ICBENS
International Conference on Bussiness and Entrepreneurship for Nation's Sustainability

PENERAPAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERBASIS ISO27001:2013 DI PT. X

IMPLEMENTATION OF INFORMATION SECURITY INFORMASI BASED ON ISO 27001:2013 AT PT. X

Darussalam[1)], Khuzainus Sajjaa[2)], Rita Yuniarti[3)]
Program Profesi Akuntansi Universitas Widyatama
Jl. Cikutra No.204A, Sukapada, Kec. Cibeunying Kidul, Kota Bandung, Jawa Barat 40125, Indonesia
Email: darussalam.5160@widyatama.ac.id[1)], khuzainus.sajjaa@widyatama.ac.id[2)], Rita.yuniarti@widyatama.ac.id[3)]

Abstrak

This research aims to analyze and evaluate the extent to which the implementation level of Information Security Management System (ISMS) is applied at Company X. The methods employed involve various approaches such as interviews, questionnaire administration, document review, observation, and assessing the maturity level based on the Information Security and Maturity Index (ISMI) with a rating scale ranging from 0 to 5. The interview results provided an assessment of the form of information security threats and controls that have been implemented. The questionnaire results indicated that compliance with standards reached 96% out of 34 presented questions. Furthermore, the document review revealed that there were three requirements in the annex standard that were not applied, including secure areas, security in development and support processes, and test data. In the gap analysis, a compliance rate of 95% out of 151 analysis points was found. Additionally, the observation results identified 6 minor non-compliance points and 1 point in the OFI (Opportunity For Improvement) category obtained during the internal audit activities. The entire research process served as a reference for determining the maturity level based on the ISMI, which resulted in an assessment of 94%, corresponding to level 5 (optimized). The findings of this research suggest that Company X needs to focus on enhancing data security through comprehensive data security awareness activities encompassing internal and third-party stakeholders, controls in project activities, collaboration with third parties, and fostering an information security risk culture throughout the organization.

***Key Words**: ISO 27001:2013, Information Security Management System, Security Information Risk, Maturity Level.*

1. PENDAHULUAN

Perkembangan dunia bisnis berlangsung sangat cepat seiring dengan keterlibatan teknologi dalam aktivitas bisnis, sehingga perusahaan dituntut untuk menerapkan konsep digitalisasi, baik pada sebagian ataupun seluruh proses bisnisnya, dalam kondisi tersebut perusahaan memerlukan fungsi dari Sistem Informasi Manajemen (SIM) sebagai fondasi penerapannya. Selain itu, Meskipun risiko yang dihadapi perusahaan disebabkan oleh pengaruh global dan revolusi industri 4.0, namun secara mengejutkan para pelaku usaha juga dihadapkan pada tantangan dari dampak pesatnya perkembangan revolusi industri yang semakin mempersulit perusahaan dan pengusaha untuk mengatasinya (**Tai, Lai, & Yang, 2020,** dalam **R. Ait Novatiani , Nunuy Nur Afiah, Roebiandini Sumantri, 2022**)

Salah satu penggunaan Sistem Informasi bagi perusahaan adalah dengan menerapkan penggunaan *Human Resource Information System* (HRIS). Perkembangan teknologi dan digitalisasi dalam dunia bisnis diikuti dengan risiko keamanan informasi, berdasarkan informasi yang diperoleh dari laporan tahunan Badan Siber dan Sandi Negara (BSSN) tahun 2022 menyebutkan bahwa jumlah notifikasi deteksi dini dan insiden siber sebanyak 1433 kasus, meskipun demikian capaian keamanan *cyber* di Indonesia dengan berdasarkan pengukuran *Skor Global Cybersecurity* Indeks (GCI) telah memenuhi target, yakni berada pada posisi 24. Lebih khusus, keamanan data pribadi menjadi perhatian penting, karena penggunaan HRIS mengolah berbagai data pribadi karyawan.

Menurut **G. J. Simons** (**2018**), keamanan informasi adalah bagaimana usaha untuk dapat mencegah penipuan (*cheating*) atau bisa mendeteksi adanya penipuan pada sistem yang berbasis informasi, di mana informasinya sendiri tidak memiliki arti fisik. Sementara, menurut **Darren Death** (**2017**) dalam buku *Information Security Management Handbook*, dijelaskan bahwa terdapat 3 (tiga) aspek yang harus dipenuhi dalam keamanan informasi di organisasi manapun, yaitu aspek kerahasiaan (*confidentiality*), keutuhan data (*data integrity*) dan ketersediaan (*availability*). Selain ketiga aspek tersebut, terdapat aspek keamanan tambahan yang harus dipenuhi yaitu otentifikasi penyediaan/penerima informasi (*authentication*) serta nir penyangkalan (*non repudiation*). Salah satu pengendalian yang secara khusus mengedepankan faktor keamanan informasi saat ini adalah ISO (*International Organization for Standardization*) 27001 (**Anarkhi, Ali and Kurnia, 2013**).

2. TINJAUAN PUSTAKA

Sistem Informasi Manajemen

Menurut **Murdick**, **Ross**, dan **Clugget** menyatakan bahwa Sistem Informasi Manajemen dengan layanan bahwa SIM itu kelompok orang, seperangkat pedoman dan petunjuk, peralatan pengolahan data yang digunakan untuk mengurangi ketidakpastian pada pengambilan keputusan dengan menghasilkan efisiensi untuk manajer pada waktu mereka dapat menggunakannya dengan efisien (**Liyas & Widyanti, 2020**), hal ini terdiri dari semua fungsi dalam organisasi seperti produksi, pemeliharaan, kualitas, sumber daya manusia, akuntansi, teknik (**Aida Wijaya, Ivan Gumilar, Arief Rahmana, Nadeem Khalid, 2019**)

Manajemen Keamanan Informasi

Menurut **Rachmawati, D., Darmawan, D., & Syahputra, R.** (**2017**) sistem keamanan informasi (*Information Security System*) adalah serangkaian langkah-langkah dan teknologi yang digunakan untuk melindungi data dan informasi dari akses yang tidak sah, perusakan, perubahan, atau pengungkapan yang tidak sah.

Sistem keamanan informasi dapat menjadi alat pengendalian internal dalam sisi keamanan informasi, yang mana pengendalian internal itu sendiri menurut **Veronica Christina**, **Andreas Sutiandi**, **Michael Frederick Korban** (**2020**), dalam **Mulyadi** (**2017**) sistem pengendalian internal merupakan suatu bentuk perencanaan yang mencakup struktur organisasi, metode terkoordinasi, dan tindakan untuk melindungi aset perusahaan, memeriksa keakuratan dan keandalan data akuntansi agar lebih tepat, mendorong efisiensi dan kepatuhan terhadap kebijakan manajemen untuk membuat karyawan lebih disiplin Tujuan utama dari sistem keamanan informasi adalah melindungi integritas, kerahasiaan, dan ketersediaan informasi. Integritas berarti bahwa informasi tetap utuh dan tidak diubah oleh pihak yang tidak berwenang. Kerahasiaan berarti bahwa informasi hanya dapat diakses oleh pihak yang berwenang. Ketersediaan berarti bahwa informasi dapat diakses oleh pihak yang berwenang pada saat yang dibutuhkan (**Kurniawan, T., 2017**). Sementara itu, menurut **Alfian, R. (2019)** sistem keamanan informasi terdiri atas beberapa komponen, seperti kebijakan keamanan informasi, infrastruktur keamanan, manajemen identitas dan akses, serta keamanan fisik.

Sistem Manajemen ISO (International Organization for Standardization)

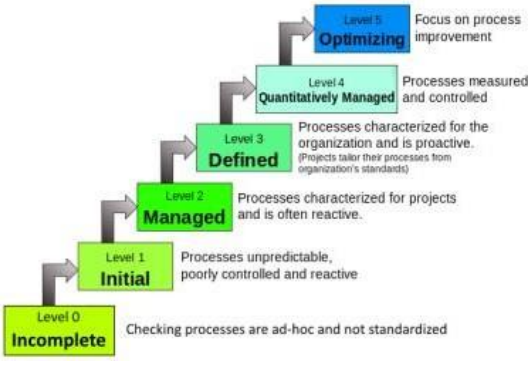
sebagai perusahaan yang bergerak dalam industry HRIS, dengan spesifik produk dalam *Payroll Management*, yang saat ini menerapkan sistem keamanan informasi ISO 27001, berfokus dalam pengelolaan risiko keamanan informasi, dengan penerapan sistem kerja *hybrid* (*Work Form Office & Anywhere*), kegiatan pengembangan produk secara rutin, dan kondisi sertifikasi ISO yang baru dalam tahapan *initial certification*.

ISO menerapkan pendekatan kerangka kerja PDCA (*plan do check act*) sebagai alat pengelolaan sistem manajemen yang diterapkan. PDCA adalah suatu pendekatan sistematis untuk mengelola proses yang meliputi empat tahap, yaitu perencanaan (*plan*), pelaksanaan (*do*), pemeriksaan (check), dan tindakan perbaikan (*act*). Pendekatan ini digunakan dalam berbagai jenis sistem manajemen ISO, termasuk ISO 9001 (manajemen mutu) dan ISO 14001 (manajemen lingkungan). Siklus PDCA (*Plan-Do-Check-Act*) adalah suatu metode

manajemen berkelanjutan yang melibatkan perencanaan, implementasi, evaluasi, dan tindakan perbaikan berkelanjutan. Siklus ini digunakan dalam banyak sistem manajemen, termasuk Sistem Manajemen ISO, untuk meningkatkan kinerja dan efektivitas organisasi (**Deming, W. E, 1986**).

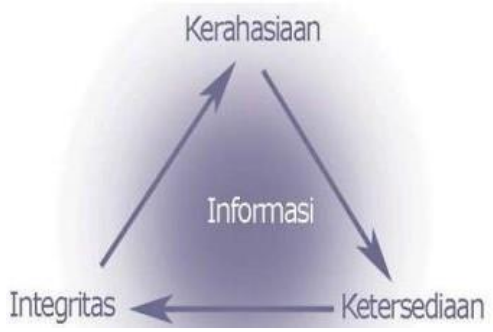
Indeks Keamanan Informasi (KAMI)

Sistem Keamanan Informasi (SKI) adalah suatu sistem yang dirancang untuk melindungi informasi dari ancaman, kerusakan, pencurian, atau penggunaan yang tidak sah. Badan Siber dan Sandi Negara (BSSN) sebagai lembaga yang bertanggung jawab dalam pengamanan siber di Indonesia telah merancang suatu Sistem Keamanan Informasi yang dikenal dengan sebutan Sistem Keamanan Informasi Nasional (SKIN) atau National Information Security System (NISS). SKIN/NISS BSSN terdiri dari tiga domain utama yaitu Domain Kebijakan Keamanan Informasi (DKKI), Domain Pengamanan Teknologi Informasi (DPTI), dan Domain Pengamanan Operasional Keamanan Informasi (DPOKI). Untuk mencapai ketiga aspek pengendalian keamanan informasi, SKIN BSSN menggunakan serangkaian kebijakan, prosedur, teknologi, dan organisasi yang terintegrasi dengan baik. SKIN BSSN didasarkan pada prinsip-prinsip yang tercantum dalam berbagai standar internasional seperti ISO/IEC 27001, ISO/IEC 27002, *NIST Cybersecurity Framework*, dan COBIT 5 (**Pedoman Umum Sistem Keamanan Informasi Nasional (SKIN), 2018**). Menurut Titus Kristanto dkk., tingkatan dalam mengukur tingkat kematangan penerapan keamanan informasi dapat terbagi ke 6 klasifikasi, yaitu *incomplete, initial, managed, defined, Quantitatively Managed,* dan *Optimizing.* Berikut disajikan ilustrasi tingkat kematangan penerapan keamanan informasi :



Sistem Manajemen Keamanan Informasi Seri ISO 27001

Menurut **ISO/IEC 27000:2014** (**2014**), *Information Security Management System* (ISMS) adalah pendekatan sistematis yang mencakup menetapkan, mengimplementasi, untuk operasional, pemantauan, peninjauan, pemeliharaan dan meningkatkan keamanan informasi pada organisasi untuk mencapai tujuan bisnis. ISO 27001 merupakan standar untuk mengaudit keamanan sebuah sistem informasi dan digunakan sebagai acuan untuk menghasilkan dokumen (temuan dan rekomendasi). Menurut **Chazar** (**2015**) ISO/IEC 27001 merupakan standar yang sering digunakan untuk mengetahui kebutuhan untuk menerapkan keamanan sistem informasi. Dengan penerapan ISO/IEC 27001 dapat melindungi aspek-aspek dari keamanan informasi yaitu *confidentiality*, *integrity* dan *availability*.



Gambar 2.1 Aspek-aspek Keamanan Informasi

Sumber : Syafrizal M: ISO 17799: Standar Sistem Manajemen Keamanan Informasi. https://www.academia.edu/5082000/ISO_17799_Standar_Sistem Manajemen_Keamanan_Informasi, diakses pada 2 Mei 2023.

Gambar 2.1 memberikan gambaran bagaimana tiga aspek keamanan informasi yang saling keterkaitan satu sama lainnya, yakni kerahasiaan, integritas dan ketersediaan. Kerahasiaan adalah kondisi informasi yang aman dari pengungkapan yang tidak disetujui, atau dari otoritas yang tidak berkepentingan terhadap informasi tersebut. Ketersediaan adalah memastikan bahwa informasi selalu tersedia untuk diakses oleh usernya. Integritas adalah dimana pihak yang memiliki kewenangan terhadap data dan informasi dapat mengendalikan dirinya untuk menggunakan informasi sebagaimana mestinya (jaminan keamanannya).

3. METODOLOGI PENELITIAN

Jenis Penelitian

Jenis penelitan ini menggunakan pendekatan kualitatif, karena data yang penulis ambil dalam bentuk fenomena dan dapat di deskripsikan, yaitu berupa wawancara dengan top management serta personal unit terkait di perusahaan, kuesioner, dan tinjauan dokumen, serta hasil observasi langsung penulis terhadap topik dan objek penelitian secara berkala dan terstruktur.

Unit Analisis dan Waktu Penelitian

Unit analisis dari penelitian ini adalah PT X adalah yang merupakan sebuah perusahaan *platform Human Resouce Information System*, yang saat ini berfokus pada payroll management, dengan rentang waktu rentang waktu Februari – Agustus 2023 di PT X.

Menurut **Chazar (2015)** ISO/IEC 27001 merupakan standar yang sering digunakan untuk mengetahui kebutuhan untuk menerapkan keamanan sistem informasi. Dengan penerapan ISO/IEC 27001 dapat melindungi aspek-aspek dari keamanan informasi yaitu *confidentiality*, *integrity* dan *availability*.

ISO 27001 memiliki 133 kontrol keamanan informasi, dan pada pelaksanaannya perusahaan dapat memilih kontrol mana yang paling relevan dengan kondisi di lapangan (**Wiryana et al., 2012**).

ISO 27001 memiliki kelebihan yaitu standar ini sangat fleksibel yang dikembangkan tergantung kebutuhan organisasi, tujuan organisasi, persyaratan keamanan dan juga SNI ISO 27001 menyediakan sertifikat implementasi Sistem Manajemen Keamanan Informasi (SMKI) yang diakui secara nasional dan internasional yang disebut *Information Security Management System* (**R.A. Kusuma, 2014**).

Operasional Variabel

Menurut **Sugiyono** (**2010**) bahwa "Operasionalisasi variabel adalah segala sesuatu yang berbentuk apa saja yang ditetapkan oleh peneliti untuk dipelajari sehingga diperoleh informasi tentang hal tersebut, kemudian ditarik kesimpulannya." Variabel dalam penelitian ini adalah Persyaratan ISO 27001:2013 (ISO/IEC 27001:2013), dengan klasifikasi dimensi dibagi menjadi 4, yaitu *plan, do, check*, dan *act*. Indikator terbagi menjadi konteks organisasi, kepemimpinan, perencanaan, dukungan, operasi, evaluasi kinerja, perbaikan, dan Pengendalian Sistem Keamanan Informasi. Penggunaan skala adalah ordinal, dengan total sebanyak 34 nomor.

Jenis dan Sumber Data Penelitian

Sumber data primer adalah sumber data yang langsung memberikan data kepada pengumpul data. Sumber ini bisa berupa orang, atau pengukuran atau instrumen-instrumen dan lain sebagainya (**Rukaesih A. Maolani, 2016**). Dalam penelitian ini, data primer diperoleh dengan melakukan observasi, kuesioner dan wawancara terstruktur dan mendalam pada narasumber yang telah ditentukan.

Sumber data sekunder adalah sumber data tidak langsung memberikan data kepada pengumpul data, misalnya lewat orang lain, atau lewat dokumen (**Rukaesih A. Maolani, 2016**). Dalam penelitian ini, data yang diperoleh dari perusahaan yang bersangkutan berupa dokumen-dokumen yang menyertakan informasi dalam menunjang penelitian (*document review*). Selain itu, dilakukan studi literatur dalam penelitian untuk memperoleh teori-teori yang berhubungan dengan penelitian ini. Adapun dalam penelitian ini seluruh jenis data meliputi data primer dan sekunder dipergunakan untuk dapat mengetahui penerapan Sistem Keamanan Informasi berbasis ISO 27001:2013, kemudian disajikan laporan hasil penelitian dan saran perbaikan.

Teknik Pengumpulan Data

Teknik pengumpulan data pada penelitian ini mencakup observasi, kuesioner, wawancara, dan dokumentasi. Observasi dilakukan dengan meninjau ketersediaan dokumen yang bersesuaian dan implementasinya sesuai dengan persyaratan ISO 2700: 2013 pada pelaksanaan Audit Internal. Kuesioner mencakup model kuesioner terbuka dan tertutup, kuesioner (angket) terbuka digunakan untuk mendapatkan data survei awal, yang bertujuan memastikan bahwa responden penelitian mengetahui dan memahami berbagai fenomena yang terkait dengan

penerapan Sistem Keamanan Informasi di PT X. Sedangkan kuesioner (angket) tertutup dalam penelitian ini digunakan untuk mengetahui persepsi secara spesifik terkait pertanyaan-pertanyaan tertentu yang ditentukan, untuk mengetahui tingkat penerapan Sistem Keamanan Informasi berbasis ISO 27001:2013 di PT X.
Pada penelitian ini wawancara dilakukan pada tahapan identifikasi masalah terkait penerapan ISO 27001:2013 di perusahaan, pembuatan dokumen *statement of applicability* (SoA), *risk assessment* dan audit internal, dimana peneliti yang berlaku sebagai auditor mengkonfirmasi kegiatan observasi yang peneliti lakukan, serta hasil pengisian kuesioner dari *auditee*, sedangkan pendekatan dokumentasi dokumentasi merupakan pelengkap dari metode observasi dan wawancara, dalam bentuk hasil observasi, rekapitulasi kuesioner dan dokumen hasil internal audit.

Populasi dan Sampel Penelitian
Dalam penelitian ini, populasi adalah karyawan PT X pada posisi kerja yang termasuk dalam cakupan penerapan Standar dan termasuk dalam struktur organisasi penerapan ISMS 27001:2013 yang telah ditentukan oleh Manajemen di PT X, yaitu bagian Top Management (CEO & Vice President of Engineer), Internal Auditor, ISMS Coordinator, Security Engineer, Site Reliability Engineer, Human Resource, dan Legal dengan total karyawan (populasi) sebanyak 11 orang Karyawan, Metode Total Sampel merupakan teknik pengambilan sampel dimana jumlah sampel sama dengan populasi. Alasan mengambil total sampling karena jumlah populasi yang kurang dari 100 seluruh populasi dijadikan sampel penelitian semuanya. (Masturoh & Anggita, 2018)
Berdasarkan teori sampel tersebut, sehingga didapati sampel dalam penelitian ini adalah sebanyak 11 orang karyawan PT X, sesuai dengan Struktur Organisasi Sistem Manajemen Keamanan Informasi PT X.

Metode Analisis
Metode analisis dalam penelitian ini mencakup reduksi data, triangulasi, dan penarikan kesimpulan.

4. HASIL DAN PEMBAHASAN
4.1 Hasil Penelitian
4.1.1 Hasil pada kegiatan wawancara
Menunjukkan bahwa penilaian konteks organisasi telah dilaksanakan melalui penyediaan analisis kebijakan dan prosedur internal dan eksternal, identifikasi kebutuhan pemangku kepentingan, penetapan cakupan aplikasi ISMS ISO 27001:2013 dalam bentuk "Keamanan Informasi di Platform Penggajian PT. X," dan penyediaan manual dokumen ISMS ISO 27001:2013 PT. X. Indikator kepemimpinan diimplementasikan melalui penyediaan pernyataan keamanan informasi dan promosinya dalam acara town hall perusahaan tahun 2022. Indikator perencanaan diimplementasikan melalui pembentukan prosedur Manajemen Risiko, penetapan Tujuan ISMS untuk tahun 2023, dan indikator dukungan diimplementasikan melalui penyediaan tenaga kerja manusia, infrastruktur, dan manajemen informasi yang terdokumentasi. Indikator operasional diimplementasikan melalui penyediaan prosedur operasional dan pengelolaan proses bisnis yang aman dari ancaman dan kerentanan keamanan informasi yang dapat dimanfaatkan. Indikator evaluasi kinerja diimplementasikan melalui penyediaan prosedur audit internal dan tinjauan manajemen. Indikator perubahan diimplementasikan melalui penerapan prinsip perbaikan berkelanjutan pada tingkat korporat, departemen, dan personal. Indikator Kontrol Sistem Keamanan Informasi diimplementasikan melalui Pedoman ISMS, Kebijakan Keamanan Informasi, Kebijakan Penggunaan TI, Kebijakan Manajemen Risiko, dan kebijakan manajemen perubahan. Berdasarkan hasil dan diskusi yang dilakukan selama kegiatan wawancara, dapat disimpulkan bahwa PT. X telah menerapkan semua indikator sistem manajemen keamanan informasi.

4.1.2 Hasil Kuesioner
Berdasarkan kuesioner yang telah dibuat, dikirimkan serta diisi oleh responden dengan jumlah 11 responden, yang mencakup pertanyaan perihal konteks organisasi, kepemimpinan, perencanaan sumber daya, operasi, evaluasi performa, peningkatan, pengendalian sistem keamanan informasi, maka didapati perspektif penerapan keamanan informasi yang dijelaskan dalam tabel berikut ini :

Tabel 4.1 Hasil Kuesioner

Nomor	Indikator	Butir Pertanyaan	Jumlah Nilai Optimal	Jumlah Penilaian Responden	Persentase Penilaian
[A]	[B]	[C]	[D]	[E]	[E/D]
1	Konteks Organisasi	3	165	165	100%
2	Kepemimpinan	3	165	165	100%
3	Perencanaan	4	220	220	100%
4	Sumber Daya	4	220	193	88%
5	Operasi	3	165	160	97%
6	Evaluasi Performa	2	110	110	100%
7	Peningkatan	1	55	55	100%
8	Pengendalian Sistem Keamanan Informasi	14	770	732	95%
	Jumlah	34	1870	1800	96%

Dari tabel 4.1 diketahui bahwa berdasarkan hasil pengisian kuesioner oleh 11 responden, dari total 34 pertanyaan, didapati nilai pemenuhan standar sebesar 96%.

4.1.3 Hasil Tinjauan Dokumen

Tinjauan dokumen dilakukan pada segala bentuk kebijakan, prosedur, dan instruksi kerja yang berlaku diperusahaan, dibandingkan dengan persyaratan standar ISO 27001:2013. Tinjauan dokumen dilakukan dengan metode analisa gap dan tinjauan *statement of applicablebility* (SoA),

Dokumen *statement of applicablebility* (SoA) menyajikan panduan tentang kontrol keamanan informasi yang relevan yang akan diimplementasikan oleh organisasi untuk melindungi informasi sensitif dan kritis dari potensi ancaman dan risiko Berdasarkan hasil penilaian relevansi penerapan standar yang tertuang dalam dokumen *Statement of Applicableability* (SoA) maka didapati dari 114 poin persyaratan, maka PT X menerapkan 111 persyaratan, sehingga 3 persyaratan dikecualikan dari penerapan dengan judgment tertentu yang sudah disepakati berdasarkan rapat tim manajemen dan koordinator ISMS di PT X dengan meninjau atau mempertimbangkan profil, sifat, serta karakteristik proses bisnis perusahaan.

Sementara analisa gap adalah membandingkan kebijakan dan praktik keamanan informasi yang telah ada di PT X dengan persyaratan yang ditetapkan oleh standar ISO 27001:2013, Berdasarkan hasil Analisa Gap tersebut, didapati hasil pemenuhan berjumlah 144 poin persyaratan atau sebesar 95% dari total seluruh poin identifikasi yang diterapkan, sementara 6 poin persyaratan (4%) belum diterapkan.

Gap yang ditemui umumnya terkait pengendalian keamanan informasi karyawan, seperti dalam bentuk screening karyawan dan pengelolaan keamanan informasi dari aktivitas kerja yang melibatkan pihak ketiga, selain itu pengelolaan pengumpulan bukti yang juga dinilai sebagai bagian dari gap pemenuhan persyaratan. Gap yang didapati selaras dengan hasil pengisian kuesioner yang dilakukan oleh para responden, yang merupakan pihak yang berkaitan langsung dengan implementasi ISO 27001:2013.

Tindak lanjut tersebut mengarah ke pemenuhan dokumen baik dalam bentuk kebijakan ataupun prosedur, dalam bentuk pembuatan dokumen baru, atau pembaruan, untuk menjamin pengendalian keamanan informasi pada beragam aktivitas kerja unit.

4.1.4 Hasil Observasi

Hasil observasi diperoleh dari kegiatan Audit Internal, yang melakukan pemeriksaan kepada seluruh unit terkait, sesuai cakupan penerapan, dokumen statement of applicabilities (SoA), dan tinjauan hasil penilaian risiko yang dilakukan. Berdasarkan kegiatan Audit Internal yang dilakukan, berikut disajikan hasil pengukurannya:

Tabel 4.2 : Hasil Pemeriksaan Internal Audit

Nomor	Indikator	Jumlah Poin Audit	Jumlah Temuan Kesesuaian	Jumlah Temuan Ketidaksesuaian		Jumlah Temuan OFI
				Minor	Major	
1	Konteks Organisasi	3	3	0	0	
2	Kepemimpinan	3	3	0	0	
3	Perencanaan	4	4	0	0	
4	Sumber Daya	4	2	2	0	
5	Operasi	3	2	0	0	
6	Evaluasi Performa	2	2	0	0	
7	Peningkatan	1	1	0	0	
8	Pengendalian Sistem Keamanan Informasi	14	9	4	0	1
	Jumlah	34	27	6	0	1

Sumber : Data Penelitian

Berdasarkan tabel 4.2 diketahui bahwa berdasarkan pemeriksaan dalam kegiatan Audit Internal, dari 34 poin Audit, didapati 27 poin kesesuaian dan 6 poin ketidaksesuaian (*minor*), dan 1 temuan kategori *opportunity for improvement*, yang mana dari ketidaksesuaian yang didapati, tidak ditemui adanya temuan ketidaksesuaian kategori major. Selanjutnya, temuan dibuat tindakan perbaikan untuk setiap ketidaksesuaian, dalam bentuk *correction* dan *corrective* :

Tabel 4.3 Penilaian Kepatuhan Audit Internal Standar ISO 27001:2013 PT X

No	Poin Audit	Bukti Temuan	Correction	Corrective	PiC
1	Perusahaan menentukan dan meningkatkan kompetensi yang memenganuhi kinerja keamanan informasinya	Kegiatan rekruitmen tahun 2023	Membuat dokumen gap kompetensi dan *training need analysis*	Membuat kebijakan atau prosedur rekruitmen karyawan, yang mencakup analisa gap dan *training need analysis*	HRGS
2	Perusahaan mengelola informasi terdokumentasi yang dibutuhkan oleh SMKI	*Record* analisa isu internal dan eksternal, serta identifikasi pihak yang bersesuaian	Membuat dokumen (*record*) bagi informasi yang belum terdokumentasi secara memadai, seperti rekaman analisa isu internal dan eksternal, serta identifikasi pihak yang berkepentingan	Menetapkan kebijakan atau prosedur pengelolaan *record* dokumen	Doc. Controller
3	Perusahaan menetapkan pengendalian keamanan informasi pada proses yang melibatkan pihak ketiga	Bentuk kerjasama dengan pihak ketiga telah tersedia, namun belum mencakup tanggung jawab keamanan informasi dan asesmennya	Melakukan tinjauan fungsi dan tanggungjawab-nya	Membuat kebijakan *supplier / third party security*	SRE
4	Perusahaan menetapkan serangkaian kebijakan untuk keamanan informasi yang dikomunikasik-an kepada karyawan dan pihak eksternal yang relevan	Prosedur kerja jarak jauh, dan bukti peninjauan kepatuhan kebijakan password	Melakukan pembaruan pada prosedur kerja jarak jauh dan melakukan monitoring kepatuhan *password policy*	Menetapkan monitoring kepatuhan password pada *password policy*	HRGS
5	Perusahaan menetapkan kebijakan pengendalian sumber daya manusia, mulai pengadaan, pemeliharaan hingga pemutusan hubungan kerja	Prosedur rekruitmen karyawan dan pengelolaan kerja karyawan	Membuat bukti rekruitmen dan *screening* karyawan	Membuat prosedur rekruitmen karyawan	HRGS
6	Perusahaan menetapkan kebijakan pengendalian fisik dan lingkungan kerja keamanan informasi di perusahaan	Prosedur perlindungan fisik dan lingkungan kerja	Pengenaan identitas karyawan secara konsisten bagi karyawan yang kerja di kantor (WFO)	Menetapkan prosedur pengenaan identitas diri dalam prosedur WFO	HRGS

Berdasarkan tabel 4.3 diketahui bahwa tindakan perbaikan *correction* adalah perbaikan pada cakupan penerapan standar, sementara kategori *corrective* dalam bentuk ketentuan dan prosedur, dengan harapan tidak terulang kembali ketidaksesuaian tersebut di masa yang akan datang.

4.2 Pembahasan

4.2.1 Pembahasan Hasil Penilaian Konteks Organisasi

Berdasarkan hasil wawancara, kuesioner, tinjauan dokumen, dan observasi yang telah dilakukan sebagaimana dijelaskan pada pembahasan di atas, maka didapati penilaian bahwa perusahaan telah menerapkan persyaratan standar terkait konteks organisasi, sebagaimana disebutkan dalam klausul 4 standar Sistem Manajemen Keamanan Informasi ISO 27001:2013, dengan bukti berupa dokumen hasil analisa SWOT keamanan informasi, daftar pihak yang berkepentingan yang disertai dengan kebutuhan dan harapannya, penentuan scope ISMS, dan manual dokumen ISMS. Sementara itu, pada penilaian indikator konteks organisasi ini, tidak ditemui adanya temuan ketidaksesuaian.

4.2.2 Pembahasan Hasil Penilaian Indikator Kepemimpinan

Berdasarkan hasil wawancara, kuesioner, tinjauan dokumen, dan observasi yang telah dilakukan sebagaimana dijelaskan pada pembahasan di atas, maka didapati penilaian bahwa perusahaan telah menerapkan persyaratan standar terkait kepemimpinan, sebagaimana disebutkan dalam klausul 5 standar Sistem Manajemen Keamanan Informasi ISO 27001:2013, dengan bukti berupa dokumen information security statement yang telah ditetapkan dan disosialisikan oleh CEO PT X, selain itu top management juga mencantumkan prinsip keamanan informasi pada ID Card karyawan, penyampaian rutin pada sesi town hall karyawan, serta dalam kegiatan awareness keamanan informasi, sebagai upaya dalam internalisasi prinsip keamanan informasi untuk setiap karyawan PT X. Sementara itu, pada penilaian indikator kepemimpinan ini, tidak ditemui adanya temuan ketidaksesuaian.

4.2.3 Pembahasan Hasil Penilaian Indikator Perencanaan

Berdasarkan hasil wawancara, kuesioner, tinjauan dokumen, dan observasi yang telah dilakukan sebagaimana dijelaskan pada pembahasan di atas, maka didapati penilaian, bahwa perusahaan telah menerapkan persyaratan standar terkait perencanaan, sebagaimana disebutkan dalam klausul 6 standar Sistem Manajemen Keamanan Informasi ISO 27001:2013, dengan bukti berupa penyediaan tujuan penerapan ISMS dalam bentuk ISMS Objectives Document, prosedur pengelolaan risiko keamanan informasi, serta struktur ISMS khusus dalam penerapan standar SMKI di PT X. Adapun pada penilaian indikator perencanaan ini, tidak ditemui adanya temuan ketidaksesuaian.

4.2.4 Pembahasan Hasil Penilaian Indikator Dukungan

Berdasarkan hasil wawancara, kuesioner, tinjauan dokumen, dan observasi yang telah dilakukan sebagaimana dijelaskan pada

pembahasan di atas, maka didapati penilaian, bahwa perusahaan telah menerapkan persyaratan standar terkait Dukungan, sebagaimana disebutkan dalam klausul 7 standar Sistem Manajemen Keamanan Informasi ISO 27001:2013, dengan bukti berupa perencanaan dan penyediaan karyawan dan infrastruktur keamanan informasi, penyediaan aktivitas pelatihan karyawan, kegiatan peningkatan *awareness* keamanan informasi, penetapan saluran komunikasi karyawan, dan pengelolaan informasi terdokumentasi. Namun demikian, dalam penialaian indikator Dukungan ini, terdapat 2 (dua) temuan ketidaksesuaian yang berkategori Minor yang didapati, yaitu berupa ketiadaan kegiatan analisa gap kompetensi, serta prosedur dan penerapan record untuk unit terkait sesuai cakupan penerapan standar ISMS. Tindak lanjut dari temuan tersebut berupa penyediaan *Gap Competence Record*, serta prosedur pengelolaan rekaman unit.

4.2.5 Pembahasan Hasil Penialain Indikator Operasi

Berdasarkan hasil wawancara, kuesioner, tinjauan dokumen, dan observasi yang telah dilakukan sebagaimana dijelaskan pada pembahasan di atas, maka didapati penilaian bahwa perusahaan telah menerapkan persyaratan standar terkait Operasi, sebagaimana disebutkan dalam klausul 8 standar Sistem Manajemen Keamanan Informasi ISO 27001:2013, dengan bukti berupa dokumen *risk assessment* and *treatment monitoring* dan *disaster recovery plan testing* (*simulation*). Adapun pada penilaian indikator Operasi ini, tidak ditemui adanya temuan ketidaksesuaian.

4.2.6 Pembahasan Hasil Penialain Indikator Evaluasi Kinerja

Berdasarkan hasil wawancara, kuesioner, tinjauan dokumen, dan observasi yang telah dilakukan sebagaimana dijelaskan pada pembahasan di atas, maka didapati penilaian bahwa perusahaan telah menerapkan persyaratan standar terkait Evaluasi Kinerja, sebagaimana disebutkan dalam klausul 9 standar Sistem Manajemen Keamanan Informasi ISO 27001:2013, dengan bukti berupa laporan pengukuran *ISMS Objectives*, laporan kegiatan dan hasil internal audit, dan laporan hasil tinjauan manajemen. Adapun pada penilaian indikator Evaluasi Kinerja ini, tidak ditemui adanya temuan ketidaksesuaian.

4.2.7 Pembahasan Hasil Penialain Indikator Perbaikan

Berdasarkan hasil wawancara, kuesioner, tinjauan dokumen, dan observasi yang telah dilakukan sebagaimana dijelaskan pada pembahasan di atas, maka didapati penilaian bahwa perusahaan telah menerapkan persyaratan standar terkait Perbaikan, sebagaimana disebutkan dalam klausul 10 standar Sistem Manajemen Keamanan Informasi ISO 27001:2013, dengan bukti berupa *correction prevention action* sesuai dokumen CPAR, peningkatan kompetensi karyawan, pembuatan serta peningkatan prosedur, dan penerapan *Mobile Device Management* untuk kegiatan operasional perusahaan. Adapun pada penilaian indikator Perbaikan ini, tidak ditemui adanya temuan ketidaksesuaian.

4.2.8 Pembahasan Hasil Penialain Indikator Pengendalian Sistem Keamanan Informasi

Berdasarkan hasil wawancara, kuesioner, tinjauan dokumen, dan observasi yang telah dilakukan sebagaimana dijelaskan pada pembahasan di atas, maka didapati penilaian bahwa perusahaan telah menerapkan persyaratan standar terkait Pengendalian Sistem Keamanan Informasi, sebagaimana disebutkan dalam *annex* standar Sistem Manajemen Keamanan Informasi ISO 27001:2013, dengan berbagai bukti sebagai berikut :

A. Kebijakan Keamanan Informasi
   Pemenuhan bukti berupa kebijakan *ISMS Guideline*, prosedur *Mobile Device Policy*, kebijakan *Bring Your Own Device Policy*, dan kontak dengan pihak otoritas.
B. Keamanan Sumber Daya Manusia
   Pemenuhan bukti hanya dalam bentuk NDA (*non-disclousure agreement*) karyawan, oleh karena itu terdapat temuan ketidaksesuaian (*minor*) dalam bagian ini, dengan tindak lanjut berupa dokumen *Human Resource Security Procedure*, yang melakukan pengendalian keamanan karyawan dari

sebelum karyawan bekerja, ketika bekerja, hingga ketika karyawan tidak melanjutkan hubungan kerja.

C. Manajemen Aset
Pemenuhan bukti berupa prosedur dan penerapan pengelolaan aset, seperti asset register, penetapan klasifikasi informasi, dan penanganan media.

D. Pengendalian Akses
Pemenuhan bukti berupa kebijakan autorisasi akses, dengan implementasi dalam bentuk *User Access Matrix* (UAM).

E. Kriptografi
Pemenuhan bukti berupa kebijakan password, namun dalam hal ini, terdapat temuan ketidaksesuaian (*minor*) berupa ketiadaan metode pemantauan kepatuhan password. Tindak lanjut dari temuan tersebut berupa pemantauan kepatuhan *password* dengan penerapan *Mobile Device Management* pada aplikasi Jumpcloud.

F. Pengendalian Keamanan Lingkungan Fisik
Dalam penilaian sub-indikator ini, terdapat temuan yang diperoleh, yaitu berupa ketiadaan prosedur dan praktik pengendalian keamanan fisik lingkungan kerja di kantor Menara Palma. Hal tersebut diketahui karena perusahaan menerapkan sistem kerja remote working, sehingga pengendalian keamanan fisik belum ditentukan secara spesifik. Tindak lanjut dari temuan ini adalah berupa pembentukan dokumen *Physical Environment Policy*, dengan implementasi berupa pengendalian fisik pada lingkungan kantor perusahaan, seperti perlindungan dokumen berdasarkan klasifikasinya, perlindungan layar dan suara (*screen and voice protection*).

G. Pengendalian Keamanan Operasi
Pemenuhan bukti berupa penetapan *operation security policy*, dengan implementasi berupa penetapan prosedur proses *coding* dan *development software*, prosedur *change management*, manajemen kapasitas, pemisahan lingkungan produksi dan *development*, pengendalian dalam perlindungan dari *malware*, penetapan prosedur *backup* dan *restore*, prosedur *logging* dan *monitoring*, manajemen kerentanan dan pengendalian aktivitas audit.

H. Pengendalian Keamanan Komunikasi
Pemenuhan bukti berupa penerapan *communication security*, dengan implementasi berupa pengendalian akses *network* dengan VPN, pengendalian transfer informasi baik dengan pengendalian media, metode dan objek transfer informasi.

I. Pengendalian Keamanan Perolehan, Peningkatan, dan Perawatan Sistem
Pemenuhan bukti berupa penerapan prosedur *application security* dan prosedur *change management*, dengan implementasi dalam keamanan pengembangan produk, dari mulai penerapan *requirement*, proses development, hingga *release update*.

J. Pengendalian Hubungan Supplier
Pemenuhan bukti sementara berupa dokumen kerjasama dengan pihak ketiga (vendor). Dalam penilaian ini didapati temuan ketidaksesuaian (minor) berupa ketiadaan asesmen pihak ketiga khususnya perihal keamanan informasi, selain itu tanggungjawab keamanan informasi belum ditetapkan secara eksplisit. Tindak lanjut dari temuan ini adalah berupa penetapan kebijakan supplier security (corrective) dan revisi dokumen kerjasama dengan pihak ketiga (correction).

K. Pengendalian Insiden Keamanan Informasi
Pemenuhan bukti berupa dokumen incident management procedure, dengan penerapan berupa incident register record, yang telah memuat konteks insiden, root cause analysis, correction, corrective, dan penanggung jawab. Dalam hal ini terdapat temuan kategori OFI (*Opportunity for Improvement*) berupa penyediaan dan leason learning dalam incident register.

L. Pengendalian Manajemen Keberlanjutan
Pemenuhan bukti berupa penetapan *business continuity management policy*, dengan implementasi berupa penetapan aspek-aspek *vulnerability* yang berdampak dengan keberlanjutan perusahaan secara langsung, yang disertai dengan simulasi dalam bentuk *disaster recovery testing*.

M. Kepatuhan

Pemenuhan bukti berupa identifikasi regulasi yang bersesuaian dengan keamanan informasi, serta adopsinya pada kebijakan internal perusahaan (*document PT X Information Security Guideline*).

4.2.9 Pengukuran Maturity Level ISO27001:2013

Setelah mengetahui hasil wawancara, pengisian kuesioner, tinjauan dokumen, dan kegiatan Audit Internal, maka dilakukan pengukuran *maturity level* untuk mengetahui sejauh mana tingkat penerapan sistem manajemen keamanan informasi standard ISO 27001:2013 dari PT X, berdasarkan klasifikasi tingkatan indeks keamanan informasi dari BSSN (KAMI). Instrumen pengukuran *maturity level* yang digunakan dijelaskan pada tabel berikut ini :

Tabel 4.4 Instrumen Pengukuran Maturity Level

Level	Skala Index Maturity	Deskripsi
0 - *Non Existent*	0% - 18%	Belum adanya permasalahan yang harus diatasi. Perusahaan merasa tidak membutuhkan mekanisme proses keamanan, sehingga tidak ada pengawasan sama sekali.
1 - *Initial/ Ad Hoc*	19% - 36%	Sudah adanya bukti bahwa perusahaan mengetahui adanya permasalahan yang harus diatasi. Perusahaan sudah memiliki inisiatif untuk melakukan keamanan, namun sifatnya masih *non-formal*.
2 - *Repeatable but Intuitive*	37% - 54%	Sudah adanya perencanaan, pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Perusahaan memiliki kebiasaan terpola untuk merencanakan keamanan yang dilakukan secara berulang, namun belum melibatkan dokumen formal.
3 - *Defined*	56% - 72%	Sudah memiliki proses keamanan yang sudah didokumentasikan dengan baik, kemudian dikomunikasikan melalui pelatihan. Perusahaan juga menyadari perlunya proses keamanan sehingga adanya aturan yang menunjukkan untuk perusahaan secara rutin melakukan keamanan.
4 - Managed and Measurable	73% - 90%	Sudah adanya proses komputerisasi dengan baik, pengembangan sistem sudah terarah dan dijalankan secara terorganisir. Proses keamanan sudah secara formal dilakukan dan secara terus menerus dievaluasi untuk meningkatkan layanan perusahaan.
5- *Optimised*	91% - 100%	Sudah mengikuti *best practice* yang ditandai dengan adanya proses otomatisasi pada sistem dengan metodologi yang tepat.

Sumber : Eri Eriana, Meiva Eka Sri Sulistyawati, dan Octa Pratama Putra. Analisis Tingkat Kematangan (Maturity Level) Dan PDCA (Plan-Do-Check-Act) Dalam Penerapan Audit Sistem Manajemen Keamanan Informasi Pada PT Indonesia Game Menggunakan. Journal of Information System Research. 4(2), pp. 632-640.

Untuk mengetahui tingkat kematangan (*maturity level*) penerapan Klausul dan Annex, maka digunakan rumus *maturity level* sebagai berikut (rumus 1) :

$$Indeks\ Maturity = \frac{\text{Hasil Penilaian}}{Target\ Capaian} x100\% \text{.....(1)}$$

Pada rumus (1) dijelaskan bagaimana mengetahui tingkat kematangan penerapan Klausal dan Annex, yaitu dengan cara menghitung hasil penilaian yang dibagi dengan target capaian kemudian di kali 100%, setelah itu dihitung secara rata-rata, untuk mengetahui nilai akhir dari tingkat kematangan penerapan keamanan informasi berdasarkan indeks KAMI BSSN.

Berdasarkan penilaian pada kegiatan Audit Internal, yang didukung dengan wawancara, pengisian kuesioner, tinjauan dokumen, serta tindak lanjut temuan hasil internal audit, maka didapati hasil pengukuran Maturity Level sebagai berikut :

Tabel 4.5 *Hasil Analisis Maturity Level Penerapan Sistem Manajemen Keamanan Informasi berdasarkan Indeks KAMI*

No	Poin Penilaian		Target	Penilaian	
	No Klausul / Annex	Objek	(Nilai)	Nilai	Persentase
1	4.1	Konteks Organisasi	5	5	100%
2	4.2		5	5	100%
3	4.3		5	5	100%
4	4.4		5	5	100%
5	5.1 - 5.2	Kepemimpinan	5	5	100%
6	5.3		5	5	100%
7	6.1.1	Perencanaan	5	5	100%
8	6.1.2		5	5	100%
9	6.1.3		5	5	100%
10	6.2		5	5	100%
11	7.1	Sumber Daya	5	5	100%
12	7.2		5	3	60%
13	7.3		5	5	80%
14	7.4		5	4	87%
15	7.5		5	3	67%
16	8.1	Operasi	5	5	100%
17	8.2-8.3		5	5	100%
18	9.1	Evaluasi Kinerja	5	5	100%
19	9.2		5	5	100%
20	10	Perbaikan	5	5	100%
21	A.5	Kebijakan keamanan informasi	5	4	80%
22	A.6	Organisasi keamanan informasi	5	5	97%
23	A.7	Keamanan sumber daya manusia	5	4	77%
24	A.8	Manajemen aset	5	5	100%
25	A.9	Kendali akses	5	5	100%
26	A.10	Kriptografi	5	5	100%
27	A.11	Keamanan fisik dan lingkungan	5	5	92%
28	A.12	Keamanan operasi	5	5	100%
29	A.13	Keamanan komunikasi	5	5	100%
30	A.14	Akuisisi, pengembangan, dan perawatan sistem	5	5	98%
31	A.15	Hubungan pemasok	5	5	92%
32	A.16	Manajemen insiden keamanan informasi	5	4	89%
33	A.17	Aspek keamanan informasi dari manajemen keberlangsungan bisnis	5	5	100%
34	A.18	Kepatuhan	5	5	93%
Total Maturity Level			**5**		**94%**

Penyajian penilaian pada tabel 4.8 menggunakan pendekatan persentase, yang mana didapati hasil penilaian *Maturity Level* mencapai 94% atau pada rentang nilai 5 (91% - 100%) dengan kategori "*Optimized*". Terdapat beberapa poin audit (klausul/annex) yang memperoleh nilai 100%, yaitu untuk konteks organisasi, kepemimpinan, perencanaan, operasi, evaluasi kinerja, perbaikan, manajemen

aset, kendali akses, kriptografi, keamanan operasi, keamanan komunikasi, dan aspek keamanan informasi dari manajemen keberlangsungan bisnis. Sementara itu, poin audit lainnya yang tidak memperoleh penilaian 100%, seperti pada sumber daya manusia dengan nilai pemenuhan rata-rata sebesar 79% berada pada level 4 (Managed and Measurable), hal itu disebabkan karena belum terdapat rekaman dokumen rekrutmen karyawan yang lengkap, tidak adanya penilaian dan dokumentasi gap kompetensi, tidak adanya prosedur pelatihan, dan evaluasi rencana kerja pelatihan. Aspek kebijakan keamanan informasi yang memperoleh nilai 3 (defined) disebabkan belum adanya kebijakan keamanan sistem kerja jarak jauh yang memadai, seperti kebijakan teleworking, bring your own device policy, dan prosedur kerja dalam dan luar kantor yang belum diperbarui. Aspek organisasi keamanan informasi yang memperoleh nilai 97% atau pada level 5 (optimized) terdapat ketidaksempurnaan dalam hal pengendalian pelaksanaan proyek. Aspek keamanan sumber daya manusia yang memperoleh penilaian sebesar 77% atau pada level penilaian 4 (Managed and Measurable), hal itu karena ketiadaan proses screening latar belakang keamanan informasi yang dilakukan pada proses penialaian dokumen curriculum vitae serta bagian sesi wawancara dengan karyawan, selain itu belum tersedianya kebijakan pengelolaan dan tindakan terhadap keamanan informasi pada lingkup karyawan. Aspek keamanan fisik dan lingkungan yang memperoleh penilaian 92% atau pada level 5 (*optimized*), terdapat ketidaksempurnaan pada implementasi pengendalian aspek keamaman fisik dan lingkungan khususnya risiko keamanan lingkungan yang disebabkan oleh prosedur kerja remote working. Aspek akuisisi, pengembangan, dan perawatan sistem yang memperoleh penilaian 98% atau pada level 5 (*Optimized*), terdapat ketidaksempurnaan pada proses *versioning* produk pada proses pengembangan produk. Aspek hubungan hubungan pemasok yang memperoleh penilaian 92% atau pada level 5 (*Optimized*), karena terdapat ketidaksempurnaan pada bagian penetapan prosedur pengendalian pemasok dan pemantauannya. Aspek Manajemen insiden keamanan informasi yang memperoleh penilaian sebesar 89% atau pada level 4 (*Managed and Measurable*), karena belum terdapat kebijakan untuk pengumpulan bukti dan prosedur pelaporan insiden keamanan informasi. Aspek kepatuhan yang memperoleh penilaian 93% atau pada level 5 (*Optimized*), karena terdapat ketidaksempurnaan pada bagian prosedur penetapan hak kekayaan intelektual produk perusahaan.

4. PENUTUP

Pada bagian penutup dijelaskan mengenai kesimpulan yang dapat diambil dari hasil penelitian yang telah dilakukan dan saran yang diperlukan baik bagi perusahaan maupun bagi penelitian selanjutnya.

Dari hasil penelitian yang dilakukan dalam penerapan Sistem Manajemen Keamanan Informasi Berbasis ISO 27001:2013 di PT. X, dapat ditarik kesimpulan bahwa PT X telah menerapkan sistem manajemen keamananan informasi dengan cukup efektif, baik dalam bentuk penyediaan kebijakan dan prosedur, serta implementasinya berdasarkan standar ISO 27001:2013. Efektifitas penerapan SMKI sebesar 94% dari total 34 poin penilaian, dengan tingkat maturitas pada kategori “optimized (level 5)” berdasarkan indeks KAMI dari BSSN.

Sementara itu, dalam penelitian ini memberikan saran pada penerapan Sistem Manajemen Keamanan Informasi untuk PT. X sebagai berikut :

1. Melakukan pemantauan pada identifikasi gap kompetensi karyawan, serta menjadikannya sebagai input dalam aktivitas *training need analysis*.
2. Membuat rekaman (record) aktivitas secara konsisten dari tiap unit yang bersesuaian dengan scope penerapan ISMS ISO 27001:2013, untuk memastikan ketersediaan informasi terdokumentasi dan input dari upaya *continual improvement.*
3. Memantau fungsi dan tanggungjawab pihak ketiga dalam penanganan keamanan informasi perusahaan.
4. Memantau dan merespon laporan monitoring kepatuhan *password* dari karyawan, yang dilakukan oleh *instrument mobile device management* yang digunakan perusahaan.
5. Melakukan *screening* latar belakang karyawan dengan konsisten, sesuai

kebijakan *human resource security* yang telah ditetapkan.

6. Memantau implementasi pengendalian keamanan fisik, sebagaimana telah diatur dalam *physical environment policy*, untuk mengantisipasi berbagai risiko yang terjadi yang disebabkan oleh pengendalian keamanan fisik yang kurang memadai.

Sedangkan penelitian ini memberikan saran bagi peneliti lain agar meningkatkan penelitian penerapan sistem manajemen keamanan informasi ISO 27001 versi 2022.

DAFTAR PUSTAKA

Arens, Alvin A., Elder, Randal J., Beasley, Mark S. (2014). *Auditing and Assurance Service, 15th edition*. England: Pearson.

ISO 31000:2018. (2018). *Risk management – Guidelines*.

ISO/IEC 27001:2013. (2013). *Information technology -- Security techniques -- Information security management systems – Requirements.*

Kusuma, R. A. (2014). *Audit Keamanan Sistem Informasi Berdasarkan Standar SNI-ISO 27001*. Yogyakarta.

Rachmawati, D., Darmawan, D., & Syahputra, R. 2017. Sistem Keamanan Informasi: Tinjauan Literatur. Jurnal Teknologi Informasi dan Komunikasi, 5(2), 72-84.

Alfian, R. 2019. *Analisis dan Perancangan istem Keamanan Informasi Menggunakan onsep ISO/IEC 27001*. Jurnal Ilmiah Teknologi Informasi Asia, 13(2), 75-82.

Apriandari W., dan Sasongko A. 2018. *Analisis Sistem Manajemen Keamanan Informasi Menggunakan Sni ISO/IEC 27001:2013 Pada Pemerintahan Daerah Kota Sukabumi (STUDI KASUS: DI DISKOMINFO KOTA SUKABUMI).* Jurnal Ilmiah SANTIKA. 8(1). 715-729. p-ISSN 2088-5407.

Bakri, M., dan Irmayana N. 2017. Analisis Dan Penerapan Sistem Manajemen Keamanan Informasi Simhp BPKP Menggunakan Standar ISO 27001. Jurnal TEKNOKOMPAK. 11(2). 41-44. ISSN 1412-9663

Basyarahil F. A., H. M. Astuti, dan B. C. Hidayanto. 2017. Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya. JURNAL TEKNIK ITS. 6(1). 122-128.

Candiawan. 2014. Analysis of ISO27001 Implementation for Enterprises and SMEs in Indonesia. Proceedings of the International Conference on Cyber-Crime Investigation and Cyber Security. Kuala Lumpur: 2014. Hal. 50-58.

Chazar, C. 2015. Standar Manajemen Keamanan Sistem Informasi Berbasis ISO 27001:2005. Jurnal Informasi, VII(2), 48-57

Culot, G., dkk. 2021. The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. The TQM Journal. 33(7). 76-105.

Kristanto, T., dkk. 2019. Analisis Manajemen Keamanan Informasi Menggunakan Standard ISO 27001:2005 Pada Staff IT Support Di Instansi XYZ. JISA (Jurnal Informatika dan Sains). 2(2). 30-33.

Kurniawan, T. 2017. *Analisis Perancangan Sistem Keamanan Informasi pada PT. XYZ dengan Menggunakan ISO 27001:2013*. Jurnal Teknik Informatika dan Sistem Informasi, 3(2), 114-123.

Liyas, Jeli Nata, dan Widyanti, Ferisca Nur. 2020. *Pengaruh Sistem Informasi Manajemen*.

Novatiani, R. Ait, dkk. 2022. *Risk Management And Other Factors Preventing Fraudulent Financial Reporting By State-Owned Enterprises In Indonesia.* Asian Economic and Financial Review. 12(8), 686-711.

Veronica, Christina, dkk. 2020. *Does the Internal Control System is a Solution? (Inventory Study at PT. X Bandung).* Solid State Technologhy. 63(3):5219- 5225.

Wijaya , Aida, dkk. 2019. *Internal Performance of an Integrated Supply Chain: Does Flexibility Matter?*. International Journal of Supply Chain Management. 8(2), 565-593.


ICBENS
International Conference on Bussiness and Entrepreneurship for Nation's Sustainability