

**EVALUASI MATURITY LEVEL KEAMANAN INFORMASI
MENGUNAKAN COBIT 2019 DAN ISO/IEC 27001:2022**

TESIS

Untuk memenuhi sebagian persyaratan memperoleh gelar
Magister Teknologi Informasi

Disusun oleh:

Zahrach Artamevia
247064518002



**PROGRAM STUDI MAGISTER TEKNOLOGI INFORMASI
FAKULTAS TEKNOLOGI KOMUNIKASI DAN INFORMATIKA
UNIVERSITAS NASIONAL**

JAKARTA

2026

HALAMAN PENGESAHAN

EVALUASI MATURITY LEVEL KEAMANAN INFORMASI MENGUNAKAN COBIT 2019 DAN ISO/IEC 27001:2022

Untuk memenuhi sebagai persyaratan memperoleh Gelar Magister Komputer

Disusun oleh:

Zahrach Artamevia
247064518002

Tesis ini telah diuji dan dinyatakan lulus pada
21 Februari 2026

Telah diperiksa dan disetujui oleh:

Dosen Pembimbing,



Prof. Agung Triayudi, S.Kom., M.Kom., Ph.D
NIDN. 0419068604

Mengetahui,
Ketua Program Studi Magister Teknologi Informasi



Ir. Asrul Sanjaya, S.T., M.T., M.Kom., Ph.D
NIDN. 0303067003

PERNYATAAN ORISINALITAS

Saya menyatakan dengan sebenar-benarnya bahwa sepanjang pengetahuan saya, di dalam naskah Tesis ini tidak terdapat karya ilmiah yang pernah diajukan oleh orang lain untuk memperoleh gelar akademik di suatu perguruan tinggi, dan tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis disitasi dalam naskah ini dan disebutkan dalam daftar pustaka.

Apabila ternyata didalam naskah Tesis ini dapat dibuktikan terdapat unsur-unsur plagiasi, saya bersedia Tesis ini digugurkan dan gelar akademik yang telah saya peroleh Magister dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku (UU No. 20 Tahun 2003, Pasal 25 ayat 2 dan Pasal 70).

Jakarta, 2 Maret 2026



Zahrach Artamevia

NIM: 247064518002

ABSTRAK

Keamanan informasi merupakan aspek penting dalam menjaga keberlangsungan operasional bisnis, khususnya pada sistem berbasis teknologi informasi yang mengelola data sensitif. PT XYZ menggunakan Claim Management System untuk mendukung proses pengelolaan klaim insentif, namun masih menghadapi permasalahan terkait risiko kehilangan data, kontrol akses yang belum optimal, serta belum adanya pengukuran tingkat kematangan tata kelola keamanan informasi. Kondisi ini menyebabkan perusahaan belum memiliki acuan yang jelas dalam mengelola dan meningkatkan keamanan sistem informasi secara terstruktur.

Penelitian ini bertujuan untuk mengevaluasi tingkat kematangan tata kelola keamanan informasi pada PT XYZ menggunakan kerangka kerja COBIT 2019 serta mengidentifikasi dan memetakan kontrol keamanan yang relevan berdasarkan standar ISO/IEC 27001:2022 sebagai dasar penyusunan rekomendasi perbaikan. Metode yang digunakan adalah metode deskriptif dengan pendekatan evaluatif melalui teknik pengumpulan data berupa kuesioner, wawancara, dan analisis dokumen. Penilaian dilakukan terhadap beberapa domain COBIT 2019 yang relevan dengan keamanan informasi, yaitu DSS04, BAI06, APO13, DSS01, dan MEA01, kemudian dilakukan analisis maturity level dan pemetaan kontrol ISO/IEC 27001:2022.

Hasil penelitian menunjukkan bahwa tingkat kematangan tata kelola keamanan informasi di PT XYZ berada pada Level 3 (Established) hingga Level 4 (Predictable). Hal ini menunjukkan bahwa proses keamanan informasi telah distandarisasi, terdokumentasi, dan dijalankan secara konsisten, serta sebagian telah dipantau menggunakan metrik yang terukur. Meskipun demikian, masih diperlukan beberapa peningkatan, seperti penguatan kontrol akses berbasis prinsip keamanan, peningkatan dokumentasi dan monitoring keamanan, serta penerapan kontrol keamanan tambahan berdasarkan ISO/IEC 27001:2022 untuk meningkatkan efektivitas tata kelola keamanan informasi.

Penelitian ini menyimpulkan bahwa penerapan kerangka kerja COBIT 2019 yang terintegrasi dengan ISO/IEC 27001:2022 dapat digunakan secara efektif untuk mengevaluasi dan meningkatkan tata kelola keamanan informasi organisasi. Hasil penelitian ini diharapkan dapat menjadi acuan bagi organisasi dalam meningkatkan tingkat kematangan keamanan informasi serta mendukung keberlangsungan operasional bisnis secara berkelanjutan.

Keywords: *Information Security, COBIT 2019, ISO/IEC 27001:2022, Maturity Level, IT Governance*



DAFTAR ISI

PENGESAHAN	2
PERNYATAAN ORISINALITAS	3
KATA PENGANTAR	4
ABSTRAK	5
DAFTAR ISI	7
DAFTAR GAMBAR	10
DAFTAR TABEL	11
BAB 1 PENDAHULUAN	12
1.1. Latar Belakang	12
1.2. Rumusan Masalah	15
1.3. Tujuan	16
1.4. Manfaat	16
1.5. Batasan Masalah	17
1.6. Sistematika Pembahasan	17
BAB 2 LANDASAN KEPUSTAKAAN	19
2.1. Landasan Kepustakaan	19
2.1.1. Manajemen Risiko	19
2.1.2. COBIT 2019	21
2.1.3. ISO/IEC 27001:2022	22
2.1.4. Disaster Recovery Plan	22
2.1.5. Information Management System	22
2.1.6. Security Information and Event Management	23
2.1.7. Penelitian Terdahulu	23
2.2 Posisi dan Kontribusi Penelitian (Research Gap)	29
BAB 3 METODOLOGI	30
3.1. Tipe Penelitian	30
3.2. Strategi dan Rancangan Penelitian	31
3.2.1. Strategi Penelitian	31

3.2.2.	Lokasi Penelitian	31
3.2.3.	Subjek Penelitian.....	31
3.3.	Teknik Pengumpulan Data	31
3.4.	Teknik Analisis Data	32
3.5.	Alasan Pemilihan Metode.....	32
3.6.	Alur Penelitian.....	33
3.7.	Problem Identification	33
3.8.	Literature Review	34
3.9.	Domain Mapping.....	35
3.10.	Interview	37
3.11.	Questionnaire.....	40
3.12.	Maturity Analysis	45
3.13.	Gap Analysis	46
3.14.	Recommendation.....	46
3.15.	Conclusion.....	47
3.16.	Metode Pemetaan Kontrol ISO/IEC 27001:2022 terhadap Proses COBIT 2019	47
BAB 4	HASIL	49
4.1	Maturity Level by COBIT 2019	50
4.2	Kontrol ISO/IEC 27001:2022	60
4.3	Analisis Implementasi Kontrol Akses Berdasarkan ISO/IEC 27001:2022	62
4.4	Pemetaan Kondisi Existing dan Rekomendasi Perbaikan Berdasarkan COBIT 2019 dan ISO/IEC 27001:2022	63
4.4.1	Kondisi Existing (Sebelum COBIT & ISO)	63
4.4.2	Pemetaan Menggunakan COBIT 2019	63
4.4.3	Pemetaan Menggunakan ISO/IEC 27001:2022.....	63
4.4.4	Perbandingan Sebelum vs Sesudah	64
4.4.5	Pemetaan Kontrol ISO/IEC 27001:2022 terhadap Proses COBIT 2019.....	64
BAB 5	PEMBAHASAN	66
5.1	Analisis Hasil Maturity Level.....	69

5.1.1 DSS04 – Manage Continuity (Level 3: Established)	69
5.1.2 BAI06 – Manage Changes (Level 4: Predictable)	69
5.1.3 APO13 – Manage Security (Level 3: Established)	70
5.1.4 DSS01 – Manage Operations (Level 3: Established)	70
5.1.5 MEA01 – Monitor, Evaluate, and Assess Performance and Conformance (Level 3: Established)	71
5.2 Rekomendasi berdasarkan horizon waktu	72
5.2.1 Rekomendasi Jangka Pendek (0–6 bulan)	72
5.2.2 Rekomendasi Jangka Menengah (6–18 bulan).....	74
5.2.3 Rekomendasi Jangka Panjang (>18 bulan)	75
BAB 6 KESIMPULAN	78
DAFTAR PUSTAKA.....	80



DAFTAR GAMBAR

Figure 1. Alur Penelitian	33
Figure 2. Domain Mapping	35
Figure 3. Domain Mapping	35
Figure 4. Domain Mapping	36
Figure 5. Domain Mapping	36
Figure 6. Domain Mapping	37



DAFTAR TABEL

Table 1. Mengukur Manajemen Risiko	19
Table 2. Maturity Level COBIT 2019	21
Table 3. Teknik Pengumpulan Data	31
Table 4. Teknik Analisis Data	32
Table 5. Table Wawancara.....	38
Table 6. Pertanyaan Kuesioner.....	41
Table 7. Hasil Kuesioner	50
Table 8. Maturity Level.....	57
Table 9. Control ISO/IEC 27001:2022.....	60
Table 10. Pemetaan Kontrol ISO/IEC 27001:2022 & COBIT 2019.....	64

