IMPLEMENTASI TATA KELOLA KEAMANAN INFORMASI PADA ASET TEKNOLOGI DENGAN PENDEKATAN ISO 27001:2022 MENGGUNAKAN METODE (*FAILURE AND EFFECT ANALYSIS*) FMEA

SKRIPSI

UIN SUNAN AMPEL
S U R A B A Y A

Disusun Oleh:

JIHAN RABBANI SAJDA
09010621008

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUNAN AMPEL
SURABAYA
2025

PERNYATAAN KEASLIAN

Saya yang bertanda tangan di bawah ini,

Nama	: JIHAN RABBANI SAJDA
NIM	: 09010621008
Program Studi	: Sistem Informasi
Angkatan	: 2021

Menyatakan bahwa saya tidak melakukan plagiat dalam penulisan skripsi saya yang berjudul: "Analisis Keamanan Informasi pada Aset Teknologi Informasi Dinas PU Bina Marga Provinsi Jawa Timur Berdasarkan Indeks KAMI Versi 5.0". Apabila suatu saat nanti terbukti saya melakukan tindakan plagiat, maka saya bersedia menerima sanksi yang telah ditetapkan.

Demikian pernyataan keaslian ini saya buat dengan sebenar-benarnya.

Surabaya, 9 Juli 2025

Yang menyatakan,

(JIHAN RABBANI SAJDA)

NIM 09010621008

LEMBAR PERSETUJUAN PEMBIMBING

Skripsi oleh

NAMA	: JIHAN RABBANI SAJDA
NIM	: 09010621008
JUDUL	: IMPLEMENTASI TATA KELOLA KEAMANAN INFORMASI PADA ASET TEKNOLOGI DENGAN PENDEKATAN ISO 27001:2022 MENGGUNAKAN METODE (FAILURE AND EFFECT ANALYSIS) FMEA

Ini telah diperiksa dan disetujui untuk diujikan.

Surabaya, 28 Mei 2025

Dosen Pembimbing 1	Dosen Pembimbing 2
Dr. Achmad Teguh Wibowo, MT., MTCN	Muhammad Andik Izzuddin, MT
NIP 198810262014031003	NIP 198403072014031001

PENGESAHAN TIM PENGUJI SKRIPSI

Skripsi Jihan Rabbani Sajda ini telah dipertahankan
di depan tim penguji skripsi
di Surabaya, 10 Juni 2025

Menyetujui,
Dosen Penguji

Penguji 1

Faris Muslihul Amin, M.Kom
NIP. 198808132014031001

Penguji 2

Noor Wahyudi, M.Kom
NIP. 198403232014031002

Penguji 3

Dr. Achmad Teguh Wibowo, M.T., MTCNA
NIP. 198810262014031003

Penguji 4

Muhammad Andik Izzuddin, M.T
NIP. 198403072014031001

Mengetahui,

Dekan Fakultas Sains dan Teknologi
UIN Sunan Ampel Surabaya

Dr. A. Saepul Hamdani, M. Pd
NIP. 196507312000031002

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN AMPEL SURABAYA
PERPUSTAKAAN
Jl. Jend. A. Yani 117 Surabaya 60237 Telp. 031-8431972 Fax.031-8413300
E-Mail: perpus@uinsby.ac.id

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI
KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika UIN Sunan Ampel Surabaya, yang bertanda tangan di bawah ini, saya:

Nama	:	Jihan Rabbani Sajda
NIM	:	09010621008
Fakultas/Jurusan	:	Sains dan Teknologi / Sistem Informasi
E-mail address	:	jihanrab19@gmail.com

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Perpustakaan UIN Sunan Ampel Surabaya, Hak Bebas Royalti Non-Eksklusif atas karya ilmiah :
☑ Sekripsi ☐ Tesis ☐ Desertasi ☐ Lain-lain (.....)
yang berjudul :

Implementasi Tata Kelola Keamanan Informasi pada Aset Teknologi dengan Pendekatan ISO 27001:2022 menggunakan Metode (Failure and Effect Analysis) FMEA

beserta perangkat yang diperlukan (bila ada). Dengan Hak Bebas Royalti Non-Ekslusif ini Perpustakaan UIN Sunan Ampel Surabaya berhak menyimpan, mengalih-media/format-kan, mengelolanya dalam bentuk pangkalan data (database), mendistribusikannya, dan menampilkan/mempublikasikannya di Internet atau media lain secara ***fulltext*** untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan atau penerbit yang bersangkutan.

Saya bersedia untuk menanggung secara pribadi, tanpa melibatkan pihak Perpustakaan UIN Sunan Ampel Surabaya, segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian pernyataan ini yang saya buat dengan sebenarnya.

Surabaya, 9 Juli 2025

Penulis

(Jihan Rabbani Sajda)

ABSTRAK

Perkembangan teknologi informasi yang pesat membawa dampak positif bagi operasional organisasi, namun juga memunculkan risiko keamanan informasi yang signifikan. Oleh karena itu, diperlukan tata kelola keamanan informasi yang efektif, salah satunya melalui penerapan standar ISO 27001:2022. Penelitian ini bertujuan untuk mengimplementasikan tata kelola keamanan informasi pada aset teknologi di Pusat Teknologi Informasi dan Pangkalan Data (PUSTIPD) Universitas Islam Negeri Sunan Ampel Surabaya (UINSA) dengan menggunakan pendekatan ISO 27001:2022 serta metode *Failure Mode and Effect Analysis* (FMEA) untuk menganalisis dan memitigasi risiko. Penelitian ini menggunakan metode kualitatif dengan teknik pengumpulan data melalui wawancara, observasi, dan analisis dokumen. Hasil penelitian menunjukkan bahwa dari berbagai aset teknologi informasi yang dimiliki PUSTIPD, terdapat sejumlah risiko dengan tingkat prioritas berbeda, di mana beberapa risiko berada pada kategori *high , medium, low* dan *very low*. Penelitian ini menghasilkan dokumen *Standar Operasional Prosedur* (SOP) sebagai bentuk pengendalian risiko yang disesuaikan dengan kontrol pada ISO 27001:2022. Dengan demikian, penelitian ini memberikan kontribusi dalam meningkatkan keamanan informasi serta mendukung kepatuhan organisasi terhadap standar internasional.

Kata Kunci : Keamanan Informasi, ISO 27001:2022, *Failure Mode and Effect Analysis* (FMEA), Tata Kelola TI, Manajemen Risiko

ABSTRACT

The rapid development of information technology has a positive impact on organizational operations, but also raises significant information security risks. Therefore, effective information security governance is needed, one of which is through the implementation of the ISO 27001:2022 standard. This study aims to implement information security governance on technology assets at the Information Technology and Database Center (PUSTIPD) of the Sunan Ampel State Islamic University of Surabaya (UINSA) using the ISO 27001:2022 approach and the Failure Mode and Effect Analysis (FMEA) method to analyze and mitigate risks. This study uses a qualitative method with data collection techniques through interviews, observations, and document analysis. The results of the study show that from the various information technology assets owned by PUSTIPD, there are a number of risks with different priority levels, where some risks are in the high, medium, low and very low categories. This study produces a Standard Operating Procedure (SOP) document as a form of risk control that is adjusted to the controls in ISO 27001:2022. Thus, this study contributes to improving information security and supporting organizational compliance with international standards.

Keywords: Information Security, ISO 27001:2022, Failure Mode and Effect Analysis (FMEA), IT Governance, Risk Management

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

DAFTAR PUSTAKA

’Abidah, I. N., Hamdani, M. A., & Amrozi, Y. (2020). Implementasi Sistem Basis Data Cloud Computing pada Sektor Pendidikan. *KELUWIH: Jurnal Sains Dan Teknologi*, *1*(2), 77–84. https://doi.org/10.24123/saintek.v1i2.2868

Abdullah, A. (2020). Public Relations in The Era of Artificial Intelligence: Peluang atau Ancaman? *Aristo*, *8*(2), 406. https://doi.org/10.24269/ars.v8i2.2629

Aditama, M. R., Dewi, F., & Praditya, D. (2023). SEIKO : Journal of Management & Business Perancangan Proses Keamanan Informasi Berdasarkan Framework ISO27001:2022. *SEIKO : Journal of Management & Business*, *6*(2), 362–376.

Adnan, N., Abdullah, S. N. H. S., Raja Yusof, R. J., Zainal, N. F. A., Qamar, F., & Yadegaridehkordi, E. (2023). A Systematic Literature Review in Robotics Experiential Learning With Computational and Adversarial Thinking. *IEEE Access*, *11*(February), 44806–44827. https://doi.org/10.1109/ACCESS.2023.3249761

Ahmad, I., Niazy, M. S., Ziar, R. A., & Khan, S. (2021). Survey on IoT: Security threats and applications. *Journal of Robotics and Control (JRC)*, *2*(1), 42–46. https://doi.org/10.18196/jrc.2150

Aini, Q., Wasiqi, N. C., Alfajri, M. F., Purwati, Y. K., Ayu, I. K., Yasmin, N. A., Islam, U., Syarif, N., Jakarta, H., & Author, C. (2024). *RISK ASSESSMENT MATURITY LEVEL OF ACADEMIC INFORMATION SYSTEM USING ISO 27001 SYSTEM SECURITY ENGINEERING-*. *5*(2), 941–954.

Alsahafi, T., Halboob, W., & Almuhtadi, J. (2022). Compliance with Saudi NCA-ECC based on ISO/IEC 27001. *Tehnicki Vjesnik*, *29*(6), 2090–2097. https://doi.org/10.17559/TV-20220307162849

Apriany, A., Wibowo, A., Manajemen, S., Informasi, K., & Risiko, M. (2022). *Analysis of the Implementation of ISO 27001: 2022 and KAMI Index in Enhancing the Information Security Management System in Consulting Firms 1,2*.

Bouncken, R. B., Qiu, Y., Sinkovics, N., & Kürsten, W. (2021). Qualitative research: extending the range with flexible pattern matching. *Review of Managerial Science*, *15*(2), 251–273. https://doi.org/10.1007/s11846-021-00451-2

Fattah Ys, M. A., Parga Zen, B., & Wasitarini, D. E. (2024). Penerapan Sistem Manajemen Keamanan Informasi ISO 27001 pada Perpusnas RI dalam mendukung Keamanan Tata Kelola Teknologi Informasi. *Cyber Security Dan Forensik Digital*, *6*(2), 76–82. https://doi.org/10.14421/csecurity.2023.6.2.4190

Fauzia Anis Sekar Ningrum, Yudha Riwanto, Inggrid Yanuar Risca Pratiwi, & Muhammad Ainul Fikri. (2024). Analisis Keamanan Sistem Informasi Perguruan Tinggi Berbasis Indeks KAMI. *Jurnal Informatika Polinema*, *10*(3), 437–444. https://doi.org/10.33795/jip.v10i3.5154

Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., & Stantchev, V. (2016). A process framework for information security management. *International Journal of Information Systems and Project Management*, *4*(4), 27–47. https://doi.org/10.12821/ijispm040402

Hoshmand, M. O., Ratnawati, S., & Korespondensi, E. P. (2023). Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity. *Jurnal Sains Dan Teknologi*, *5*(2), 679–686. https://doi.org/10.55338/saintek.v5i2.2347

Indonesia, B. (2022). *Keamanan informasi, keamanan siber dan perlindungan privasi — Sistem manajemen keamanan informasi — Persyaratan*. *2022*.

Informasi, J., Darmawan, I., Mansyur, M. U., Imam, K. Z., & Syahdan, M. (2023). *Evaluasi Keamanan Privilege Terintegerasi JSON Web Token pada Sistem Informasi Akademik*. *5*(2), 6–7. https://doi.org/10.37034/jidt.v5i1.368

Jelita, L. D. A., Al Azam, M. N., & Nugroho, A. (2024). Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/EIC 27001:2022. *Jurnal SAINTEKOM*, *14*(1), 84–94. https://doi.org/10.33020/saintekom.v14i1.623

Karyati, J. A. dan C. M. (2023). *Perancangan Sistem Manajemen Keamanan*

Informasi (SMKI) Berdasarkan ISO 27001:2022 (Studi Kasus Data Center Dinas Komunikasi dan Informatika Kota Tangerang Selatan). *5*, 1–14. https://www.ncbi.nlm.nih.gov/books/NBK558907/

Khamil, D. I., Made, G., Sasmita, A., Agung, A., & Hary, N. (2022). *Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Kami 4 . 2 Dan ISO / IEC 27001 : 2013 (Studi Kasus : Diskominfo Kabupaten Gianyar)*. *9*(3), 1948–1960.

Kurniawan, A. W., & Salman, M. (2023). Recommendations for designing information security framework in government procurement of goods/services certification systems based on ISO 27001:2022. *Gema Wiralodra*, *14*(2), 804–809. https://doi.org/10.31943/gw.v14i2.477

Mardivta, H., & Herdiansyah, M. I. (2022). Pengelolaan Aset (Studi Kasus : Satuan Kerja Teknologi Informasi Pt . Bukit Asam , Tbk). *Jurnal Ilmiah MATRIK*, *24*(1), 1–9.

Mundt, M., & Baier, H. (2023). Enabling Protection Against Data Exfiltration by Implementing ISO 27001:2022 Update. *International Journal on Cybernetics & Informatics*, *12*(5), 43–59. https://doi.org/10.5121/ijci.2023.120505

Pujiani, F., & Bisma, R. (2024). *Strategi Optimalisasi Manajemen Konfigurasi untuk Keamanan Informasi Berdasarkan ISO / IEC 27001 : 2022*. *05*(03), 223–228.

Quchi, M. M., Hakimi, M., & Fazil, A. W. (2024). Human factors in cybersecurity: An in depth analysis of user centric studies. *Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID*, *3*(01), 20–33. https://doi.org/10.58471/esaprom.v3i01

Ramadan, R. A., Aboshosha, B. W., Alshudukhi, J. S., Alzahrani, A. J., El-Sayed, A., & Dessouky, M. M. (2021). Cybersecurity and Countermeasures at the Time of Pandemic. *Journal of Advanced Transportation*, *2021*(2003). https://doi.org/10.1155/2021/6627264

Rashid, M. H. U., Zobair, S. A. M., Chowdhury, M. A. I., & Islam, A. (2020). Corporate governance and banks' productivity: evidence from the banking industry in Bangladesh. *Business Research*, *13*(2), 615–637.

https://doi.org/10.1007/s40685-020-00109-x

Sakti, S., Listyanto, F. W., Damayanti, R. I., & Ningtyas, M. A. (2022). *Manajemen Risiko Keamanan Informasi Menggunakan Standar ISO 27001 : 2022 Studi Kasus Komisi Pemilihan Umum*. 1–12.

Saputri, S. N., Salisah, F. N., Maita, I., & Rozanda, N. E. (2024). *Penggunaan Metode FMEA dalam Penilaian Manajemen Risiko Keamanan Sistem Informasi Rumah Sakit*. 95–109.

Sinaga, R. (2024). Pengembangan Model Penilaian Kepatuhan Salah Satu Perguruan Tinggi Terhadap Standar ISO 27001:2022. *Jurnal Teknik Informatika Dan Sistem Informasi*, *9*(3), 381–394. https://doi.org/10.28932/jutisi.v9i3.6850

Sinaga, R., & Taan, F. (2024). Penerapan ISO/IEC 27001:2022 dalam Tata Kelola Keamanan Sistem Informasi: Evaluasi Proses dan Kendala. *Nuansa Informatika*, *18*(2), 46–54. https://doi.org/10.25134/ilkom.v18i2.205

Sontan Adewale Daniel, & Samuel Segun Victor. (2024). Emerging Trends in Cybersecurity for Critical Infrastructure Protection: a Comprehensive Review. *Computer Science & IT Research Journal*, *5*(3), 576–593. https://doi.org/10.51594/csitrj.v5i3.872

Surya, M., Setiawan, A., Safitri, E. M., Asyam, M., Taufiqurahman, T., & Pratama, M. A. (2023). *Analisis Manajemen Risiko Keamanan Sistem Informasi Rocketic . id menggunakan Metode OCTAVE dan FMEA Analysis of Information Security Risk Management in Rocketic . id using OCTAVE and FMEA Method*. *11*(3), 504–514. https://doi.org/10.26418/justin.v11i3.66628

Waruwu, M. (2023). Pendekatan Penelitian Pendidikan: Metode Penelitian Kualitatif, Metode Penelitian Kuantitatif dan Metode Penelitian Kombinasi (Mixed Method). *Bhineka Tunggal Ika: Kajian Teori Dan Praktik Pendidikan PKn*, *9*(2), 99–113. https://doi.org/10.36706/jbti.v9i2.18333

Yasarah Hisprastin*, 1, I. M. (2021). *Ishikawa Diagram dan Failure Mode Effect Analysis (FMEA) sebagai Metode yang sering digunakan dalam Manajemen Risiko Mutu di Industri*. *6*(1), 1–9.