IDENTIFIKASI RISIKO KEAMANAN INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2022 PADA DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI DIY

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

LEONSIUS FALDI KAUM

21.83.0671

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

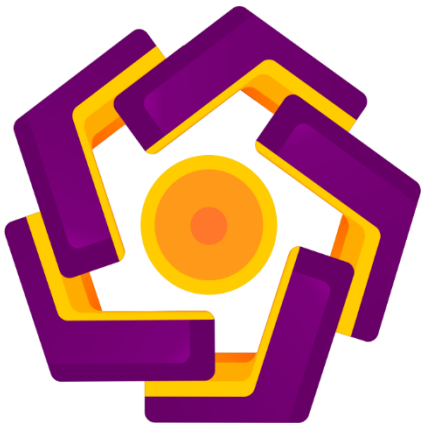
2025

IDENTIFIKASI RISIKO KEAMANAN INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2022 PADA DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI DIY

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer



disusun oleh

LEONSIUS FALDI KAUM

21.83.0671

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

HALAMAN PERSETUJUAN

SKRIPSI

IDENTIFIKASI RISIKO KEAMANAN INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2022 PADA DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI DIY

yang disusun dan diajukan oleh

Leonsius Faldi Kaum

21.83.0671

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 26 Agustus 2025

Dosen Pembimbing,

Melwin Syafrizal, S.Kom., M.Eng., Ph.D.
NIK. 190302105

HALAMAN PENGESAHAN

SKRIPSI

IDENTIFIKASI RISIKO KEAMANAN INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2022 PADA DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI DIY

yang disusun dan diajukan oleh

Leonsius Faldi Kaum

21.83.0671

Telah dipertahankan di depan Dewan Penguji
pada tanggal 17 September 2025

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Muhammad Koprawi, S.Kom., M.Eng. **NIK. 190302454**	
Dr. Dony Ariyus, S.S., M.Kom. **NIK. 190302128**	
Melwin Syafrizal, S.Kom., M.Eng., Ph.D. **NIK. 190302105**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 17 September 2025

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Leonsius Faldi Kaum
NIM : 21.83.0671

Menyatakan bahwa Skripsi dengan judul berikut:

Identifikasi Risiko Keamanan Informasi Berdasarkan Standar Iso/Iec 27001:2022 Pada Dinas Komunikasi Dan Informatika Provinsi DIY

Dosen Pembimbing : Melwin Syafrizal, Skom., M.Eng., Ph.D.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 17 September 2025

Yang Meny

Leonsius Faldi Kaum

HALAMAN PERSEMBAHAN

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas limpahan rahmat dan karunia-Nya sehingga skripsi ini dapat terselesaikan dengan baik.

Dengan penuh kerendahan hati, karya ini penulis persembahkan kepada:

1. Almarhum orang tua tercinta, yang semasa hidupnya telah memberikan kasih sayang, doa, teladan, dan dukungan yang menjadi sumber kekuatan bagi penulis. Semoga almarhum beristirahat dalam damai bersama Kristus dan memperoleh terang kehidupan kekal.
2. Keluarga besar,terutama kakak-kakak saya atas perhatian dan dorongan moral yang selalu menguatkan dalam menghadapi berbagai tantangan.
3. Dosen pembimbing dan penguji, atas bimbingan, arahan, serta ilmu berharga yang diberikan selama proses penelitian dan penyusunan skripsi ini.
4. Teman-teman seperjuangan, atas kebersamaan, motivasi, dan semangat yang senantiasa menyertai perjalanan akademik ini.
5. Almamater tercinta, sebagai wadah menimba ilmu dan mengembangkan diri untuk memberi manfaat bagi masyarakat dan dunia pendidikan.

Semoga karya ini menjadi ungkapan bakti dan syukur, sekaligus bermanfaat bagi pengembangan ilmu pengetahuan.

KATA PENGANTAR

Puji Syukur kepada Tuhan Yang Maha Esa, yang telah memberikan limpahan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan penyusunan skripsi dengan judul "Identifikasi Risiko Keamanan Informasi Berdasarkan Standar Iso/Iec 27001:2022 Pada Dinas Komunikasi dan Informatika Yogyakarta" tepat pada waktunya.

Skripsi ini disusun untuk memenuhi salah satu syarat dalam menyelesaikan pendidikan Sarjana Komputer pada Program Studi Ilmu Komputer Universitas Amikom Yogyakarta. Oleh karena itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Bapak Melwin Syafrizal, S.Kom., M.Eng., Ph.D. selaku dosen pembimbing yang telah dengan sabar memberikan bimbingan, saran, dan motivasi selama proses penyusunan skripsi ini.
2. Bapak/Ibu Tim Dosen Penguji, yang telah memberikan masukan dan evaluasi yang sangat berharga demi kesempurnaan skripsi ini.
3. Bapak/Ibu Dosen Program Studi Teknik Komputer di Universitas Amikom Yogyakarta yang telah memberikan ilmu dan wawasan selama masa perkuliahan.
4. Kedua orang tua dan Keluarga, kakak-kakak saya tercinta, yang tidak henti memberikan doa, dukungan moral, dan semangat selama penulis menjalani proses akademik.
5. Teman-teman dan rekan seperjuangan yang senantiasa memberikan support, semangat serta saling membantu dalam menyelesaikan skripsi ini.

Penulis menyadari skripsi ini masih memiliki kekurangan dan dengan terbuka menerima kritik serta saran yang membangun untuk perbaikan di masa mendatang.

Yogyakarta, 4 September 2025

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR LAMBANG DAN SINGKATAN

ISMS	Information Security Management System (Sistem Manajemen Keamanan Informasi)
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
ISO/IEC 27001:2022	Standar internasional untuk sistem manajemen keamanan informasi
ISO 31000:2018	Standar internasional untuk manajemen risiko
CIA	Confidentiality, Integrity, Availability (prinsip dasar keamanan informasi)
PDCA	Plan–Do–Check–Act (siklus perbaikan berkelanjutan)
SOP	Standard Operating Procedure (Prosedur Operasional Standar)
IT	Information Technology (Teknologi Informasi)
TIK	Teknologi Informasi dan Komunikasi
OPD	Organisasi Perangkat Daerah
DIY	Daerah Istimewa Yogyakarta
Diskominfo	Dinas Komunikasi dan Informatika
SoA	Statement of Applicability (dokumen penerapan kontrol ISMS)
Risk Register	Daftar hasil identifikasi, analisis, dan evaluasi risiko
L	Likelihood (tingkat kemungkinan terjadinya risiko)
I	Impact (tingkat dampak apabila risiko terjadi)
R = L × I	Rumus perhitungan skor risiko berdasarkan matriks risiko

DAFTAR ISTILAH

ISMS (Information Security Management System)	Sistem manajemen keamanan informasi yang berbasis standar ISO/IEC 27001:2022 untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi.
ISO/IEC 27001:2022	Standar internasional yang menetapkan persyaratan untuk sistem manajemen keamanan informasi.
ISO 31000:2018	Standar internasional untuk manajemen risiko yang memberikan prinsip, kerangka kerja, dan proses manajemen risiko.
Annex A ISO/IEC 27001:2022	Lampiran yang berisi daftar kontrol keamanan informasi yang dapat diterapkan organisasi.
Diskominfo (Dinas Komunikasi dan Informatika)	Instansi pemerintah daerah yang bertugas dalam pengelolaan komunikasi, informatika, statistik, dan persandian.
Gap Analysis	Metode analisis untuk mengidentifikasi kesenjangan antara kondisi saat ini dengan standar yang diharapkan.
Likelihood	Tingkat kemungkinan suatu risiko terjadi.
Impact	Besarnya dampak atau konsekuensi yang ditimbulkan jika suatu risiko terjadi.
Risk Matrix	Alat untuk mengukur tingkat risiko berdasarkan kombinasi likelihood dan impact.
Risk Register	Daftar yang memuat hasil identifikasi, analisis, evaluasi, dan mitigasi risiko.
Mitigasi Risiko	Tindakan pengendalian yang dirancang untuk mengurangi kemungkinan atau dampak risiko keamanan informasi.
PDCA (Plan–Do–Check–Act)	Siklus perbaikan berkelanjutan dalam penerapan ISMS untuk memastikan efektivitas kontrol keamanan informasi.
CIA Triad	Tiga prinsip dasar keamanan informasi: Confidentiality (kerahasiaan), Integrity (integritas), dan Availability (ketersediaan).

INTISARI

Keamanan informasi merupakan faktor penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data, terutama bagi instansi pemerintah yang mengelola layanan publik digital. Dinas Komunikasi dan Informatika (Diskominfo) Provinsi Daerah Istimewah Yogyakarta (DIY) sebagai penggerak program Jogja Smart Province menghadapi potensi kebocoran data, serangan siber, dan gangguan operasional yang dapat menurunkan kualitas pelayanan serta kepercayaan masyarakat. Hal ini menunjukkan perlunya identifikasi dan evaluasi risiko keamanan informasi secara sistematis agar kelemahan dapat diketahui dan ditangani dengan tepat.

Penelitian ini menggunakan metode kuantitatif dengan jenis penelitian deskriptif. Data diperoleh melalui observasi checklist ISO/IEC 27001:2022, wawancara semi-terstruktur, dan telaah dokumentasi. Analisis dilakukan berdasarkan kerangka ISO 31000 yang meliputi identifikasi, analisis likelihood dan impact, evaluasi tingkat risiko menggunakan matriks, serta penyusunan rekomendasi mitigasi. Hasil pengukuran dituangkan dalam persentase kepatuhan kontrol dan peta risiko (risk register) untuk menggambarkan kondisi keamanan informasi di Diskominfo Provinsi DIY.

Hasil penelitian menunjukkan sebagian besar kontrol keamanan informasi telah diterapkan dengan baik, dengan tingkat risiko pada kategori rendah hingga sedang. Hal ini mengindikasikan bahwa sistem manajemen keamanan informasi Diskominfo Provinsi DIY cukup memadai, meski masih terdapat kelemahan pada manajemen aset informasi dan kontrol akses. Penelitian ini memberikan dasar rekomendasi penguatan kebijakan keamanan informasi, serta dapat dimanfaatkan instansi pemerintah lain sebagai referensi penerapan ISO/IEC 27001:2022.

Kata kunci: ISO/IEC 27001:2022, risiko keamanan informasi, manajemen risiko, kontrol ISMS, Diskominfo.

ABSTRACT

Information security is an important factor in maintaining the confidentiality, integrity, and availability of data, especially for government agencies that manage digital public services. The Yogyakarta Communication and Information Agency (Diskominfo), as the driving force behind the Jogja Smart Province program, faces potential data breaches, cyber-attacks, and operational disruptions that could reduce service quality and public trust. This highlights the need for systematic identification and evaluation of information security risks so that weaknesses can be identified and addressed appropriately.

This study uses a quantitative method with a descriptive research type. Data was obtained through observation of the ISO/IEC 27001:2022 checklist, semi-structured interviews, and documentation review. The analysis was conducted based on the ISO 31000 framework, which includes identification, likelihood and impact analysis, risk level evaluation using a matrix, and the formulation of mitigation recommendations. The measurement results were presented in terms of control compliance percentages and a risk register to illustrate the information security conditions at the Yogyakarta Communication and Information Agency.

The results of the study indicate that most information security controls have been implemented effectively, with risk levels ranging from low to moderate. This suggests that the information security management system of the Yogyakarta Communication and Information Agency is adequate, although there are still weaknesses in information asset management and access controls. This research provides a basis for recommendations to strengthen information security policies and can be utilized by other government agencies as a reference for the implementation of ISO/IEC 27001:2022.

Keyword: *ISO/IEC 27001:2022, information security risk, risk management, ISMS controls, Ministry of Communication and Information Technology.*