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

Analisis Tingkat Kematangan dan Penerapan Model PDCA ISO/IEC 27001 dalam Penguatan Tata Kelola Keamanan Informasi di PT. XYZ

Naya Amanda Pradisia [1]*, Festy Winda Sari [2]**,**
* Teknik Informatika, Politeknik Negeri Batam
** Rekayasa Keamanan Siber, Politeknik Negeri Batam
Naya.4332201045@students.polibatam.ac.id [1], festy@polibatam.ac.id [2]

Article Info

Article history:

Received …
Revised …
Accepted …

Keyword:

ISO/IEC 27001:2022, COBIT 2019, ISMS, PDCA.

ABSTRACT

Perkembangan teknologi informasi mendorong perusahaan untuk memperkuat tata kelola keamanan informasi melalui penerapan Information Security Management System (ISMS). PT. XYZ telah menerapkan ISO/IEC 27001:2022, namun evaluasi penerapan siklus Plan-Do-Check-Act (PDCA) belum dilakukan secara terukur. Penelitian ini bertujuan untuk menganalisis tingkat kematangan penerapan PDCA pada tata kelola keamanan informasi di PT. XYZ menggunakan Process Capability Model COBIT 2019. Metode penelitian yang digunakan adalah mixed-method dengan pengumpulan data melalui kuesioner, wawancara, dan dokumentasi. Hasil penelitian menunjukkan tingkat kematangan sebesar 88,75% atau berada pada Level 4 (Quantitative). Hasil tersebut menunjukkan bahwa penerapan ISMS telah berjalan dengan baik dan konsisten, meskipun masih terdapat beberapa kekurangan pada aspek awareness, monitoring, dokumentasi evaluasi, dan *corrective action*. Oleh karena itu, diperlukan peningkatan evaluasi dan perbaikan berkelanjutan untuk mencapai kondisi optimal.

I. PENDAHULUAN

Perkembangan teknologi informasi yang sangat pesat menuntut organisasi untuk memperkuat sistem pengelolaan keamanan informasinya. Informasi kini menjadi salah satu aset utama yang bernilai strategis, sehingga perlindungan terhadap risiko kebocoran, penyalahgunaan, atau kehilangan data menjadi krusial [1]. Merujuk pada standar internasional ISO/IEC 27001:2022, organisasi disarankan untuk mengadopsi kerangka kerja yang sistematis melalui *Information Security Management System* (ISMS) guna menjaga aspek kerahasiaan, integritas, dan ketersediaan informasi [2]. Dalam operasionalnya, standar ini menggunakan pendekatan siklus *Plan-Do-Check-Act* (PDCA) sebagai fondasi untuk memastikan adanya perbaikan berkelanjutan [3].

Namun, dalam praktiknya di lapangan, penerapan PDCA sering kali tidak berjalan seimbang. Banyak organisasi yang cenderung berfokus pada eksekusi implementasi teknis (*Do*), tetapi luput melakukan evaluasi obyektif (*Check*) dan tindakan perbaikan (*Act*) [4]. Kegagalan dalam mengukur kematangan siklus PDCA secara obyektif ini menyebabkan investasi keamanan informasi menjadi tidak efisien. Tanpa adanya metrik yang jelas, perusahaan akan kesulitan membedakan antara proses yang sudah berjalan optimal dan proses yang sekadar memenuhi syarat administratif (*paper-based compliance*). Ketiadaan evaluasi pada fase pengawasan dan perbaikan ini akan menghasilkan laporan *Management Review* yang reaktif. Oleh karena itu, pengukuran tingkat kematangan PDCA menjadi sangat mendesak untuk dilakukan guna mengubah data evaluasi kualitatif menjadi matriks kuantitatif yang *actionable*, sehingga jajaran manajemen dapat menetapkan skala prioritas perbaikan secara tepat sasaran.

Kondisi tersebut selaras dengan permasalahan di PT. XYZ, sebuah perusahaan manufaktur elektronik di Indonesia yang telah menerapkan ISMS. Berdasarkan observasi awal, mekanisme *management review* di perusahaan ini belum sepenuhnya didukung oleh analisis mendalam terhadap tingkat kematangan penerapan PDCA. Mengingat pentingnya tata kelola yang terstruktur, batasan penelitian ini difokuskan secara spesifik pada evaluasi tata kelola (*governance*)

e-ISSN: 2548-6861

keamanan informasi yang diatur dalam Klausa 6 hingga 10 ISO/IEC 27001:2022 [2]. Penelitian ini tidak mencakup pengujian audit teknis operasional spesifik yang terdapat pada daftar kontrol Annex A, karena Klausa 6-10 merupakan fondasi tata kelola manajerial yang mendasari pemilihan dan implementasi kontrol teknis tersebut. Untuk mengukur tata kelola ini, penelitian menggunakan pendekatan *Process Capability Model* (PCM) dari COBIT 2019 yang mampu memberikan skala penilaian numerik terukur [5]. Penggunaan COBIT 2019 dan ISO/IEC 27001 sebagai pendekatan evaluasi keamanan informasi juga telah diterapkan pada penelitian sebelumnya [11] menggunakan COBIT 2019 dan ISO/IEC 27001:2022 untuk mengevaluasi tingkat kematangan keamanan informasi, sedangkan Aflakhah dan Soewito [12] menggunakan kedua framework tersebut untuk penilaian keamanan informasi dan penyusunan rencana mitigasi. Oleh karena itu, penelitian ini menggunakan ISO/IEC 27001:2022 sebagai objek evaluasi dan COBIT 2019 PCM sebagai model pengukuran tingkat kematangan proses.

Penelitian ini memiliki tiga tujuan utama. Pertama, menganalisis tingkat kematangan penerapan siklus PDCA ISO/IEC 27001 pada ISMS di PT. XYZ. Kedua, mengidentifikasi faktor-faktor yang memengaruhi keberhasilan dan hambatan dalam penerapan PDCA. Ketiga, menyusun kerangka rekomendasi perbaikan berbasis analisis kesenjangan yang dapat diterjemahkan menjadi mekanisme input *actionable* untuk memperkuat proses *Management Review* di PT. XYZ.

II. METODE

A. Jenis, Sifat, dan Pendekatan Penelitian

Jenis penelitian yang digunakan adalah metode campuran (*mixed-method*). Penelitian ini menggunakan pendekatan kuantitatif yang berfokus proses pengukuran terhadap tingkat kematangan keamanan informasi, serta pendekatan kualitatif yang didasarkan pada analisis kejadian alamiah di lingkungan perusahaan [7]. Dalam pelaksanaannya, penelitian ini menggunakan *framework* (kerangka kerja) COBIT 2019 sebagai standar acuan pengukuran kematangan dan ISO/IEC 27001:2022 sebagai standar acuan tata kelola keamanan informasi yang dievaluasi. Integrasi data dilakukan melalui teknik triangulasi, dimana hasil pengukuran kuantitatif (*maturity level*) digunakan untuk mengidentifikasi area kritikal, kemudian dianalisis lebih lanjut dengan data kualitatif dari wawancara untuk menemukan akar permasalahan.

B. Subjek dan Teknik Pengumpulan Data

Pada penelitian ini, peneliti menggunakan beberapa metode pengumpulan data untuk memperoleh informasi yang akurat, yaitu:

1. Data Primer
   Merupakan data yang diperoleh secara langsung dari sumber pertama di lokasi penelitian melalui:
   a. Kuesioner
      Diberikan kepada responden kunci (*key informants*) yang telah dipilih dari populasi di PT. XYZ menggunakan teknik *purposive sampling*. Responden dipilih dengan kriteria: (1) terlibat langsung dalam implementasi ISMS, (2) memiliki pemahaman terhadap kebijakan keamanan informasi, dan (3) memiliki pengalaman kerja minimal 1 tahun. Sebanyak 11 responden dipilih karena memiliki peran dan tanggung jawab yang berkaitan langsung dengan pengelolaan keamanan informasi di PT. XYZ, sehingga mampu memberikan informasi yang relevan terhadap proses yang dievaluasi dalam penelitian ini. Penelitian ini tidak bertujuan melakukan generalisasi statistik terhadap seluruh populasi perusahaan, melainkan mengevaluasi implementasi ISMS berdasarkan perspektif pihak-pihak yang terlibat langsung dalam pengelolaan dan pelaksanaan tata kelola keamanan informasi. Kuesioner ini berisi pernyataan-pernyataan yang disusun berdasarkan indikator tata kelola pada Klausa 6 hingga 10 ISO/IEC 27001:2022 yang dipetakan ke dalam siklus PDCA.
   b. Wawancara
      Dilakukan secara mendalam dengan responden kunci untuk mengidentifikasi faktor penghambat dan akar permasalahan (*root cause*) dari kesenjangan keamanan yang ditemukan pada hasil kuesioner.

2. Data Sekunder
   Merupakan data pendukung yang digunakan untuk memperkuat analisis dan validasi, meliputi:
   a. Studi Pustaka
      Peneliti mencari dan menelaah sumber pustaka yang relevan, baik berupa buku metodologi maupun jurnal penelitian terdahulu mengenai audit keamanan informasi dan standar ISO/IEC 27001.
   b. Dokumentasi
      Peneliti membaca dokumen internal yang relevan di PT. XYZ, seperti kebijakan keamanan informasi, laporan hasil audit internal, serta bukti pendukung lainnya yang berkaitan dengan persiapan dan pelaksanaan *Management Review*.

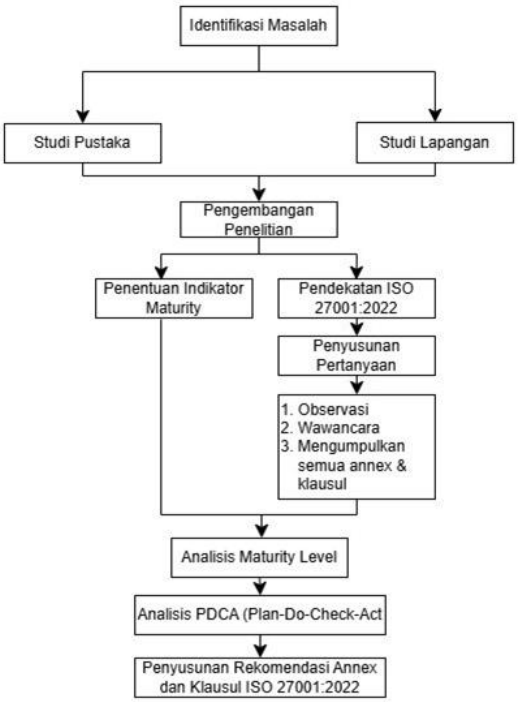
C. Metode Analisis Data

Data kuesioner menggunakan skala likert (1-5) yang disusun berdasarkan indikator pada Klausa 6 hingga 10 ISO/IEC 27001:2022 dan telah melalui proses review oleh dosen pembimbing ntuk memastikan kesesuaian instrumen dengan tujuan penelitian. Selanjutnya, data dianalisis menggunakan perhitungan *Index Maturity* dengan rumus:

$$Indeks\ Kematangan = \frac{Total\ Skor\ Aktual}{Total\ Skor\ Maksimal} x\ 100$$

Hasil persentase tersebut dipetakan ke dalam *Capability Level* COBIT 2019 (0-5) [5]. Tingkat kematangan aktual (*As-Is*) kemudian dibandingkan dengan target perusahaan (*To-Be*) untuk menghasilkan *Gap Analysis*. Penentuan tingkat kematangan yang diharapkan (To-Be) dilakukan melalui validasi dengan pihak yang bertanggung jawab terhadap implementasi ISMS di PT. XYZ. Berdasarkan hasil validasi tersebut, perusahaan menetapkan target tingkat kematangan pada Level 5 (Optimizing) sebagai kondisi ideal yang ingin dicapai pada seluruh klausa yang dievaluasi. Kesenjangan (*gap*) tersebut selanjutnya dianalisis mendalam menggunakan metode kualitatif *Root Cause Analysis* (RCA) berdasarkan hasil wawancara dan bukti dokumen guna mengidentifikasi akar permasalahan dan memberikan rekomendasi perbaikan bagi *Management Review.*

D. Alur Penelitian



Penelitian ini dilaksanakan melalui tahapan yang sistematis untuk memastikan seluruh tujuan penelitian tercapai dengan baik. Alur tahapan penelitian (sebagaimana diilustrasikan pada Gambar 1) dijabarkan sebagai berikut:

Tabel 1. Deskripsi Alur Penelitian

Tahapan Penelitian	Penjelasan
Identifikasi Masalah	Merupakan tahap awal untuk merumuskan urgensi penelitian terkait belum optimalnya evaluasi siklus PDCA pada tata kelola keamanan informasi di PT. XYZ.
Studi Pustaka dan Studi Lapangan	Dilakukan secara paralel. Studi pustaka dilakukan untuk menghimpun landasan teori terkait ISO/IEC 27001:2022 dan model kematangan COBIT, sedangkan studi lapangan dilakukan untuk observasi awal kondisi aktual di perusahaan.
Pengembangan Penelitian	Mengembangkan rancangan penelitian berdasarkan hasil studi pendahuluan untuk menetapkan metode pengukuran yang paling tepat.
Penentuan Indikator dan Pendekatan ISO 27001:2022	Tahap ini berjalan paralel, di mana indikator kematangan (*maturity level*) ditentukan berdasarkan batasan persyaratan sistem manajemen pada Klausa 6 hingga 10 ISO/IEC 27001:2022.
Penyusunan Pertanyaan dan Pengumpulan Data	Berdasarkan indikator tersebut, disusun kuesioner dan panduan wawancara. Pengumpulan data lapangan dilakukan melalui tiga teknik utama: observasi, wawancara mendalam dengan responden kunci, serta pengumpulan bukti-bukti dokumen penerapan klausa.
Analisis *Maturity Level*	Mengolah data kuantitatif dari kuesioner untuk mendapatkan persentase tingkat kematangan aktual (*As-Is*) dan mengidentifikasi kesenjangannya (*Gap Analysis*) terhadap kondisi ideal (*To-Be*).
Analisis PDCA (*Plan-Do-Check-Act*)	Menyelaraskan hasil kematangan numerik dengan temuan wawancara untuk mengevaluasi fase mana dalam siklus PDCA yang paling lemah dan menemukan akar masalahnya (*Root Cause Analysis*).
Penyusunan Rekomendasi	Merumuskan tindakan korektif dan matriks rekomendasi perbaikan tata kelola yang bersifat *actionable* untuk digunakan sebagai input dalam

e-ISSN: 2548-6861

	pelaksanaan *Management Review*.

E. Identifikasi Proses Tata Kelola Keamanan Informasi

Tahap ini mengidentifikasi dan memetakan proses tata kelola keamanan informasi di PT. XYZ berdasarkan prinsip peningkatan berkelanjutan. Pemetaan dilakukan dengan menyelaraskan siklus *Plan-Do-Check-Act* (PDCA) terhadap klausa tata kelola ISO/IEC 27001:2022 seperti pada Tabel 2.

Tabel 2. Pemetaan PDCA pada ISO 2700:2022

Domain PDCA	**Klausa ISO/IEC 27001:2022**
PLAN (Perencanaan)	Klausa 6: *Planning*
DO (Pelaksanaan)	Klausa 7: *Support*
CHECK (Evaluasi)	Klausa 8: *Operations* Klausa 9: *Performance Evaluation*
ACT (Peningkatan)	Klausa 10: *Improvement*

Klausa 6: *Planning*	
6.1	*Actions to Address Risks and Opportunities*
6.2	*Information Security Objectives and Planning*
6.3	*Planning of Changes*
Klausa 7: *Do*	
7.1	*Resources*
7.2	*Competence*
7.3	*Awareness*
7.4	*Communication*
7.5	*Documented Infromation*
Klausa 8: *Operations*	
8.1	*Operational Planning and Control*
8.2	*Information Security Risk Assesments*
8.3	*Information Seurity Risk Trreatment*
Klausa 9: *Performance Evaluations*	
9.1	*Monitoring, Meaurement, Analysis, and Evaluation*
9.2	*Internal Audit*
9.3	*Management Review*
Klausa 10: *Improvement*	
10.1	*Continual Improvement*
10.2	*Nonconformity and Corrective Action*

III. HASIL DAN PEMBAHASAN

Pada bab ini dijelaskan hasil pengukuran tingkat kematangan tata kelola keamanan informasi di PT. XYZ berdasarkan ISO/IEC 27001:2022. Hasil penelitian diperoleh dari data kuesioner yang diisi oleh responden yang terlibat dalam implementasi ISMS. Setelah nilai tingkat kematangan diperoleh, dilakukan validasi melalui wawancara terhadap aspek yang memiliki nilai paling rendah untuk mengetahui kondisi implementasi dan penyebab kesenjangan yang terjadi.

A. Analisis Pernyataan Kuesioner

Pada tahap ini dilakukan analisis terhadap setiap pernyataan kuesioner yang telah disusun berdasarkan subdomain ISO/IEC 27001:2022, yang mencakup fase Plan-Do-Check-Act (PDCA) pada Klausa 6 hingga Klausa 10 dengan kriteria responden yang terlibat dalam ISMS.

B. Analisis Responden

Analisis responden dilakukan untuk mengetahui karakteristik responden yang terlibat dalam penelitian. Responden merupakan pihak yang terlibat dalam implementasi ISMS di PT. XYZ dan memiliki pemahaman terhadap tata kelola keamanan informasi berdasarkan ISO/IEC 27001:2022.

Tabel 3. Data Responden Penelitian

No	**Peran dalam ISMS**	**Jabatan**	**Jumlah**
1	*ISMS Manager*	*Head of IT Security*	1
2	*Engineer System 2*	*Head of IT Infrastructure Lead*	1
3	*IT Analyst*	*IT Security GRC & Planning Lead*	1
4	*Asst. Engineer 2*	*IT Security GRC & Planning Analyst*	1
5	*IT Analyst*	*IT Security Application & SOC Lead*	1
6	*Asst. Engineer 2*	*IT Security Application & SOC Analyst*	1
7	*Asst. Engineer 2*	*IT Developer Operations*	1
8	*Senior Sytem Engineer*	*System Administrator*	1
9	*Asst. Engineer 2*	*IT Helpdesk*	3
Jumlah responden			11

C. Perhitungan Tingkat Kematangan

Berdasarkan data kuesioner yang telah dikumpulkan dari kuesioner, data tersebut diolah dengan hasil nilai rata-rata berdasarkan jawaban dari semua responden, dan penilaian tingkat model capability process. Kuesioner menggunakan skala likert yang mana responden akan menjawab pertanyaan dengan urutan angka yang berisi definisi.

Tabel 4. Nilai Indeks Skala Likert pada Kuesioner

Nilai	Keterangan
1	Sangat Tidak Setuju
2	Tidak Setuju
3	Cukup
4	Setuju
5	Sangat Setuju

Tabel 5. Level Capability Model

Level	Skala Index Maturity	Keterangan
0	0%-18%	*Non Existent*
1	19% - 36%	*Initial*
2	37% - 54%	*Managed*
3	56% - 72%	*Defined*
4	73% - 90%	*Quantitative*
5	91% - 100%	*Optimizing*

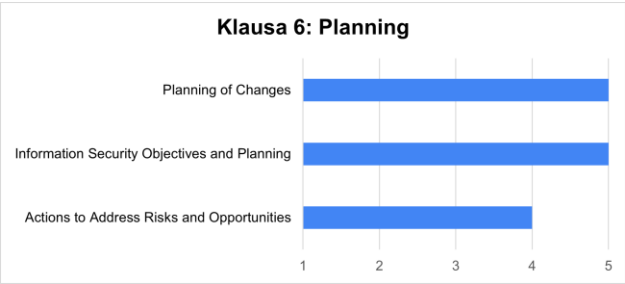
D. Perhitungan Tingkat Kematangan

Detail nilai tingkat kematangan tiap sub klausa ISO 27001:2022 dari hasil kuesioner dapat dijelaskan sebagai berikut:

Tabel 6. Hasil Perhitungan Kuesioner Klausa 6

Klausa 6: *Planning*	Keterangan	Nilai
6.1	*Actions to Address Risks and Opportunities*	*4*
6.2	*Information Security Objectives and Planning*	*5*
6.3	*Planning of Changes*	*5*

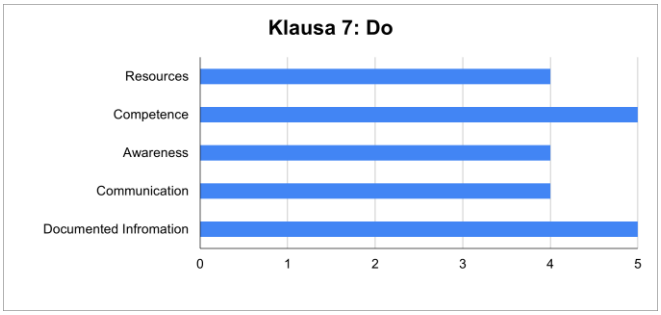
Gambar 2. Hasil Perhitungan Kuesioner Klausa 6 dalam Grafik



Tabel 7. Hasil Perhitungan Kuesioner Klausa 7

Klausa 7: *Do*	Keterangan	Nilai
7.1	*Resources*	4
7.2	*Competence*	5
7.3	*Awareness*	4
7.4	*Communication*	4
7.5	*Documented Infromation*	*5*

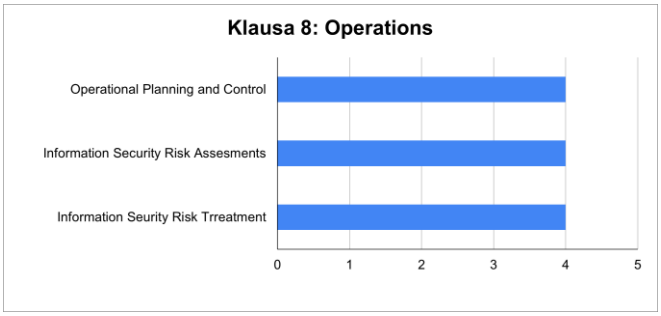
Gambar 3. Hasil Perhitungan Kuesioner Klausa 7 dalam Grafik



Tabel 8. Hasil Perhitungan Kuesioner Klausa 8

Klausa 8: *Operations*	Keterangan	Nilai
8.1	*Operational Planning and Control*	4
8.2	*Information Security Risk Assesments*	4
8.3	*Information Seurity Risk Trreatment*	4

Gambar 4. Hasil Perhitungan Kuesioner Klausa 8 dalam Grafik

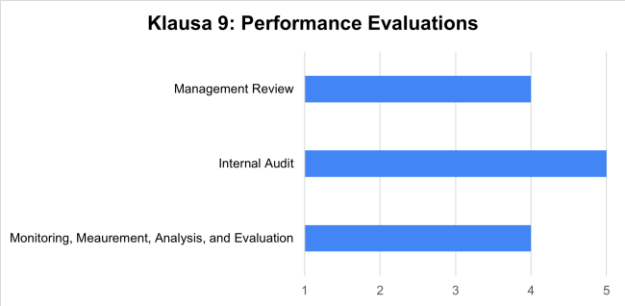


Tabel 9. Hasil Perhitungan Kuesioner Klausa 9

Klausa 9: *Performance Evaluations*	Keterangan	Nilai
9.1	*Monitoring, Meaurement, Analysis, and Evaluation*	4
9.2	*Internal Audit*	5
9.3	*Management Review*	4

e-ISSN: 2548-6861

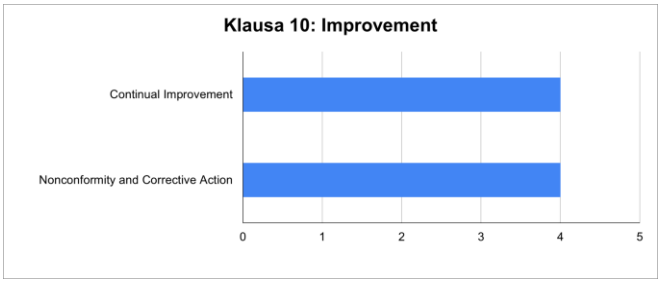
Gambar 5. Hasil Perhitungan Kuesioner Klausa 9 dalam Grafik



Tabel 10. Hasil Perhitungan Kuesioner Klausa 10

Klausa 10: *Improvements*	**Keterangan**	**Nilai**
10.1	*Continual Improvement*	4
10.2	*Nonconformity and Corrective Action*	4

Gambar 6. Hasil Perhitungan Kuesioner Klausa 10 dalam Grafik



E. Nilai keseluruhan domain ISO 27001:2022

Nilai tingkat kematangan secara keseluruhan dipeoleh dengan menjumlahkan seluruh skor dari responden, kemudian dibandingkan dengan total skor maksimal untuk menghasilkan nilai dalam bentuk persentase.

$$Indeks\ Kematangan = \frac{Total\ Skor\ Aktual}{Total\ Skor\ Maksimal} x\ 100$$

$$= \frac{781}{880} x\ 100\ = 88.75\%$$

Berdasarkan hasil perhitungan tersebut, diperoleh nilai tingkat kematangan keseluruhan sebesar 88,75% yang berada pada Level 4 (*Quantitative*). Hasil ini menunjukkan bahwa penerapan tata kelola keamanan informasi berdasarkan ISO/IEC 27001:2022 di PT. XYZ telah berjalan dengan baik, dan dikelola secara konsisten, meskipun masih terdapat peluang peningkatan menuju kondisi yang lebih optimal.

Tabel 11. Nilai Keseluruhan Klausa

Klausa	**Keterangan**	**Nilai**
Klausa 6	*Planning*	4.6
Klausa 7	*Do*	4.4
Klausa 8	*Operations*	4
Klausa 9	*Performance Evaluations*	4.3
Klausa 10	*Improvement*	4

F. Kesenjangan Hasil Tingkat Kematangan

Gambar 7. Perbandingan Nilai Kematangan pada Domain PDCA Saat Ini Dengan Nilai Kematangan Yang Diharapkan

Tabel 12. Kesenjangan Tata Kelola Teknologi Informasi pada PT. XYZ Berdasarkan Domain PDCA

Domain	***As-Is***	***To-Be***	***Gap***
ISO/IEC 27001:2022 Klausa 6-10	4	5	1

Kesenjangan yang dapat dilihat dari data tersebut menunjukkan bahwa tingkat kematangan penerapan tata kelola keamanan informasi di PT. XYZ saat ini telah berada pada level 4 (*Quantitative*), namun masih terdapat gap sebesar 1 level dibandingkan kondisi yang diharapkan yaitu level 5 (*Optimizing*).

Tabel 13. Hasil Kesenjangan Tingkat Kematangan Per Klausa

Klausa	***As-Is***	***To-Be***	***Gap***
Klausa 6	4.6	5	0.4
Klausa 7	4.4	5	0.6

Klausa 8	4	5	1
Klausa 9	4.3	5	0.7
Klausa 10	4	5	1

G. Analisis Root Cause Analyis (RCA)

Berdasarkan *hasil gap analysis*, dilakukan *Root Cause Analysis (*RCA) untuk mengidentifikasi akar penyebab dari kesenjangan yang masih ditemukan pada penerapan ISMS di PT. XYZ. Analisis dilakukan berdasarkan hasil wawancara dan telaah dokumen terhadap setiap klausa yang dievaluasi. Hasil RCA tersebut disajikan pada Tabel 14 dan digunakan sebagai dasar dalam penyusunan rekomendasi perbaikan.

Tabel 14. Hasil *Root Cause Analysis*

Klausa	***Root Cause***
Klausa 6	Belum terdapat mekanisme formal *risk assessment* dan *change management* yang terdokumentasi dalam proses perubahan sistem maupun tools keamanan informasi.
Klausa 7	Keterbatasan sumber daya dan media sosialisasi menyebabkan pelaksanaan awareness keamanan informasi belum dilakukan secara rutin dan merata kepada seluruh pengguna.
Klausa 8	Proses monitoring keamanan endpoint masih dilakukan secara manual, bergantung pada koordinasi dengan pihak produksi, serta jumlah personel yang terbatas.
Klausa 9	Belum terdapat jadwal review dan dokumentasi hasil monitoring yang konsisten sehingga proses evaluasi belum berjalan optimal.
Klausa 10	Evaluasi pasca-insiden dan *corrective action* belum terdokumentasi secara formal sebagai bagian dari proses *continual improvement.*

Dapat dilihat hasil RCA pada Tabel 14, akar permasalahan yang paling dominan ditemukan pada Klausa 8 (Operation) dan Klausa 10 (Improvement), yang juga merupakan klausa dengan nilai gap tertinggi sebesar 1.

H. Prioritas Rekomendasi Perbaikan

Berdasarkan hasil gap analysis, prioritas rekomendasi perbaikan ditentukan berdasarkan nilai kesenjangan antara kondisi aktual (*As-Is*) dan kondisi yang diharapkan (*To-Be*). Semakin besar nilai gap yang diperoleh, maka semakin tinggi kebutuhan peningkatan pada klausul tersebut. Hasil analisis menunjukkan bahwa Klausul 8 (*Operation*) dan Klausul 10 (*Improvement*) memiliki nilai gap terbesar sebesar 1 sehingga menjadi prioritas utama perbaikan. Temuan ini juga diperoleh dari hasil wawancara yang menunjukkan masih terdapat kendala pada proses monitoring keamanan informasi, *risk treatment, corrective action*, dan *continual improvement.*

IV. KESIMPULAN

Hasil analisis dari 10 sub klausa dapat disusun dalam bentuk tabel mengenai temuan masalah dan rekomendasinya seperti pada tabel berikut.

Tabel 15. Temuan Masalah dan Rekomendasi Klausa 6

Klausa 6: *Planning*		
No	**Temuan Masalah**	**Rekomendasi**
1	Perubahan penggunaan *tools* keamanan informasi belum selalu disertai dengan analisis risiko dan peluang secara terdokumentasi sebelum implementasi dilakukan	Melakukan pembahasan mengenai risiko yang dapat terjadi dengan penggunaan *tools* keamanan baru, supaya tidak terjadi insiden berulang.
2	Perubahan alur monitoring keamanan informasi belum selalu disertai dengan evaluasi dan perencanaan perubahan secara terdokumentasi.	Melakukan dokumentasi dan evaluasi ketika akan melakukan perubahan terhadap alur monitoring keamanan.

Tabel 16. Temuan Masalah dan Rekomendasi Klausa 7

Klausa 7: *Do*		
No	**Temuan Masalah**	**Rekomendasi**
1	*Awareness* keamanan informasi belum tersampaikan secara merata kepada seluruh pengguna di lingkungan perusahaan.	Mengembangkan LMS (Learning Management System) sebagai media awareness mandiri bagi karyawan.
2	Penyampaian kebijakan keamanan informasi belum tersosialisasi secara merata.	Menambahkan media awareness fisik seperti poster keamanan informasi pada setiap area kerja.

Tabel 17. Temuan Masalah dan Rekomendasi Klausa 8

Klausa 8: *Operations*		
No	**Temuan Masalah**	**Rekomendasi**
1	Monitoring keamanan endpoint belum dilakukan secara konsisten sesuai jadwal	Menyusun SOP dan jadwal inspeksi yang disepakati

e-ISSN: 2548-6861

	yang telah ditetapkan, yaitu sebanyak 2x dalam satu bulan.	bersama pihak produksi.
2	Tindak lanjut terhadap hasil monitoring keamanan *endpoint* belum memiliki mekanisme eskalasi dan penanganan yang terstruktur	Menyusun mekanisme eskalasi dan tindak lanjut hasil monitoring keamanan *endpoint* secara jelas

Tabel 18 Temuan Masalah dan Rekomendasi Klausa 9

Klausa 9: *Performance Evaluations*		
No	**Temuan Masalah**	**Rekomendasi**
1	Dokumentasi dan rekapitulasi hasil monitoring insiden keamanan informasi belum dilakukan secara rutin dan konsisten tiap minggu.	Menyusun jadwal weekly review terhadap hasil monitoring SIEM
2	Tindak lanjut terhadap hasil audit dan monitoring keamanan informasi masih memerlukan evaluasi berkala.	Melakukan evaluasi berkala terhadap true positive dan false positive alert

Tabel 19. Temuan Masalah dan Rekomendasi Klausa 10

Klausa 10: *Improvement*		
No	**Temuan Masalah**	**Rekomendasi**
1	Tindakan corrective action terhadap insiden malware belum memiliki prosedur eskalasi dan evaluasi lanjutan yang terdokumentasi.	Melakukan *post-incident review* setelah insiden keamanan terjadi
2	Perubahan atau perbaikan proses keamanan informasi belum seluruhnya disertai evaluasi lanjutan untuk mencegah terulangnya permasalahan yang sama	Melakukan evaluasi lanjutan setelah penerapan tindakan perbaikan keamanan informasi
3	Dokumentasi tindakan perbaikan (*corrective action*) terhadap insiden keamanan informasi belum dilakukan secara konsisten	Meningkatkan dokumentasi *corrective action* pada setiap insiden keamanan informasi

Berdasarkan hasil penelitian yang telah dilakukan terhadap penerapan tata kelola keamanan informasi berdasarkan ISO/IEC 27001:2022 pada PT. XYZ, maka dapat disimpulkan sebagai berikut:

1. Berdasarkan hasil analisis tingkat kematangan pada domain ISO/IEC 27001:2022 Klausa 6 hingga Klausa 10 yang mencakup siklus *Plan-Do-Check-Act* (PDCA), diperoleh nilai tingkat kematangan keseluruhan sebesar 88,75% atau berada pada Level 4 (*Quantitative*). Hasil tersebut menunjukkan bahwa penerapan tata kelola keamanan informasi di PT. XYZ telah berjalan dengan baik, terukur, dan dikelola secara konsisten.

2. Berdasarkan hasil pengukuran pada masing-masing klausa, diperoleh nilai Klausa 6 (*Planning*) sebesar 4,6, Klausa 7 (*Support*) sebesar 4,4, Klausa 8 (*Operations*) sebesar 4,0, Klausa 9 (*Performance Evaluation*) sebesar 4,3, dan Klausa 10 (*Improvement*) sebesar 4,0. Hasil tersebut menunjukkan bahwa seluruh domain telah berada pada tingkat kematangan yang baik dan mendekati kondisi optimal (*Optimizing*).

3. Berdasarkan hasil *gap analysis* diperoleh kesenjangan sebesar 1 level antara kondisi saat ini (*As-Is*) pada level 4 (*Quantitative*) dengan kondisi yang diharapkan (*To-Be*) pada level 5 (*Optimizing*). Kesenjangan tersebut menunjukkan bahwa meskipun penerapan ISMS telah berjalan dengan baik, masih diperlukan peningkatan dan evaluasi berkelanjutan untuk mencapai kondisi yang lebih optimal.

4. Hasil penelitian menunjukkan masih terdapat beberapa temuan pada proses tata kelola keamanan informasi, seperti perubahan penggunaan tools keamanan informasi yang belum selalu disertai analisis risiko terdokumentasi, *awareness* keamanan informasi yang belum dilakukan secara berkala, monitoring kontrol keamanan *endpoint* yang belum konsisten sesuai jadwal, serta dokumentasi hasil monitoring dan *corrective action* yang belum dilakukan secara konsisten. Oleh karena itu, rekomendasi yang diberikan yaitu melakukan evaluasi berkala terhadap proses keamanan informasi, meningkatkan awareness dan sosialisasi keamanan informasi, memperkuat monitoring keamanan endpoint, serta meningkatkan dokumentasi dan evaluasi *corrective action* sebagai bagian dari *continual improvement* ISMS di PT. XYZ.

.

DAFTAR PUSTAKA

[1] Von Solms, R., & Van Niekerk, J., "From information security to cyber security," *Computers & Security*, vol. 38, pp. 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.

[2] "ISO 27001:2022 Information Security Management System Guide (ISO 27000 Information Security Management)".

[3] E. Riana, M. E. S. Sulistyawati, and O. P. 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," *J. Inf. Syst. Res.*, vol. 4, no. 2, pp. 632–640, 2023.M. Wegmuller, J. P. von der Weid, P. Oberson, & N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," *Prosiding ECOC'00*, 2000, paper 11.3.4, p. 109.

[4] R. A. Putra, "Analisis Tingkat Kematangan Keamanan Informasi Menggunakan ISO 27001:2013 pada Perusahaan Telekomunikasi," *J. Telekomun.*, 2021

[5] ISACA, *COBIT 2019 Framework: Governance and Management Objectives*. Rolling Meadows, IL: Information Systems Audit and Control Association, 2019

[6] *J. W. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, 4th ed. Thousand Oaks, CA: SAGE Publications, 2014.*

[7] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Bandung: Alfabeta, 2019.

[8] R. Priyono, *Metode Penelitian Kuantitatif dan Kualitatif: Teori dan Aplikasi*. Surabaya: Zifatama Publisher, 2018.

[9] S. Suryanto and A. Andriani, *"Penilaian Kematangan Tata Kelola TI Menggunakan COBIT 2019 pada Instansi Pemerintah," J. Tata Kelola TI, 2022.*

[10] Z. Artamevia and A. Triayudi, *"Evaluation of Maturity Level Information Security Using COBIT 2019 and ISO/IEC 27001:2022,"* 2025.

[11] 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, no. 10, pp. 223–237, Oct. 2023