dan prosedur keamanan informasi yang diterapkan sudah sinkron dengan standar yang diakui.

3.Wawancara dengan Pihak yang Berwenang: Peneliti melakukan wawancara menggunakan pihak yg berwenang, seperti manajer IT serta staf keamanan informasi, untuk memahami bagaimana kebijakan serta prosedur keamanan informasi diterapkan pada PT JSL.

hasil dari proses audit pada level organisasi menunjukkan bahwa PT JSL sudah memiliki kebijakan serta prosedur keamanan informasi yang lengkap, tetapi masih terdapat beberapa area yang perlu diperbaiki, seperti pengelolaan akses yang belum sepenuhnya efektif.

Level Teknologi pada level teknologi, proses audit dilakukan untuk mengevaluasi efektivitas langkah-langkah keamanan teknologi yang diterapkan di PT JSL. Langkah-langkah yang diambil adalah sebagai berikut:

1.Pengumpulan Data: Peneliti mengumpulkan data tentang konfigurasi sistem keamanan, seperti firewall, antivirus, serta sistem deteksi intrusi.

2.Analisis Data: Peneliti menganalisis data yang terkumpul untuk mengevaluasi apakah konfigurasi sistem keamanan sudah sinkron dengan standar yang diakui.

3.Pengujian Sistem Keamanan: Peneliti melakukan pengujian sistem keamanan untuk mengevaluasi efektivitas langkah-langkah keamanan teknologi yang diterapkan.

hasil dari proses audit pada level teknologi menunjukkan bahwa PT JSL telah memiliki sistem keamanan yang efektif, tetapi masih terdapat beberapa area yang perlu diperbaiki, seperti pengelolaan patch yang belum sepenuhnya efektif.

Level Operasional pada level operasional, proses audit dilakukan untuk mengevaluasi efektivitas langkah-langkah keamanan operasional yang diterapkan di PT JSL. Langkah-langkah yang diambil adalah sebagai berikut:

1.Pengumpulan Data: Peneliti mengumpulkan data perihal mekanisme operasional, seperti prosedur pengelolaan akses serta mekanisme penanganan data sensitif.

2.Analisis Data: Peneliti menganalisis data yang terkumpul untuk mengevaluasi apakah mekanisme operasional sudah sesuai dengan standar yang diakui.

3.Wawancara dengan Karyawan: Peneliti melakukan wawancara dengan karyawan untuk memahami bagaimana mekanisme operasional diterapkan di PT JSL.

hasil dari proses audit pada level operasional menunjukkan bahwa PT JSL telah memiliki prosedur operasional yang efektif, tetapi masih terdapat beberapa area yang perlu diperbaiki, seperti pengelolaan akses yang belum sepenuhnya efektif.

PEMBAHASAN

A. Analisis Kepatuhan terhadap ISO 27002

Analisis kepatuhan terhadap standar ISO 27002 sangat penting buat menilai sejauh mana perusahaan telah menerapkan kontrol keamanan informasi yang direkomendasikan. ISO 27002 memberikan pedoman perihal berbagai kontrol yang dapat diimplementasikan untuk melindungi kerahasiaan, integritas, dan ketersediaan data. dengan melakukan audit sistem informasi, PT JSL bisa mengidentifikasi celah dalam implementasi kontrol tersebut dan menentukan langkah-langkah perbaikan yang diperlukan.

B. Cobit 4.1

COBIT dikembangkan oleh IT Governance Institute (ITGI), sebuah divisi dari Information System Audit and Control Association (ISACA) .

C. Maturity Level

ISO 17799 memberikan kontrol keamanan tetapi tidak bagaimana kontrol itu dikembangkan atau diatur.Ini disebabkan ISO bukan standar teknis juga bukan untuk teknologi tertentu.Oleh karena itu tidak ada mekanisme penilaian atau metode evaluasi

(Gunawan dan Suhono, 2006: 135),sehingga pengidentifikasian maturity level mengacu pada kerangka kerja COBIT atau CCMI (Capability Marturity Model For Integration).Model yang digunakan untukmengendalikan proses teknologi informasi yang terdiri dari pengembangan suatu metode penilaian sehingga suatu organisasi dapat mengukur dirinya sendiri dari noneksisten ke tingkat optimal (value 0 sampai dengan value 5)

D. Deskripsi Solusi berdasarkan ISO 27002 dan COBIT 4.1

Framework ISO 27002 memberikan panduan untuk implementasi kontrol keamanan, sedangkan COBIT 4.1 digunakan untuk mengevaluasi tingkat kematangan. Kombinasi keduanya memberikan pendekatan komprehensif untuk mengidentifikasi celah keamanan dan memilih tindakan perbaikan.

E. Proses Audit pada semua Level

Proses audit keamanan gosip dilakukan di 3 level, yaitu level strategis, level maksud, dan level tindakan. Berikut merupakan penjelasan tentang bagaimana proses audit dilakukan di setiap level dan bagaimana hal ini berkontribusi di keseluruhan audit.

1.Level Strategis

pada level strategis, proses audit dilakukan untuk mengidentifikasi tujuan, kebutuhan, dan prioritas keamanan informasi pada PT Jaya Sawit Langkat (PT JSL). Proses audit ini melibatkan pengumpulan data tentang visi, misi,

serta strategi perusahaan, dan pengumpulan data mengenai risiko keamanan informasi yang dihadapi oleh perusahaan. hasil dari proses audit ini digunakan untuk menciptakan strategi keamanan informasi yang efektif dan sesuai dengan tujuan perusahaan.

2.Level Maksud

pada level maksud, proses audit dilakukan untuk mengidentifikasi kontrol keamanan informasi yang diharapkan untuk mencapai tujuan keamanan informasi yang sudah ditetapkan di level strategis. Proses audit ini melibatkan pengumpulan data tentang prosedur, pola, dan praktik keamanan informasi yang sudah ditetapkan oleh perusahaan. hasil dari proses audit ini digunakan untuk memastikan bahwa kontrol keamanan informasi yang sudah ditetapkan sesuai dengan tujuan keamanan informasi dan standar yang diakui.

3.Level Tindakan

pada level tindakan, proses audit dilakukan untuk mengidentifikasi kepatuhan terhadap kontrol keamanan informasi yang sudah ditetapkan pada level maksud. Proses audit ini melibatkan pengumpulan data mengenai tindakan yang diambil oleh karyawan serta penggunaan sistem informasi. hasil dari proses audit ini digunakan untuk memastikan bahwa tindakan yang diambil oleh karyawan dan penggunaan sistem informasi sesuai dengan mekanisme, pola, dan praktik keamanan informasi yang sudah ditetapkan.

Proses audit pada setiap level berkontribusi di keseluruhan audit menggunakan cara mengidentifikasi tujuan, kebutuhan, dan prioritas keamanan informasi, mengidentifikasi kontrol keamanan informasi yang dibutuhkan untuk mencapai tujuan keamanan informasi, dan mengidentifikasi kepatuhan terhadap kontrol keamanan informasi yang sudah ditetapkan. hasil dari proses audit pada setiap level digunakan untuk membangun strategi keamanan informasi yang efektif dan sesuai dengan tujuan perusahaan, memastikan bahwa kontrol keamanan informasi yang sudah ditetapkan sesuai dengan tujuan keamanan informasi serta

standar yang diakui, dan memastikan bahwa tindakan yang diambil oleh karyawan dan penggunaan sistem informasi sesuai dengan prosedur, pola, serta praktik keamanan informasi yang sudah ditetapkan. dengan demikian, proses audit di setiap level membantu memmastikan bahwa keseluruhan sistem keamanan informasi pada PT Jaya Sawit Langkat (PT JSL) berfungsi secara efektif dan efisien.

Integrasi hasil Audit di Setiap Level

1.Keterkaitan Antara Level

Setiap level audit saling terkait dan memberikan umpan balik yang penting. hasil dari level strategis memberikan panduan untuk level maksud, sementara hasil dari level maksud menjadi dasar untuk level tindakan. dengan demikian, audit yang dilakukan di setiap level membentuk suatu siklus yang berkelanjutan untuk perbaikan keamanan informasi.

2.Identifikasi Kelemahan dan Peluang perbaikan

Proses audit di setiap level membantu dalam mengidentifikasi kelemahan dalam kontrol keamanan yang ada. misalnya, Jika audit pada level tindakan menunjukkan bahwa karyawan tidak mematuhi prosedur yang ditetapkan, hal ini dapat mengarah pada revisi kebijakan di level maksud untuk meningkatkan pelatihan dan kesadaran keamanan.

3.Peningkatan Kepatuhan

dengan melakukan audit di seluruh level, PT JSL dapat memastikan bahwa semua aspek dari sistem manajemen keamanan informasi (SMKI) diperiksa dan dievaluasi. Hal ini berkontribusi di peningkatan kepatuhan terhadap standar ISO 27002 dan kontrol keamanan yang ditetapkan, dan membantu perusahaan dalam memenuhi persyaratan regulasi yang relevan.

4.Pengambilan Keputusan yang Lebih Baik

hasil audit yang komprehensif dari semua level memberikan informasi yang diharapkan untuk pengambilan keputusan yang lebih baik. Manajemen dapat menggunakan data serta analisis dari audit untuk merumuskan

kebijakan serta strategi yang lebih baik pada mengelola risiko keamanan informasi.

5.Peningkatan kepercayaan Stakeholder

dengan menunjukkan bahwa audit dilakukan secara menyeluruh di seluruh level, PT JSL dapat meningkatkan kepercayaan stakeholder, termasuk pelanggan, mitra bisnis, dan regulator. Hal ini penting untuk membangun reputasi perusahaan sebagai entitas yang bertanggung jawab dalam mengelola keamanan informasi.

F. Pentingnya Evaluasi dan Monitoring untuk Optimalisasi Keamanan Informasi

Evaluasi dan monitoring adalah tahap penting pada proses audit keamanan informasi. Tujuan dari evaluasi dan monitoring adalah untuk mengevaluasi efektivitas langkah-langkah keamanan yang diterapkan dan memantau kemajuan dalam implementasi rekomendasi yang diberikan.

Langkah-Langkah penilaian dan Monitoring

Berikut adalah langkah-langkah yang diambil dalam evaluasi dan monitoring:

1.Pengumpulan Data

Peneliti mengumpulkan data tentang implementasi rekomendasi yang diberikan, termasuk data tentang kemajuan dalam implementasi, tantangan yang dihadapi, serta hasil yang diperoleh.

2.Analisis Data

Peneliti menganalisis data yang terkumpul untuk mengevaluasi efektivitas implementasi rekomendasi dan memantau kemajuan dalam implementasi.

3.Wawancara dengan Pihak yang Berwenang

Peneliti melakukan wawancara dengan pihak yang berwenang, seperti manajer IT dan staf keamanan informasi, untuk memahami bagaimana implementasi rekomendasi yang diberikan.

4.Pengujian Sistem Keamanan

Peneliti melakukan pengujian sistem keamanan untuk mengevaluasi efektivitas implementasi rekomendasi yang diberikan.

Hasil evaluasi serta monitoring menunjukkan bahwa implementasi rekomendasi yang diberikan sudah berkontribusi pada peningkatan efektivitas langkah-langkah keamanan yang diterapkan pada PT Jaya Sawit Langkat (PT JSL). Berikut adalah beberapa hasil yang diperoleh:

1.Peningkatan Efektivitas Langkah-Langkah Keamanan

Implementasi rekomendasi yang diberikan sudah berkontribusi pada peningkatan efektivitas langkah-langkah keamanan yang diterapkan pada PT JSL.

2.Pengurangan Risiko Keamanan

Implementasi rekomendasi yang diberikan telah berkontribusi pada pengurangan risiko keamanan yang dihadapi oleh PT JSL.

3.Peningkatan kesadaran Keamanan

Implementasi rekomendasi yang diberikan telah berkontribusi pada peningkatan kesadaran keamanan di kalangan karyawan PT JSL.

HASIL DAN PEMBAHASAN

Penentuan Ruang Lingkup Audit Keamanan Sistem informasi dilakukan dengan cara menentukan objektif kontrol yang akan digunakan. Perusahaan perlu melakukan pemilihan terhadap kontrol-kontrol yang ada dengan memperhatikan kebutuhan organisasinya, bagaimana cara penerapan dan penetapan resiko Jika kontrol tersebut tidak dipenuhi. Kontrol didesain untuk menyampaikan kepastian bahwa tindakan manajerial yang dilakukan dapat menyampaikan kepastian bahwa

tujuan usaha akan dicapai serta kejadian yang tidak diinginkan akan dapat dicegah, dideteksi, dan diperbaiki (Sarno, 2009). Tabel 1 adalah pemetaan dari panduan yang dipergunakan terhadap klausul-klausul ISO 27002.

TABEL I

Pemetaan Klausul ISO 27002

Klausul	Deskripsi
8	Keamanan SDM
9	Keamanan Fisik dan Lingkungan
10	Manajemen Komunikasi dan Operasi
11	Kontrol Akses
13	Manajemen Kejadian Keamanan Informasi
14	Manajemen Kelangsungan Bisnis

A. Pelaksanaan Audit Kepatutan dan Penentuan Maturity Level

Pelaksanaan audit kepatutan menghasilkan dokumen wawancara, bukti-bukti audit, temuan audit dan nilai tingkat kematangan tiap kontrol keamanan.. Dokumen wawancara diperoleh saat prosedur pembuatan pertanyaan dari pernyataan yang sebelumnya dibuat. Bukti-bukti dan temuan audit diperoleh saat dilakukan wawancara kepada perusahaan. Setelah didapatkan bukti-bukti dan temuan audit tersebut kemudian dievaluasi dan dianalisa lalu menentukan nilai tingkat kemampuan tiap-tiap kontrol keamanan. Contoh kerangka kerja perhitungan nilai maturity level dapat dilihat pada Tabel 2, untuk contoh hasil perhitungan tingkat kemampuan dapat dilihat pada Tabel 3.

TABEL 2

Contoh Kerangka Kerja Perhitungan Maturity Level

Nama Proses	

	Mengelola Lingkungan Fisik		
Nomor Proses	**DS12**	**Level Kedewasaan**	**0**
No	**Pernyataan**		**Bobot**
1	Terdapat kebutuhan untuk perlindungan fasilitas sumber daya komputer		1.00
2	Terdapat kebutuhan untuk perlindungan fasilitas sumber daya komputer		1.00
Total Bobot			2.00

Apakah sepakat?

Tidak Sama Sekali	**Sedikit**	**Dalam tingkatan tertentu**	**Seluruhnya**	**NILAI**
0.00	0.33	0.66	1.00	
			√	1.00
			√	1.00
Tingkat Kepatuhan		1.00	**Total Nilai**	2.00

TABEL 3

Contoh Hasil Maturity Level Klausul 9 Keamanan Fisik dan Lingkungan

Objektif Kontrol	Kontrol keamanan	Cobit IT Processes	Maturity COBIT 4.1	Maturity ISO 27002
9.1 Wilayah Aman	9.1.1 Pembatas Keamanan Fisik	DS12	3.10	3.30
	9.1.2 Kontrol Masuk Fisik	DS12	2.77	2.99
	9.1.3 Keamanan Kantor, Ruang, dan Fasilitasnya	DS12	3.11	3.11
	9.1.4 Perlindungan Terhadap Ancaman Dari Luar dan Sekitar	DS12	3.30	3.30

Objektif Kontrol	Kontrol Kemananan	Cobit IT Processes	Maturity COBIT 4.1	Maturity ISO 27002	Rata-Rata Objektif Kontrol
9.1 Wilayah Aman (Lanjutan)	9.1.5Bekerja di Wilayah Aman	PO4	2.98	2.50	2.55
		PO6	2.64		
		A13	1.56		
		DS12	3.14		
	9.1.6Akses Publik, Tempat Pengiriman, dan Penurunan Barang	DS5	1.95	2.56	
		DS12	3.11		
9.2 Keamanan Peralatan	9.2.1Letak Peralatan dan Pengamanannya	DS5	1.90	2.54	2.70
		DS12	3.20		
	9.2.2Utilitas Pendukung	DS12	3.15	3.05	

	9.2.4Pemeliharaan Peralatan	AI3	1.60	2.54	
		DS12	3.90		
		DS13	2.60		
	9.2.6Keamanan untuk Pembuangan atau Pemanfaatan Kembali Peralatan Hak Pemanfaatan	DS11	2.34	2.54	
	9.2.7Hak Pemanfaatan	PO6	2.50	2.78	
		DS12	3.20		
Maturnity Level Klausul 9					2.79

TABEL 4
Hasil Maturity Level Seluruh Klausul yang Digunakan

Klausul	Deskripsi	Maturity Level
8	Keamanan SDM	2.72
9	Keamanan Fisik dan Lingkungan	2.79
10	Manajemen Komunikasi dan Operasi	2.20
11	Kontrol Akses	2.26
13	Manajemen Kejadian Keamanan Informasi	2.52
14	Manajemen Kelangsungan Bisnis	2.43
Nilai Maturity Level		2.49

Berdasarkan nilai rata-rata maturity level keseluruhan sebesar 2.49, implementasi kontrol keamanan pada PT JSL dapat dikategorikan menengah. Hal ini menunjukkan bahwa:Perusahaan sudah memulai penerapan kontrol keamanan informasi sinkron ISO 27002.tetapi, banyak kontrol masih memerlukan optimasi untuk mencapai tingkat kematangan yang lebih tinggi

B.Temuan audit dan rekomendasi

Objektif Kontrol	Kontrol Keamanan	Temuan Audit	Rekomendasi
9.1.1 wilayah aman	Pembatas Keamanan Fisik	tidak adanya pembatas yang memadai di beberapa area penting	Pasang pagar atau penghalang fisik tambahan di area kritis serta tambahkan sistem keamanan seperti kartu akses.
9.1.3 Keamanan kantor	Keamanan Ruang	Peralatan sensitif disimpan di lokasi yang praktis diakses oleh pihak yang tidak berwenang.	Relokasi alat-alat sensitif ke ruang aman menggunakan akses terbatas.
10.1.1 Manajemen Operasi	prosedur Backup Data	tidak ada kebijakan atau sistem untuk melakukan backup data secara rutin.	Implementasikan kebijakan backup otomatis harian serta gunakan sistem penyimpanan data yang terdistribusi untuk memastikan redundansi.

11.2.2 Kontrol Akses	Manajemen Akses Pengguna	Akun pengguna lama yang tidak aktif belum dihapus, sehingga berisiko digunakan oleh pihak yang tidak berwenang.	Lakukan audit akun pengguna secara bersiklus serta hapus atau nonaktifkan akun yang tidak digunakan.
13.1.1Manajemen peristiwa	Pelaporan insiden Keamanan	tidak ada prosedur standar untuk melaporkan dan menangani insiden keamanan informasi.	buat dan sosialisasikan prosedur pelaporan insiden keamanan, dan latih karyawan dalam mengidentifikasi serta merespons ancaman secara cepat.
14.1.1 Kelangsungan usaha	Perencanaan Pemulihan bencana	tidak terdapat planning pemulihan bencana yang terdokumentasi, sebagai akibatnya proses bisnis terganggu Jika terjadi insiden besar .	Susun dan uji rencana pemulihan bencana yang meliputi langkah-langkah untuk menjaga kelangsungan operasional saat terjadi peristiwa besar .

8.1.1 pembinaan Karyawan	kesadaran Keamanan informasi	Karyawan memiliki taraf kesadaran yang rendah perihal pentingnya keamanan informasi, dan tidak terdapat pelatihan rutin yang diberikan.	Selenggarakan program pelatihan keamanan informasi secara berkala untuk semua karyawan, termasuk simulasi penanganan ancaman siber.

SIMPULAN

Penelitian ini berhasil mengevaluasi tingkat kepatuhan PT JSL terhadap standar ISO 27002 pada konteks keamanan informasi. hasil audit menunjukkan bahwa meskipun perusahaan sudah memulai penerapan kontrol keamanan informasi, tingkat kematangan implementasi masih berada pada kategori menengah dengan nilai rata-rata 2.49. Hal ini menandakan adanya banyak area yang memerlukan perbaikan, terutama pada hal pembinaan karyawan serta kesadaran akan pentingnya keamanan informasi.

Beberapa masalah yang diidentifikasi termasuk kurangnya prosedur untuk pelaporan insiden keamanan, manajemen akses pengguna yang tidak optimal, dan tidak adanya planning pemulihan bencana yang terdokumentasi. oleh karena itu, disarankan agar PT JSL menaikkan program pelatihan keamanan informasi secara berkala, melakukan audit sistem secara rutin, dan menyusun prosedur yang jelas untuk menangani insiden keamanan. dengan langkah-langkah ini, diharapkan PT JSL dapat menaikkan keamanan data, mengurangi risiko serangan siber, dan menaikkan kepercayaan pelanggan terhadap sistem informasi yang dikelola. dengan demikian, penelitian ini menyampaikan wawasan krusial bagi PT JSL serta perusahaan lain pada upaya meningkatkan keamanan informasi dan kepatuhan terhadap standar internasional yang relevan

DAFTAR PUSTAKA

Sakinah, F., & Setiawan, B. (2014). Indeks Penilaian Kematangan (Maturity) Manajemen Keamanan Layanan TI. Jurnal Teknik ITS, 3(2), A222-A227.

Nafisa, F. A., Yasirandi, R., & Utomo, R. G. (2023). Information Security Audit Analysis on Cloud Providers Using ISO/IEC 27017: 2015 at PT. XYZ. eProceedings of Engineering, 10(3).

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

Vansuri, R., Fauzi, A., Prasetyo, E. T., Negara, R., Ramadhan, R., Restu, A. M., & Firmansyah, R. R. (2023). Peran CIA (Confidentiality, Integrity, Availability) Terhadap Manajemen Keamanan Informasi. Jurnal Ilmu Multidisplin, 2(1), 106-113.

Halim, M. (2012). TA: Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27002 Pada PT. Aneka Jaya Baut Sejahtera (PT. AJBS) (Doctoral dissertation, STIKOM Surabaya).

Burgdorf, M., & Jendria, K. (2022). ISO 27002 revisited: Struktur und Maßnahmen der ISO 27002: 2022-02. Datenschutz und Datensicherheit-DuD, 46(5), 301-304.

Malatji, M. (2023, January). Management of enterprise cyber security: A review of ISO/IEC 27001: 2022. In 2023 International conference on cyber management and engineering (CyMaEn) (pp. 117-122). IEEE.

José, D. A. M., Dupski, D. S., & Amilkar, K. (2024). Framework for Security Risk Assessment (FSRA) and Fuzzy Risk Inference System (FRIS) based on Standard ISO/IEC 27002: 2022. Revista de Informática Teórica e Aplicada, 31(2), 43-55.

Tanuwijaya, H. (2022). Analisis Keamanan Sistem Informasi Perdagangan Terintegrasi Menggunakan Standar ISO 27002. Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi, 11(3), 571-582.

Khatibian, N., Hasan gholoi pour, T., & Abedi Jafari, H. (2010). Measurement of knowledge management maturity level within organizations. Business strategy series, 11(1), 54-70.