Journal of Applied Informatics and Computing (JAIC)
Vol.x, No.x, Juli 201x, pp. xx~xx
e-ISSN: 2548-6861

Evaluasi Tingkat Kematangan Keamanan Informasi Berbasis ISO/IEC 27001:2022 pada Perusahaan Manufaktur (Studi Kasus: PT XYZ)

Raisya Marsandra [1]*, Nur Cahyono Kushardianto [2]**
* Rekayasa Keamanan Siber, Jurusan Teknik Informatika, Politeknik Negeri Batam
** Teknik Komputer, Jurusan Teknik Informatika, Politeknik Negeri Batam
raisya.4332211017@polibatam.ac.id [1], anung@polibatam.ac.id [2]

Article Info

Article history:

Received …
Revised …
Accepted …

Keyword:

information security maturity, ISO/IEC 27001:2022, COBIT 2019, process capability model, gap analysis.

ABSTRACT

The manufacturing sector has been the most frequently targeted by ransomware for three consecutive years, with most attacks directed at production systems. This study evaluates the information security maturity of PT XYZ, a manufacturing company in Batam, based on ISO/IEC 27001:2022 using the COBIT 2019 Process Capability Model (PCM). A mixed-methods explanatory sequential design was employed. Quantitative data were first collected through a structured questionnaire covering Clauses 4–10 and 93 Annex A controls, each scored on the COBIT 2019 PCM scale, and were then deepened through guided interviews and document analysis to explain the quantitative results. Following a separated assessment approach, capability indices for Clauses 4–10 and Annex A were calculated independently rather than merged into a single overall score. Results show four of seven clauses at Level 1 (Performed), two clauses (Planning and Support) reaching Level 2 (Managed), and Clause 5 Leadership recording the lowest level, Level 0 (Incomplete). Within Annex A, three of four domains sit at Level 1 (Performed), while Domain A.6 People controls is the only domain meeting the Level 3 (Established) target. Qualitative findings confirm that the primary weakness lies in governance, namely the absence of a formal information security policy, internal audit, and a designated ISMS role, rather than technical capacity. The study recommends establishing a formal policy and ISMS role, documenting currently ad-hoc controls as SOPs, and conducting periodic internal audits to support certification readiness.

I. PENDAHULUAN

Di era digital, informasi telah menjadi aset strategis bagi perusahaan manufaktur, yang menopang proses produksi, rantai pasok, hingga pengambilan keputusan. Namun, ketergantungan pada teknologi juga meningkatkan risiko keamanan siber. Laporan [1] mencatat kerugian global akibat kejahatan siber mencapai angka triliunan dolar setiap tahunnya. Lebih spesifik, [2] menyebut sektor manufaktur sebagai sektor paling sering diserang ransomware tiga tahun berturut-turut, dengan sekitar 71% serangan langsung menyasar sistem produksi.

Standar internasional ISO/IEC 27001:2022 hadir sebagai panduan untuk membangun Sistem Manajemen Keamanan Informasi (SMKI) yang berfokus pada siklus *Plan-Do-Check-Act*, mulai dari identifikasi risiko, implementasi kontrol, hingga peningkatan berkelanjutan. Versi terbaru menyederhanakan jumlah kontrol dari 114 menjadi 93 kontrol yang dikelompokkan ke dalam empat tema, yaitu kontrol organisasional, sumber daya manusia, fisik, dan teknologi. Meskipun penelitian penerapan ISO/IEC 27001 telah banyak dilakukan, sebagian besar masih berfokus pada kepatuhan terhadap kontrol dan belum menggambarkan kualitas proses yang mendukung penerapannya. Padahal, keberhasilan SMKI tidak hanya ditentukan oleh keberadaan kontrol, tetapi juga oleh bagaimana proses direncanakan, dijalankan, dipantau, dan ditingkatkan secara berkelanjutan. Dalam penerapannya, siklus PDCA mencakup identifikasi dan evaluasi risiko, implementasi kontrol, pemantauan kinerja, serta tindakan korektif dan preventif untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi [3].

e-ISSN: 2548-6861

Penelitian terdahulu masih banyak yang menggunakan pendekatan kepatuhan sederhana atau skala penilaian non-baku. [4] dan [5] menunjukkan bahwa COBIT 2019 dengan skala *capability level* mampu memberikan gambaran terukur dan terstruktur mengenai kondisi pengelolaan TI. Sementara itu, [6] telah mengombinasikan COBIT 2019 dan ISO/IEC 27001:2022 di sektor ritel, namun belum ada yang secara spesifik menerapkan kombinasi tersebut di lingkungan manufaktur. Dari tinjauan ini, teridentifikasi dua celah penelitian. Pertama, sebagian besar evaluasi masih menggunakan ISO/IEC 27001:2013 atau skala tidak terstandar. Kedua, studi yang mengkaji ISO/IEC 27001:2022 dengan instrumen terukur di sektor manufaktur masih terbatas.

Pemilihan ISO/IEC 27001:2022 pada penelitian ini didasarkan pada beberapa pertimbangan. Versi 2022 merupakan revisi terbaru yang menyederhanakan struktur kontrol dari 114 menjadi 93 kontrol dan mengelompokkannya ke dalam empat tema, sehingga memudahkan pemetaan kontrol terhadap kondisi perusahaan dan mengurangi tumpang tindih antar kontrol dibandingkan versi 2013. Selain itu, versi 2022 mengakomodasi kontrol baru yang relevan dengan ancaman siber terkini, seperti intelijen ancaman, keamanan layanan cloud, dan pemantauan aktivitas, sehingga lebih sesuai untuk perusahaan manufaktur yang bergantung pada sistem produksi digital.

Penelitian ini bertujuan untuk: (1) menilai tingkat kematangan keamanan informasi PT XYZ berdasarkan seluruh klausul dan 93 kontrol ISO/IEC 27001:2022 menggunakan skala COBIT 2019 PCM; (2) mengidentifikasi kesenjangan antara kondisi aktual dengan target Level 3 (*Established*) sebagai tingkat kesiapan pra-sertifikasi; dan (3) menyusun rekomendasi strategis untuk mendukung kesiapan perusahaan menuju sertifikasi.

II. METODE

A. Rancangan Penelitian

Penelitian ini menggunakan *mixed methods* dengan *explanatory sequential design* yaitu pendekatan yang mengumpulkan dan menganalisis data kuantitatif terlebih dahulu, lalu menindaklanjutinya dengan data kualitatif untuk menjelaskan dan memperdalam temuan kuantitatif [7]. Desain ini dipilih karena penilaian tingkat kapabilitas menghasilkan skor terukur yang memerlukan penjelasan kontekstual mengenai penyebab suatu level tercapai atau tidak tercapai. Data kuantitatif diperoleh melalui pengisian instrumen berbasis skala COBIT 2019 PCM, kemudian hasil skor tersebut menjadi dasar penyusunan fokus wawancara untuk menggali konteks kebijakan dan hambatan implementasi. Pendekatan berurutan seperti ini telah diterapkan pada evaluasi sistem informasi yang mengombinasikan kuesioner dan wawancara mendalam [8]. Sejalan dengan [9] dan [10], kombinasi data numerik dan tematik diperlukan untuk mengungkap dimensi implementasi yang saling melengkapi.

Dari sisi sifat, studi ini bersifat deskriptif-evaluatif, bertujuan menggambarkan kondisi aktual implementasi ISO/IEC 27001:2022 di PT XYZ secara sistematis dan faktual [11]. Integrasi kedua jenis data dilakukan pada tahap pembahasan, dengan menggunakan temuan kualitatif untuk menjelaskan hasil kuantitatif dan mengonfirmasi atau menjelaskan perbedaan yang muncul.

B. Objek dan Ruang Lingkup Penelitian

Penelitian dilakukan di PT XYZ, sebuah perusahaan manufaktur yang berlokasi di Batam. Teknik *purposive sampling* digunakan untuk memilih responden yang terlibat langsung dalam pengelolaan keamanan informasi, yaitu divisi *IT*, *Human Resource (HR)*, *Top Management*, dan *Finance*. Ruang lingkup penilaian mencakup Klausul 4 sampai 10 beserta 93 kontrol Annex A ISO/IEC 27001:2022. Penelitian difokuskan pada evaluasi tingkat kematangan dan penyusunan rekomendasi, serta tidak mencakup tahap implementasi perbaikan maupun verifikasi sertifikasi.

Tabel 1. Deskripsi Peran Departemen

Departement	Peran
IT	Bertanggung jawab atas operasional, pemeliharaan, dan keamanan sistem informasi.
HR	Mengelola kebijakan keamanan SDM, pelatihan kesadaran keamanan, serta proses rekrutmen dan pemberhentian.
Top Management	Berwenang dalam pengambilan keputusan strategis, penetapan kebijakan keamanan informasi, dan alokasi anggaran.
Finance	Menangani data keuangan sensitif dan terlibat dalam evaluasi risiko keuangan terkait keamanan informasi.

Data kuantitatif dikumpulkan terlebih dahulu melalui instrumen terstruktur berbasis 93 kontrol Annex A (A.5–A.8) dan Klausul 4–10 ISO/IEC 27001:2022, dengan setiap kontrol dinilai menggunakan skala COBIT 2019 PCM (0–5). Selanjutnya, dilakukan wawancara dengan responden kunci untuk menjelaskan dan mengonfirmasi hasil skor kuantitatif. Untuk mengurangi bias penilaian mandiri, skor yang diperoleh diverifikasi terhadap bukti dokumenter yang relevan, seperti kebijakan, prosedur operasional standar, log insiden, dan catatan konfigurasi, sebagaimana ditegaskan oleh [10] bahwa setiap kontrol harus didukung bukti dokumenter yang relevan. Skor akhir suatu kontrol

ditetapkan berdasarkan kesesuaian antara jawaban responden dan bukti yang dapat diverifikasi.

Untuk penilaian ini, seluruh 93 kontrol di Annex A dan semua klausul dianggap berlaku (applicable). Meskipun PT XYZ tidak melaksanakan sendiri aktivitas teknis tingkat lanjut tertentu secara lokal (seperti pengujian kerentanan dan pengembangan perangkat lunak yang dialihdayakan ke perusahaan induk di luar negeri), lokasi setempat tetap memiliki tanggung jawab atas pengelolaan dan pengawasan aktivitas tersebut. Oleh karena itu, kontrol-kontrol ini dimasukkan dalam penilaian untuk memberikan gambaran lengkap mengenai tanggung jawab tata kelola organisasi secara keseluruhan.

C. Justifikasi Pemilihan Model Penilaian

Pemilihan COBIT 2019 PCM didasarkan pada tiga pertimbangan. Pertama, modelnya aksesibel secara akademik dan praktis karena dokumentasi dan panduannya tersedia luas, berbeda dengan ISO/IEC TS 33052:2016 yang terbatas aksesnya. Kedua, model ini terbukti efektif untuk penilaian kematangan ISMS berbasis ISO 27001 pada berbagai konteks organisasi. Ketiga, skala level 0-5 setara secara struktural dengan model penilaian proses internasional, sehingga hasil penilaian dapat dibandingkan.

Selain itu, COBIT 2019 dipilih dibandingkan COBIT 5 karena menyediakan model penilaian yang lebih lengkap. COBIT 5 hanya memiliki satu model pengukuran, yaitu capability level yang mengacu pada ISO/IEC 15504/33000, sedangkan COBIT 2019 melengkapinya dengan maturity level yang diselaraskan dengan Capability Maturity Model Integration (CMMI) [12]. COBIT 2019 juga merupakan pembaruan yang mengakomodasi perkembangan tata kelola TI terkini, sehingga lebih relevan untuk penilaian pada saat penelitian dilakukan.

Kombinasi COBIT dan ISO 27001 telah dipresedenkan dalam sejumlah studi. Almeida et al. mengembangkan model penilaian COBIT 5 dan ISO 27001 secara simultan serta menunjukkan keterkaitan kuat antara praktik proses COBIT dan kontrol ISO 27001 [13]. Aflakhah dan Soewito menggabungkan COBIT 2019 dan ISO 27001 untuk evaluasi maturity sekaligus penyusunan rencana mitigasi [14]. Artamevia dan Triayudi mengombinasikan COBIT 2019 dan ISO/IEC 27001:2022 untuk evaluasi maturity level [6], sedangkan penerapan COBIT 2019 pada sektor manufaktur divalidasi oleh Nugroho dan Ginardi [15]. Sebagai keterbatasan, sebagian besar preseden tersebut masih memasangkan COBIT dengan ISO 27001:2013, dan preseden spesifik yang memadukan COBIT 2019 PCM dengan ISO/IEC 27001:2022 masih terbatas. Penelitian ini diarahkan untuk mengisi keterbatasan tersebut.

D. Instrumen dan Skala Penelitian

Tingkat kemampuan proses diukur menggunakan COBIT 2019 Process Capability Model (PCM) dengan enam tingkatan sebagaimana ditunjukkan pada Tabel 2. Setiap kontrol diberi skor 0 sampai 5 sesuai kondisi penerapannya, lalu nilai kapabilitas dihitung sebagai rata-rata skor seluruh kontrol yang dinilai dengan rumus berikut.

Tabel 2. Pemetaan Level Kapabilitas terhadap Evaluasi Keamanan ISO/IEC 27001:2022

Level	Label	Interpretasi untuk Kontrol ISO/IEC 27001:2022
0	*Incomplete*	Kontrol tidak dijalankan. Tidak ada kebijakan, prosedur, atau aktivitas keamanan yang dapat diidentifikasi terkait kontrol ini.
1	*Performed*	Kontrol dijalankan secara informal dan bergantung pada inisiatif individu. Tidak ada dokumentasi, prosedur, atau perencanaan yang mendukung pelaksanaannya.
2	*Managed*	Kontrol direncanakan dan dipantau. Terdapat kebijakan atau prosedur awal yang mengatur pelaksanaannya, namun belum diterapkan secara seragam di seluruh organisasi.
3	*Established*	Kontrol dilaksanakan menggunakan prosedur yang terdokumentasi dan distandarisasi secara organisasional. Luaran kontrol dihasilkan secara konsisten.
4	*Predictable*	Kontrol dipantau menggunakan metrik kuantitatif. Efektivitasnya terukur dan variasi kinerja dapat dideteksi serta dikoreksi secara sistematis.
5	*Optimizing*	Kontrol terus ditingkatkan secara proaktif berdasarkan evaluasi kinerja dan perubahan ancaman. Perbaikan berkelanjutan terdokumentasi dan diinstitusionalisasi.

Setiap kontrol dinilai berdasarkan bukti pelaksanaan yang dapat diverifikasi. Nilai indeks kapabilitas tiap domain dihitung dari rata-rata skor kontrol pada domain tersebut.

$$Skor\ Kontrol = \frac{Jumlah\ skor\ seluruh\ responden}{jumlah\ responden}$$

e-ISSN: 2548-6861

$$Indeks\ Kapabilitas = \frac{Jumlah\ skor\ seluruh\ kontrol}{Jumlah\ kontrol\ yang\ dinilai}$$

Hasil perhitungan indeks kapabilitas kemudian dikonversi ke tingkat kapabilitas menggunakan rentang nilai pada Tabel 3. Rentang nilai indeks pada Tabel 3 mengacu pada kriteria konversi indeks tingkat kematangan yang digunakan dalam [11].

Tabel 3. Skala Penilaian *Process Capability Level*

Level	Label	Rentang Nilai Indeks
0	*Incomplete*	0,0 - 0,50
1	*Performed*	0,51 - 1,50
2	*Managed*	1,51 - 2,50
3	*Established*	2,51 - 3,50
4	*Predictable*	3,51 - 4,50
5	*Optimizing*	4,51 - 5,00

E. Panduan Wawancara

Untuk menjamin penelitian dapat direplikasi, penilaian tidak hanya bergantung pada pengisian instrumen kuesioner, tetapi juga dikonfirmasi dan diklarifikasi melalui wawancara semi-terstruktur dengan responden kunci di masing-masing divisi. Wawancara ini bertujuan memastikan skor *self-assessment* yang diberikan responden konsisten dengan kondisi aktual di lapangan, sekaligus menjelaskan konteks di balik skor yang diperoleh. Panduan wawancara terdiri dari pertanyaan kunci yang diturunkan dari persyaratan setiap klausul dan kontrol Annex A. Panduan wawancara lengkap disajikan pada Lampiran, sedangkan contoh pertanyaan kunci beserta tujuan penggaliannya per kelompok responden ditunjukkan pada Tabel 4.

Tabel 4. Contoh Pertanyaan Kunci dan Tujuannya

Responden	Pertanyaan Inti	Tujuan
***Top Management* (Klausul 5)**	Apakah manajemen puncak memahami dan mendukung penerapan ISMS? Dalam bentuk apa dukungan itu diwujudkan?	Mengonfirmasi ada/tidaknya kebijakan formal dan dukungan kepemimpinan untuk menjelaskan skor rendah pada Klausul 5.
IT (Klausul 8, Domain A.8)	Kontrol apa saja yang sudah berjalan saat ini, seperti antivirus, firewall, backup, atau MFA?	Memverifikasi implementasi teknis dan status dokumentasi kontrol untuk membedakan antara kontrol yang "berjalan" vs "terdokumentasi secara formal".
HR (Domain A.6)	Apakah ada program pelatihan atau sosialisasi keamanan informasi untuk karyawan?	Mengonfirmasi alasan mengapa Domain A.6 mencapai Level 3 (karena prosedur SDM berjalan) serta mengidentifikasi celah koordinasi dengan IT.
***Finance* (Domain A.5)**	Apakah ada inventaris aset informasi yang mencakup data keuangan? Siapa yang mengelolanya?	Memeriksa penerapan kontrol aset dan keterlibatan unit bisnis dalam manajemen risiko untuk menjelaskan skor rendah di Domain A.5.

F. Tahapan Penelitian

:

Gambar 1. Tahapan Penelitian.

Penelitian ini terdiri dari tahapan yang dirancang secara sistematis untuk menjamin proses penelitian yang terstruktur dan ilmiah. Tahapan-tahapan tersebut adalah sebagai berikut:

Tabel 5. Tahapan Penelitian

Tahapan Penelitian	Penjelasan
Identifikasi Masalah	Mengidentifikasi kondisi aktual keamanan informasi PT XYZ

Studi Literatur	Peneliti mengkaji ISO/IEC 27001:2022, COBIT 2019 PCM, dan penelitian terdahulu
Pengumpulan Data	Data kuantitatif dikumpulkan terlebih dahulu melalui pengisian instrumen, kemudian ditindaklanjuti dengan pengumpulan data kualitatif melalui wawancara dan analisis dokumen untuk mendalami hasil kuantitatif
Analisis Data	Data kuantitatif dianalisis secara deskriptif menggunakan formula indeks untuk menghasilkan skor capability level per domain. Data kualitatif dianalisis secara tematik. Kedua analisis dilakukan terpisah sebelum digabungkan
Integrasi Hasil	Temuan kualitatif dari wawancara digunakan untuk menjelaskan dan memperdalam hasil kuantitatif. Inkonsistensi ditindaklanjuti dengan konfirmasi kepada responden
Penyusunan Rekomendasi	Menyusun rekomendasi yang diprioritaskan berdasarkan besaran gap dan kelayakan implementasi di PT XYZ

III. HASIL DAN PEMBAHASAN

A. Hasil Penilaian Tingkat Kematangan (Capability Level)

Penilaian tingkat kematangan dilakukan terhadap Klausul 4 sampai 10 dan 93 kontrol Annex A ISO/IEC 27001:2022. Setiap kontrol dinilai pada skala 0 sampai 5 berdasarkan bukti penerapan yang dapat diverifikasi, kemudian dihitung rata-ratanya per kontrol, per klausul, dan per domain Annex.

Indeks kapabilitas Klausul 4–10 dan indeks kapabilitas Annex A disajikan secara terpisah dan tidak digabungkan menjadi satu angka keseluruhan tunggal. Pemisahan ini dilakukan karena Klausul 4–10 mengukur persyaratan sistem manajemen, sedangkan Annex A mengukur implementasi kontrol keamanan. Keduanya memiliki karakteristik dan jumlah kontrol yang berbeda sehingga penggabungan langsung tidak dapat dijamin ekuivalen secara metodologis.

1) Indeks Kapabilitas Klausul 4–10

Perhitungan indeks kapabilitas Klausul 4–10 dilakukan dengan menjumlahkan rata-rata skor seluruh kontrol dalam setiap klausul, lalu membaginya dengan jumlah kontrol dalam klausul tersebut. Hasil per klausul kemudian disajikan secara individual tanpa dirata-ratakan menjadi satu angka tunggal klausul 4–10.

Tabel 6. Hasil Perhitungan Klausul 4–10

Klausul	Keterangan	Kontrol	Nilai	Level
4	*Context of the Organization*	4	1.00	1
5	*Leadership*	3	0.33	0
6	*Planning*	3	2.00	2
7	*Support*	5	1.60	2
8	*Operation*	4	1.00	1
9	*Performance Evaluation*	3	0.67	1
10	*Improvement*	2	1.50	1

Klausul 4 *Context of the Organization* mencapai Level 1 – *Performed* (4 kontrol). Klausul 5 *Leadership* mencapai Level 0 – *Incomplete* (3 kontrol), menjadi klausul dengan tingkat kematangan terendah karena seluruh kontrolnya belum diterapkan. Klausul 6 Planning mencapai Level 2 – *Managed* (3 kontrol). Klausul 7 *Support* juga mencapai Level 2 – *Managed* (5 kontrol). Klausul 8 *Operation* mencapai Level 1 – *Performed* (4 kontrol). Klausul 9 *Performance Evaluation* mencapai Level 1 – Performed (3 kontrol). Klausul 10 *Improvement* mencapai Level 1 – *Performed* (2 kontrol).

Secara lebih rinci, rendahnya nilai pada Klausul 5 Leadership disebabkan belum adanya kebijakan keamanan informasi tertulis yang disahkan, belum ditetapkannya peran penanggung jawab ISMS, dan belum adanya komunikasi formal mengenai tujuan keamanan informasi ke seluruh divisi. Klausul 9 Performance Evaluation yang berada pada Level 1 mencerminkan belum pernah dilaksanakannya audit internal ISMS maupun tinjauan manajemen. Sementara itu, Klausul 6 Planning dan Klausul 7 Support memperoleh nilai tertinggi karena perusahaan telah memiliki alokasi anggaran keamanan serta sumber daya teknis dasar, meskipun pelaksanaannya belum didukung dokumentasi formal.

2) Indeks Kapabilitas Annex A

Perhitungan indeks kapabilitas Annex A dilakukan per domain menggunakan rumus yang sama: rata-rata skor seluruh kontrol dalam domain tersebut.

Tabel 7. Hasil Perhitungan Domain Annex A

Domain	Keterangan	Kontrol	Nilai	Level
A.5	*Organizational Controls*	37	0.88	1
A.6	*People Controls*	8	3.15	3
A.7	*Physical Controls*	14	1.50	1
A.8	*Technological Controls*	34	1.18	1

e-ISSN: 2548-6861

Domain A.5 Organizational controls, A.7 Physical controls, dan A.8 Technological controls mencapai Level 1 (Performed). Domain A.6 People controls mencapai Level 3 (Established), menjadi satu-satunya domain yang memenuhi target.

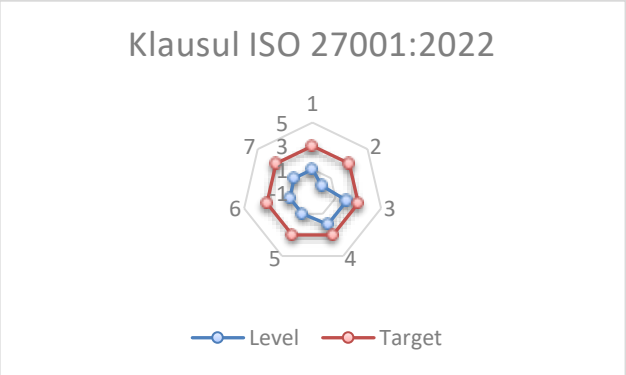
Domain A.6 People Controls memperoleh nilai tertinggi karena perusahaan telah menjalankan background check karyawan, mencantumkan klausul kerahasiaan dalam kontrak kerja, melaksanakan pelatihan kesadaran keamanan minimal satu kali per tahun, serta memiliki prosedur pencabutan akses saat karyawan berhenti. Sebaliknya, Domain A.5 Organizational Controls memperoleh nilai rendah karena sebagian besar kontrol tata kelola, seperti kebijakan, manajemen insiden, dan pengelolaan pemasok, belum terdokumentasi. Domain A.8 Technological Controls berada pada Level 1 karena kontrol teknis dasar seperti firewall dan backup telah berjalan tanpa SOP tertulis, sedangkan kontrol lanjutan seperti kriptografi, pengujian kerentanan, dan secure development lifecycle belum berjalan.

B. Analisis Kesenjangan

Analisis kesenjangan dilakukan dengan membandingkan level aktual setiap klausul dan domain terhadap target Level 3 – *Established*. Target ini ditetapkan berdasarkan definisi Level 3 dalam COBIT 2019 PCM, yaitu tingkat minimum di mana proses keamanan informasi dapat dikatakan terdefinisi dan dijalankan secara konsisten.

Tabel 8. Hasil Gap Analysis Klausul ISO 27001:2022

Klausul	Level	Target	Gap
4	1	3	2
5	0	3	3
6	2	3	1
7	2	3	1
8	1	3	2
9	1	3	2
10	1	3	2

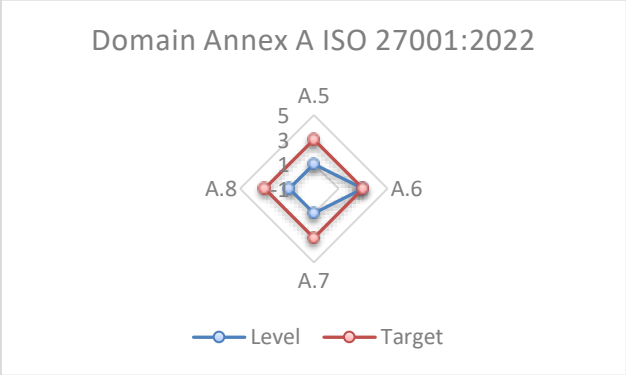


Gambar 2. Pemetaan Kesenjangan Tingkat Kapabilitas Klausul ISO 27001:2022.

Gap terbesar terdapat pada Klausul 5 *Leadership* (*gap* 3 level). Empat klausul, yaitu Klausul 4, 8, 9, dan 10, memiliki *gap* 2 level, sedangkan Klausul 6 *Planning* dan Klausul 7 *Support* memiliki *gap* terkecil, yaitu 1 level. Pola ini menunjukkan kelemahan sistemik pada dimensi tata kelola dan evaluasi ISMS, bukan pada pelaksanaan teknis semata; kedua klausul dengan *gap* terendah justru berkaitan langsung dengan ketersediaan sumber daya dan perencanaan dasar, bukan kebijakan formal tingkat strategis.

Tabel 9. Hasil Gap Analysis Domain ISO 27001:2022

Domain	Level	Target	*Gap*
A.5	1	3	2
A.6	3	3	0
A.7	1	3	2
A.8	1	3	2



Gambar 3. Pemetaan Kesenjangan Tingkat Kapabilitas Domain ISO 27001:2022.

Gap terbesar terdapat pada domain A.5 *Organizational controls*, A.7 *Physical controls*, dan A.8 *Technological controls*, masing-masing dengan gap 2 level. Domain A.6 *People controls* telah mencapai target dengan gap 0 level.

C. Pembahasan Temuan Kualitatif

Hasil wawancara mengonfirmasi bahwa kendala utama keamanan informasi di PT XYZ terletak pada aspek tata kelola, bukan semata kapasitas teknis. Hal ini tercermin pada skor terendah di Domain A.5 (*Organizational*, Level 1) dan Klausul 5 (*Leadership*, Level 0). Perusahaan belum memiliki kebijakan keamanan informasi formal yang disahkan manajemen, belum menunjuk penanggung jawab khusus (misalnya CISO), dan belum pernah melakukan audit internal ISMS atau tinjauan manajemen terkait keamanan informasi. Selain itu, meskipun pernah terjadi insiden keamanan informasi di masa lalu, belum ada prosedur formal untuk melaporkan dan

mendokumentasikan insiden tersebut. Saat ini, dukungan manajemen puncak baru sebatas alokasi anggaran untuk memenuhi permintaan kepatuhan dari klien, dan belum mencakup penetapan tujuan keamanan informasi secara formal yang dikomunikasikan ke seluruh divisi.

Pola serupa juga terlihat pada operasional teknis perusahaan. Pada Domain A.8 (*Technological*, Level 1), kontrol dasar seperti *antivirus*, *firewall*, dan *backup* sejatinya sudah berjalan, namun belum memiliki SOP resmi sehingga pelaksanaannya bergantung pada rutinitas personel tanpa landasan yang dapat diaudit. Pengujian kerentanan (*vulnerability assessment*) juga belum dilakukan secara mandiri, karena aktivitas tersebut sepenuhnya bergantung pada perusahaan pusat di luar negeri. Instalasi perangkat lunak pada sistem operasional saat ini hanya dapat dilakukan oleh tim IT, namun belum ada pemisahan formal antara lingkungan pengembangan, pengujian, dan produksi.

D. Rekomendasi

Berdasarkan peta kesenjangan dan temuan kualitatif, disusun rekomendasi perbaikan yang diprioritaskan menurut tingkat kekritisan gap dan kelayakan implementasinya di PT XYZ. Rekomendasi mengacu pada kontrol ISO/IEC 27001:2022 dan praktik terbaik dalam literatur. Ringkasan rekomendasi prioritas disajikan pada Tabel 9.

Tabel 10. Rekomendasi Perbaikan

Kontrol	Kondisi Aktual	Rekomendasi
Klausul 4.1, 4.2	Tujuan ISMS dan identifikasi pihak berkepentingan belum ditetapkan.	Analisis konteks organisasi, identifikasi pihak berkepentingan, dan dokumentasikan hasilnya sebagai dasar ruang lingkup ISMS.
Klausul 5.2, 5.3 Annex 5.4	Tidak ada kebijakan keamanan informasi tertulis, peran ISMS belum ditunjuk, dan belum ada komunikasi resmi ke karyawan.	Susun dan sahkan kebijakan keamanan informasi. Tunjuk penanggung jawab ISMS secara formal melalui SK. Komunikasikan kebijakan dan tanggung jawab keamanan informasi ke seluruh karyawan melalui saluran resmi.
Annex 5.7	Tidak ada pemantauan aktif terhadap perkembangan ancaman siber.	Langganan atau akses sumber intelijen ancaman yang relevan (CERT, vendor keamanan, komunitas industri). Tetapkan prosedur evaluasi ancaman secara berkala dan integrasikan hasilnya ke dalam proses manajemen risiko.
Annex 5.20, 5.21, 5.23	Tidak ada klausul keamanan dalam kontrak pemasok, tidak ada pengelolaan rantai pasok TIK, dan layanan *cloud* tidak dikelola secara formal.	Tambahkan klausul keamanan ke seluruh kontrak pemasok dan susun prosedur pengelolaan keamanan layanan *cloud*.
Annex 5.25, 5.26, 5.27, 5.28	Tidak ada prosedur respons, dokumentasi, pembelajaran, maupun pengumpulan bukti insiden. Insiden *malware* yang terjadi ditangani sepenuhnya *ad hoc.*	Susun prosedur manajemen insiden *end-to-end*. Tunjuk tim respons insiden dan lakukan simulasi berkala.
Annex 5.29	Tidak ada rencana keberlangsungan bisnis sama sekali.	Susun *Business Continuity Plan*, tetapkan RTO dan RPO untuk sistem kritikal, dan uji rencana secara berkala.
Annex 5.35	Pengelolaan keamanan informasi belum pernah ditinjau secara independen.	Jadwalkan tinjauan independen minimal satu kali per tahun dan dokumentasikan temuan serta tindak lanjutnya.
Annex 6.7	Tidak ada kebijakan yang mengatur perlindungan informasi saat bekerja di luar kantor.	Susun kebijakan remote working mencakup penggunaan perangkat, jaringan, dan penanganan data sensitif.
Annex 7.1	Tidak ada area aman yang terdefinisi secara formal.	Tetapkan dan dokumentasikan perimeter keamanan fisik berdasarkan tingkat sensitivitas aset.
Klausul 9.2, 9.3	Audit internal ISMS dan *management review* belum	Susun program audit internal ISMS tahunan dan jadwalkan *management review* berkala dengan

e-ISSN: 2548-6861

	pernah dilaksanakan.	dokumentasi keputusan tindak lanjut.
Annex 8.24, 8.25, 8.26	Tidak ada kebijakan kriptografi, *secure development lifecycle*, maupun persyaratan keamanan aplikasi.	Susun kebijakan kriptografi dan terapkan *secure development lifecycle* di seluruh tahap pengembangan sistem.
Annex 8.30	Pengembangan yang dialihdayakan tidak diawasi secara formal, tanpa klausul keamanan maupun *security testing*.	Tetapkan prosedur pengawasan vendor pengembangan termasuk klausul keamanan dalam kontrak dan security testing sebelum serah terima.
Annex 8.34	Sistem produksi tidak pernah diaudit keamanannya secara terencana.	Susun dan jadwalkan prosedur audit keamanan sistem produksi secara berkala dengan dokumentasi temuan dan tindak lanjut.

Implementasi rekomendasi tersebut diharapkan dapat meningkatkan tingkat kematangan PT XYZ menuju Level 3 (*Established*) atau lebih tinggi, sehingga proses keamanan informasi berjalan secara konsisten, terdokumentasi, dan dapat dievaluasi secara berkelanjutan.

Selain perbaikan pada kontrol yang masih rendah, Domain A.6 People Controls yang telah mencapai Level 3 (Established) juga memerlukan tindak lanjut agar dapat dipertahankan dan ditingkatkan menuju Level 4 (Predictable). Peningkatan ini dilakukan dengan menetapkan metrik kuantitatif untuk memantau efektivitas kontrol sumber daya manusia, misalnya persentase kehadiran pelatihan kesadaran keamanan, waktu rata-rata pencabutan hak akses saat karyawan berhenti, dan jumlah pelanggaran kebijakan yang tercatat. Metrik tersebut dievaluasi secara berkala sehingga variasi kinerja dapat dideteksi dan dikoreksi secara sistematis, sebagai dasar peningkatan berkelanjutan menuju Level 5 (Optimizing).

IV. KESIMPULAN

Penelitian ini mengevaluasi tingkat kematangan keamanan informasi PT XYZ berdasarkan ISO/IEC 27001:2022 dengan COBIT 2019 *Process Capability Model* melalui desain eksplanatori berurutan. Sesuai karakteristik keduanya, hasil penilaian disajikan terpisah antara Klausul 4 sampai 10 dan Annex A, tanpa digabung menjadi satu angka tunggal.

Pada Klausul 4 sampai 10, empat dari tujuh klausul berada pada Level 1 (*Performed*). Dua klausul, yaitu Klausul 6 *Planning* dan Klausul 7 *Support*, mencapai Level 2 (Managed) dan menjadi klausul tertinggi. Klausul 5 *Leadership* mencatat nilai terendah sebesar 0,33 dan berada pada Level 0 (Incomplete). Pada Annex A, domain A.6 *People Controls* mencapai Level 3 (*Established*) dengan indeks 3,15 dan menjadi satu-satunya domain pemenuh target. Tiga domain lain, yaitu A.5 *Organizational Controls*, A.7 *Physical Controls*, dan A.8 *Technological Controls*, berada pada Level 1 (*Performed*).

Analisis kesenjangan terhadap target Level 3 (*Established*) memperlihatkan gap terbesar pada Klausul 5 *Leadership* sebesar 3 level, sementara Klausul 6 dan Klausul 7 mencatat gap terkecil di antara klausul lain, yaitu 1 level. Pada domain Annex A, A.5, A.7, dan A.8 memiliki gap 2 level, sedangkan A.6 People Controls mencapai target dengan gap 0 level. Pola ini memperlihatkan kelemahan utama PT XYZ terletak pada dimensi tata kelola, bukan pelaksanaan teknis. Akar persoalannya mencakup ketiadaan kebijakan keamanan informasi formal, belum adanya audit internal, dan belum ditetapkannya peran ISMS oleh manajemen puncak.

Berdasarkan temuan tersebut, penelitian merekomendasikan tiga prioritas perbaikan. Pertama, penetapan kebijakan keamanan informasi formal dan penunjukan penanggung jawab ISMS pada level kepemimpinan. Kedua, perumusan prosedur tertulis untuk kontrol organisasional dan teknis berstatus ad hoc, termasuk penanganan insiden dan *business continuity*. Ketiga, pelaksanaan audit internal dan *management review* berkala untuk memastikan evaluasi efektivitas SMKI.

Penelitian ini terbatas pada lingkup internal PT XYZ di Batam dan tidak mencakup tahap implementasi maupun verifikasi sertifikasi. Penelitian lanjutan disarankan untuk menguji efektivitas rekomendasi setelah diterapkan melalui penilaian ulang dengan instrumen sama.

DAFTAR PUSTAKA

[1] "Cybercrime To Cost The World 8 Trillion Annually In 2023." Accessed: Dec. 05, 2025. [Online]. Available: https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

[2] "Making cyber resilience a top priority for manufacturers | World Economic Forum." Accessed: Dec. 09, 2025. [Online]. Available: https://www.weforum.org/stories/2024/06/manufacturers-face-cyber-threats-cyber-resilience-culture/

[3] E. Riana, M. Sulistyawati, and O. Putra, "Analisis Tingkat Kematangan (Maturity Level) Dan PDCA (Plan-Do-Check-Act) Dalam Penerapan Audit Sistem Manajemen Keamanan Informasi Pada PT Indonesia Game Menggunakan Metode ISO 27001:2013," *Journal of Information System Research (JOSH)*, vol. 4, pp. 632–640, Jan. 2023, doi: 10.47065/josh.v4i2.2552.

[4] A. Pratama, D. Yulisda, and M. Fajar, "Analisis Tingkat Kemampuan (Capability Level) Teknologi Informasi Menggunakan Framework Cobit 2019 Domain Dss (Deliver, Service, And Support) Studi Kasus Diskominfo Kota Pematang Siantar," *Jurnal TIKA*, vol. 8, pp. 10–16, Apr. 2023, doi: 10.51179/tika.v8i1.1781.

[5] Y. Widasari and N. Oktadini, "Capability Level Assessment of IT Governance in the SIAP KOJA Application Using the COBIT 2019 Framework," *Journal of Applied Informatics and Computing*, vol. 9, pp. 3706–3715, Dec. 2025, doi: 10.30871/jaic.v9i6.11433.

[6] Z. Artamevia and A. Triayudi, "EVALUATION OF MATURITY LEVEL INFORMATION SECURITY USING COBIT 2019 AND ISO/IEC 27001:2022," *JIKO (Jurnal Informatika dan Komputer)*, vol. 8, pp. 181–187, Nov. 2025, doi: 10.33387/jiko.v8i3.10704.

[7] John W. Creswell and Vicki L. Plano Clark, "Designing and Conducting Mixed Methods Research," 2017.

[8] Immanuel Candra Irawan and Meidyna Renaningdyah Pelenkahu, "Evaluasi Penggunaan Sistem Informasi Akademik Berbasis Web [eCampuz]: Pendekatan Mixed Methods terhadap Kepuasan Pengguna," *Jurnal Teknologi dan Informatika*, vol. 3, no. 1, pp. 82–92, Aug. 2025, doi: 10.70539/jti.v3i1.53.

[9] R. Sinaga and F. Taan, "Penerapan ISO/IEC 27001:2022 dalam Tata Kelola Keamanan Sistem Informasi: Evaluasi Proses dan Kendala," *NUANSA INFORMATIKA*, vol. 18, no. 2, pp. 46–54, Jul. 2024, doi: 10.25134/ilkom.v18i2.205.

[10] V. Monev, "Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002," in *2020 International Conference on Information Technologies (InfoTech)*, Sep. 2020, pp. 1–5. doi: 10.1109/InfoTech49733.2020.9211066.

[11] T. Shimels and L. Lessa, "Maturity of information systems' security in Ethiopian banks: case of selected private banks," *International Journal of Industrial Engineering and Operations Management*, vol. 5, no. 2, pp. 86–103, Jan. 2023, doi: 10.1108/IJIEOM-10-2021-0014.

[12] S. Samsinar and R. Sinaga, "Information Technology Governance Audit at XYZ College Using COBIT Framework 2019," *BERKALA SAINSTEK*, vol. 10, p. 58, Jun. 2022, doi: 10.19184/bst.v10i2.30325.

[13] R. Almeida, R. Lourinho, M. da Silva, and R. Pereira, " A Model for Assessing COBIT 5 and ISO 27001 Simultaneously ," in *2018 IEEE 20th Conference on Business Informatics (CBI)* , Los Alamitos, CA, USA: IEEE Computer Society, Jul. 2018, pp. 60–69. doi: 10.1109/CBI.2018.00016.

[14] E. Aflakhah and B. Soewito, "Assessing Information Security Using COBIT 2019 and ISO 27001:2013 for Developing a Mitigation Plan," *International Journal of Engineering Trends and Technology*, vol. 71, pp. 223–237, Oct. 2023, doi: 10.14445/22315381/IJETT-V71I10P221.

[15] A. Nugroho and H. Ginardi, "Information Technology Governance Analysis to Reduce Information Security Risks Using Cobit 2019: A Case Study of Manufacturing Companies," *Jurnal Indonesia Sosial Teknologi*, vol. 5, no. 8, p. 3722, 2024, doi: https://doi.org/10.59141/jist.v5i8.1198.

e-ISSN: 2548-6861

Lampiran

https://drive.google.com/file/d/1Lt0xaPKgI5bP20eMDlERxEW0GS6LRWr1/view?usp=sharing