Implementasi ISO 27001:2022 sebagai Kerangka Manajemen Keamanan Informasi untuk Meningkatkan Kepatuhan Regulasi di PT XYZ

1st David Tri Wijayanto
Faculty of Industrial Engineering
Telkom University
Bandung, Indonesia
davidwijayanto@student.telkomuniversity.ac.id

2 st Rd. Rohmat Saedudin
Faculty of Industrial Engineering
Telkom University
Bandung, Indonesia
rdrohmad @telkomuniversity.ac.id

3st Mochamad Teguh Kurniawan
Faculty of Industrial Engineering
Telkom University
Bandung, Indonesia
teguhkurniawan@telkomuniversity.ac.id

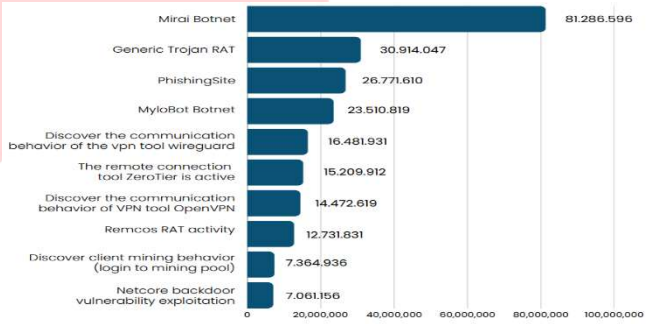
Perusahaan financial technology (fintech) seperti PT XYZ menghadapi tantangan signifikan dalam menjaga keamanan informasi akibat tingginya ketergantungan terhadap sistem digital dan tuntutan regulasi dari UU ITE, PP PSTE, serta peraturan OJK dan Bank Indonesia. Penelitian ini bertujuan untuk mengimplementasikan kerangka kerja ISO/IEC 27001:2022 guna meningkatkan pengelolaan keamanan informasi dan kepatuhan regulasi. Pendekatan yang digunakan adalah siklus *Plan–Do–Check–Act* (PDCA) dengan metode kualitatif pada divisi *IT Security & Operation, IT & Network,* serta *IT Planning & Development*. Hasil studi menunjukkan bahwa dari 93 kontrol pada Annex A ISO/IEC 27001:2022, sebanyak 76 kontrol telah diterapkan, sedangkan 17 kontrol lainnya belum diimplementasikan, sehingga tingkat kesiapan mencapai 82%. Penelitian ini menghasilkan dokumen Statement of Applicability (SoA) yang mencakup status implementasi serta justifikasi kontrol, dan juga merekomendasikan perbaikan strategis dalam pengelolaan keamanan informasi. Temuan ini menunjukkan bahwa implementasi ISO 27001:2022 dapat memperkuat ketahanan sistem, menjaga integritas data, serta meningkatkan kepercayaan pemangku kepentingan terhadap layanan digital PT XYZ.

Kata kunci—ISO 27001:2022, keamanan informasi, regulasi, SOA, manajemen risiko, fintech

I. PENDAHULUAN

Kemajuan teknologi informasi telah mendorong transformasi digital di berbagai sektor, termasuk industri fintech. PT XYZ, sebagai perusahaan penyedia platform *Fintech* Inovasi Keuangan Digital, sangat bergantung pada sistem teknologi informasi untuk mendukung keberlangsungan bisnis. Dalam konteks ini, keamanan informasi menjadi aspek yang sangat vital, mencakup kerahasiaan, integritas, dan ketersediaan data sebagai fondasi dari kepercayaan pelanggan dan kelangsungan layanan.

Namun, pesatnya perkembangan teknologi di sektor fintech juga diikuti oleh meningkatnya ancaman siber. Laporan Badan Siber dan Sandi Negara (BSSN) tahun 2024 mencatat ribuan serangan siber yang terjadi di Indonesia, meliputi botnet, trojan RAT, phishing, exploit, dan backdoor, yang dapat menyebabkan pencurian data nasabah, gangguan operasional, serta kerugian finansial. Lemahnya kesadaran keamanan dari sisi pengguna maupun organisasi memperburuk situasi ini.



GAMBAR 1
Serangan Siber Di Indonesia Tahun 2024

Respon terhadap situasi tersebut ditunjukkan melalui berbagai regulasi yang dikeluarkan oleh otoritas nasional, seperti UU ITE No. 11 Tahun 2008, PP No. 71 Tahun 2019 tentang PSTE, Perpres No. 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital, serta regulasi dari Bank Indonesia dan OJK terkait sistem pembayaran dan inovasi teknologi sektor keuangan. Regulasi-regulasi ini menuntut perusahaan untuk memiliki sistem keamanan informasi yang tidak hanya kuat secara teknis, tetapi juga sesuai standar internasional.

Salah satu standar yang diakui secara global adalah ISO/IEC 27001:2022. Standar ini menyediakan kerangka kerja sistematis dalam pengelolaan keamanan informasi, mencakup proses identifikasi aset, penilaian risiko, serta penerapan kontrol keamanan melalui *Statement of Applicability* (SoA). Implementasi ISO 27001:2022 diyakini dapat membantu PT XYZ dalam meminimalkan risiko, meningkatkan kepatuhan regulasi, dan memperkuat kepercayaan pelanggan.

Namun, implementasi standar ini tidak terlepas dari tantangan, seperti kurangnya pemahaman teknis, resistensi terhadap perubahan organisasi, serta keterbatasan sumber daya. Oleh karena itu, diperlukan kajian yang mendalam untuk mengevaluasi kesiapan dan kesesuaian penerapan ISO 27001:2022 di PT XYZ, khususnya dalam konteks pengelolaan aplikasi mobile yang diperuntukkan bagi pekerja migran Indonesia sebagai bagian dari layanan utama perusahaan.

Penelitian ini diharapkan dapat memberikan rekomendasi strategis dan teknis dalam upaya optimalisasi implementasi

ISO 27001:2022 di PT XYZ, serta berkontribusi terhadap pengembangan literatur akademik di bidang manajemen keamanan informasi di sektor teknologi dan keuangan digital di Indonesia.

II. KAJIAN TEORI

A. Definisi Keamanan Informasi

Keamanan informasi merupakan upaya sistematis untuk melindungi aset informasi dari berbagai ancaman yang dapat memengaruhi aspek kerahasiaan, integritas, dan ketersediaan, atau dikenal dengan CIA Triad.

1) *Confidentiality* memastikan bahwa data hanya diakses oleh pihak berwenang, sementara
2) *Integrity* menjaga keakuratan dan keutuhan data.
3) *Availability* menjamin akses terhadap informasi kapan pun dibutuhkan. Studi oleh Halim et al.[2] menekankan bahwa penerapan CIA Triad penting untuk menjaga kepercayaan pengguna dan integritas sistem digital.

Keamanan informasi bukan semata tanggung jawab divisi TI, tetapi seluruh elemen organisasi harus terlibat secara aktif[3]. Andriyani dan Handayani [4] menyatakan bahwa integrasi prinsip CIA dalam kebijakan organisasi meningkatkan ketahanan terhadap ancaman siber maupun kesalahan internal. Oleh karena itu, pemahaman mendalam mengenai prinsip CIA sangat penting sebagai fondasi dalam implementasi ISO/IEC 27001:2022.

B. Sistem Manajemen Keamanan Informasi (SMKI)

Sistem Manajemen Keamanan Informasi (SMKI) merupakan kerangka kerja formal berbasis ISO/IEC 27001:2022 yang dirancang untuk melindungi aset informasi dari ancaman dengan menjaga kerahasiaan, integritas, dan ketersediaan informasi (CIA Triad) [5]. SMKI diimplementasikan melalui pendekatan *Plan-Do-Check-Act* (PDCA) guna memastikan siklus perbaikan berkelanjutan dalam keamanan informasi [6].

Penerapan SMKI terbukti meningkatkan efektivitas kontrol keamanan serta membantu organisasi dalam memenuhi kepatuhan terhadap regulasi. Studi sebelumnya menunjukkan bahwa dokumen seperti *Statement of Applicability* (SoA) dan kebijakan berbasis PDCA mendukung tata kelola TI yang kuat serta memperkuat kepercayaan pemangku kepentingan[7], [8]

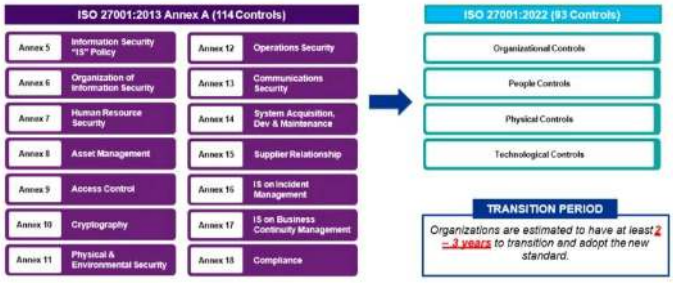
C. Framework Sistem Manajemen Keamanan Informasi

1) *ISO/IEC 27001*

ISO/IEC 27001 merupakan standar internasional yang dikembangkan oleh International Organization for Standardization (ISO) dan International Electrotechnical Commission (IEC) untuk menetapkan kerangka kerja Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management System* (ISMS) [5]. Standar ini pertama kali diterbitkan pada tahun 2005, lalu diperbarui pada tahun 2013 dan terakhir pada 2022 untuk menyesuaikan dengan dinamika ancaman keamanan siber dan perkembangan teknologi informasi [9].

ISO/IEC 27001:2022 mencakup proses identifikasi, penerapan, pemantauan, dan peningkatan kontrol keamanan informasi yang berkelanjutan. Perubahan besar pada versi 2022 adalah reorganisasi struktur kontrol: dari 114 kontrol dalam 14 domain pada versi 2013 menjadi 93 kontrol yang diklasifikasikan ke dalam empat kategori utama, yaitu:*Organizational*, *People*, *Physical*, dan *Technological Controls* [10].

Penyederhanaan ini bertujuan untuk meningkatkan fleksibilitas penerapan dan kemudahan dalam proses audit, serta menyesuaikan standar terhadap kebutuhan organisasi modern seperti cloud computing dan kerja jarak jauh.



GAMBAR 2
Perbandingan ISO/EIC 27001:2013 vs ISO/EIC 27001:2022

Standar ini mendukung pendekatan sistematis dan terukur dalam manajemen risiko informasi, serta menjadi acuan utama dalam meningkatkan kepatuhan terhadap regulasi dan membangun kepercayaan pemangku kepentingan.

2) *ISO/IEC 27002*

ISO/IEC 27002 merupakan standar pendukung ISO/IEC 27001 yang menyediakan panduan praktis dalam penerapan kontrol keamanan informasi yang tercantum pada Annex A [5]. Standar ini memuat praktik terbaik terkait pengelolaan kontrol, termasuk pengendalian akses, kebijakan penggunaan sistem, dan pemantauan keamanan [11]. Dengan demikian, ISO/IEC 27002 berfungsi sebagai referensi operasional dalam pelaksanaan Sistem Manajemen Keamanan Informasi (SMKI) di lingkungan organisasi.

Sukmaji et al.[11] menjelaskan bahwa ISO/IEC 27002 mendukung penerapan kontrol keamanan yang lebih efektif dan terukur dalam proses bisnis sehari-hari. Rokhman [12] menemukan bahwa penerapan ISO/IEC 27002 pada sektor Usaha Kecil dan Menengah (UKM) dapat meningkatkan kesadaran keamanan serta memperkuat kebijakan internal. Selain itu, standar ini dirancang fleksibel dan dapat diadaptasi oleh berbagai jenis organisasi, termasuk institusi pendidikan, sektor publik, dan industri [13]. Standar ini juga berperan menjaga stabilitas operasional organisasi tanpa mengabaikan perlindungan terhadap aset informasi [14].

D. Manajemen Risiko

1) Definisi Manajemen Risiko

Manajemen risiko merupakan proses sistematis untuk mengidentifikasi, menilai, dan mengendalikan potensi risiko yang dapat menghambat pencapaian tujuan organisasi. Dalam konteks teknologi informasi, pendekatan ini menjadi penting untuk mengelola ketidakpastian yang dapat

berdampak terhadap sumber daya dan kelangsungan operasional [15]

Supriyanto dan Widodo [16] menekankan bahwa manajemen risiko tidak hanya bertujuan menghindari kerugian, tetapi juga mendukung pengambilan keputusan berbasis analisis data. Proses ini mencakup penilaian terhadap kemungkinan dan dampak dari berbagai ancaman, serta penerapan kontrol mitigasi yang sesuai. Dalam keamanan informasi, manajemen risiko menjadi landasan utama untuk menentukan skala prioritas perlindungan terhadap aset yang bernilai tinggi dan rentan terhadap serangan siber.

2) Pentingnya Manajemen Risiko (Risk Management)

Manajemen risiko memiliki peran strategis dalam memastikan kelangsungan operasional dan pencapaian tujuan organisasi, khususnya dalam pengelolaan teknologi informasi dan perlindungan data. Dengan semakin meningkatnya kompleksitas sistem dan ancaman siber, organisasi dituntut menerapkan pendekatan proaktif guna menjaga kerahasiaan, integritas, dan ketersediaan informasi.

Rahmawati et al. [17] menyatakan bahwa penerapan manajemen risiko yang efektif memungkinkan organisasi mengidentifikasi ancaman secara dini dan mengambil tindakan preventif untuk meminimalkan dampak kerugian. Tanpa pendekatan tersebut, risiko gangguan operasional, kehilangan data, kerugian finansial, hingga penurunan reputasi menjadi semakin besar.

Sedangkan, Damayanti dan Siregar [18] menegaskan bahwa manajemen risiko juga berkontribusi pada efisiensi operasional dan kepatuhan terhadap standar seperti ISO/IEC 27001. Evaluasi risiko secara berkala memungkinkan organisasi merespons perubahan lingkungan dengan lebih adaptif serta menjaga keandalan dan keamanan sistem informasi secara menyeluruh.

3) *Penilaian Risiko (Risk Assessment)*

Penilaian risiko keamanan informasi adalah proses sistematis untuk mengidentifikasi, menganalisis, dan mengevaluasi risiko yang dapat memengaruhi kerahasiaan, integritas, dan ketersediaan aset informasi organisasi. Dalam konteks ISO/IEC 27001, penilaian risiko menjadi inti dari implementasi Sistem Manajemen Keamanan Informasi (SMKI) dan dilakukan secara berkala agar dapat menyesuaikan dengan perubahan lingkungan bisnis dan teknologi [19].

Proses penilaian risiko diawali dengan memahami konteks organisasi, mencakup isu internal maupun eksternal serta harapan dari pemangku kepentingan. Risiko diidentifikasi berdasarkan klasifikasi aset informasi seperti perangkat keras, perangkat lunak, dokumen digital, serta sumber daya manusia yang terlibat dalam pengelolaan sistem informasi. Hasil penilaian ini selanjutnya digunakan untuk menentukan tingkat risiko dan menetapkan langkah mitigasi yang sesuai.

Berikut adalah contoh klasifikasi tingkat risiko berdasarkan nilai dampak dan kemungkinan:

TABEL 1
Nilai/level Risiko Kemanan Informasi

Level Risiko	Dampak					Nilai/ Level	Keterangan/Tingkat penanganan risiko
Frekuensi	1	2	3	4	5		
1	I	I	II	III	IV	I (*Informational*)	Risiko masih diterima, tidak perlu dilakukan pengendalian
2	I	II	II	IV	IV	II (*Low*)	Risiko masih diterima, tidak perlu dilakukan pengendalian
3	II	II	III	IV	IV	III (*Medium*)	Pemantauan berkala, tidak diwajibkan untuk memiliki program penurunan risiko
4	II	III	IV	IV	V	IV (*High*)	Harus ada program penurunan risiko
5	III	III	IV	V	V	V (*Critical*)	Harus ada program penurunan risiko, Menjadi prioritas utama

E. *SOA (Statement of Applicability)*

Statement of Applicability (SoA) merupakan dokumen penting dalam implementasi Sistem Manajemen Keamanan Informasi (SMKI) berbasis ISO/IEC 27001. SoA memuat daftar kontrol keamanan dari Annex A ISO/IEC 27001, status penerapannya, serta justifikasi terhadap kontrol yang diterapkan atau tidak diterapkan [1]. Dokumen ini berfungsi sebagai penghubung antara hasil penilaian risiko dengan kontrol keamanan yang dipilih, sekaligus sebagai bukti bahwa organisasi mengelola risiko secara sistematis dan sesuai kebutuhan.

Afriansyah dan Mahardika [3] menekankan bahwa SoA yang disusun dengan baik mendukung identifikasi tanggung jawab pengendalian keamanan, meningkatkan efektivitas manajemen risiko, dan memastikan kepatuhan terhadap regulasi. Dengan demikian, SoA memiliki nilai strategis yang melampaui fungsi administratif, karena menjadi fondasi dalam keberlanjutan penerapan SMKI.

III. METODE

Penelitian Penelitian ini menggunakan pendekatan kualitatif dengan metode riset lapangan untuk memperoleh data faktual dan empiris yang mendalam terkait implementasi Sistem Manajemen Keamanan Informasi (SMKI) berbasis ISO/IEC 27001:2022 di PT XYZ. Pendekatan ini bertujuan untuk memahami fenomena secara kontekstual dan eksploratif melalui interaksi langsung dengan sumber data utama. Adapun teknik pengumpulan data yang digunakan meliputi:

A. Penyebaran Kuesioner

Kuesioner disusun berdasarkan klausul-klausul dalam ISO/IEC 27001:2022 dan digunakan untuk mengukur tingkat penerapan kontrol keamanan informasi serta kepatuhan terhadap regulasi yang berlaku. Instrumen ini disebarkan kepada tim yang terlibat langsung dalam pengelolaan sistem

informasi, seperti Divisi IT, IT Security, dan Network Operation.

B. Wawancara Mendalam *(In-depth Interview)*

Wawancara dilakukan terhadap personel kunci di lingkungan PT XYZ untuk menggali pemahaman, pengalaman, serta tantangan dalam implementasi ISO/IEC 27001:2022. Teknik ini bertujuan untuk mengidentifikasi praktik keamanan yang telah diterapkan serta aspek-aspek yang masih memerlukan peningkatan.

C. Observasi Langsung

Observasi dilakukan terhadap sistem, dokumen, infrastruktur, dan kontrol keamanan yang diterapkan di lingkungan kerja PT XYZ. Tujuannya adalah untuk memperoleh informasi aktual mengenai pelaksanaan kebijakan keamanan informasi serta mengevaluasi kesesuaiannya dengan standar ISO/IEC 27001:2022.

D. Studi Dokumentasi *(Literature and Document Review)*

Peneliti melakukan penelaahan terhadap dokumen internal perusahaan seperti kebijakan, prosedur operasional standar (SOP), dan bukti penerapan kontrol keamanan informasi. Selain itu, referensi eksternal berupa jurnal ilmiah, regulasi nasional, serta standar internasional juga dikaji untuk memperkuat analisis teoritis dan kontekstual.

Melalui kombinasi teknik pengumpulan data tersebut, penelitian ini diharapkan dapat memberikan gambaran yang menyeluruh serta menghasilkan rekomendasi strategis guna meningkatkan efektivitas implementasi SMKI di PT XYZ.

IV. HASIL DAN PEMBAHASAN

A. Gambaran Umum PT XYZ

PT XYZ merupakan perusahaan yang bergerak di bidang teknologi informasi dan layanan digital, termasuk dalam pengembangan aplikasi mobile untuk pekerja migran Indonesia. Dalam mendukung operasionalnya, PT XYZ sangat bergantung pada sistem informasi, perangkat keras dan lunak, serta sumber daya manusia yang memiliki tanggung jawab terhadap keamanan informasi. Oleh karena itu, implementasi ISO/IEC 27001:2022 menjadi penting untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi.

B. Penilaian terhadap Situasi dan Kondisi Saat Ini

1) Identifikasi Aset Informasi

Dalam konteks penerapan ISO 27001, pencatatan aset merupakan langkah awal yang krusial. Daftar aset berisi informasi lengkap terkait data, sistem, perangkat, dokumen, dan komponen lain yang digunakan dalam operasional organisasi dan memiliki nilai strategis terhadap keamanan informasi.

Identifikasi aset dilakukan melalui observasi langsung, review dokumentasi, serta wawancara dengan Tim IT. Hasil identifikasi tersebut dirangkum dalam Tabel IV.2 Kategori Aset Informasi PT XYZ berikut:

TABEL 3
Ringkasan Kategori Aset Informasi PT XYZ

No	Kategori Aset	Contoh Aset Utama	Kategori Keamanan
1	Software	SIEM, Packet Capture, Threat Intel, NIDS/HIDS	Kritikal
2	Hardware Forensik	EnCase, Tableau TX1, Laptop Forensic	Kritikal
3	Hardware Operasional	PC, Monitor, Keyboard	Non-Kritikal
4	Data dan Informasi	Dokumen Evidence, SK, Laporan, Chain of Custody	Kritikal
5	Storage	NAS, HDD Eksternal	Kritikal

Aset-aset yang dikategorikan sebagai kritikal, seperti tools monitoring, forensic tools, dan dokumen internal rahasia, menunjukkan fokus penting dalam perlindungan data dan sistem inti.

C. Penilaian Risiko Keamanan Informasi

1) *Metode Penilaian Risiko*

Penilaian risiko keamanan informasi di PT XYZ dilakukan dengan mengacu pada kerangka ISO/IEC 27005 yang mendukung implementasi ISO/IEC 27001:2022. Tahapan penilaian meliputi identifikasi risiko, analisis risiko berdasarkan kemungkinan dan dampaknya, evaluasi tingkat risiko, serta penetapan pengendalian yang sesuai. Penilaian ini mencakup aset informasi berupa *software*, *hardware*, file digital dan kertas, sistem, proses, serta keterlibatan pihak ketiga dan personil internal.

2) Hasil Penilaian Risiko

Dari hasil evaluasi yang dilakukan, teridentifikasi 16 risiko dengan kategori tinggi (*high risk*) yang dinilai memiliki dampak signifikan terhadap keberlangsungan operasional serta keamanan informasi di lingkungan PT XYZ. Risiko-risiko tersebut muncul akibat berbagai kelemahan seperti kontrol akses yang tidak optimal, kurangnya pengawasan terhadap pihak ketiga, hingga prosedur backup yang tidak berjalan efektif. Adapun tindakan mitigasi yang telah diterapkan mencakup penggunaan prosedur formal, kontrol teknis seperti hardening dan pemantauan log, serta kebijakan berbasis peran (*role-based policy*).

Berikut adalah ringkasan risiko dengan kategori tinggi:

TABEL 4
Risiko dengan Kategori Tinggi (*High Risk*)

No	Jenis Aset	Risiko	Kontrol yang Ada	Level Risiko
1	Digital File	Informasi terpapar ke pihak tidak berwenang	Prosedur clean *desk & clear screen*	High
2	Software	Sistem tidak mencapai target kinerja	Perencanaan dan pengujian sistem	High

3	Software	Sistem overload	Pemantauan kapasitas	High
4	Software	Serangan malware / dongle hilang	Antivirus & penyimpanan aman	High
5	Software	Akses user tidak berwenang	Hardening & respons insiden	High
6	Software	Perubahan sistem tidak terotorisasi	Prosedur manajemen perubahan	High
7	Software	User tanpa izin akses sistem	Kontrol akses & pemantauan aktivitas	High
8	Software	Penyalahgunaan akses administrator	Pembatasan & audit log	High
9	Digital File	Akses berlebihan oleh pihak ketiga	Pembatasan & *review* akses	High
10	Digital File	Data tidak dapat direstore	Backup berkala	High
11	System	Sistem dibobol	VA & pentest rutin	High
12	Hardware	Kerusakan perangkat keras	Maintenance rutin	High
13	Digital File	Kehilangan data	Antivirus & backup eksternal	High
14	Software	Peretasan karena celah software	Patch rutin & endpoint security	High
15	People	Penyalahgunaan posisi kepercayaan	Kebijakan berbasis role	High
16	Digital File	Penyalahgunaan email	Penggunaan email resmi perusahaan	High

3) Dampak Risiko dengan Kategori Tinggi *(High Risk)*

Analisis lebih lanjut terhadap risiko tinggi yang ditemukan menunjukkan berbagai dampak signifikan, termasuk gangguan layanan, kebocoran informasi, dan kerusakan sistem. Penyebab umum dari risiko-risiko tersebut antara lainlemahnya kontrol akses, kurangnya dokumentasi prosedur perubahan, serta tidak optimalnya kebijakan backup dan perlindungan endpoint. Rangkuman risiko tersebut disajikan dalam tabel berikut:

TABEL 5
Dampak Risiko Tinggi Keamanan Informasi

No	Risiko Tinggi yang Ditemukan	Dampak	Penyebab Umum
1	Informasi terpapar ke pihak tidak berwenang	Kebocoran data	Akses yang tidak dikontrol dengan baik
2	Sistem tidak mencapai target kinerja	Gangguan operasional	Tidak optimalnya perencanaan dan kapasitas
3	Overload sistem	Penurunan performa	Beban sistem tidak dipantau
4	Serangan malware atau hilangnya dongle	Gangguan & kehilangan lisensi	Kurangnya proteksi endpoint
5	Akses tidak sah ke sistem	Ancaman insider	Lemahnya kontrol akses
6	Perubahan sistem tidak terotorisasi	Sistem rusak	Tidak adanya prosedur manajemen perubahan
7	Penyalahgunaan hak administrator	Sistem disalahgunakan	Tidak ada review log atau pembatasan hak istimewa
8	Vendor mengakses data kritikal secara ilegal	Kebocoran eksternal	Tidak adanya pengawasan akses pihak ketiga
9	Data tidak bisa dipulihkan saat insiden	Kehilangan data permanen	Backup tidak berjalan efektif
10	Sistem dibobol (hacking)	Gangguan besar	Tidak adanya VA/Pentest rutin

D. Current State Assessment

Penilaian kondisi saat ini dilakukan untuk mengevaluasi kesesuaian implementasi pengendalian keamanan informasi di PT XYZ terhadap ISO/IEC 27001:2022. Hasil assessment menunjukkan bahwa meskipun kebijakan dasar keamanan informasi telah tersedia dan disahkan oleh manajemen, implementasi di berbagai area masih belum optimal. Beberapa kontrol belum terdokumentasi secara formal, seperti prosedur manajemen akses, pengujian keamanan sistem, serta pengelolaan insiden keamanan.

Selain itu, pengamanan aset fisik seperti ruang SOC belum didukung pemantauan dan pencatatan aktivitas yang memadai. Dari sisi teknologi, kontrol atas akses istimewa, penggunaan perangkat monitoring, dan pengamanan cloud service masih bergantung pada vendor eksternal tanpa pengawasan internal yang kuat. Prosedur formal seperti change management, backup, dan pengujian sistem belum diterapkan secara konsisten.

Secara umum, PT XYZ telah memiliki dasar-dasar tata kelola keamanan informasi, namun perlu perbaikan signifikan dalam dokumentasi, sosialisasi, dan pengawasan agar sepenuhnya memenuhi standar ISO/IEC 27001:2022.

E. Pembahasan Hasil

Hasil penilaian menunjukkan bahwa PT XYZ telah melakukan identifikasi aset informasi secara menyeluruh dan mulai menerapkan kontrol dasar sesuai ISO/IEC 27001:2022. Namun, masih ditemukan 16 risiko dengan kategori tinggi, seperti akses tidak sah, serangan malware, kebocoran data, serta kegagalan backup. Risiko-risiko tersebut utamanya disebabkan oleh lemahnya kontrol akses, belum adanya prosedur formal yang terdokumentasi, serta minimnya pengawasan terhadap pihak ketiga.

Current State Assessment juga menunjukkan bahwa sebagian besar kontrol belum diterapkan secara konsisten.

Beberapa kebijakan keamanan informasi memang telah tersedia, namun banyak prosedur pelaksanaannya belum diformalkan, disosialisasikan, atau dimonitor secara berkala. Kelemahan ditemukan pada aspek teknis seperti pengelolaan hak istimewa, pengamanan cloud, backup log, hingga pengujian keamanan sistem. Di sisi fisik, pencatatan dan pemantauan aktivitas di ruang SOC juga masih belum optimal.

Kondisi ini menunjukkan bahwa meskipun fondasi tata kelola keamanan informasi sudah terbentuk, PT XYZ masih memerlukan upaya signifikan dalam peningkatan dokumentasi, pelaksanaan kontrol, serta penguatan budaya keamanan informasi. Dengan menerapkan perbaikan berkelanjutan, perusahaan dapat meningkatkan efektivitas perlindungan aset informasi dan memenuhi standar serta kewajiban regulasi yang berlaku.

V. KESIMPULAN

Penelitian ini menyimpulkan bahwa implementasi ISO/IEC 27001:2022 sebagai kerangka Sistem Manajemen Keamanan Informasi (SMKI) di PT XYZ telah memberikan kontribusi signifikan dalam meningkatkan kepatuhan terhadap regulasi serta memperkuat tata kelola keamanan informasi. Pertama, proses identifikasi, klasifikasi, dan pencatatan aset informasi telah dilakukan secara sistematis sesuai standar, mencakup aset seperti digital file, perangkat keras, perangkat lunak, sistem, proses, hingga sumber daya manusia. Pendekatan ini menjadi dasar bagi penerapan kontrol keamanan yang relevan dan efektif.

Kedua, evaluasi risiko menunjukkan bahwa PT XYZ masih menghadapi ancaman terhadap kerahasiaan, integritas, dan ketersediaan informasi, dengan beberapa aset berada pada kategori risiko menengah hingga tinggi. Mitigasi dilakukan berdasarkan prinsip-prinsip ISO 27001:2022, melalui penerapan kontrol seperti pengendalian akses, pelabelan informasi, serta proteksi fisik dan teknis.

Ketiga, tingkat kesiapan implementasi ISO/IEC 27001:2022 dinilai tinggi, dengan 76 dari 93 kontrol (sekitar 82%) telah diimplementasikan. Hal ini mencerminkan komitmen kuat perusahaan dalam menjaga keamanan informasi. Penelitian ini juga berhasil menyusun dokumen Statement of Applicability (SoA) yang merinci status penerapan dan justifikasi masing-masing kontrol, menjadi acuan penting dalam tata kelola keamanan informasi berkelanjutan di lingkungan PT XYZ.

VI. REFERENSI

[1] BSSN, “LANSKAP KEAMANAN SIBER INDONESIA 2024,” Jakarta, Apr. 2024.

[2] C. D. A. D. N. A. F. Abdul Halim Harahap1, “Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder,” *Jurnal Manajemen dan Pemasaran Digital*, vol. 1, pp. 73–83, Apr. 2023, Accessed: Jun. 25, 2025. [Online]. Available: https://siberpublisher.org/index.php/JMPD/article/view/34/38

[3] I. Hardaningtyas, R. Andryana, and T. R. Hermansyah, “Analisis Implementasi ISO 27001 dalam Penguatan Sistem Manajemen Keamanan Informasi di Lembaga Pemerintah,” *Jurnal Teknologi dan Sistem Informasi*, vol. 2, no. 1, pp. 45–52, 2021.

[4] R. Andriyani and R. Handayani, “Peran CIA Triad dalam Peningkatan Keamanan Informasi Organisasi,” *Jurnal Teknologi dan Keamanan Siber*, vol. 3, no. 2, pp. 60–66, 2020.

[5] ISO/IEC, “Information security management systems,” Geneva, Switzerland, 2022.

[6] ST. , M. Dadan Rahmat, “Perencanaan Sistem Manajemen Keamanan Informasi Menggunakan Standar SNI ISO/IEC 27001: 2013,” *Jurnal Informatika*, vol. 6, no. 6, pp. 37–41, Dec. 2019.

[7] S. A. Sholikhatin, A. Setyanto, S. Si, E. T. Luthfi, and M. Kom, “Analisis Keamanan Sistem Informasi Dengan ISO 27001 (Studi Kasus: Sistem Informasi Akademik Universitas Muhammadiyah Purwokerto),” *Jurnal IT CIDA*, vol. 4, no. 1, 2018.

[8] T. Hartati, G. P. Mindara, and C. L. Mindara, “Sistem Manajemen Keamanan Informasi Perlindungan Nilai Matakuliah berbasis ISO 27001,” *Jurnal ICT : Information Communication & Technology*, vol. 23, no. 1, pp. 117–123, 2023, [Online]. Available: https://ejournal.ikmi.ac.id/index.php/jict-ikmi

[9] S. Bijlmakers, “The International Organization for Standardization A Seventy-Five-Year Journey toward Organizational Resilience”, doi: 10.2202/1940-0004.1140/pdf?stream=true.

[10] S. Clarissa and G. Wang, “Assessing Information Security Management Using ISO 27001:2013,” *Jurnal Indonesia Sosial Teknologi*, vol. 4, no. 9, pp. 1361–1371, Sep. 2023, doi: 10.59141/jist.v4i9.739.

[11] M. Sukmaji, R. Yasirandi, and Al Makky, . “Information Security Policy and SOP as the Access Control Document of PT. Jui Shin Indonesia Using ISO/IEC 27002:2013,” *Jurnal Pilar Nusa Mandiri*, vol. 19, no. 1, pp. 45–52, 2023.

[12] F. Rokhman, “Implementasi ISO/IEC 27002 dalam Rangka Meningkatkan Sistem Keamanan Informasi pada Usaha Kecil Menengah,” *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 5, no. 2, pp. 101–109, 2018.

[13] A. Supriyanto and K. Mustofa, “Analisis Penerapan ISO/IEC 27002 untuk Menilai Tingkat Kematangan Keamanan Informasi pada Perguruan Tinggi Negeri,” *Jurnal Penelitian dan Pengembangan Teknologi Informasi*, vol. 9, no. 1, pp. 15–24, 2021.

[14] Nurul Fadhylah Octariza, “Analisis Sistem Manajemen Keamanan Informasi Menggunakan Standar ISO/IEC 27001 dan ISO/IEC 27002 pada Kantor Pusat PT Jasa Marga,” Universitas Islam Negeri Syarif Hidayatullah Jakarta, Jakarta, 2019.

[15] H. Sutrisno, A. Rahmawati, and D. Nugroho, “Analisis Manajemen Risiko Teknologi Informasi Menggunakan Pendekatan ISO 27005 pada Sistem Informasi Akademik,” *Jurnal Teknologi dan Sistem Informasi*, vol. 3, no. 2, pp. 110–117, 2022.

[16] A. Supriyanto and S. Widodo, “mplementasi Manajemen Risiko Berbasis ISO 31000 dalam Pengelolaan Keamanan Informasi,” *Jurnal Penelitian Ilmu Komputer*, pp. 75–83, 2021.

[17] R. Rahmawati, R. Maulana, and D. Septiani, “Penerapan Manajemen Risiko dalam Pengelolaan Sistem Informasi Berbasis ISO 27001,” *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 8, no. 2, pp. 215–222, 2021.

[18] D. Damayanti and H. Siregar, “ Peran Manajemen Risiko dalam Meningkatkan Efektivitas Sistem Keamanan Informasi,” vol. 4, no. 1, pp. 45–53, 2022.

[19] S. Ardiansyah and F. Nugroho, “Evaluasi Risiko Keamanan Informasi dalam Implementasi ISO 27001,” *Jurnal Keamanan Siber*, vol. 9, no. 1, pp. 44–52, 2021.