p_ISNN: 2776-7418 e-ISSN 2746-508X
JIKI (JURNAL ILMU KOMPUTER DAN INFORMATIKA)
Vol. 7 No. 1, Juli, 2026, Hal. 95-102

ANALISIS KEAMANAN SISTEM INFORMASI BERDASARKAN STANDAR ISO 27001 PADA JARINGAN KLINIK KRESNA

Willy Adriati[1] , Dedi Irawan[2], Gunayanti Kemalasari Siregar[3]
[1,2,3] S1 Ilmu Komputer, Fakultas Ilmu Komputer, Universitas Muhammadiyah Metro

[1,2,3]Jl. Gatot Subroto No.100, Yosodadi, Kec. Metro Timur, Kota Metro, Lampung 34381
[1]adriatiwilly0@gmail.com, [2]dedi.mti@gmail.com, [3]gunayanti2017@gmail.com

Abstrak *:* Kemajuan teknologi informasi mendorong organisasi kesehatan untuk memastikan keamanan data dan sistem informasi yang digunakan. Klinik Kresna Medical Center telah menerapkan sistem informasi berbasis jaringan client-server untuk mendukung layanan kesehatan. Namun, insiden peretasan yang mengakibatkan gangguan operasional menunjukkan adanya kelemahan dalam pengelolaan keamanan informasi. Penelitian ini bertujuan menilai kesesuaian kebijakan keamanan informasi Klinik Kresna dengan standar ISO 27001, mengukur tingkat kematangan (maturity level) keamanan, mengidentifikasi kerentanan jaringan, serta memberikan rekomendasi perbaikan. Penelitian menggunakan metode studi kasus dengan pendekatan kualitatif melalui observasi, wawancara, dan dokumentasi, serta audit keamanan informasi berbasis ISO 27001. Penilaian dilakukan menggunakan model maturity level pada lima klausul ISO 27001, yaitu keamanan sumber daya manusia, manajemen aset, keamanan fisik dan lingkungan, manajemen komunikasi dan operasi, serta pengendalian akses. Analisis dilakukan dengan siklus Plan–Do–Check–Act (PDCA). Hasil penelitian menunjukkan bahwa tingkat kematangan keamanan informasi di Klinik Kresna berada pada kategori menengah, dengan beberapa kebijakan telah diterapkan namun belum optimal, khususnya pada pengelolaan aset, kontrol akses, dan perlindungan jaringan dari ancaman eksternal. Ditemukan kerentanan pada infrastruktur jaringan yang berpotensi dimanfaatkan pihak tidak bertanggung jawab. Rekomendasi yang diberikan meliputi perbaikan kebijakan keamanan, peningkatan prosedur teknis, pelatihan sumber daya manusia, dan penguatan sistem pengendalian akses.

Kata Kunci : Keamanan Informasi, ISO 27001, Maturity Level, Audit Sistem Informasi.

Abstract: *Advances in information technology encourage healthcare organizations to ensure the security of their data and information systems. Kresna Medical Center has implemented a client-server network-based information system to support healthcare services. However, a hacking incident that resulted in operational disruptions indicates weaknesses in information security management. This study aims to assess the compliance of Kresna Clinic's information security policy with the ISO 27001 standard, measure its security maturity level, identify network vulnerabilities, and provide recommendations for improvement. The study used a case study method with a qualitative approach through observation, interviews, and documentation, as well as an ISO 27001-based information security audit. The assessment was conducted using a maturity level model for five ISO 27001 clauses: human resource security, asset management, physical and environmental security, communication and operations management, and access control. The analysis was conducted using the Plan–Do–Check–Act (PDCA) cycle. The results indicate that Kresna Clinic's information security maturity level is in the medium category, with several policies implemented but not optimal, particularly in asset management, access control, and network protection from external*

threats. Vulnerabilities were found in the network infrastructure that could potentially be exploited by irresponsible parties. Recommendations provided include improving security policies, enhancing technical procedures, training human resources, and strengthening access control systems..

Keywords: *Information Security, ISO 27001, Maturity Level, Information System Audit.*

PENDAHULUAN

Perkembangan teknologi informasi yang sangat pesat telah membawa dampak signifikan terhadap berbagai bidang, termasuk layanan kesehatan. Sistem informasi menjadi komponen penting untuk mendukung operasional dan manajemen organisasi, dengan tujuan menghasilkan data yang akurat, relevan, dan tepat waktu. Namun, seiring dengan manfaat yang ditawarkan, terdapat pula risiko yang mengancam keamanan data, seperti pencurian informasi, kebocoran data, hingga peretasan sistem. Hal ini menuntut adanya pengelolaan keamanan informasi yang baik, termasuk pengujian dan evaluasi sistem secara berkala. Klinik Kresna Medical Center, sebagai salah satu penyedia layanan kesehatan di Kabupaten Lampung Timur, telah mengimplementasikan sistem informasi berbasis jaringan client-server untuk menunjang pelayanan pasien. Meskipun demikian, hasil wawancara menunjukkan adanya insiden peretasan yang memanfaatkan teknik phishing, yang menyebabkan gangguan pada komputer administrasi dan menimbulkan kekhawatiran terkait privasi serta keamanan data pasien. Kondisi ini menjadi latar belakang pentingnya penelitian untuk mengevaluasi keamanan sistem informasi di Klinik Kresna berdasarkan standar ISO 27001, yang merupakan standar internasional dalam manajemen keamanan informasi.

Permasalahan yang diangkat dalam penelitian ini meliputi empat hal utama, yaitu bagaimana kebijakan keamanan informasi di Klinik Kresna dibandingkan dengan standar ISO 27001, sejauh mana tingkat kematangan (maturity level) penerapan keamanan sistem informasi, kerentanan jaringan yang terdeteksi dari hasil pengujian, serta rekomendasi perbaikan yang tepat untuk meningkatkan keamanan sistem dan jaringan. Tujuan penelitian ini adalah menilai kesesuaian kebijakan keamanan informasi dengan standar ISO 27001, mengukur tingkat kematangan penerapan keamanan sistem, mengidentifikasi kerentanan jaringan, serta memberikan rekomendasi yang relevan dan aplikatif. Secara teoritis, kajian ini berlandaskan pada konsep sistem informasi, keamanan informasi, keamanan jaringan, arsitektur jaringan komputer, audit sistem informasi, serta prinsip dan klausul dalam ISO/IEC 27001:2013 yang memuat kebijakan, pengelolaan aset, kontrol akses, keamanan fisik dan lingkungan, hingga manajemen insiden keamanan.

Rencana pemecahan masalah dilakukan melalui metode studi kasus yang mencakup observasi langsung, wawancara dengan pihak terkait, serta analisis dokumen kebijakan dan infrastruktur sistem. Audit keamanan dilaksanakan menggunakan kerangka ISO 27001 dengan pendekatan model maturity level untuk mengukur implementasi setiap kontrol keamanan. Hasil temuan akan dianalisis guna merumuskan rekomendasi strategis dan teknis yang dapat diterapkan untuk meningkatkan keamanan sistem informasi. Penelitian ini juga mengacu pada studi terdahulu yang membahas penerapan ISO 27001 pada sektor layanan publik dan kesehatan, yang menunjukkan bahwa standar ini mampu membantu organisasi meminimalkan risiko keamanan informasi secara efektif. Diharapkan hasil penelitian ini tidak hanya bermanfaat bagi Klinik Kresna Medical Center dalam meningkatkan keamanannya, tetapi juga berkontribusi pada pengembangan dan pendayagunaan ilmu komputer, khususnya

di bidang manajemen keamanan informasi dan jaringan.

KAJIAN PUSTAKA DAN LANDASAN TEORI

Definisi Analisis

Analisis adalah proses sistematis untuk menyelidiki, menguraikan, dan memahami suatu peristiwa atau masalah dengan memecahnya ke dalam bagian-bagian kecil guna menemukan fakta, hubungan antarbagian, serta memperoleh pemahaman menyeluruh. Tujuannya tidak hanya menjelaskan fenomena, tetapi juga mencari akar masalah melalui langkah-langkah seperti pengamatan, evaluasi, dan pembuktian untuk menghasilkan solusi atau wawasan yang mendalam.

Keamanan Informasi

Keamanan informasi merupakan upaya melindungi aset informasi dari ancaman yang dapat mengakibatkan kerugian, baik dalam bentuk kehilangan data, kerusakan sistem, atau penyalahgunaan (Pattiradjawane dkk., 2023; Puriwigati & Buana, 2020). Sistem Manajemen Keamanan Informasi (SMKI) seperti ISO 27001 menjadi kerangka acuan untuk memastikan kelangsungan bisnis dan meminimalkan risiko.

Sistem Informasi

Sistem informasi adalah kombinasi antara teknologi informasi dan tindakan manusia untuk mengelola, memproses, dan menghasilkan informasi yang relevan bagi pengguna (Ladjamudin; Listiani dkk., 2020). Pada Klinik Kresna, sistem informasi digunakan untuk pengelolaan data pasien, rekam medis, dan proses administrasi.

Keamanan Jaringan

Keamanan jaringan bertujuan mencegah, mengenali, dan mengatasi ancaman yang mengganggu operasi jaringan komputer (Akbar dkk., 2021; Saputro dkk., 2020). Prinsip keamanan jaringan mengacu pada CIA: Confidentiality, Integrity, dan Availability.

Jaringan Komputer

Jaringan komputer adalah kumpulan perangkat yang saling terhubung untuk berbagi data dan sumber daya (Fathinuddin dkk., 2023; Ardhiansyah dkk., 2020). Pada Klinik Kresna digunakan jaringan client-server untuk menghubungkan komputer administrasi dengan server utama.

ISO/IEC 27001

ISO/IEC 27001 adalah standar internasional untuk SMKI yang mengatur pengelolaan keamanan informasi melalui 14 klausul, 35 objektif kontrol, dan 144 kontrol keamanan. Standar ini fleksibel dan dapat disesuaikan dengan kebutuhan organisasi (Meyliana dkk., 2020).

Model PDCA (Plan-Do-Check-Act)

PDCA digunakan dalam implementasi SMKI untuk memastikan adanya perbaikan berkelanjutan (Arnason & Willet, 2008).

- Plan: merencanakan kebijakan dan prosedur keamanan.
- Do: menerapkan kebijakan dan kontrol.
- Check: mengevaluasi efektivitas kontrol.
- Act: melakukan tindakan perbaikan.

METODE

Metode penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus yang difokuskan pada sistem informasi dan jaringan di Klinik Kresna Medical Center. Penelitian dilaksanakan di Kabupaten Lampung Timur dengan waktu pelaksanaan mengikuti tahapan observasi, wawancara, dan dokumentasi terhadap pengelola sistem informasi, administrasi, serta pihak terkait lainnya. Data primer diperoleh melalui observasi langsung terhadap infrastruktur jaringan dan sistem yang digunakan, wawancara untuk menggali informasi kebijakan keamanan, serta dokumentasi dari arsip dan catatan resmi klinik. Data sekunder diperoleh melalui studi pustaka terhadap buku, jurnal, dan referensi terkait keamanan informasi, jaringan komputer, audit sistem informasi, dan standar ISO/IEC 27001:2013. Analisis dilakukan menggunakan model maturity level yang diadopsi dari ISO 27001 untuk

menilai tingkat kematangan penerapan kontrol keamanan, dengan proses pengolahan data meliputi identifikasi kebijakan, pengukuran tingkat implementasi, evaluasi kerentanan jaringan, serta perumusan rekomendasi perbaikan keamanan sistem informasi dan jaringan.

HASIL DAN PEMBAHASAN

Hasil Penelitian

Penelitian ini dilakukan di Klinik Kresna Medical Center, yang menggunakan sistem informasi berbasis client-server untuk pengelolaan data pasien dan rekam medis. Evaluasi keamanan dilakukan dengan standar ISO/IEC 27001 menggunakan model PDCA (Plan–Do–Check–Act).

Tahap Plan

1) Identifikasi aset: Aset utama meliputi server web, database rekam medis, aplikasi klinik, dan perangkat workstation administrasi. Aset pendukung meliputi perangkat jaringan (router, switch, fiber optic), CCTV, printer, dan proyektor.
2) Penilaian nilai aset: Dilakukan scoring berdasarkan kepentingan, kerentanan, dan dampak kerusakan. Database dan server web mendapat nilai tertinggi karena menyimpan data sensitif pasien.
3) Perumusan kebijakan awal: Merancang rancangan kebijakan keamanan berdasarkan klausul ISO 27001 yang dipilih.

Tahap Do

- Audit keamanan: Dilakukan pengukuran tingkat kematangan (*maturity level*) pada lima klausul ISO 27001:

1) Klausul 7 – Keamanan Sumber Daya Manusia
2) Klausul 8 – Pengelolaan Aset
3) Klausul 11 – Keamanan Fisik dan Lingkungan
4) Klausul 12 – Keamanan Operasi
5) Klausul 13 – Keamanan Komunikasi
6) Pengujian kerentanan jaringan: Menggunakan perangkat lunak seperti Wireshark untuk memonitor lalu lintas data, pemeriksaan konfigurasi perangkat jaringan, dan pengecekan akses perangkat.

- Temuan:

1) Backup data belum berjalan secara terjadwal.
2) Beberapa perangkat jaringan memiliki password default.
3) Transfer data antar perangkat belum sepenuhnya terenkripsi.

Tahap Check

- Analisis maturity level:

1) Rata-rata maturity level: 2–3 (kategori *cukup*).
2) Klausul dengan nilai terendah: Keamanan SDM dan Keamanan Operasi.
3) Klausul dengan nilai relatif baik: Pengelolaan Aset.

- Kesenjangan dengan standar:

1) Tidak adanya pelatihan keamanan rutin.
2) Tidak adanya dokumentasi kebijakan keamanan formal.
3) Pengelolaan kerentanan teknis belum terstruktur.

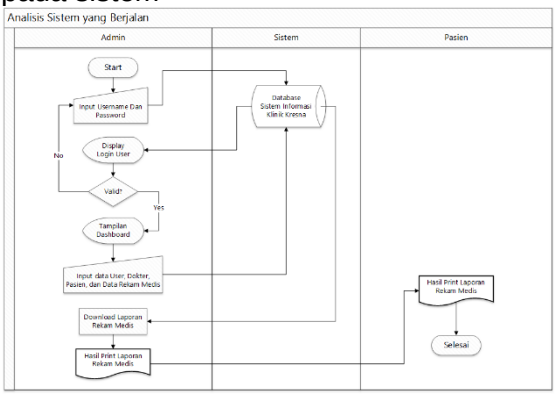
Tahap Act

1) Rekomendasi teknis: Implementasi firewall dan VPN, enkripsi end-to-end untuk data sensitif, serta penggunaan autentikasi ganda pada akses server.
2) Rekomendasi administratif: Penyusunan SOP keamanan informasi, penetapan jadwal pelatihan, dan audit internal berkala setiap 6 bulan.

Flowchart

Proses dimulai dengan admin memasukkan username dan password untuk login ke sistem. Jika informasi login tidak valid, sistem akan menampilkan ulang halaman login. Setelah login berhasil, admin diarahkan ke dashboard utama, yang menyediakan fitur untuk mengelola data, seperti input data user, dokter, pasien, dan rekam medis. Data yang dikelola ini disimpan dalam database sistem informasi klinik. Admin juga dapat mengunduh laporan rekam medis, yang kemudian bisa dicetak sesuai kebutuhan.

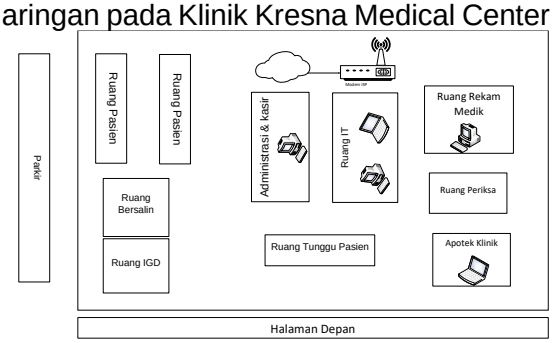
Proses ini berakhir ketika laporan berhasil dicetak, menunjukkan penyelesaian tugas pada sistem



Gambar 1. Flowchart Sistem yang berjalan

Denah Topologi jaringan

Berikut adalah gambaran denah topologi jaringan pada Klinik Kresna Medical Center



Gambar 2. Denah Topologi jaringan

Aset Utama

aset utama yang diidentifikasi oleh penulis di Klinik Kresna Medical Center

No	Nama Aset	Jenis	Penjelasan	Lokasi
1	*Database* ERM (Elektronik Rekam Medik)	Informasi	*Database* berisi data sistem Informasi ERM	Klinik Kresna Medical Center

Tabel 1. Aset utama

Aset Pendukung

aset pendukung yang diidentifikasi penulis pada Klinik Kresna Medical Center di Taman Negeri, Way Bungur, Lampung Timur

No	Nama Aset	Jenis	Penjelasan	Lokasi
1	Desktop (*Personal Computer*)	Hardware	Komputer yang dipakai oleh karyawan	Klinik Kresna Medical Center
2	Server WEB	Hardware	Digunakan pada Web KLINIK KRESNA untuk mengakses Web data KLINIK KRESNA	Klinik Kresna Medical Center
3	WHM *(Web Host Manager)*	Software	Tools yang digunakan untuk mengelola akun cPanel	Klinik Kresna Medical Center
4	Windows 10	Software	Operating system yang digunakan pada komputer karyawan	Klinik Kresna Medical Center
5	Microsoft Office 2013	Software	Pengolah data yang digunakan pada komputer karyawan	Klinik Kresna Medical Center
6	CCTV	Fasilitas Pendukung	kamera pengintai yang dapat merekam gambar dan suara	Klinik Kresna Medical Center
7	Printer	Fasilitas Pendukung	Hardware output yang memiliki fungsi sebagai alat pencetak menggunakan media kertas	Klinik Kresna Medical Center
8	Proyektor	Fasilitas Pendukung	Hardware output yang memiliki fungsi sebagai alat yang ada di layar monitor menjadi tampil di layar besar	Klinik Kresna Medical Center
9	Fiber Optic	Jaringan	Kabel jaringan yang dapat mentransmisi data melalui media cahaya	Klinik Kresna Medical Center
10	Switch	Jaringan	Perangkat yang berfungsi sebagai alat penghubung antar komputer	Klinik Kresna Medical Center
11	Wi-Fi	Jaringan	Berfungsi untuk komunikasi atau transfer program dan data	Klinik Kresna Medical Center
12	Router	Jaringan	Perangkat yang berfungsi menghubungkan beberapa jaringan yang sama atau berbeda	Klinik Kresna Medical Center

Tabel 2. Aset Pendukung

Nilai Aset = NC+NI+NA

di mana NC, NI, dan NA mewakili nilai dari kerahasiaan, keutuhan, dan ketersediaan aset tersebut.

No	Nama Aset	Nilai Confidentiality (NC)	Nilai Integrity (NI)	Nilai Availability (NA)	Nilai Aset
1	Database ERM (Elektronik Rekam Medik)	2	1	3	**6**

Tabel 3. Nilai Aset Utama

No	Nama Aset	Nilai Confidentiality (NC)	Nilai *Integrity (NI)*	Nilai Availability (NA)	Nilai Aset
1	*Desktop (PC)*	1	3	1	**5**
2	*Server* WEB	2	2	3	**7**
3	WHM (*Web Host Manager*)	3	2	3	**8**
4	*Windows* 10	1	3	1	**5**
5	*Microsoft Office 2013*	1	3	1	**5**
6	*CCTV*	2	3	3	**8**
7	*Printer*	2	4	1	**7**
8	Proyektor	2	1	2	**5**
9	*Fiber Optic*	3	4	3	**10**
10	*Switch*	3	4	3	**10**
11	*Wi-Fi*	2	3	1	**6**
12	*Router*	3	4	3	**10**

Tabel 4. Nilai Aset Pendukung

Pemilihan Objektif Kontrol dan Kontrol Keamanan Berdasarkan ISO 27001

Tahap selanjutnya setelah penulis melakukan pengukuran terhadap besarnya

risiko yang ada pada aset milik Klinik Kresna Medical Center adalah memilih tindakan atau kontrol yang dapat mengurangi nilai risiko yang sudah diukur sebelumnya. Dalam pemilihan objektif kontrol dan kontrol keamanan pada penelitian ini, penulis mengacu kepada objektif kontrol dan kontrol yang terdapat pada ISO 27001 yang telah disesuaikan dengan insiden yang pernah terjadi sebelumnya pada Klinik kresna medical center. Di bawah ini merupakan objektif kontrol dan kontrol keamanan yang penulis gunakan:

Klausul	Objektif Kontrol	Kontrol Keamanan
7. Keamanan Sumber Daya Manusia	7.1 Sebelum Bekerja	7.1.1 Penyaringan
	7.2 Selama Bekerja	7.2.1 Tanggung Jawab Manajemen
		7.2.2 Kesadaran keamanan informasi,pendidikan dan pelatihan
8. Manajemen Aset	8.1 Tanggung Jawab Untuk Aset	8.1.1 Inventarisasi Aset
		8.1.2 Kepemilikan Aset
	8.2 Klasifikasi Informasi	8.2.1 Klasifikasi Informasi
9. Kontrol Akses	9.1 Kebutuhan Bisnis terhadap Kontrol Akses	9.1.1 Kebijakan Kontrol Akses
		9.1.2 Akses ke jaringan dan layanan jaringan
11. Keamanan Fisik dan Lingkungan	11.1 Area Aman	11.1.2 Kontrol Entri fisik
		11.1.3 Mengamankan kantor, ruangan, dan fasilitas
		11.1.4 Pengamanan terhadap ancaman eksternal dan lingkungan
	11.2 Peralatan	11.2.2 Utilitas Pendukung
		11.2.3 Keamanan Kabel
		11.2.4 Pemeliharaan Peralatan
12 Keamanan Operasi	12.2 Perlindungan dari *Malware*	12.2.1 Kontrol terhadap *Malware*
	12.3 *Backup*	12.3.1 *Backup* Informasi
13 Keamanan Komunikasi	13.1 Manajemen Keamanan Jaringan	13.1.1 Kontrol Jaringan

Tabel 5. Objektif Kontrol dan Kontrol keamanan

Tahapan *Act*

Tahapan yang dilakukan setelah mengukur *maturity level* dari tiap-tiap objektif kontrol serta kontrol keamanan pada Klinik kresna medical center yaitu melakukan Penelusuran bukti terhadap pernyataan-pernyataan yang ada pada kontrol keamanan. Penelusuran bukti ini berguna untuk mencocokkan nilai *maturity level* yang sudah diberikan oleh beberapa responden dalam kuisioner dengan kondisi sebenarnya yang ada pada Klinik kresna medical center.

Setelah tahap penelusuran bukti selesai dilakukan, maka langkah terakhir adalah memberikan rekomendasi bagi Klinik kresna medical center untuk dapat mempebaiki serta meningkatkan kontrol keamanan yang sesuai dengan standar ISO 27001. Ringkasan perhitungan nilai rata-rata *maturity level* dari seluruh klausul yang ada akan dijelaskan di bawah ini.

Klausul	*Maturity Level*
Klausul 7 Keamanan Sumber Daya Manusia	1.75
Klausul 8 Manajemen Aset	1.6
Klausul 9 Kontrol Akses	1.25
Klausul 11 Keamanan Fisik dan Lingkungan	1.48
Klausul 12 Keamanan Operasi	1.05
Klausul 13 Keamanan Komunikasi	1.6
Total	**8.73**
Rata-Rata	**1.45**

Tabel 6. Nilai Maturity Level Seluruh Klausul

KESIMPULAN

Kebijakan keamanan informasi di Klinik Kresna telah mengikuti standar ISO 27001 dengan baik, namun masih terdapat celah, khususnya dalam menghadapi ancaman keamanan siber modern, sehingga penerapannya perlu diperketat untuk mengurangi risiko kebocoran data dan serangan siber. Sistem keamanan informasi di Klinik Kresna memiliki tingkat kematangan yang moderat atau standar, di mana beberapa aspek telah diterapkan dengan baik, tetapi masih diperlukan penguatan dalam praktik audit serta pembaruan kebijakan secara berkala. Selain itu, hasil audit keamanan mengungkap adanya beberapa kerentanan dalam jaringan, terutama pada aspek enkripsi data dan kontrol akses, yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab jika tidak segera ditangani dengan langkah mitigasi yang tepat.

Berdasarkan hasil penelitian yang telah dilakukan mengenai Analisis Keamanan Sistem Informasi Berdasarkan Standar ISO 27001, dapat disimpulkan beberapa hal sebagai berikut:

1) Penerapan Keamanan Informasi Berbasis ISO 27001. Penelitian ini menunjukkan bahwa standar ISO 27001 dapat digunakan sebagai acuan yang efektif dalam menilai dan meningkatkan sistem keamanan informasi suatu organisasi. Standar ini

membantu dalam identifikasi risiko keamanan, penerapan kontrol yang tepat, serta evaluasi kematangan sistem keamanan informasi.

2) Penilaian Tingkat Kematangan Keamanan Informasi. Melalui model maturity level, penelitian ini berhasil mengukur tingkat kesiapan dan kematangan keamanan informasi di organisasi yang diteliti. Hasil penelitian menunjukkan bahwa ada aspek yang telah memenuhi standar, namun masih terdapat beberapa celah yang perlu ditingkatkan untuk mencapai tingkat keamanan yang lebih optimal.
3) Identifikasi Kerentanan dalam Keamanan Jaringan. Penelitian ini menemukan adanya kerentanan dalam sistem jaringan yang dapat berpotensi menjadi celah keamanan bagi pihak yang tidak bertanggung jawab. Identifikasi kerentanan ini menjadi langkah awal dalam penguatan sistem keamanan berbasis ISO 27001.
4) Rekomendasi Berbasis Hasil Audit dan Pengujian Keamanan. Berdasarkan hasil audit keamanan informasi, penelitian ini memberikan rekomendasi yang dapat digunakan untuk meningkatkan tingkat keamanan sistem informasi. Rekomendasi ini mencakup aspek keamanan sumber daya manusia, pengelolaan aset, keamanan fisik dan lingkungan, manajemen komunikasi dan operasi, serta pengendalian akses yang merupakan bagian dari standar ISO 27001.
5) Kontribusi Penelitian terhadap Pengembangan Keamanan Informasi . Secara akademik, penelitian ini memberikan wawasan yang lebih mendalam tentang pentingnya keamanan informasi dalam suatu organisasi. Selain itu, penelitian ini juga membuktikan bahwa penerapan standar ISO 27001 dapat menjadi solusi yang sistematis dalam meningkatkan ketahanan sistem terhadap ancaman siber dan risiko keamanan lainnya.

Kesimpulan ini menunjukkan bahwa penelitian yang dilakukan telah menjawab rumusan masalah dan mencapai tujuan yang telah ditetapkan, yakni menilai sistem keamanan informasi, mengidentifikasi tingkat kematangan sistem, menemukan kerentanan yang ada, serta memberikan rekomendasi untuk peningkatan keamanan informasi sesuai standar ISO 27001.

REFERENSI

[1] Afriantoro, I., Islami, N. A., Yahya, A., Hadikristanto, W., & others. (2023). Peningkatan Kompetensi Guru Dan Siswa Melalui Pelatihan Jaringan Komputer Pada Siswa SMK Islam Darurrohman Sukawangi Kabupaten Bekasi. VIDHEAS: Jurnal Nasional Abdimas Multidisiplin, 1(1), 114–122.

[2] Akbar, M., Agung, T. A., Marcellino, I. I., & Fauzi, A. (2021). Analisis Keamanan Jaringan Komputer Pada Sekolah Menengah Atas Negeri 04 Bandung. Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI), 4(4), 258–264.

[3] Republik Indonesia. (2014). Undang-Undang Republik Indonesia Nomor 5 Tahun 2014 Tentang Aparatur Sipil Negara. Algiffary, A., Herdiansyah, M. I., & Kunang, Y. N. (2023). Audit Keamanan Sistem Informasi Manajemen Rumah Sakit Dengan Framework COBIT 2019 Pada RSUD Palembang BARI. Journal of Applied Computer Science and Technology, 4(1), 19–26.

[4] Amala, R., Mewengkang, A., & Djamen, A. C. (2023). Analisis dan Perancangan Jaringan Komputer di

SMK Negeri 2 Bitung. Edutik: Jurnal Pendidikan Teknologi Informasi dan Komunikasi, 3(2), 260-269.

[5] Ansori, Y. Z., Budiman, I. A., & Nahdi, D. S. (2019). Islam Dan Pendidikan Multikultural. Jurnal Cakrawala Pendas, 5(2), 110–115. https://doi.org/10.31949/jcp.v5i2.1370 Ardiansyah, Risnita, & Jailani, M. S. (2023). Teknik Pengumpulan Data Dan Instrumen Penelitian Ilmiah Pendidikan Pada Pendekatan Kualitatif dan Kuantitatif. Jurnal IHSAN : Jurnal Pendidikan Islam, 1(2), 1–9. https://doi.org/10.61104/ihsan.v1i2.57

[6] Ardhiansyah, M., Noris, S., & Andrianto, R. (2020). Jaringan Komputer. Pamulang: Unpam Press.

[7] Arnason, Sigurjon T. and Willett, Keith D. 2008. How to Achieve 27001 Certification: An Example of Applied Compliance Management. Florida: Auerbach Publications.

[8] Aspriyono, H., & Susanto, A. (2024). Jaringan komputer dan perkembangannya. Penerbit Andi.7] Arnason, Sigurjon T. and Willett, Keith D. 2008. How to Achieve 27001 Certification: An Example of Applied Compliance Management. Florida: Auerbach Publications.

[9] Azizah, N. (2019). Audit Sistem Informasi Menggunakan Framework COBIT 4.1 Pada E-Learning UNISNU Jepara. Simetris: Jurnal Teknik Mesin, Elektro dan Ilmu Komputer, 8(1), 377–382. [10] Bagono, B. J., & others. (2022). Optimalisasi Jaringan Wide Area Network Menggunakan Software Defined Network Viptela. Jurnal Sibernetika, 7(2), 49–61.