The Indonesian Journal of Computer Science
www.ijcs.net
Volume 13, Issue 4, August 2024
https://doi.org/10.33022/ijcs.v13i4.4166

Rekomendasi Implementasi 11 Kontrol keamanan informasi baru ISO 27001:2022 di Perusahaan *HealthTech* XYZ

Bimantoro Suryo Wibowo[1], Rizal Fathoni Aji[2]
bimantoro.suryo@ui.ac.id[1], rizal@cs.ui.ac.id[2]
[1,2]Univesity of Indonesia

Informasi Artikel

Diterima : 20 Jun 2024
Direvisi : 10 Jul 2024
Disetujui : 25 Jul 2024

Kata Kunci

keamanan informasi, analisis *gap*, iso 27001, *annex controls, compliance*

Abstrak

Penelitian ini bertujuan untuk merekomendasikan implementasi kontrol *annex* baru dalam ISO 27001:2022, dengan panduan dari ISO 27002:2022, untuk PT XYZ. Pertanyaan penelitian yang diangkat adalah: (1) Apa kesenjangan yang ada antara kontrol keamanan informasi saat ini di PT XYZ dengan persyaratan ISO 27001:2022? (2) Rekomendasi spesifik apa yang dapat menutup kesenjangan ini? Dengan menggunakan pendekatan studi kasus kualitatif, data dikumpulkan pada Mei 2024 melalui *purposive sampling*, wawancara, observasi, dan analisis dokumen. Temuan mengungkapkan bahwa meskipun beberapa kontrol sudah diimplementasikan sebagian, lainnya masih kurang dokumentasi penuh dan SOP. Rekomendasi terperinci diberikan untuk memastikan kepatuhan dengan standar yang diperbarui, menekankan formalitas dalam bentuk SOP. Penelitian ini menawarkan panduan praktis bagi organisasi yang bertransisi ke ISO 27001:2022, meningkatkan kesiapan keamanan siber dan kepatuhan terhadap regulasi perlindungan data yang ketat.

Keywords

information security, gap analysis, iso 27001, annex controls, compliance

Abstract

This study aims to recommend the implementation of new annex controls in ISO 27001:2022, guided by ISO 27002:2022, for PT XYZ. The research questions addressed are: (1) What are the existing gaps between PT XYZ's current information security controls and the requirements of ISO 27001:2022? (2) What specific recommendations can close these gaps? Using a qualitative case study approach, data were collected in May 2024 through purposive sampling, interviews, observations, and document analysis. Findings reveal that while some controls are partially implemented, others lack full documentation and SOPs. Detailed recommendations were provided to ensure compliance with updated standards, emphasizing formalization into SOPs. This study offers practical guidance for organizations transitioning to ISO 27001:2022, enhancing cybersecurity readiness and compliance with stringent data protection regulations.

A. Pendahuluan

Tren insiden keamanan informasi menunjukkan peningkatan yang signifikan setiap tahun. Menurut laporan tahunan [1], tercatat kenaikan lebih dari 15% dalam jumlah pelanggaran data dan serangan siber dibandingkan tahun sebelumnya, yang menggarisbawahi bahwa ancaman siber semakin canggih dan beragam. Khususnya, sektor *healthcare* mengalami 1,378 insiden, dengan 88.5% di antaranya telah terkonfirmasi terjadi kasus *data disclosure*.

Di Indonesia, Undang-Undang Perlindungan Data Pribadi (PDP) No. 27 Tahun 2022 telah disahkan, yang memberlakukan persyaratan ketat bagi perusahaan untuk melindungi data pelanggan. UU ini juga menetapkan hukuman berat bagi perusahaan yang tidak patuh, termasuk pembubaran izin korporasi jika terjadi kebocoran data dan terbukti lalai dalam menjaga data tersebut [2].

ISO 27001 adalah standard internasional yang menyediakan kerangka kerja untuk *Information Security Management System* (ISMS) secara sistematis dan proaktif. Standard ini telah diperbarui menjadi ISO 27001:2022 untuk menyesuaikan dengan evolusi ancaman siber dan teknologi, termasuk peningkatan perlindungan untuk layanan komputasi awan dan pengenalan kontrol keamanan baru [3]. Penerapan ISO 27001 menunjukkan bahwa perusahaan berupaya untuk menjaga data pribadi pelanggan dengan sebuah sistem manajemen yang terstandardisasi dan diakui secara internasional. Konsistensi perusahaan dalam mengimplementasikan ISO 27001 secara berkelanjutan menjadi penting dan harus dipertahankan, termasuk harus patuh dengan standard ISO 27001 yang terbaru [4].

PT XYZ, merupakan perusahaan yang beroperasi dalam industri layanan kesehatan digital, dengan core bisnis utamanya adalah layanan telemedicine, telah tersertifikasi ISO 27001:2013 dan sudah lulus audit eksternal *surveillance* yang kedua pada Januari 2024. Saat ini perusahaan sudah memenuhi seluruh kontrol keamanan informasi ISO 27001:2013, hal ini dibuktikan dengan tidak adanya temuan dari auditor eksternal pada saat proses *surveillance* ke-2 ISO 27001:2013 dilakukan.

Kemunculan ISO 27001:2022 menjadikan transisi ke standard terbaru ini sangat penting bagi PT XYZ untuk mempertahankan kepatuhan terhadap regulasi dan memastikan kepercayaan pelanggan. Berdasarkan hasil identifikasi permasalahan yang dilakukan oleh peneliti didapatkan informasi bahwa, perusahaan ini memiliki fokus untuk mengimplementasikan *annex* kontrol keamanan informasi baru pada ISO 27001:2022. Sehingga dari penjabaran informasi tersebut, pertanyaan penelitian ini adalah: (1) Bagaimana kondisi eksisting kontrol keamanan informasi di PT XYZ dan apa *gap* antara kondisi eksisting dengan persyaratan kontrol *annex* baru pada ISO 27001:2022? (2) Apa rekomendasi spesifik untuk implementasi kontrol *annex* baru di PT XYZ berdasarkan hasil analisis *gap* yang telah dilakukan? Tujuan penelitian ini dapat memberikan informasi bagi PT XYZ mengenai analisis *gap* antara kondisi *current state* kontrol keamanan informasi dengan *future state* yang sesuai dengan persyaratan kontrol *annex* baru pada ISO 27001:2022 dan apa rekomendasi spesifik untuk mengimplementasikan kontrol *annex* baru tersebut berdasarkan hasil *gap* yang telah dilakukan. Penelitian ini juga diharapkan dapat memberikan gambaran serta panduan bagi perusahaan dengan sektor dan model bisnis sejenis

yang sudah terimplementasi ISO 27001:2013 dan ingin melakukan transisi implementasi ISO 27001:2022 spesifiknya untuk kontrol *annex* barunya.

B. Tinjauan Literatur

Bab ini memberikan landasan teoretis dan konteks mengenai implementasi Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan standar ISO 27001:2022 dan panduan ISO 27002:2022. Tinjauan pustaka mencakup berbagai aspek yang terkait dengan SMKI, ISO 27001, dan ISO 27002, serta faktor-faktor yang mempengaruhi keberhasilan implementasi kontrol keamanan informasi dalam perusahaan, khususnya dalam konteks transisi dari ISO 27001:2013 ke ISO 27001:2022.

Sistem Manajemen Keamanan Informasi (SMKI)

Sistem Manajemen Keamanan Informasi (SMKI) menerapkan proses manajemen risiko untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi. Dalam perencanaan pengamanan informasi, organisasi harus mendefinisikan ruang lingkup penerapan serta mengidentifikasi isu-isu terkait baik dari lingkungan internal maupun eksternal. Definisi ruang lingkup ini mencakup identifikasi aset informasi penting, pemetaan ancaman potensial, dan penilaian kerentanan yang ada. Organisasi perlu melakukan penilaian risiko dengan menggunakan metodologi yang sesuai, seperti analisis risiko kualitatif dan kuantitatif, untuk mengukur dampak dan kemungkinan terjadinya insiden keamanan. Hasil dari penilaian risiko ini akan menjadi dasar untuk merencanakan penerapan kontrol yang memadai terhadap risiko yang teridentifikasi, dengan tujuan meminimalkan potensi kerugian dan meningkatkan ketahanan terhadap serangan siber [8, 10, 13, 17].

SMKI harus menjadi bagian integral dan terintegrasi dengan proses perusahaan serta seluruh struktur manajemen perusahaan. Keamanan informasi harus menjadi pertimbangan utama dalam perencanaan proses, sistem informasi, dan kontrol. Ini berarti bahwa kebijakan dan prosedur keamanan informasi harus selaras dengan tujuan bisnis perusahaan dan didukung oleh komitmen dari manajemen puncak. Pengembangan budaya keamanan yang kuat di seluruh organisasi adalah kunci untuk memastikan bahwa semua karyawan memahami pentingnya keamanan informasi dan mematuhi kebijakan yang telah ditetapkan. Selain itu, pemantauan dan evaluasi berkelanjutan terhadap efektivitas kontrol keamanan yang diterapkan harus dilakukan untuk memastikan bahwa sistem keamanan informasi tetap relevan dan efektif dalam menghadapi ancaman yang terus berkembang [9, 14-16].

ISO 27001

ISO 27001 adalah standar internasional untuk Sistem Manajemen Keamanan Informasi (SMKI), dirancang untuk membantu organisasi menetapkan, mengimplementasikan, memelihara, dan meningkatkan SMKI [7]. SMKI dalam ISO 27001:2022 melibatkan pembentukan, operasi, pemeliharaan, pengawasan, dan peningkatan keamanan informasi secara berkesinambungan. Dibandingkan dengan ISO 27001:2013, ISO 27001:2022 mengalami perubahan kecil hingga sedang, dengan tetap mempertahankan 10 klausul utama. *Annex* A berkurang dari

114 menjadi 93 kontrol, dan domain kontrol berkurang dari 14 menjadi 4. Perubahan ini termasuk restrukturisasi dan penambahan beberapa kontrol baru, dengan fokus yang lebih besar pada keamanan siber dan privasi [3, 5]. Struktur ISO/IEC 27001:2022 mencakup 10 klausul dan 93 kontrol yang dikelompokkan ke dalam 4 domain kontrol sebagai berikut:

Klausul dalam ISO/IEC 27001:2022: 1. *Scope*, 2.*Normative references*, 3. *Terms and definitions*, 4. *Context of the organization*, 5. *Leadership*, 6. *Planning*, 7. *Support*, 8. *Operation*, 9. *Performance evaluation*, 10. *Improvement*. Dan terdapat 4 kategori domain *annex control*, antara lain: A.5 *Organizational controls* terdapat 37 *annex control*, A.6 *People Controls* terdapat 8 *annex control*, A.7 *Physical Controls* terdapat 14 *annex control*, dan A.8 *Technological Controls* terdapat 34 *annex*. Sehingga total keseluruhan *Annex control* pada ISO/IEC 27001:2022 adalah 93 butir dimana 11 diantara 93 kontrol *annex* tersebut merupakan kontrol baru yang akan dijabarkan pada Tabel 1. *Annex* kontrol baru di ISO/IEC 27001:2022 [3].

Tabel 1. *Annex* kontrol baru di ISO/IEC 27001:2022

No	***Annex Control***
1	*A.5.7 Threat intelligence*
2	*A.5.23 Information Security for use of cloud services*
3	*A.5.30 ICT Readiness for business continuity*
4	*A.7.4 Physical Security Monitoring*
5	*A.8.9 Configuration Management*
6	*A.8.10 Information Deletion*
7	*A.8.11 Data Masking*
8	*A.8.12 Data Leakage Prevention*
9	*A.8.16 Monitoring Services*
10	*A.8.22 Web Filtering*
11	*A.8.28 Secure Coding*

ISO 27002

ISO 27002:2022 adalah panduan yang memberikan rincian implementasi untuk kontrol keamanan yang tercantum dalam ISO 27001:2022. Standar ini dirancang untuk membantu organisasi mengembangkan dan menerapkan kontrol keamanan informasi yang efektif dan sesuai dengan kebutuhan spesifik mereka. ISO 27002 menyediakan panduan praktis yang mencakup berbagai aspek, termasuk kebijakan keamanan, organisasi keamanan informasi, keamanan sumber daya manusia, manajemen aset, kontrol akses, enkripsi, dan keamanan fisik serta lingkungan [6]. Dengan mengikuti praktik terbaik yang diuraikan dalam ISO 27002, organisasi dapat memastikan bahwa setiap kontrol keamanan diterapkan dengan cara yang efektif, efisien, dan sesuai dengan standar internasional. Panduan ini juga mencakup rekomendasi tentang cara mengelola risiko keamanan informasi, memastikan keberlanjutan bisnis, dan mematuhi persyaratan hukum serta peraturan yang relevan [4].

Lebih lanjut, ISO 27002:2022 menekankan pentingnya penilaian risiko yang berkelanjutan dan penyesuaian kontrol keamanan sesuai dengan perkembangan ancaman siber dan teknologi. Panduan ini memberikan kerangka kerja yang

fleksibel yang dapat disesuaikan dengan berbagai jenis organisasi, termasuk sektor kesehatan digital seperti PT XYZ. Dengan mengacu pada ISO 27002, PT XYZ dapat mengidentifikasi celah dalam kontrol keamanan saat ini dan merumuskan action plan untuk mengimplementasikan kontrol *annex* baru yang diperlukan oleh ISO 27001:2022 [11]. Pendekatan ini tidak hanya memastikan bahwa PT XYZ tetap patuh terhadap standar internasional tetapi juga meningkatkan kesiapan dan ketahanan organisasi terhadap ancaman siber yang terus berkembang. Dengan demikian, penggunaan ISO 27002 sebagai landasan untuk rekomendasi implementasi akan membantu PT XYZ mencapai tujuan keamanan informasi secara holistik dan berkelanjutan.

C. Metode Penelitian

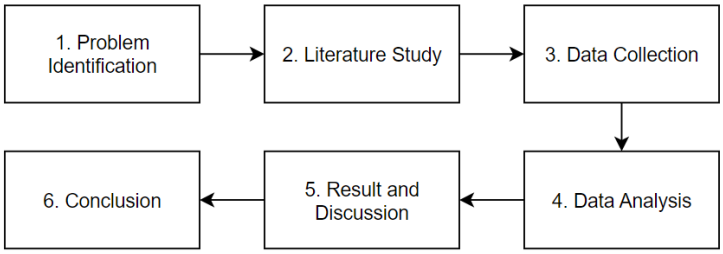
Penelitian yang dilakukan menggunakan metode deskriptif kualitatif, dengan pendekatan studi kasus [12]. Objek penelitian ini adalah PT XYZ, sebuah perusahaan yang perlu melakukan transisi implementasi ke ISO 27001:2022, dengan fokus utama pada 11 kontrol baru yang terdapat dalam standar tersebut. PT XYZ dipilih sebagai studi kasus karena peneliti ingin memberikan rekomendasi implementasi untuk 11 kontrol baru ini berdasarkan analisis *current state* perusahaan saat ini dan memastikan kepatuhan dengan standar ISO 27001:2022 [18].

Periode penelitian dilakukan selama bulan Mei 2024. Teknik pengambilan sampel yang digunakan adalah purposive sampling, yang dipilih untuk memastikan informan yang terlibat memiliki kualifikasi dan informasi yang relevan untuk penelitian ini. Informan yang dipilih termasuk seorang PIC perusahaan yang bertanggung jawab atas semua pekerjaan terkait ISO 27001 dan seorang pakar yang berpengalaman dalam audit, pelatihan, dan konsultasi dalam konteks ISO 27001. Identitas informan dilindungi menggunakan pseudonim sesuai dengan etika penelitian.

Sumber data penelitian ini terdiri dari data primer dan sekunder yang diperoleh melalui wawancara dengan narasumber, studi literatur, analisis dokumen, dan observasi lapangan. Metode pengumpulan data melibatkan wawancara semi-terstruktur dengan pertanyaan sekuensial dan beberapa pertanyaan lanjutan, studi literatur untuk memahami konteks teoritis, analisis dokumen terkait kebijakan dan prosedur perusahaan, serta observasi lapangan untuk memverifikasi hasil wawancara dan memastikan apakah kebijakan kontrol keamanan informasi telah diterapkan dalam aktivitas kerja sehari-hari.

Fokus observasi adalah untuk memverifikasi hasil wawancara dengan *stakeholder* perusahaan dan memastikan bahwa analisis dokumen terkait kebijakan kontrol keamanan informasi telah dilakukan dalam aktivitas kerja yang berlangsung. Data yang dikumpulkan akan dianalisis untuk menghasilkan gambaran *current state* implementasi kontrol baru ISO 27001:2022 di PT XYZ. Analisis ini akan menentukan apakah dari 11 kontrol baru tersebut, ada yang sudah diimplementasikan dalam proses kerja dan terdokumentasi dalam SOP, atau belum. Seluruh temuan ini kemudian akan dipetakan ke kondisi *future state* yang mengacu pada standar ISO 27002:2022 sebagai panduan teknis untuk memenuhi persyaratan ISO 27001:2022.

Seluruh hasil analisis akan digunakan untuk memberikan rekomendasi spesifik bagi PT XYZ dalam mengimplementasikan kontrol *annex* baru pada ISO 27001:2022. Sehingga perusahaan dapat mencapai kepatuhan penuh terhadap standar terbaru dan meningkatkan keamanan informasi secara keseluruhan.



Gambar1. Alur Penelitian

D. Hasil dan Pembahasan

Pada bagian ini, dilakukan pengumpulan data untuk mendapatkan kondisi *current-state* kontrol keamanan informasi PT XYZ. Selanjutnya, dilakukan analisis *gap* (*gap analysis*) untuk mengidentifikasi perbedaan antara kondisi existing dan kondisi ideal yang diharapkan. Berdasarkan hasil analisis *gap*, diberikan rekomendasi implementasi untuk setiap kontrol keamanan informasi yang belum sesuai dengan acuan ISO 27002:2022.

Kondisi *current state* Kontrol *Annex* PT XYZ

Wawancara dengan PIC utama yang mengurusi seluruh hal tentang ISO 27001 di PT XYZ, yaitu *Senior IT GRC Specialist* sekaligus *Information Security Manager*, mengungkapkan berbagai kondisi *current-state* kontrol keamanan informasi di perusahaan ini. Terdapat 11 kontrol *annex* keamanan informasi baru dalam ISO 27001:2022, yaitu: A.5.7 *Threat Intelligence*, A.5.23 *Information Security for use of cloud services*, A.5.30 *ICT Readiness for business continuity*, A.7.4 *Physical Security Monitoring*, A.8.9 *Configuration Management*, A.8.10 *Information Deletion*, A.8.11 *Data Masking*, A.8.12 *Data Leakage Prevention*, A.8.16 *Monitoring Services*, A.8.23 *Web Filtering*, dan A.8.28 *Secure Coding*. Dari 11 kontrol tersebut, ditemukan bahwa 3 *Annex* kontrol (A.5.23 *Information Security for use of cloud services*, A.8.10 *Information Deletion*, dan A.8.11 *Data Masking*) sudah dilaksanakan secara parsial sesuai ISO 27001:2022, 1 kontrol (A.5.7 *Threat Intelligence*) belum dilakukan sama sekali, dan sisanya sudah dilakukan sesuai kaidah dan persyaratan ISO.

Dokumen yang dianalisis meliputi SOP, kebijakan, dan laporan audit yang terkait dengan proses aktivitas kerja sesuai kontrol keamanan informasi terbaru ISO 27001:2022. Temuan utama dari analisis dokumen menunjukkan bahwa dari 11 kontrol *annex*, hanya Annex kontrol 5.30 ICT *Readiness for business continuity* yang sudah dibakukan dalam bentuk SOP, sementara kontrol lainnya belum terdokumentasi secara formal dalam SOP. Observasi lapangan dilakukan untuk memverifikasi temuan dari wawancara dan studi dokumen. Observasi ini melibatkan pengecekan langsung terhadap aktivitas kerja di lapangan untuk

memastikan kesesuaian dengan kontrol keamanan informasi terbaru ISO 27001:2022. Hasil observasi menunjukkan bahwa meskipun sebagian besar kontrol sudah dilaksanakan, hanya sedikit yang sudah dibakukan dalam SOP. Tabel 2. merupakan hasil tabulasi kondisi eksisting (*current state*) dari setiap kontrol keamanan informasi yang diimplementasikan di PT XYZ:

Tabel 2. Kondisi eksisting (*current state*) kontrol keamanan informasi di PT XYZ

No	Kontrol Keamanan Informasi	Aktivitas Kerja	Dokumentasi (SOP)	Status Implementasi
1	*A.5.7 Threat Intelligence*	Tidak dilakukan	Tidak ada	Belum sesuai
2	*A.5.23 Cloud Services*	Dilakukan parsial	Tidak ada	Parsial
3	*A.5.30 Business Continuity*	Dilakukan	Ada	Sesuai
4	*A.7.4 Physical Security*	Dilakukan	Tidak ada	Sesuai
5	*A.8.9 Configuration Management*	Dilakukan	Tidak ada	Sesuai
6	*A.8.10 Information Deletion*	Dilakukan parsial	Tidak ada	Parsial
7	*A.8.11 Data Masking*	Dilakukan parsial	Tidak ada	Parsial
8	*A.8.12 Data Leakage Prevention*	Dilakukan	Tidak ada	Sesuai
9	*A.8.16 Monitoring Services*	Dilakukan	Tidak ada	Sesuai
10	*A.8.23 Web Filtering*	Dilakukan	Tidak ada	Sesuai
11	*A.8.28 Secure Coding*	Dilakukan	Tidak ada	Sesuai

Gap analysis dan Rekomendasi Implementasi Kontrol *Annex*

Analisis *gap* dilakukan dengan memetakan kondisi *current-state* terhadap kondisi ideal yang diharapkan sesuai dengan persyaratan ISO 27001:2022 dan pedoman teknis ISO 27002:2022. *Gap analysis* ini mengidentifikasi area-area di mana kontrol keamanan informasi belum sesuai dan membutuhkan pembenahan untuk mencapai kepatuhan penuh. Berdasarkan hasil *gap analysis*, berikut adalah rekomendasi spesifik untuk setiap kontrol keamanan informasi yang belum sesuai:

Kontrol 5.7 *Threat Intelligence*: PT XYZ perlu mengimplementasikan serangkaian langkah yang mencakup pengumpulan, analisis, dan penyebaran informasi ancaman. Pertama, perusahaan harus mengidentifikasi dan memilih sumber informasi yang relevan, baik internal maupun eksternal, seperti laporan vendor keamanan, *database* ancaman, komunitas keamanan, dan intelijen dari

pihak ketiga. Informasi yang dikumpulkan harus dianalisis menggunakan alat analisis ancaman untuk mengkategorikan dan menghubungkannya dengan konteks organisasi. *Threat intelligence* kemudian harus dibagi menjadi tiga lapisan: strategi, taktik, dan operasional, dan dilaporkan secara berkala kepada tim keamanan dan pihak terkait lainnya. Selain itu, hasil analisis ancaman harus diintegrasikan ke dalam proses manajemen risiko keamanan informasi organisasi, dan digunakan untuk memperbarui serta memperbaiki kontrol pencegahan dan deteksi teknis.

Kontrol 5.23 ***Information Security for use of Cloud Services:*** PT XYZ harus menetapkan proses yang komprehensif untuk akuisisi, penggunaan, manajemen, dan penghentian layanan *cloud* sesuai dengan persyaratan keamanan informasi organisasi. Pertama, perusahaan perlu menyusun kebijakan khusus tentang penggunaan layanan *cloud* yang mencakup semua aspek dari akuisisi hingga penghentian layanan. Kebijakan ini harus dikomunikasikan kepada semua pihak yang berkepentingan. Selain itu, peran dan tanggung jawab antara penyedia layanan *cloud* dan PT XYZ harus didefinisikan dan didokumentasikan dengan jelas, termasuk kriteria seleksi layanan *cloud*, persyaratan keamanan informasi, serta prosedur untuk penanganan insiden keamanan terkait layanan *cloud*. Pengawasan dan evaluasi berkelanjutan terhadap penggunaan layanan *cloud* juga harus dilakukan untuk memastikan manajemen risiko yang efektif.

Kontrol 7.4 ***Physical Security Monitoring***: PT XYZ harus memastikan bahwa area fisik perusahaan dipantau secara terus-menerus untuk mencegah akses fisik yang tidak sah. Ini dapat dicapai dengan memasang sistem pengawasan seperti CCTV, alarm deteksi intrusi, dan perangkat lunak manajemen informasi keamanan fisik, baik yang dikelola secara internal maupun oleh penyedia layanan pemantauan. Akses ke bangunan yang menampung sistem kritis harus dipantau terus-menerus untuk mendeteksi akses yang tidak sah atau perilaku mencurigakan. Sistem pemantauan harus dilengkapi dengan alarm yang dipasang di pintu dan jendela eksternal, dan area yang tidak berpenghuni harus selalu diberi alarm. Sistem pemantauan juga harus dilindungi dari akses yang tidak sah untuk mencegah informasi pengawasan diakses oleh pihak yang tidak berwenang.

Kontrol 8.9 ***Configuration Management***: PT XYZ harus mendefinisikan dan mengimplementasikan proses serta alat untuk menegakkan konfigurasi yang ditetapkan, termasuk konfigurasi keamanan untuk perangkat keras, perangkat lunak, layanan, dan jaringan. Konfigurasi standar harus didokumentasikan dan diperbarui secara berkala sesuai dengan ancaman dan kerentanan baru yang teridentifikasi. Perusahaan juga harus mencatat dan memantau semua perubahan konfigurasi, memastikan bahwa perubahan tersebut mengikuti proses manajemen perubahan yang telah ditentukan. Pemantauan konfigurasi harus dilakukan secara teratur untuk memverifikasi pengaturan konfigurasi dan menilai aktivitas yang dilakukan, dengan segala penyimpangan yang ditemukan segera ditangani.

Kontrol 8.10 ***Information Deletion***: PT XYZ perlu memastikan bahwa informasi yang tidak lagi diperlukan dihapus dengan metode yang sesuai untuk mencegah

pengungkapan yang tidak diinginkan. Metode penghapusan harus dipilih berdasarkan persyaratan bisnis dan hukum yang relevan, seperti penghapusan elektronik atau kriptografi. Hasil penghapusan harus dicatat sebagai bukti. Selain itu, PT XYZ harus memastikan bahwa penyedia layanan yang menangani penghapusan informasi juga memberikan bukti penghapusan yang memadai. Proses penghapusan informasi ini harus diotomatisasi sesuai dengan kebijakan topik-spesifik organisasi.

Kontrol 8.11 ***Data Masking*****:** PT XYZ harus menerapkan teknik masking data, pseudonimisasi, atau anonimisasi untuk melindungi data sensitif, terutama PII. Teknik ini harus diverifikasi untuk memastikan data telah dimasking atau dianonimkan dengan memadai. PT XYZ juga harus mempertimbangkan penggunaan teknik tambahan seperti enkripsi, nulling, substitusi, dan penggantian nilai dengan hash. Ketika data diobfuscate, perusahaan harus memberikan opsi kepada prinsipal PII untuk meminta agar pengguna tidak dapat melihat data yang diobfuscate.

Kontrol 8.12 ***Data Leakage Prevention*****:** PT XYZ harus menerapkan langkah-langkah pencegahan kebocoran data pada sistem, jaringan, dan perangkat yang memproses, menyimpan, atau mengirimkan informasi sensitif. Ini termasuk mengidentifikasi dan mengklasifikasikan informasi untuk melindungi dari kebocoran, memantau saluran kebocoran data seperti email dan perangkat penyimpanan portabel, serta menggunakan alat pencegahan kebocoran data untuk memantau dan mencegah pengungkapan informasi sensitif. Perusahaan juga harus mempertimbangkan pembatasan kemampuan pengguna untuk menyalin dan menempel data ke layanan, perangkat, dan media penyimpanan di luar kendali organisasi.

Kontrol 8.16 ***Monitoring Services*****:** PT XYZ harus memantau jaringan, sistem, dan aplikasi untuk perilaku anomali dan mengambil tindakan yang sesuai untuk mengevaluasi potensi insiden keamanan informasi. Lingkup dan tingkat pemantauan harus ditentukan sesuai dengan persyaratan bisnis dan keamanan informasi, serta mempertimbangkan hukum dan regulasi yang relevan. Sistem pemantauan harus mencakup lalu lintas jaringan masuk dan keluar, akses ke sistem, konfigurasi file, dan log dari alat keamanan. Pemantauan harus dilakukan secara real-time atau pada interval periodik sesuai dengan kebutuhan organisasi, dengan sistem yang mampu menangani data besar dan memberikan notifikasi real-time.

Kontrol 8.23 ***Web Filtering*****:** PT XYZ harus mengelola akses ke situs web eksternal untuk mengurangi paparan terhadap konten berbahaya. Ini dapat dicapai dengan mengidentifikasi jenis situs web yang boleh atau tidak boleh diakses oleh karyawan, serta menggunakan teknologi filter web untuk memblokir akses ke situs web berbahaya yang diketahui, server command and *control*, dan situs berbagi konten ilegal. Kebijakan penggunaan sumber daya online harus ditetapkan dan dikomunikasikan kepada karyawan, termasuk pelatihan tentang penggunaan aman dan tepat dari sumber daya online.

Kontrol 8.28 ***Secure Coding*****:** PT XYZ harus menerapkan prinsip pengkodean aman dalam pengembangan perangkat lunak untuk mencegah kerentanan keamanan. Perusahaan harus menetapkan proses organisasi untuk memastikan praktik pengkodean aman diterapkan, baik dalam pengembangan internal maupun dalam produk dan layanan yang disediakan oleh pihak ketiga. Perencanaan sebelum pengkodean harus mencakup ekspektasi organisasi dan prinsip-prinsip pengkodean aman yang disetujui, konfigurasi alat pengembangan untuk mendukung pengkodean aman, dan pelatihan bagi pengembang dalam menulis kode yang aman. Selama pengkodean, perusahaan harus menggunakan teknik pengkodean yang aman, seperti *pair programming*, *peer review*, dan *security iterations*. Setelah perangkat lunak dibuat operasional, pembaruan harus dikemas dan diterapkan dengan aman, dan kerentanan keamanan yang dilaporkan harus ditangani dengan segera.

Rekomendasi ini kemudian divalidasi dengan seorang pakar yang berpengalaman dalam audit, pelatihan, dan konsultan ISO 27001 dengan pengalaman profesional lebih dari 18 tahun. Pakar memberikan masukan terkait rekomendasi yang diberikan dan memastikan bahwa rekomendasi tersebut sudah sesuai dengan standar ISO 27001:2022 dan ISO 27002:2022.

Tabel 3. Rekomendasi Implementasi Kontrol Keamanan Informasi Berdasarkan Hasil *Gap analysis* di PT XYZ

No	Kontrol Keamanan Informasi	Rekomendasi Implementasi	Tindakan yang Disarankan	SOP yang Perlu Dibuat
1	*A.5.7 Threat Intelligence*	Mengumpulkan dan menganalisis informasi ancaman	Menetapkan proses pengumpulan dan analisis	*SOP Threat Intelligence*
2	*A.5.23 Cloud Services*	Menetapkan kebijakan penggunaan layanan *cloud*	Menyusun kebijakan dan mengelola risiko	*SOP Cloud Service*
3	*A.7.4 Physical Security*	Memantau akses fisik tidak sah	Memasang dan mengelola CCTV dan alarm	*SOP Physical Security*
4	*A.8.9 Configuration Management*	Mengelola konfigurasi perangkat keras dan perangkat lunak	Mendefinisikan dan memantau konfigurasi	*SOP Configuration Management*
5	*A.8.10 Information Deletion*	Menghapus informasi yang tidak diperlukan	Memilih metode penghapusan yang aman	*SOP for Deletion of Information*
6	*A.8.11 Data Masking*	Menerapkan teknik masking	Menggunakan teknik masking,	*SOP Masking Data*

No	Kontrol Keamanan Informasi	Rekomendasi Implementasi	Tindakan yang Disarankan	SOP yang Perlu Dibuat
		data	pseudonimisasi, anonimisasi	
7	*A.8.12 Data Leakage Prevention*	Mencegah kebocoran data	Menggunakan alat pencegahan kebocoran data	*SOP for Data Leakage Prevention*
8	*A.8.16 Monitoring Services*	Memantau perilaku anomali	Menggunakan alat pemantauan jaringan dan sistem	*SOP Monitoring Service*
9	*A. 8.23 Web Filtering*	Mengelola akses ke situs web eksternal	Menetapkan aturan akses dan menggunakan filter web	*SOP Filter Web*
10	*A. 8.28 Secure Coding*	Menggunakan prinsip pengkodean aman	Menerapkan pengkodean aman dalam pengembangan	*Secure Coding SOP*

E. Simpulan

Sebagai kesimpulan, penelitian ini berhasil mengidentifikasi keadaan kontrol keamanan informasi saat ini di PT XYZ dan memetakan kesenjangan antara kondisi yang ada dan keadaan masa depan yang diinginkan sesuai ISO 27001: 2022. Studi ini memberikan rekomendasi implementasi yang spesifik dan terperinci untuk 11 kontrol *annex* baru, berdasarkan pedoman ISO 27002:2022. Rekomendasi ini, divalidasi oleh seorang ahli dan didapatkan hasil bahwa rekomendasi ini secara signifikan meningkatkan kepatuhan PT XYZ terhadap ISO 27001:2022 dan memastikan bahwa semua kontrol keamanan diterapkan di setiap proses aktivitas kerja yang dilakukan dan didokumentasikan secara efektif serta dibakukan kedalam bentuk SOP. Implementasi rekomendasi ini berdampak signifikan terhadap kepatuhan PT XYZ, terutama dengan proses terperinci untuk *cloud services* dan *Threat Intelligence*. Meskipun menghadapi tantangan dalam memperbarui SOP dan melatih karyawan, PT XYZ dapat mengatasi masalah ini melalui serangkaian pelatihan internal kepada karyawan dan dibantu dengan adanya masukan dan proses validasi kepada pihak eksternal yang memiliki kepakaran di bidang ISO 27001 ini.

Studi ini berkontribusi secara signifikan pada bidang keamanan informasi, menawarkan panduan praktis bagi perusahaan lain yang menjalani transisi serupa ke ISO 27001: 2022. Penelitian di masa depan dapat fokus pada studi longitudinal untuk mengamati efektivitas jangka panjang dari kontrol ini dan mengembangkan metode analisis kesenjangan baru untuk pemantauan kepatuhan yang lebih efisien. Dengan mengikuti rekomendasi implementasi terperinci dan mempertahankan peningkatan berkelanjutan, PT XYZ dapat memastikan kepatuhan berkelanjutan terhadap standar keamanan informasi terbaru, sehingga meningkatkan postur

keamanan dan kesiapan mereka secara keseluruhan terhadap ancaman siber yang berkembang.

F. Referensi

[1] Verizon. 2024 Data Breach Investigations Report _ Verizon - 2024-dbir-data-breach-investigations-report.pdf 2024.

[2] Undang-undang Perlindungan Data Pribadi. Undang-undang perlindungan data pribadi, 2022.

[3] ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - *Information Security Management System*s - Requirements. 2022;2010.

[4] Rajak C, Bharti J, Mateen A, Mehndiratta N, Chauhan J, Marndi R. A Roadmap to ISMS ISO 27001 Implementation Process. 3rd Int Conf Range Technol ICORT 2023 2023:1–5. https://doi.org/10.1109/ICORT56052.2023.10249115.

[5] Malatji M. Management of enterprise cyber security: A review of ISO/IEC 27001:2022. 2023 Int Conf Cyber Manag Eng CyMaEn 2023 2023:117–22. https://doi.org/10.1109/CyMaEn57228.2023.10051114.

[6] Tong CKS, Wong ETT. Implementation of *Information Security Management System* (ISMS) Aligned with ISO 27001. Gov Pict Arch Commun Syst 2019:53–70. https://doi.org/10.4018/978-1-59904-672-3.ch004.

[7] Tintin R, Hidalgo M. Could an ISMS Model (ISO/IEC 27001:2013 Standard) Implementation Really Protect Public Data? 2023 9th Int Conf EDemocracy EGovernment, ICEDEG 2023 2023:1–5. https://doi.org/10.1109/ICEDEG58167.2023.10122109.

[8] Bayona S, Wilber C, Milagros L, Carlos M. Implementation of NTP ISO/IEC 27001 in Public Institutions: Case Study 2024;1:410–6.

[9] Kurii Y, Opirskyy I. Iso 27001: Analysis of Changes and Compliance Features of the New Version of the Standard. Cybersecurity Educ Sci Tech 2023;3:46–55. https://doi.org/10.28925/2663-4023.2023.19.4655.

[10] Guo H, Wei M, Huang P, Chekole EG. Enhance Enterprise Security through Implementing ISO/IEC 27001 Standard. 2021 IEEE Int Conf Serv Oper Logist Informatics, SOLI 2021 2021:1–6. https://doi.org/10.1109/SOLI54607.2021.9672401.

[11] Condolo C, Romero S, Ticona W. Implementation of an *Information Security Management System* to Improve the IT Security of an Agricultural Tool Manufacturing Company. Proc 14th Int Conf *Cloud* Comput Data Sci Eng Conflu 2024 2024:177–83. https://doi.org/10.1109/Confluence60223.2024.10463232.

[12] Zaini Miftach. Implementing the ISO/IEC 27001 ISMS Standard. 2016.

[13] Hsu C, Wang T, Lu A. The impact of ISO 27001 certification on firm performance. Proc Annu Hawaii Int Conf Syst Sci 2016;2016-March:4842–8. https://doi.org/10.1109/HICSS.2016.600.

[14] 27001:2013 I. Information technology – Security techniques – *Information Security Management System*s – Requirements 2013:44.

[15] Monev V. Data Leakage Prevention in ISO 27001: Compliance and Implementation. 2023 37th Int Conf Inf Technol InfoTech 2023 - Proc 2023:1–5. https://doi.org/10.1109/InfoTech58664.2023.10266873.
[16] Mullany L, Stockwell P. Qualitative, quantitative and mixed methods research (Dörnyei). 2021. https://doi.org/10.4324/9781315707181-60.
[17] Safonova OM, Lontsikh NP, Golovina EY, Elshin V V., Koniuchov VY. Methodology for creating, implementing and system effectiveness evaluation of the business processes' information security system. Proc 2020 IEEE Int Conf "Quality Manag Transp Inf Secur Inf Technol IT QM IS 2020 2020:127–31. https://doi.org/10.1109/ITQMIS51053.2020.9322855.