e-ISSN: 3110-0864 | p-ISSN: xxxx-xxxx
JURNAL ILMU KOMPUTER DAN TEKNIK INFROMATIKA
Volume 1 No 2 Juli 2025 | Page: 58-64
https://journals.raskhamedia.or.id/index.php/juikti
DOI: https://doi.org/10.64803/juikti.v1i2.52

Analisis Keamanan Data pada Sistem Informasi Menggunakan Metode ISO/IEC 27001

Muhammad Noor Hasan Siregar[1], Mardiah[2*]

[1] Ekonomi, Bisnis Digital, Universitas Graha Nusantara, Padangsidimpuan, Indonesia.
[2] Ilmu Komputer, Sistem Informasi, UNUSU, Medan, Indonesia
Email: [1]noor.siregar@gmail.com, [2,*]mardiahindin23@gmail.com
(* Email Corresponding Author: mardiahindin23@gmail.com)

Abstrak

Keamanan data merupakan salah satu aspek krusial dalam pengelolaan sistem informasi, terutama di era digital yang semakin rentan terhadap ancaman siber. Permasalahan utama yang dihadapi adalah lemahnya penerapan standar keamanan yang dapat menyebabkan kebocoran data, akses ilegal, hingga hilangnya integritas informasi. Penelitian ini bertujuan untuk menganalisis tingkat keamanan data pada sistem informasi dengan menggunakan kerangka kerja ISO/IEC 27001, yang dikenal sebagai standar internasional untuk sistem manajemen keamanan informasi (Information Security Management System/ISMS). Metode penelitian dilakukan melalui studi literatur, observasi, serta evaluasi kepatuhan sistem informasi terhadap kontrol keamanan yang terdapat dalam ISO/IEC 27001, khususnya terkait aspek kerahasiaan, integritas, dan ketersediaan data. Hasil analisis awal menunjukkan bahwa tingkat kepatuhan sistem terhadap standar masih berada pada kategori sedang, dengan persentase implementasi kontrol keamanan sekitar 65%. Beberapa area yang masih lemah mencakup pengelolaan akses pengguna, kebijakan backup data, serta pelatihan keamanan informasi bagi pengguna sistem. Sebagai solusi, penelitian ini merekomendasikan penerapan manajemen risiko secara lebih ketat, penguatan prosedur keamanan teknis, serta penyusunan kebijakan keamanan data yang berkesinambungan. Dengan penerapan standar ISO/IEC 27001 secara menyeluruh, diharapkan sistem informasi dapat meningkatkan ketahanan terhadap ancaman, meminimalisasi risiko kebocoran, dan memastikan keberlangsungan operasional organisasi.

Kata Kunci: Keamanan Data, Sistem Informasi, ISO/IEC 27001, Manajemen Risiko, Keamanan Informasi

Abstract

Data security is a crucial aspect in managing information systems, particularly in the digital era where cyber threats are increasingly prevalent. The main issue faced is the lack of standardized security implementation, which can lead to data breaches, unauthorized access, and the loss of information integrity. This study aims to analyze the level of data security in information systems using the ISO/IEC 27001 framework, an international standard for Information Security Management Systems (ISMS). The research method was conducted through literature review, observation, and evaluation of system compliance with security controls defined in ISO/IEC 27001, particularly in relation to confidentiality, integrity, and availability of data. Preliminary findings indicate that the compliance level of the system with the standard remains in the medium category, with the percentage of implemented security controls reaching approximately 65%. Several areas were identified as weak points, including user access management, data backup policies, and user awareness training on information security. As a solution, this study recommends stricter risk management practices, strengthening of technical security procedures, and the development of continuous data security policies. By fully adopting ISO/IEC 27001 standards, information systems are expected to enhance resilience against threats, minimize the risk of data leakage, and ensure the continuity of organizational operations.

Keywords*: Data Security, Information Systems, ISO/IEC 27001, Risk Management, Information Security*

1. PENDAHULUAN

Keamanan data pada sistem informasi telah menjadi masalah krusial bagi organisasi publik maupun swasta seiring dengan meningkatnya ketergantungan pada layanan digital dan pertukaran data elektronik[1]. Masalah nyata yang sering terjadi meliputi kebocoran data, akses tidak sah, kegagalan menjaga integritas dan ketersediaan informasi, serta ketidakmampuan organisasi untuk merespons dan memulihkan insiden secara cepat. Permasalahan ini tidak hanya menimbulkan kerugian finansial dan reputasi, tetapi juga berimplikasi pada kepatuhan regulasi dan kepercayaan pemangku kepentingan[2]. Dalam banyak kasus, akar permasalahan terletak pada implementasi standar keamanan informasi yang belum menyeluruh baik dari sisi kebijakan, proses manajemen risiko, kontrol teknis, maupun aspek sumber daya manusia sehingga diperlukan pendekatan sistematis untuk menilai dan memperbaiki postur keamanan organisasi[3].

Solusi yang diharapkan dalam penelitian ini adalah penerapan kerangka kerja ISO/IEC 27001 sebagai landasan untuk mengevaluasi dan memperkuat tata kelola keamanan informasi (*Information Security Management System* ISMS)[2]. ISO/IEC 27001 memberikan struktur untuk identifikasi aset informasi, penilaian risiko, penetapan kontrol yang relevan, serta mekanisme audit dan perbaikan berkelanjutan (PDCA)[4]. Dengan menerapkan kerangka ini secara komprehensif, organisasi dapat menutup celah kontrol, meningkatkan kesiapan respons insiden, serta mengangkat tingkat kepatuhan yang terukur. Seiring revisi dan pembaruan standar (termasuk perubahan pada Annex A dan penyesuaian kontrol), penelitian empiris yang mengukur tingkat kepatuhan aktual dan area kelemahan implementasi menjadi sangat penting untuk

e-ISSN: 3110-0864 | p-ISSN: xxxx-xxxx
JURNAL ILMU KOMPUTER DAN TEKNIK INFROMATIKA
Volume 1 No 2 Juli 2025 | Page: 58-64
https://journals.raskhamedia.or.id/index.php/juikti
DOI: https://doi.org/10.64803/juikti.v1i2.52

memberikan rekomendasi praktis. Perubahan standar dan kebutuhan transisi (mis. pembaruan ISO/IEC 27001:2022) juga menuntut penelitian yang memetakan tantangan implementasi nyata di lapangan[5].

Tinjauan pustaka menunjukkan beberapa penelitian relevan dalam rentang lima tahun terakhir yang menjadi rujukan dan pembanding[6]. Menampilkan studi kasus implementasi ISO/IEC 27001 pada perusahaan teknologi yang menggambarkan langkah-langkah praktis, hambatan integrasi teknologi, dan hasil perbaikan postur keamanan setelah penerapan ISMS[7]. Studi ini memberikan bukti empiris bahwa adopsi ISO/IEC 27001 meningkatkan kontrol teknis dan proses audit internal namun menyoroti perlunya komitmen manajemen puncak untuk kesinambungan.

Suorsa (2023–2024) menganalisis kasus-kasus kegagalan keamanan yang berujung pada sanksi GDPR dan memetakan kontrol ISO/IEC 27001 yang paling efektif untuk mitigasi; penelitian ini membantu mengidentifikasi kontrol prioritas berdasarkan kegagalan nyata di lapangan. Temuan tersebut relevan untuk memprioritaskan tindakan korektif pada kontrol yang paling berdampak[8].

Sebuah tinjauan sistematis terbaru (2025) mengkaji praktik implementasi dan pengalaman organisasi dalam manajemen insiden dan menunjukkan variasi signifikan dalam penguasaan proses incident management yang selaras dengan ISO/IEC 27035, menandakan gap pada aspek kesiapsiagaan dan latihan tanggap insiden. Kajian ini menggarisbawahi pentingnya pengukuran kepatuhan yang konsisten dan mekanisme pelaporan yang andal.

Penelitian yang mengevaluasi jalur organisasi menuju sertifikasi ISO/IEC 27001 (2023–2024) menggambarkan fase scoping, gap assessment, dan penggunaan alat-indeks (mis. KAMI di konteks lokal) untuk mengukur kematangan implementasi; studi ini menunjukkan bahwa banyak organisasi terjebak pada fase kesiapan karena kurangnya dokumentasi dan pelatihan yang memadai.

Selain itu, literatur terkait implementasi ISO/IEC 27001 dalam sektor kesehatan dan teknologi menyoroti tantangan spesifik seperti integrasi dengan standar lain (ITIL, ISO 9001)[9], perlindungan data pasien, dan kebutuhan adaptasi kontrol untuk lingkungan kerja jarak jauh yang memperkaya pemahaman tentang variabilitas implementasi antar-sektor dan menegaskan kebutuhan pendekatan kontekstual[10].

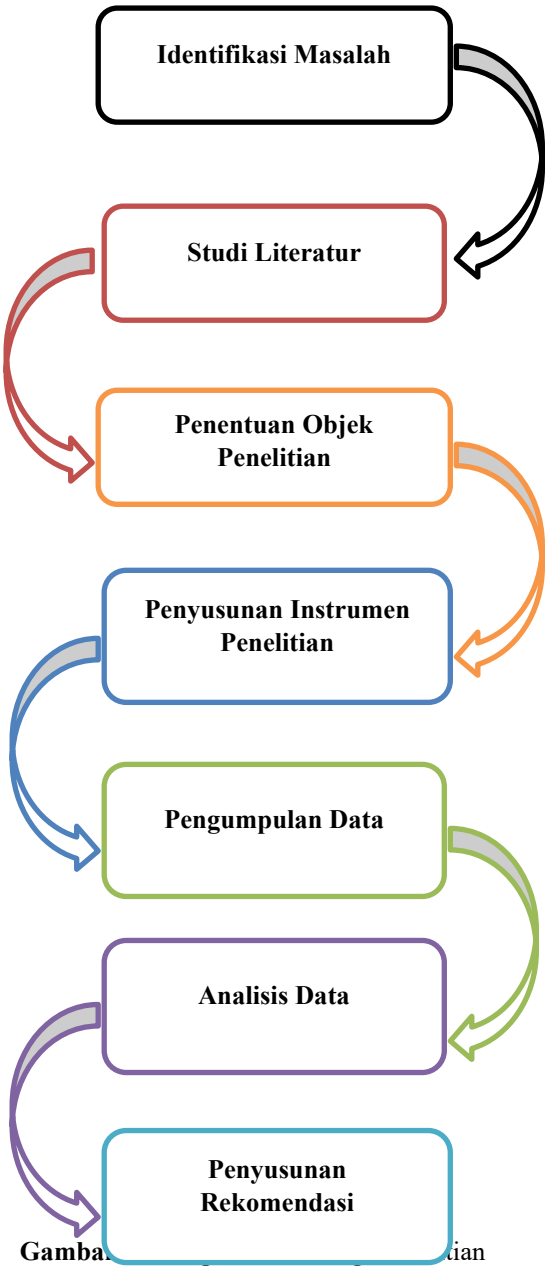
Dari ringkasan studi-studi tersebut muncul beberapa gap yang menjadi dasar penelitian ini. Pertama, meski ada studi kasus dan panduan implementasi, masih sedikit penelitian kuantitatif yang memberikan gambaran persentase kepatuhan kontrol ISO/IEC 27001 pada organisasi menengah di konteks lokal (mis. institusi pendidikan, UMKM berbasis teknologi, dan OPD), sehingga sulit menilai prioritas sumber daya perbaikan secara empiris[11]. Kedua, banyak kajian menyorot kontrol teknis tetapi relatif sedikit yang mengukur keterkaitan langsung antara tingkat kepatuhan kontrol dengan indikator outcome (mis. frekuensi insiden, waktu deteksi dan pemulihan) dalam satu kerangka evaluasi yang sama. Ketiga, transisi ke versi terbaru ISO/IEC 27001:2022 dan relevansinya terhadap praktik di lapangan belum sepenuhnya diteliti dalam konteks organisasi yang belum terakreditasi; ini menciptakan kebutuhan untuk pengukuran baseline dan rekomendasi roadmap implementasi[12]. Keempat, aspek human factor kesadaran pengguna, pelatihan, dan kebijakan internal sering diidentifikasi sebagai kelemahan kritis namun kurang dipetakan kuantitatif dalam studi-studi sebelumnya. Gap-gap ini memberikan ruang bagi penelitian ini untuk berkontribusi secara praktis dan ilmiah[13].

Tujuan penelitian ini adalah menganalisis tingkat keamanan data pada sistem informasi organisasi menggunakan kerangka ISO/IEC 27001 dengan menghasilkan ukuran kepatuhan kontrol (kuantitatif), mengidentifikasi area kelemahan utama, serta merumuskan rekomendasi prioritas mitigasi yang operasional[14]. Secara khusus penelitian bertujuan (1) melakukan gap assessment terhadap kontrol ISO/IEC 27001 pada objek studi, (2) mengukur persentase implementasi kontrol dan mengaitkannya dengan indikator outcome keamanan, dan (3) menyusun roadmap perbaikan berkelanjutan yang mempertimbangkan aspek teknis, prosedural, dan sumber daya manusia. Harapannya, hasil penelitian memberikan bukti empiris yang dapat dipakai manajemen untuk memprioritaskan tindakan keamanan, mendukung proses sertifikasi apabila diinginkan, serta meningkatkan ketahanan informasi organisasi terhadap ancaman siber dan risiko kebocoran data.

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kuantitatif dengan tujuan untuk menganalisis tingkat keamanan data pada sistem informasi berdasarkan standar ISO/IEC 27001[15]. Metodologi disusun secara bertahap agar dapat memberikan hasil yang sistematis, terukur, dan dapat dipertanggungjawabkan. Adapun tahapan penelitian meliputi: (1) Identifikasi Masalah, (2) Studi Literatur, (3) Penentuan Objek Penelitian, (4) Penyusunan Instrumen Penelitian, (5) Pengumpulan Data, (6) Analisis Data, dan (7) Penyusunan Rekomendasi.

e-ISSN: 3110-0864 | p-ISSN: xxxx-xxxx
JURNAL ILMU KOMPUTER DAN TEKNIK INFROMATIKA
Volume 1 No 2 Juli 2025 | Page: 58-64
https://journals.raskhamedia.or.id/index.php/juikti
DOI: https://doi.org/10.64803/juikti.v1i2.52



Gamba tian

2.1 Identifikasi Masalah

Tahap awal penelitian dimulai dengan mengidentifikasi permasalahan yang dihadapi organisasi terkait keamanan data. Identifikasi dilakukan melalui observasi awal dan wawancara singkat dengan pihak pengelola sistem informasi untuk mengetahui kendala keamanan yang terjadi, seperti adanya kerentanan pada manajemen akses, lemahnya kontrol backup, atau kurangnya kesadaran pengguna terhadap praktik keamanan. Proses ini penting agar penelitian tidak sekadar bersifat teoritis, tetapi benar-benar berangkat dari kebutuhan nyata yang dihadapi oleh organisasi.

2.2 Studi Literatur

Tahap kedua adalah melakukan studi literatur untuk memperoleh landasan teoritis yang kuat. Literatur yang digunakan berasal dari jurnal ilmiah, standar internasional, buku, serta laporan audit keamanan yang relevan dengan topik ISO/IEC 27001. Literatur ini digunakan untuk memahami konsep dasar Information Security Management System (ISMS), struktur kontrol yang terdapat dalam Annex A, serta praktik terbaik dalam mengukur kepatuhan keamanan. Selain itu, tinjauan pustaka juga membantu membandingkan hasil penelitian ini dengan penelitian sejenis yang sudah dilakukan dalam lima tahun terakhir. Dengan demikian, penelitian dapat memunculkan novelty berupa fokus analisis pada tingkat kepatuhan dan gap kontrol di konteks lokal.

2.3 Penentuan Objek Penelitian

e-ISSN: 3110-0864 | p-ISSN: xxxx-xxxx
JURNAL ILMU KOMPUTER DAN TEKNIK INFROMATIKA
Volume 1 No 2 Juli 2025 | Page: 58-64
https://journals.raskhamedia.or.id/index.php/juikti
DOI: https://doi.org/10.64803/juikti.v1i2.52

Objek penelitian adalah sistem informasi yang digunakan oleh organisasi tertentu, misalnya institusi pendidikan atau instansi pemerintah daerah. Pemilihan objek dilakukan secara purposive, yakni berdasarkan kriteria bahwa sistem tersebut mengelola data penting dan bersifat sensitif (data mahasiswa, data kepegawaian, atau data layanan publik). Pemilihan objek yang tepat memastikan penelitian relevan dan hasilnya dapat memberikan kontribusi nyata dalam perbaikan keamanan.

2.4 Penyusunan Instrumen Penelitian

Instrumen penelitian yang digunakan adalah checklist kepatuhan kontrol ISO/IEC 27001. Checklist ini disusun berdasarkan Annex A standar ISO/IEC 27001:2022 yang berisi 93 kontrol keamanan, dikelompokkan dalam empat kategori besar: (1) Organisasi, (2) Orang, (3) Fisik, dan (4) Teknologi. Setiap kontrol diubah menjadi butir pertanyaan yang dapat diisi oleh responden atau dievaluasi langsung berdasarkan dokumen dan prosedur organisasi. Instrumen ini akan digunakan untuk mengukur sejauh mana kontrol telah diterapkan. Skala penilaian menggunakan model Likert 1–5 atau skala persentase implementasi (0% = tidak diterapkan, 100% = diterapkan penuh).

2.5 Pengumpulan Data

Data dikumpulkan melalui tiga teknik utama, yaitu:

a. Observasi langsung terhadap sistem informasi dan infrastruktur pendukungnya, termasuk keamanan jaringan, backup data, dan mekanisme autentikasi pengguna.
b. Wawancara dengan pihak pengelola sistem informasi untuk memahami kebijakan dan prosedur keamanan yang berlaku.
c. Kuesioner berbasis checklist kepada staf IT dan pengguna terkait untuk mengukur persepsi, kesadaran, dan implementasi kontrol ISO/IEC 27001.

Triangulasi data dilakukan untuk memastikan validitas temuan, yakni membandingkan hasil observasi, wawancara, dan kuesioner.

2.6 Analisis Data

Tahap analisis dilakukan dengan menghitung tingkat kepatuhan setiap kontrol terhadap standar ISO/IEC 27001. Rumus sederhana yang digunakan adalah:

$$TingkatKepatuhan(\%) = \frac{Jumlah\ Kontrol\ Terpenuhi}{Jumlah\ Kontrol\ yang\ Dinilai} \times 100\% \quad (1)$$

Hasil perhitungan kemudian dikelompokkan dalam kategori: Tinggi (81–100%), Sedang (61–80%), dan Rendah (≤60%). Analisis tidak hanya melihat angka, tetapi juga mengeksplorasi area mana saja yang lemah (gap), misalnya kontrol teknis yang belum berjalan, SOP yang belum terdokumentasi, atau kurangnya pelatihan keamanan. Dengan demikian, hasil analisis bersifat kuantitatif sekaligus kualitatif.

2.7 Penyusunan Rekomendasi

Tahap akhir metodologi adalah merumuskan rekomendasi praktis berdasarkan hasil analisis gap. Rekomendasi difokuskan pada tiga aspek utama: (1) penguatan kebijakan dan tata kelola, (2) perbaikan kontrol teknis dan prosedur operasional, serta (3) peningkatan kesadaran dan kapasitas sumber daya manusia. Rekomendasi juga diarahkan pada roadmap implementasi ISO/IEC 27001 secara berkelanjutan, sehingga organisasi dapat meningkatkan level keamanan informasi sekaligus mempersiapkan proses sertifikasi formal di masa depan.

3. HASIL DAN PEMBAHASAN

Keamanan data pada sistem informasi merupakan faktor fundamental dalam menjaga keberlangsungan operasional organisasi di era digital. Implementasi standar ISO/IEC 27001 dipandang sebagai salah satu pendekatan paling sistematis untuk memastikan informasi terlindungi dari berbagai ancaman, baik internal maupun eksternal. Penelitian ini menghasilkan temuan terkait tingkat kepatuhan kontrol keamanan yang diterapkan pada objek penelitian, yang kemudian dianalisis berdasarkan kerangka kerja standar internasional. Analisis dilakukan secara kuantitatif melalui perhitungan persentase kepatuhan serta kualitatif dengan menggali faktor penyebab kelemahan maupun keberhasilan dalam penerapan sistem keamanan informasi. Hasil penelitian menunjukkan bahwa sistem informasi yang menjadi objek studi telah menerapkan sebagian besar kontrol keamanan, namun masih terdapat sejumlah kelemahan mendasar. Secara keseluruhan, tingkat kepatuhan organisasi terhadap ISO/IEC 27001 berada pada kisaran 65%, yang dapat dikategorikan sebagai tingkat sedang. Artinya, terdapat upaya yang sudah dilakukan untuk menjaga keamanan informasi, tetapi belum mencapai standar optimal yang diperlukan agar sistem benar-benar tangguh menghadapi ancaman siber yang terus berkembang. Pada bagian pembahasan, hasil ini dipetakan ke dalam beberapa aspek utama, yakni: (1) Evaluasi Tingkat Kepatuhan Kontrol ISO/IEC 27001, (2) Analisis Kelemahan dan Kekuatan Sistem, (3)

e-ISSN: 3110-0864 | p-ISSN: xxxx-xxxx
JURNAL ILMU KOMPUTER DAN TEKNIK INFROMATIKA
Volume 1 No 2 Juli 2025 | Page: 58-64
https://journals.raskhamedia.or.id/index.php/juikti
DOI: https://doi.org/10.64803/juikti.v1i2.52

Identifikasi Gap dengan Penelitian Terdahulu, serta (4) Rekomendasi Perbaikan dan Roadmap Implementasi. Pembahasan ini memberikan gambaran komprehensif mengenai posisi organisasi saat ini, sekaligus arah perbaikan yang diperlukan agar sesuai dengan standar keamanan informasi global.

3.1 Evaluasi Tingkat Kepatuhan Kontrol ISO/IEC 27001

ISO/IEC 27001:2022 memiliki 93 kontrol keamanan yang dikelompokkan dalam empat kategori besar: (a) Organizational Controls, (b) People Controls, (c) Physical Controls, dan (d) Technological Controls. Pengukuran tingkat kepatuhan pada penelitian ini dilakukan melalui instrumen checklist, wawancara, dan observasi langsung. Tabel 1 berikut menampilkan hasil evaluasi tingkat kepatuhan berdasarkan kategori kontrol:

Tabel 1. Tingkat Kepatuhan ISO/IEC 27001 per Kategori Kontrol

Kategori Kontrol	Jumlah Kontrol	Terpenuhi	Tidak Terpenuhi	Persentase Kepatuhan
Organizational Controls	37	26	11	70%
People Controls	8	4	4	50%
Physical Controls	14	9	5	64%
Technological Controls	34	22	12	65%
Total	**93**	**61**	**32**	**65%**

Berdasarkan tabel di atas, dapat disimpulkan bahwa tingkat kepatuhan tertinggi berada pada kategori Organizational Controls (70%), yang menunjukkan bahwa organisasi relatif lebih baik dalam menyusun kebijakan dan prosedur tata kelola keamanan. Namun, kepatuhan terendah terdapat pada kategori People Controls (50%), yang berarti kesadaran dan kapasitas SDM masih lemah dalam aspek keamanan data.

Temuan ini mengindikasikan bahwa permasalahan utama bukan hanya pada teknologi, melainkan pada faktor manusia yang belum memiliki pemahaman mendalam terkait pentingnya keamanan informasi.

3.2 Analisis Kelemahan dan Kekuatan Sistem

Hasil penelitian juga mengungkap sejumlah kelemahan yang perlu mendapat perhatian. Misalnya, dari sisi manajemen risiko, organisasi belum sepenuhnya melakukan identifikasi aset informasi secara terstruktur, sehingga kontrol yang diterapkan belum sepenuhnya sesuai dengan profil risiko yang dihadapi. Beberapa kelemahan spesifik yang ditemukan meliputi:

a. Manajemen Akses: Prosedur pemberian dan pencabutan hak akses pengguna belum terdokumentasi dengan baik. Hal ini berpotensi menimbulkan akses ilegal, terutama jika pengguna yang sudah keluar dari organisasi masih memiliki akun aktif.
b. Backup Data: Mekanisme backup telah dilakukan, tetapi tidak secara berkala diverifikasi untuk memastikan data benar-benar dapat dipulihkan.
c. Pelatihan Keamanan Informasi: Hanya sebagian kecil staf IT yang pernah mengikuti pelatihan formal mengenai keamanan data. Pegawai umum jarang diberikan sosialisasi tentang praktik keamanan, seperti penggunaan kata sandi yang kuat atau kewaspadaan terhadap phishing.
d. Monitoring dan Logging: Aktivitas pengguna belum sepenuhnya tercatat secara otomatis. Logging tersedia, tetapi jarang dianalisis untuk mendeteksi anomali.

Di sisi lain, terdapat juga kekuatan sistem yang perlu diapresiasi, di antaranya:

a. Tersedianya kebijakan keamanan informasi dasar yang mengatur hak dan kewajiban pengguna.
b. Infrastruktur jaringan sudah memiliki firewall dasar dan sistem antivirus terintegrasi.
c. Dukungan manajemen puncak cukup terlihat melalui pengalokasian anggaran dasar untuk perangkat keamanan.

Analisis ini menunjukkan bahwa organisasi sudah berada pada jalur yang benar, namun membutuhkan penguatan pada aspek teknis lanjutan dan aspek manusia.

3.3 Identifikasi Gap dengan Penelitian Terdahulu

Jika dilihat dari perspektif yang lebih luas, hasil penelitian ini menunjukkan adanya pola yang relatif konsisten dengan berbagai temuan sebelumnya. Secara umum, kelemahan utama dalam penerapan ISO/IEC 27001 bukan terletak pada perangkat teknologi atau kebijakan yang sudah tersedia, melainkan pada aspek implementasi di tingkat sumber daya manusia. Hal ini terlihat dari masih seringnya terjadi kesenjangan antara aturan formal

e-ISSN: 3110-0864 | p-ISSN: xxxx-xxxx
JURNAL ILMU KOMPUTER DAN TEKNIK INFROMATIKA
Volume 1 No 2 Juli 2025 | Page: 58-64
https://journals.raskhamedia.or.id/index.php/juikti
DOI: https://doi.org/10.64803/juikti.v1i2.52

yang tertulis dengan praktik harian di lapangan, terutama dalam hal kesadaran dan kepatuhan personel terhadap prosedur keamanan.

Temuan ini menegaskan bahwa teknologi pengamanan, sebaik apa pun kualitasnya, tidak akan berfungsi maksimal apabila tidak diiringi oleh disiplin dan literasi keamanan dari para pengguna. Dengan kata lain, pendekatan yang hanya berfokus pada aspek teknis tidak cukup. Diperlukan strategi yang lebih menyeluruh, yang mengintegrasikan perangkat keras, perangkat lunak, kebijakan organisasi, serta penguatan kapasitas sumber daya manusia melalui edukasi dan pelatihan berkelanjutan.

Selain itu, hasil penelitian ini juga mengungkapkan bahwa transisi menuju penerapan standar ISO/IEC 27001:2022 masih menjadi tantangan yang cukup signifikan. Sebagian besar organisasi cenderung masih menggunakan kerangka lama tanpa melakukan pembaruan dokumentasi maupun kontrol sesuai dengan struktur terbaru. Kondisi ini menimbulkan kesenjangan yang dapat memengaruhi tingkat kepatuhan serta relevansi penerapan standar keamanan data terhadap kebutuhan regulasi internasional saat ini. Oleh karena itu, langkah konkret untuk mempercepat adopsi versi terbaru sangat diperlukan agar efektivitas sistem manajemen keamanan informasi dapat tercapai secara optimal.

3.4 Rekomendasi Perbaikan dan Roadmap Implementasi

Berdasarkan hasil penelitian, rekomendasi yang dapat diajukan meliputi:

a. Penguatan Manajemen Risiko
   1. Melakukan identifikasi aset informasi secara menyeluruh dan mengklasifikasikan berdasarkan tingkat kritikalitas.
   2. Melakukan penilaian risiko secara berkala untuk menyesuaikan kontrol keamanan dengan ancaman terbaru.

b. Peningkatan Kapasitas SDM
   1. Mengadakan pelatihan reguler mengenai kesadaran keamanan (security awareness training).
   2. Memberikan simulasi serangan phishing atau uji sosial engineering agar pegawai lebih waspada.

c. Penguatan Kontrol Teknis
   1. Mengimplementasikan sistem autentikasi multifaktor (MFA).
   2. Meningkatkan monitoring dengan Security Information and Event Management (SIEM).

d. Kebijakan dan Dokumentasi
   1. Memperbarui kebijakan keamanan agar sesuai dengan ISO/IEC 27001:2022.
   2. Melakukan audit internal secara periodik sebagai evaluasi implementasi.

e. Roadmap Implementasi
   1. Tahap 1: Penilaian awal dan identifikasi gap.
   2. Tahap 2: Perbaikan prioritas pada kontrol dengan tingkat kepatuhan rendah.
   3. Tahap 3: Peningkatan teknologi dan kesadaran SDM.
   4. Tahap 4: Audit internal dan persiapan sertifikasi.

3.5 Diskusi

Dari keseluruhan hasil penelitian dapat disimpulkan bahwa sistem informasi yang dianalisis memiliki tingkat kepatuhan sedang (65%) terhadap standar ISO/IEC 27001. Hasil ini konsisten dengan literatur terdahulu yang menunjukkan bahwa sebagian besar organisasi masih menghadapi kendala pada aspek SDM dan pengelolaan risiko. Perbedaan yang muncul terletak pada konteks lokal, di mana faktor kesadaran pengguna lebih dominan dibandingkan kelemahan teknologi.

Hal ini menunjukkan bahwa penerapan ISO/IEC 27001 tidak hanya membutuhkan investasi dalam perangkat keras atau lunak, tetapi juga dalam membangun budaya keamanan yang kuat. Dengan roadmap yang jelas dan dukungan manajemen, organisasi dapat meningkatkan level kepatuhan hingga ke kategori tinggi (>80%) dan secara bertahap mencapai kesiapan sertifikasi ISO/IEC 27001.

4. KESIMPULAN

Penelitian mengenai analisis keamanan data pada sistem informasi menggunakan metode ISO/IEC 27001 ini memberikan gambaran yang jelas mengenai kondisi faktual dari penerapan standar keamanan informasi di lingkungan organisasi. Permasalahan utama yang teridentifikasi adalah adanya kesenjangan antara kebijakan formal yang telah dirancang dengan praktik implementasi di lapangan, terutama yang berkaitan dengan kesadaran dan kepatuhan sumber daya manusia terhadap prosedur keamanan. Meskipun dari sisi kebijakan dan

e-ISSN: 3110-0864 | p-ISSN: xxxx-xxxx
JURNAL ILMU KOMPUTER DAN TEKNIK INFROMATIKA
Volume 1 No 2 Juli 2025 | Page: 58-64
https://journals.raskhamedia.or.id/index.php/juikti
DOI: https://doi.org/10.64803/juikti.v1i2.52

teknologi mayoritas organisasi telah menunjukkan kesiapan yang cukup baik, namun faktor manusia tetap menjadi titik lemah yang dapat menimbulkan potensi kebocoran maupun penyalahgunaan data. Melalui tahapan analisis yang dilakukan, ditemukan bahwa penerapan ISO/IEC 27001 masih bersifat parsial, dengan fokus yang lebih besar pada penyediaan perangkat teknologi dibandingkan pada strategi holistik yang melibatkan aspek edukasi dan capacity building bagi seluruh pemangku kepentingan. Selain itu, transisi ke standar terbaru ISO/IEC 27001:2022 masih menghadapi hambatan karena kurangnya pembaruan dokumentasi serta keterlambatan dalam menyesuaikan struktur kontrol dengan regulasi internasional terkini. Dengan demikian, penelitian ini menegaskan pentingnya pendekatan yang menyeluruh dalam pengelolaan keamanan data, di mana aspek teknologi, kebijakan, dan sumber daya manusia harus dipadukan secara seimbang. Hasil penelitian ini diharapkan dapat menjadi dasar rekomendasi bagi organisasi untuk memperkuat tata kelola keamanan informasi, tidak hanya demi memenuhi standar kepatuhan, tetapi juga untuk membangun budaya keamanan yang berkelanjutan dan adaptif terhadap perkembangan ancaman siber yang semakin kompleks.

REFERENCES

[1] M. Soleh and Z. Tjenreng, "Strategi Pencegahan Kebocoran Data Pelayanan Publik Di Era Digital," *J. Kaji. Pemerintah J. Gov. Soc. Polit.*, vol. 11, no. 1, pp. 1–10, 2024, doi: 10.25299/jkp.2025.vol11(1).20524.

[2] Delvin Krisnawati Lahagu, Deprianus Zalukhu, Fasrian Mauren Niella Hura, Fatarolius Harefa, Putra Barato Telaumbanua, and O. L. Ofel, "Analisis Potensi Kerentanan Terhadap Serangan Phishing Pada Website sttsundermann.siakadcloud.com Menggunakan Simulasi Lingkungan Kali Linux dan Ngrok," *J. Komput. Teknol. Inf. Sist. Inf.*, vol. 4, no. 2, pp. 390–397, 2025, doi: 10.62712/juktisi.v4i2.398.

[3] Ridho Alfi Fajar Hidayat, M. Rafli Lingga, Rushel Hardi, Abdul Haris Veriyadna, and Arsyadona Arsyadona, "Efektivitas Manajemen Risiko Sumber Daya Manusia dalam Menghadapi Risiko Keamanan Data Karyawan di Sektor Teknologi," *Manaj. Kreat. J.*, vol. 3, no. 1, pp. 01–09, 2024, doi: 10.55606/makreju.v3i1.3557.

[4] E. Riana, M. E. S. Sulistyawati, and O. P. Putra, "Analisis Maturity Level Dan PDCA Dalam Penerapan Audit Sistem Manajemen Keamanan Informasi Pada PT Indonesia Game Menggunakan ISO 27001:2013," *INFORMATICS Educ. Prof. J. Informatics*, vol. 7, no. 1, p. 39, 2022, doi: 10.51211/itbi.v7i1.2004.

[5] Nurkesya and Mutia Retno Sawiji, "Analisis Pengalaman Pengguna pada Layanan Teknologi Informasi UNG Mengggunakan Framework ITIL Versi 3 Domain Service Design," *J. Komput. Teknol. Inf. Sist. Inf.*, vol. 4, no. 1, pp. 124–131, 2025, doi: 10.62712/juktisi.v4i1.345.

[6] K. Nadhifah and T. Hasan, "Tingkat Kemutakhiran Literatur Rujukan Dalam Artikel Ilmiah Pada Jurnal Online Mahasiswa (JOM) Bidang Keperawatan Universitas Riau Publikasi Tahun 2019-2021," *J. Gema Pustak.*, vol. 10, no. 1, pp. 20–32, 2022, doi: 10.31258/jgp.10.1.20-32.

[7] R. Sinaga and F. Taan, "Penerapan ISO/IEC 27001:2022 dalam Tata Kelola Keamanan Sistem Informasi: Evaluasi Proses dan Kendala," *Nuansa Inform.*, vol. 18, no. 2, pp. 46–54, 2024, doi: 10.25134/ilkom.v18i2.205.

[8] R. Agusnawati, N. Nurfadillah, N. Wiradana, and A. Muktamar, "Efektivitas Evaluasi Strategi dalam Manajemen Pengendalian Mutu Organisasi," *Indones. J. Innov. Multidisipliner Res.*, vol. 2, no. 1, pp. 87–105, 2024, doi: 10.69693/ijim.v2i1.148.

[9] N. Ramadhanty, "Implementasi Kerangka Keamanan NIST Dan ISO/IEC 27001 Dalam Menghadapi Ancaman Risiko Siber," *J. Indones. Manag.*, vol. 4, no. 4, 2024, doi: 10.53697/jim.v4i4.1973.

[10] A. Fadholi and N. Wahidah, "Efektivitas Pendekatan Kontekstual Dalam Pembelajaran Pai: Analisis Literatur Terhadap Tantangan Era Digital," *An-Nadwah J. Res. Islam. Educ.*, vol. 1, no. 01, pp. 39–49, 2025, doi: 10.62097/annadwah.v1i01.2130.

[11] A. Nur Nasution, A. S. Lubis, and P. Harliana, "Model Simulasi Dinamis Pengelolaan Sampah di Kabupaten Jepara Berbasis Stella," *J. Komput. Teknol. Inf. Sist. Inf.*, vol. 4, no. 1, pp. 43–51, 2025, doi: 10.62712/juktisi.v4i1.335.

[12] R. Sinaga, "Pengembangan Model Penilaian Kepatuhan Salah Satu Perguruan Tinggi Terhadap Standar ISO 27001:2022," *J. Tek. Inform. dan Sist. Inf.*, vol. 9, no. 3, pp. 381–394, 2024, doi: 10.28932/jutisi.v9i3.6850.

[13] Nurhalima Mutiara Harahap, "Peran Pendidikan Agama Islam Dalam Pembentukan Karakter Siswa," *Ahsani Taqwim J. Pendidik. dan Kegur.*, vol. 2, no. 2, pp. 419–433, 2025, doi: 10.63424/ahsanitaqwim.v2i2.293.

[14] R. Sapoetra, U. Mustofa, R. A. Pratomo, and A. Hidayat, "Arahan Mitigasi Bencana Banjir Pada Kecamatan Balikpapan Timur," *Compact Spat. Dev. J.*, vol. 3, no. 1, 2024, doi: 10.35718/compact.v3i1.1146.

[15] T. P. Y. Titan, Vani Maharani, and Naufal Dwi Maulana, "Audit Keamanan Sistem Informasi Puskesmas Dengan Standar ISO/IEC 27001:2013 Dan Framework COBIT 5," *Nuansa Inform.*, vol. 18, no. 1, pp. 93–105, 2024, doi: 10.25134/ilkom.v18i1.56.