

**PERANCANGAN TAHAPAN KEAMANAN INFORMASI BERBASIS
ISO 27001:2022 BERDASARKAN ANALISIS RISIKO
MENGUNAKAN OCTAVE DAN FMEA DI PERUSAHAAN X**

TUGAS AKHIR



**SARA WIRDYA
1232923007**

**PROGRAM STUDI TEKNIK INDUSTRI
FAKULTAS TEKNIK DAN ILMU KOMPUTER
UNIVERSITAS BAKRIE
JAKARTA
2026**

**PERANCANGAN TAHAPAN KEAMANAN INFORMASI BERBASIS
ISO 27001:2022 BERDASARKAN ANALISIS RISIKO
MENGUNAKAN OCTAVE DAN FMEA DI PERUSAHAAN X**

TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik



**SARA WIRDYA
1232923007**

**PROGRAM STUDI TEKNIK INDUSTRI
FAKULTAS TEKNIK DAN ILMU KOMPUTER
UNIVERSITAS BAKRIE
JAKARTA
SEPTEMBER 2026**

HALAMAN PERNYATAAN ORISINALITAS

**Tugas akhir ini adalah hasil karya saya sendiri, dan
semua sumber baik yang dikutip maupun dirujuk
telah saya nyatakan dengan benar.**

Nama : Sara Wirdya

NIM : 1232923007

Tanda Tangan : 

Tanggal : 07 September 2026

HALAMAN PENGESAHAN

Tugas akhir ini diajukan oleh :

Nama : Sara Wirdya
NIM : 1232923007
Program Studi : Teknik Industri
Fakultas : Teknik dan Ilmu Komputer
Judul Tugas Akhir : **Perancangan Tahapan Keamanan Informasi Berbasis ISO 27001:2022 Berdasarkan Analisis Risiko Menggunakan OCTAVE Dan FMEA Di Perusahaan X**

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan dalam mengikuti sidang tugas akhir untuk memperoleh gelar Sarjana pada Program Studi Teknik Industri, Fakultas Teknik dan Ilmu Komputer, Universitas Bakrie.

DEWAN PENGUJI

Pembimbing : Annissa Fanya, S.T., M.Sc

()

Penguji : Adi Budipriyanto, S.T, M.T, Dr, IPM, CSCM

()

Penguji : Tri Susanto, S.E., M.T., CIPM

()

Ditetapkan di : Jakarta

Tanggal : 07 September 2026

KATA PENGANTAR

Dengan segala rasa syukur dan terima kasih, peneliti panjatkan ke hadirat Allah SWT atas segala rahmat, taufik, dan hidayah-Nya sehingga peneliti dapat menyelesaikan Tugas akhir Skripsi yang berjudul **“Perancangan Tahapan Keamanan Informasi Berbasis ISO 27001:2022 Berdasarkan Analisis Risiko Menggunakan OCTAVE Dan FMEA Di Perusahaan X”**.

Penyusunan tugas akhir ini tentunya tidak lepas dari dukungan, bimbingan, serta bantuan dari berbagai pihak. Oleh karena itu, dengan segala kerendahan hati, peneliti menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Ibu Annisa Fanya, S.T, M.Sc selaku dosen pembimbing utama, yang telah memberikan bimbingan, arahan, dan motivasi selama proses penyusunan tugas akhir ini.
2. Seluruh dosen di Program Studi Teknik Industri, yang telah memberikan bekal ilmu pengetahuan dan pengalaman berharga selama masa perkuliahan.
3. Manajemen dan seluruh pihak di Perusahaan X yang telah memberikan izin, data, dan dukungan selama proses pengumpulan informasi dan studi lapangan.
4. Kedua orang tua tercinta, suami, dan anak-anak tersayang atas doa, semangat, dan kasih sayang yang tiada henti.
5. Rekan-rekan mahasiswa serta sahabat-sahabat peneliti yang senantiasa memberikan dukungan moral dan teknis selama proses penyusunan tugas akhir ini.

Peneliti menyadari bahwa tugas akhir ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan demi penyempurnaan tugas akhir ini ke depannya. Akhir kata, semoga tugas akhir skripsi ini dapat memberikan manfaat dan kontribusi, baik bagi peneliti, institusi, maupun pihak-pihak terkait lainnya.

Jakarta, 07 September 2026

Penulis,

Sara Wirdya

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI

Sebagai sivitas akademik Universitas Bakrie, saya yang bertanda tangan di bawah ini:

Nama : Sara Wirdya
NIM : 1232923007
Program Studi : Teknik Industri
Fakultas : Teknik dan Ilmu Komputer
Jenis Tugas Akhir : Skripsi

demikian pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Bakrie **Hak Bebas Royalti Noneksklusif (Non-exclusive Royalty-Free Right)** atas karya ilmiah saya yang berjudul :

“PERANCANGAN TAHAPAN KEAMANAN INFORMASI BERBASIS ISO 27001:2022 BERDASARKAN ANALISIS RISIKO MENGGUNAKAN OCTAVE DAN FMEA DI PERUSAHAAN X”

berserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Bakrie berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta untuk kepentingan akademis.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta
Pada tanggal :

Yang menyatakan



Sara Wirdya

1232923007

PERANCANGAN TAHAPAN KEAMANAN INFORMASI BERBASIS ISO 27001:2022 BERDASARKAN ANALISIS RISIKO MENGGUNAKAN OCTAVE DAN FMEA DI PERUSAHAAN X

Sara Wirdya

ABSTRAK

Keamanan informasi penting untuk menjaga keberlangsungan proses bisnis Perusahaan X yang bergantung pada sistem informasi. Penelitian ini bertujuan merancang tahapan keamanan informasi berbasis ISO 27001:2022 melalui analisis risiko menggunakan Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) dan Failure Mode and Effect Analysis (FMEA). OCTAVE digunakan untuk mengidentifikasi aset kritis, ancaman, dan kerentanan, sedangkan FMEA digunakan untuk menentukan prioritas risiko berdasarkan Severity, Occurrence, dan Detection. Hasil penelitian mengidentifikasi empat aset utama, yaitu ERP, HCGA, Database, serta Server dan Jaringan. Risiko prioritas yang diperoleh meliputi ketiadaan pedoman keamanan informasi dengan RPN 720, malware/ransomware 576, eksploitasi jaringan melalui BYOD 576, dan phishing 245. Risiko tersebut dipetakan terhadap ISO 27001:2022 sebagai dasar penyusunan tiga rancangan SOP, yaitu SOP Tata Kelola Keamanan Informasi, SOP Penggunaan Aset dan Perangkat Pribadi (BYOD), serta SOP Penanganan Insiden Keamanan dan Kesadaran Siber. Evaluasi teoritis menunjukkan estimasi penurunan RPN masing-masing menjadi 96, 144, 72, dan 63. Nilai tersebut merupakan estimasi rancangan pengendalian karena SOP belum diimplementasikan.

Kata kunci: Keamanan Informasi, ISO 27001:2022, OCTAVE, FMEA, Standar Operasional Prosedur.

DESIGN OF AN ISO 27001:2022-BASED INFORMATION SECURITY FRAMEWORK BASED ON RISK ANALYSIS USING OCTAVE AND FMEA AT COMPANY X

Sara Wirdya

ABSTRACT

Information security is essential for maintaining business process continuity at Company X, which relies heavily on information systems. This study aims to design information security stages based on ISO 27001:2022 through risk analysis using the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) and Failure Mode and Effect Analysis (FMEA) methods. OCTAVE is used to identify critical assets, threats, and vulnerabilities, while FMEA is used to determine risk priorities based on Severity, Occurrence, and Detection. The study identifies four main assets: ERP, HCGA, Database, and Server and Network infrastructure. The priority risks are the absence of information security guidelines with an RPN of 720, malware/ransomware with an RPN of 576, network exploitation through BYOD with an RPN of 576, and phishing with an RPN of 245. These risks are mapped to ISO 27001:2022 as the basis for designing three SOPs: Information Security Governance, Asset and Personal Device Usage (BYOD), and Security Incident Handling and Cybersecurity Awareness. The theoretical evaluation estimates the respective RPN values to decrease to 96, 144, 72, and 63. These values are theoretical estimates because the SOPs have not yet been implemented.

Keywords: Information Security, ISO 27001:2022, OCTAVE, FMEA, Standard Operating Procedure.

DAFTAR ISI

HALAMAN PERNYATAAN ORISINALITAS	iii
HALAMAN PENGESAHAN	iv
KATA PENGANTAR	v
ABSTRAK.....	vii
ABSTRACT	viii
DAFTAR ISI	ix
DAFTAR GAMBAR	xii
DAFTAR LAMPIRAN.....	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	4
1.3 Tujuan Penelitian	4
1.4 Manfaat	5
1.5 Batasan Masalah	5
BAB II TINJAUAN PUSTAKA	6
2.1 Teknik Industri dan Perancangan Sistem Kerja.....	6
2.1.1 Ruang Lingkup Keilmuan Teknik Industri	6
2.1.2 Konsep Sistem Kerja	7
2.1.3 Rekayasa Kualitas dan Keandalan sebagai Dasar Manajemen Risiko	7
2.1.4 Standar Operasional Prosedur sebagai Luaran Perancangan Sistem	8
2.2 Sistem Informasi (SI).....	9
2.3 Keamanan Informasi.....	9
2.4 Sistem Manajemen Keamanan Informasi	10
2.4.1 Keamanan Informasi Untuk Organisasi	11
2.4.2 Manajemen Risiko Keamanan Informasi	12
2.4.3 Proses Manajemen Keamanan Informasi	12
2.5 Aset	13
2.5.1 Aset Informasi	13
2.5.2 Manajemen Aset	14
2.6 ISO 27001:2022	14
2.6.1 Struktur ISO 27001:2022	15
2.6.2 Tujuan Keamanan dan Tujuan Perlindungan dari ISO 27001:2022	16
2.7 Metode OCTAVE	16
2.8 Penerapan Tiga Fase OCTAVE dalam Penelitian	18
2.9 FMEA (Failure Mode and Effect Analysis).....	19
2.9.1 Membuat Kriteria Dampak Severity, Occurrence, Detection (SOD)	20
2.9.2 Membuat Nilai Dampak (Severity)	20
2.9.3 Penentuan Nilai Kejadian (Occurrence)	21
2.9.4 Penentuan Nilai Deteksi (Detection)	22
2.10 Manajemen Proses Bisnis (Business Process Management)	23
2.11 Standar Operasional Prosedur (SOP).....	25
2.12 Penelitian Terdahulu	26
BAB III METODE PENELITIAN.....	30
3.1 Lokasi dan Waktu	30
3.2 Batas Penelitian.....	30
3.3 Jenis dan Pendekatan Penelitian	30
3.4 Bahan dan Alat.....	30

3.5 Diagram Alir Penelitian	31
3.6 Integrasi OCTAVE dan FMEA	40
3.7 Peran ISO 27001:2022 dalam Penelitian	40
BAB IV ANALISIS DAN PEMBAHASAN	41
4.1 Gambaran Umum Objek Penelitian	41
4.2 Analisis Proses Bisnis	42
4.3 Identifikasi Risiko Keamanan Siber Menggunakan Metode OCTAVE	46
4.3.1 Identifikasi Aset Informasi Kritis	46
4.3.2 Identifikasi Ancaman	48
4.3.3 Identifikasi Kerentanan	51
4.4 Analisis dan Penilaian Risiko Menggunakan Metode FMEA	51
4.4.1 Penentuan Skor S-O-D	52
4.4.2 Perhitungan Risk Priority Number (RPN)	55
4.4.3 Penetapan Prioritas Risiko (Risk Evaluation)	57
4.5.1 Pemetaan Risiko ke Kontrol ISO 27001:2022	59
4.5.2 Analisis Kesenjangan (Gap Analysis) atau Rekomendasi Kontrol	60
4.6 Perancangan Standar Operasional Prosedur (SOP)	63
4.6.1 Rancangan SOP Tata Kelola Keamanan Informasi (Umum)	64
4.6.2 Rancangan SOP Penggunaan Aset dan Perangkat Pribadi (BYOD)	67
BAB V KESIMPULAN DAN SARAN.....	75
5.1 Kesimpulan	75
5.2 Saran	76
DAFTAR PUSTAKA	77
LAMPIRAN	81

DAFTAR TABEL

Tabel 2.1 Tabel Penilaian Severity	20
Tabel 2.2 Tabel Penilaian Occurrence	21
Tabel 2.3 Tabel Penilaian Detection	23
Tabel 2.4 Perbandingan Penelitian Terdahulu	26
Tabel 3.1 Rangkaian Kegiatan Tahap Perencanaan.....	32
Tabel 3.2 Rangkaian Kegiatan Tahap Pengumpulan Data	33
Tabel 3.3 Rangkaian Kegiatan Tahap Analisis Risiko	34
Tabel 3.4 Kriteria Penentuan Tingkat Kekritisitas Aset.....	36
Tabel 3.5 Rangkaian Kegiatan Tahap Pengelolaan Risiko.....	37
Tabel 3.6 Rangkaian Kegiatan Tahap Penyusunan SOP	39
Tabel 4.1 Identifikasi Aset Informasi Kritis	46
Tabel 4.2 Identifikasi Ancaman Berbasis Aset.....	49
Tabel 4.3 Identifikasi Kerentanan.....	51
Tabel 4.4 Penentuan Nilai Dampak (Severity)	53
Tabel 4.5 Penentuan Nilai Kejadian (Occurrence)	54
Tabel 4.6 Penentuan Nilai Deteksi (Detection)	55
Tabel 4.7 Perhitungan Risk Priority Number (RPN)	55
Tabel 4.8 Penetapan Prioritas Risiko (Risk Evaluation).....	58
Tabel 4.9 Pemetaan Risiko ke Klausul ISO 27001:2022.....	59
Tabel 4.10 Analisis Kesenjangan (Gap Analysis) atau Rekomendasi Kontrol	61
Tabel 4.11 Evaluasi Risiko Pasca Perancangan (Estimasi Penurunan RPN)	73

DAFTAR GAMBAR

Gambar 1.1 Jumlah Kasus Kebocoran Data Perusahaan Yang Terjadi di Indonesia	1
Gambar 2.1 Tujuan ISO 27001	16
Gambar 3.1 Alir Penelitian	31
Gambar 4.1 Peta Proses Bisnis	43
Gambar 4.2 Rancangan SOP Tata Kelola Keamanan Informasi (Umum)	65
Gambar 4.3 Rancangan SOP Penggunaan Aset dan Perangkat Pribadi (BYOD)	68
Gambar 4.4 Rancangan SOP Penanganan Insiden Keamanan dan Kesadaran Siber	71

DAFTAR LAMPIRAN

Lampiran 1. Daftar Pertanyaan Wawancara	81
---	----