# Analisis Kesiapan Dokumen Dan Pelaksanaan Kegiatan Keamanan Informasi Berdasarkan Iso27001:2022 Di Lembaga XYZ

1st Owen Caudinata
*S1 Sistem Informasi*
*Telkom University*
Bandung, Indonesia
owencaudinata@student.telkomuniversity.ac.id

2nd Umar Yunan Kurnia Septo Herdiyanto, S.T., M.T
*S1 Sistem Informasi*
*Telkom University*
Bandung, Indonesia
umaryunan@telkomuniversity.ac.id

3rd Rd. Rohmat Saedudin, S.T., M.T., Ph.D
*S1 Sistem Informasi*
*Telkom University*
Bandung, Indonesia
rdrohmat@telkomuniversity.ac.id

***Keamanan informasi adalah aspek krusial dalam menjaga kelangsungan dan kepercayaan sistem informasi, terutama dengan meningkatnya jumlah ancaman siber. LEMBAGA XYZ, sebagai lembaga yang menangani data sensitif, perlu memastikan kesiapan langkah-langkah keamanannya untuk memenuhi standar internasional. ISO 27001:2022 memberikan kerangka kerja untuk membangun, menerapkan, memelihara, dan terus meningkatkan Sistem Manajemen Keamanan Informasi (ISMS). Namun, banyak organisasi, termasuk LEMBAGA XYZ, menghadapi tantangan dalam menerapkan standar ini secara penuh karena adanya kesenjangan dalam dokumentasi dan proses operasional. Penelitian ini bertujuan untuk menganalisis kesiapan dokumentasi keamanan dan pelaksanaan kegiatan keamanan informasi di LEMBAGA XYZ berdasarkan ISO 27001:2022. Penelitian ini menggunakan pendekatan kualitatif dengan metode analisis kesenjangan dan penilaian checklist untuk mengevaluasi kerangka keamanan yang ada dengan persyaratan ISO. Hasil penelitian mengidentifikasi kesenjangan dalam dokumentasi, kebijakan, dan praktik keamanan yang perlu diperbaiki untuk mencapai kepatuhan penuh. Selain itu, rekomendasi diberikan untuk meningkatkan posisi keamanan LEMBAGA XYZ, memastikan manajemen risiko yang lebih baik dan kesiapan untuk sertifikasi.***

***Kata kunci — Keamanan Informasi, ISO 27001:2022, LEMBAGA XYZ, Analisis Kesenjangan, Penilaian Kepatuhan***

## I. PENDAHULUAN

Keamanan informasi kini menjadi krusial dalam menjaga keberlangsungan organisasi, terutama di tengah ancaman siber yang merugikan secara finansial dan reputasi. Serangan seperti *ransomware* dan *phishing* telah menyebabkan kerugian global lebih dari $1 triliun pada 2021, setara 1% GDP dunia [1]. Target serangan kini meluas dari individu hingga institusi besar.

ISO 27001 hadir sebagai standar internasional yang menyediakan kerangka kerja untuk mengelola keamanan informasi melalui ISMS, melindungi kerahasiaan, integritas, dan ketersediaan data. Standar ini membantu organisasi mengurangi risiko dan memenuhi regulasi yang ketat [2], serta meningkatkan ketahanan terhadap serangan siber.

Meski penting, implementasi ISO 27001 sering terkendala oleh kurangnya pemahaman. Berdasarkan penelitian, banyak perguruan tinggi di Indonesia masih berada di *Level* 2 dan 3 kematangan ISMS, menunjukkan kesenjangan keamanan. Area seperti Pengembangan Sistem (A14) dan Kepatuhan (A18) menunjukkan celah signifikan yang perlu diatasi [3]

ISO 27001 menyediakan kebijakan dan kontrol, termasuk pengelolaan data, pembatasan akses, serta perlindungan fisik dan lingkungan. Salah satu area krusial adalah A.5: Kebijakan Keamanan Informasi, yang membantu organisasi mengatasi ancaman dengan kebijakan yang terstruktur [3]. Implementasi ISMS yang efektif mendatangkan manfaat jangka panjang, termasuk membangun kepercayaan pelanggan. Melalui standar ini, organisasi dapat memperkuat reputasi dan memastikan kepatuhan terhadap regulasi seperti ISO27001, GDPR dan kerangka kerja lainnya [4].

## II. KAJIAN TEORI

Bab ini akan membahas berbagai landasan teori yang mendukung penelitian dan mencakup konsep-konsep utama yang relevan dengan ruang lingkup studi.

### A. *Information Security Management System* (ISMS)

*Information Security Management System* adalah pendekatan yang mengintegrasikan kebijakan, prosedur, dan kontrol untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi organisasi. Berbasis pada ISO 27001, ISMS bertujuan mengidentifikasi dan mengelola risiko terhadap informasi sensitif dengan menerapkan kontrol seperti pembatasan akses dan enkripsi. Pendekatan berbasis risiko ini memungkinkan organisasi untuk menilai dan mengurangi ancaman secara berkelanjutan [5].

### B. *International Organization for Standardization* (ISO)

*International Organization for Standardization* merupakan sebuah organisasi internasional yang memainkan peran penting dalam pengembangan standar global. Dalam jurnal *The Journal of Technology Transfer* disebutkan bahwa standar yang dikembangkan ISO tidak hanya mendukung inovasi dan efisiensi, tetapi juga menjadi alat strategis yang dapat dimanfaatkan oleh negara dan perusahaan untuk memperkuat daya saing mereka serta memengaruhi arah pengembangan teknologi di tingkat [6].

### C. ISO 27001:2022

ISO 27001:2022 adalah standar internasional untuk sistem manajemen keamanan informasi (*Information Security Management Systems*) yang secara luas diadopsi untuk memastikan kerahasiaan, integritas, dan ketersediaan informasi mereka. Standar ISO 27001 berfokus pada pendirian, penerapan, pemeliharaan, dan peningkatan berkelanjutan dari ISMS dalam suatu organisasi. Standar ini menyediakan kerangka kerja bagi organisasi untuk mengidentifikasi dan menilai risiko keamanan informasi, menetapkan tujuan dan kontrol keamanan, serta memantau dan meninjau efektivitas kontrol yang telah diterapkan [7].

D. *Gap Analysis*

*Gap Analysis* merupakan teknik yang digunakan untuk mengevaluasi kesenjangan antara kondisi terkini suatu sistem, proses, atau organisasi dengan kondisi yang diinginkan atau diharapkan. Analisis ini sering dilakukan dengan mengidentifikasi dan membandingkan praktik, metode, atau hasil terkini dengan yang diinginkan atau diperlukan agar sistem, proses, atau organisasi dapat berfungsi dengan baik [8].

E. *Penetration Testing*

*Penetration Testing* (Pentest) adalah pengujian keamanan yang meniru serangan siber untuk mengidentifikasi kerentanan suatu sistem atau jaringan sebelum dapat dimanfaatkan oleh musuh di dunia nyata. *Pentest* dapat dikategorikan sebagai serangan musuh semu oleh tim evaluasi yang bersahabat pada sistem komputer yang dimaksud untuk menemukan cara untuk menembus kontrol keamanan sistem, menembus perimeter keamanan perlindungan untuk memperoleh informasi sensitif, memperoleh layanan yang tidak sah, atau menyebabkan kerusakan pada sistem yang menolak layanan kepada pengguna yang sah [9].

## III. METODE

A. Kerangka Teoretis

Dalam penelitian ini, model konseptual yang digunakan mengacu pada *Design Science Research* (DSR) yang dikembangkan oleh Hevner, yang membagi proses penelitian ke dalam tiga komponen inti: *Environment*, *IS Research*, dan *Knowledge Base*. Ketiga komponen ini membentuk jalur sistematis yang menghubungkan permasalahan dunia nyata dengan solusi desain yang berlandaskan pada kajian ilmiah.

Komponen *Environment* merepresentasikan konteks eksternal dari organisasi yang menjadi objek studi. Ini mencakup pemetaan terhadap sumber daya manusia (*people*), struktur organisasi, infrastruktur teknologi, serta permasalahan yang telah terdefinisi dengan jelas. Faktor-faktor ini menjadi titik awal dalam mengidentifikasi kebutuhan bisnis dan tantangan yang dihadapi oleh ORGANISASI XYZ dalam menerapkan ISMS berbasis ISO 27001:2022.

Selanjutnya, komponen *IS Research* berfokus pada pengembangan artifact serta evaluasi dan justifikasi terhadap solusi yang diusulkan. Hal ini mencakup perancangan rekomendasi kontrol keamanan informasi, analisis kesenjangan terhadap standar ISO, serta validasi melalui studi kasus pada ORGANISASI XYZ. Proses ini memastikan bahwa solusi yang dikembangkan relevan dengan kondisi eksisting dan dapat diterapkan secara praktis.

Komponen ketiga, yaitu *Knowledge Base*, menyediakan landasan teoretis dan metodologis untuk penelitian. Komponen ini mencakup teori-teori fundamental dalam bidang keamanan informasi, tata kelola TI, dan transformasi digital, serta kerangka kerja ISO 27001:2022. Strategi penelitian yang digunakan mengombinasikan pendekatan *Design Science Research* dengan metode studi kasus, melalui pengumpulan data berupa wawancara semi-terstruktur dan telaah dokumen, serta analisis isi (*content analysis*) dalam menginterpretasi temuan [10].

B. Penyelesaian Masalah

Kerangka pemecahan masalah dalam penelitian ini mengintegrasikan dua pendekatan yang saling melengkapi: siklus *Plan–Do–Check–Act* (PDCA) dan metode MoSCoW. PDCA berfungsi sebagai siklus manajemen terstruktur untuk mendorong perbaikan berkelanjutan, sementara MoSCoW memberikan kerangka kerja prioritisasi untuk menentukan tindakan mana yang harus didahulukan berdasarkan tingkat urgensi dan dampaknya.


GAMBAR 1

1. *Plan* (Perencanaan)
   Identifikasi dan analisis gap antara kondisi eksisting dengan persyaratan ISO 27001:2022. Penetapan tujuan dan sasaran untuk menutup celah yang ada. Penyusunan rencana tindakan (*action plan*) berdasarkan hasil analisis gap, termasuk pembagian tugas, alokasi sumber daya, dan penjadwalan.
2. *Do* (Pelaksanaan)
   Implementasi rencana tindakan yang telah disusun, termasuk penyesuaian kebijakan, prosedur, dan kontrol keamanan informasi sesuai dengan standar baru. Memberikan pelatihan dan sosialisasi kepada seluruh pihak terkait untuk memastikan pemahaman yang mendalam mengenai perubahan yang dilakukan.
3. *Check* (Pemeriksaan)
   Melakukan audit internal untuk mengevaluasi efektivitas implementasi rencana tindakan. Memastikan seluruh elemen sistem manajemen keamanan informasi (ISMS) sesuai dengan persyaratan ISO 27001:2022.
4. *Act* (Tindak Lanjut)
   Melakukan tindakan perbaikan berdasarkan hasil audit dan evaluasi. Melakukan iterasi untuk memastikan peningkatan berkelanjutan dalam implementasi ISMS.


GAMBAR 2

Metode MoSCoW digunakan untuk memprioritaskan tindakan yang harus dilakukan selama proses persiapan sertifikasi. Metode ini mengklasifikasikan kebutuhan berdasarkan urgensi dan dampaknya sebagai berikut:

1. *Must Have* – Elemen kritis yang wajib ada untuk mencapai sertifikasi ISO 27001:2022. Tanpa elemen ini, sistem keamanan informasi tidak akan memenuhi standar yang ditetapkan. Contohnya termasuk kebijakan keamanan informasi yang terdokumentasi, identifikasi risiko, dan kontrol akses terhadap data sensitif.
2. *Should Have* – Elemen penting yang mendukung penerapan standar keamanan informasi secara efektif, namun tidak sepenuhnya wajib untuk keperluan sertifikasi. Contoh elemen ini meliputi sistem pemantauan yang lebih rinci, peningkatan pelatihan bagi karyawan, dan penguatan kapasitas infrastruktur keamanan.
3. *Could Have* – Elemen tambahan yang dapat meningkatkan efektivitas dan efisiensi sistem keamanan informasi, namun tidak memiliki dampak signifikan terhadap proses sertifikasi. Contohnya termasuk sistem pemantauan keamanan otomatis atau pengembangan dashboard analitik lanjutan untuk pelaporan insiden keamanan.
4. *Won't Have* (*for now*) – Elemen yang tidak relevan atau belum mendesak untuk diterapkan pada tahap awal implementasi. Elemen ini dapat dipertimbangkan di masa mendatang jika diperlukan, namun saat ini bukan merupakan prioritas. Contohnya seperti teknologi eksperimental atau fitur tambahan yang tidak secara langsung memengaruhi kepatuhan terhadap standar keamanan informasi.

C. Pengumpulan Data

TABEL 1

| Metode Pengumpulan | Jenis Data | Kegiatan | Alat |
|---|---|---|---|
| *Semi-structured interview* | Primer | Melakukan wawancara dengan serangkain topik pertanyaan yang telah tersusun untuk memenuhi kebutuhan penelitian dari pihak terkait secara langsung. | *Offline meeting* dan *online meeting* menggunakan *platform* seperti Google Meet/Zoom. |
| *Internal and External Document Triangulation* | Sekunder | Mengumpulkan dan mengkaji berbagai sumber data, seperti jurnal, artikel, dan dokumen terkait dengan Lembaga XYZ, dengan tujuan memperoleh referensi lebih lengkap dan mendalam. | Dokumen *internal* dan dokumen *eksternal*. |

## IV. HASIL DAN PEMBAHASAN

A. Hasil Penerapan Klausa

Berikut merupakan hasil penerapan SMKI berdasarkan analisis kondisi *eksisting* penerapan klausa ISO 27001:2022 pada Lembaga XYZ.

TABEL 2

| Judul Klausa | Status |
|---|---|
| Klausa 5 Nomor 2 | Belum Terpenuhi Secara Menyeluruh |
| Klausa 6.1.3 nomor 2 dan 3 | Belum Terpenuhi |
| Klausa 8 nomor 3 | Belum Terpenuhi Secara Menyeluruh |

Berdasarkan hasil analisis kondisi *eksisting* pada Lembaga XYZ dapat disimpulkan bahwa Lembaga XYZ telah secara efektif membangun, menerapkan, memelihara dan terus meningkatkan sistem manajemen keamanan informasi yang sesuai dengan standar ISO 27001:2022, namun terdapat 3 klausa yang belum terpenuhi.

B. Rekomendasi

Berikut merupakan rekomendasi yang diberikan penulis kepada LEMBAGA XYZ berdasarkan analisis gap dari kondisi *eksisting* terhadap penerapan kontrol ISO 27001:2022.

TABEL 3

| *Klausa* | Eksisting | Catatan |
|---|---|---|
| Klausa 5 Nomor 2 | SK No.12 Tahun 2023 | Policy untuk stakeholder external, diperlukan policy untuk stakeholder external, mungkin bisa digabung dengan SOP Walidata nantinya |
| Klausa 6.1.3 nomor 2 dan 3 | Belum ada | SoA / Master Data, dan Risk treatment. Belum adanya SoA atau master file yang dipadukan menjadi satu hingga terpadu serta langkah-langkah mitigasi risiko yang jelas |
| Klausa 8 nomor 3 | ITSA Web CSIRT LEMBAGA XYZ. | Implementasi perubahan pada ISMS. Perlunya evidence yang lebih kuat menunjukkan adanya perubahan ISMS yang berjalan |

1. Klausul 5 Nomor 2 – Peran Stakeholder Eksternal

LEMBAGA XYZ belum menetapkan peran keamanan informasi bagi pihak eksternal seperti vendor dan mitra kerja. Dokumen SK No.12 Tahun 2023 hanya mengatur aspek internal. Untuk memenuhi klausul ini, perlu disusun kebijakan pengelolaan stakeholder eksternal yang menetapkan tanggung jawab, standar keamanan minimum, serta alur komunikasi dan penanganan insiden. Dokumen pendukung seperti SOP vendor, MoU, dan formulir evaluasi pemasok juga perlu disiapkan. Kebijakan ini akan meningkatkan kepercayaan, memperjelas peran pihak ketiga, dan mendukung kelancaran audit.

2. Klausul 6.1.3 Nomor 2 & 3 – Statement of Applicability dan Risk Treatment Plan

LEMBAGA XYZ belum memiliki Statement of Applicability (SoA) maupun risk treatment plan. Hal ini menyebabkan status kontrol Annex A dan langkah mitigasi risiko tidak terdokumentasi dengan baik. Untuk memenuhi klausul ini, perlu dibuat SoA yang memuat status implementasi setiap kontrol dan alasan pengecualiannya, serta risk treatment plan yang menjelaskan mitigasi, penanggung jawab, dan tenggat waktu. Dokumen ini akan meningkatkan kepastian kontrol, konsistensi pelaksanaan, dan kesiapan audit sertifikasi.

3. Klausul 8 Nomor 3 – Operasionalisasi Kontrol Keamanan

Kontrol operasional dan manajemen perubahan belum terdokumentasi meskipun telah ada inisiatif dari CSIRT. Untuk memenuhi klausul ini, LEMBAGA XYZ perlu menyusun prosedur manajemen perubahan, mencatat aktivitas operasional keamanan, dan menyediakan bukti pelaksanaan seperti log perubahan, laporan audit, serta dokumentasi insiden. Langkah ini akan memperkuat pengendalian perubahan, meningkatkan respons terhadap insiden, dan mendukung keberlanjutan ISMS.

## V. KESIMPULAN

Berdasarkan hasil analisis, LEMBAGA XYZ telah memenuhi sebagian besar persyaratan ISO/IEC 27001:2022, terutama pada aspek kebijakan keamanan, struktur organisasi, dan pengelolaan aset. Namun, masih terdapat gap pada Klausul 5.2 (peran stakeholder eksternal), Klausul 6.1.3 (Statement of Applicability dan risk treatment plan), serta Klausul 8.3 (dokumentasi pengendalian operasional). Untuk mencapai kepatuhan penuh, diperlukan penyusunan kebijakan stakeholder eksternal, SoA, risk treatment plan, serta dokumentasi perubahan dan insiden. Langkah ini akan meningkatkan transparansi, efektivitas, dan kesiapan sertifikasi. Peneliti menyarankan integrasi checklist ISO 27001 dalam audit internal, serta pengembangan evaluasi lanjutan dengan pendekatan kuantitatif, perluasan objek ke instansi lain, dan pendalaman analisis kontrol Annex A serta manajemen risiko.

## REFERENSI


[1] A. Kokaji and A. Goto, "An analysis of economic losses from cyberattacks: based on input–output model and production function," *J Econ Struct*, vol. 11, no. 1, Dec. 2022, doi: 10.1186/s40008-022-00286-4.

[2] D. Taman, "Impacts of Financial Cybercrime on Institutions and Companies," vol. 8, no. 30, pp. 477–488, Feb. 2024, doi: 10.21608/ajahs.2024.341707.

[3] I. Mantra, A. A. Rahman, and H. Saragih, "Maturity Framework Analysis ISO 27001: 2013 on Indonesian Higher Education," 2020. [Online]. Available: www.sciencepubco.com/index.php/IJET

[4] M. Alshar'e, "CYBER SECURITY FRAMEWORK SELECTION: COMPARISION OF NIST AND ISO27001," *Applied computing Journal*, pp. 245–255, Feb. 2023, doi: 10.52098/acj.202364.

[5] Sarah Kuzankah Ewuga, Zainab Efe Egieya, Adedolapo Omotosho, and Abimbola Oluwatoyin Adegbite, "ISO 27001 IN BANKING: AN EVALUATION OF ITS IMPLEMENTATION AND EFFECTIVENESS IN ENHANCING INFORMATION SECURITY," *Finance & Accounting Research Journal*, vol. 5, no. 12, pp. 405–425, Jan. 2024, doi: 10.51594/farj.v5i12.684.

[6] K. Blind and M. von Laer, "Paving the path: drivers of standardization participation at ISO," *Journal of Technology Transfer*, vol. 47, no. 4, pp. 1115–1134, Aug. 2022, doi: 10.1007/s10961-021-09871-4.

[7] C. Daah, A. Qureshi, I. Awan, and S. Konur, "Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework," *Electronics (Switzerland)*, vol. 13, no. 5, Mar. 2024, doi: 10.3390/electronics13050865.

[8] C. Alordiah, "MIND THE GAP: EXPLORING EFFECTIVE STRATEGIES FOR CONDUCTING GAP ANALYSIS IN EDUCATIONAL STUDIES,"

2023. [Online]. Available: https://www.researchgate.net/publication/374420184

[9] S. Reddy Mamilla, "A Study of Penetration Testing Processes and Tools," 2021. [Online]. Available: https://scholarworks.lib.csusb.edu/etd/1220

[10] R. Alan, ; A R Vom Brocke, and J. Brocke, "Article 2 9-15-2023 Recommended Citation Recommended Citation Hevner," *Print) Journal of Information Systems Education*, vol. 34, no. 3, p. 264, 2023.