e-*ISSN 2548-6438*
p-ISSN 2614-7173

EVALUASI KEAMANAN SISTEM INFORMASI AKADEMIK DI STMIK JAYAKARTA BERDASARKAN ISO/IEC 27001:2022

EVALUATION OF ACADEMIC INFORMATION SYSTEM SECURITY BASED ON ISO/IEC 27001:2022

Desiani Zalukhu [1], Verdi Yasin [2], Akmal Budi Yulianto [3]
[1]Program Studi Sistem Informasi
Sekolah Tinggi Manajemen Informatika dan Komputer Jayakarta
Email: 24565001@stmik.jayakarta.ac.id

Abstrak

Meningkatnya penggunaan sistem informasi akademik di perguruan tinggi menuntut perhatian serius terhadap aspek keamanan informasi. Penelitian ini bertujuan untuk mengevaluasi tingkat kesesuaian keamanan sistem informasi akademik di STMIK Jayakarta dengan mengacu pada standar ISO/IEC 27001:2022. Ruang lingkup evaluasi mencakup identifikasi aset informasi, penilaian risiko berdasarkan potensi ancaman dan dampak, serta analisis kesenjangan terhadap delapan klausul utama ISO/IEC 27001:2022. Metode yang digunakan adalah pendekatan *Plan-Do-Check-Act (PDCA)* dengan dukungan *checklist* standar dan analisis risiko berbasis CIA (*Confidentiality, Integrity, Availability*). Hasil penelitian menunjukkan bahwa dari sepuluh aset yang dianalisis, lima aset tergolong berisiko tinggi dan lima berisiko sedang. Selain itu, ditemukan ketidaksesuaian pada empat klausul utama, yaitu 5.2 (kebijakan keamanan informasi), 6.1.2 (perencanaan penilaian risiko), 9.2 (audit internal), dan 9.3 (tinjauan manajemen). Penelitian ini menyimpulkan bahwa implementasi keamanan sistem informasi akademik di STMIK Jayakarta masih perlu ditingkatkan untuk mencapai kesesuaian penuh terhadap standar ISO/IEC 27001:2022. Berdasarkan temuan tersebut, direkomendasikan penerapan kontrol keamanan tambahan berupa penyusunan daftar risiko formal, strategi mitigasi terdokumentasi, pelaksanaan audit berkala, serta perbaikan dokumentasi evaluasi manajemen.

Kata Kunci: Sistem Informasi Akademik, Keamanan Informasi, ISO/IEC 27001, Analisis Kesenjangan

Abstract

The increasing use of academic information systems in higher education demands serious attention to information security. This study aims to evaluate the level of security conformity of academic information systems at STMIK Jayakarta

regarding the ISO/IEC 27001: 2022 standard. The evaluation scope includes identifying information assets, risk assessment based on potential threats and impacts, and gap analysis against the eight main clauses of ISO/IEC 27001:2022. The method used is the Plan-Do-Check-Act (PDCA) approach with a standard checklist and CIA-based risk analysis (Confidentiality, Integrity, Availability). The results showed that five of the ten assets analysed were classified as high risk and five as medium risk. In addition, non-conformities were found in four main clauses, namely 5.2 (information security policy), 6.1.2 (risk assessment planning), 9.2 (internal audit), and 9.3 (management review). This study concludes that the implementation of academic information system security at STMIK Jayakarta still needs to be improved to achieve full compliance with the ISO/IEC 27001: 2022 standard. Based on these findings, it is recommended to implement additional security controls in the form of formal risk register preparation, documented mitigation strategies, periodic audits, and improved management evaluation documentation.

Keywords: Academic Information System, Information Security, ISO/IEC 27001, Gap Analysis

PENDAHULUAN

Meningkatnya ketergantungan institusi pendidikan tinggi terhadap sistem informasi akademik (SIA) menuntut perhatian serius terhadap aspek keamanan informasi. Sistem ini tidak hanya memproses data administratif, tetapi juga menyimpan aset informasi penting seperti data mahasiswa, nilai, kurikulum, dan dokumen akademik lainnya. Keamanan informasi dalam konteks ini mencakup perlindungan terhadap kerahasiaan, integritas, dan ketersediaan data akademik. Namun, berbagai penelitian menunjukkan bahwa penerapan sistem keamanan informasi di sektor pendidikan masih menghadapi tantangan signifikan, mulai dari lemahnya kontrol kebijakan, kurangnya prosedur tanggap insiden, hingga belum optimalnya manajemen risiko[1],[2].

ISO/IEC 27001:2022 merupakan standar internasional yang digunakan untuk merancang, menerapkan, dan mengevaluasi sistem manajemen keamanan informasi (SMKI). Standar ini menekankan pendekatan berbasis risiko serta penguatan kontrol keamanan yang disesuaikan dengan karakteristik organisasi[3]. Dalam konteks pendidikan tinggi, penerapan ISO/IEC 27001 terbukti relevan untuk menjaga keandalan layanan digital yang menjadi tulang punggung sistem akademik modern. Studi sebelumnya menunjukkan bahwa tingkat kesiapan keamanan informasi pada sistem akademik masih belum sepenuhnya memenuhi standar, terutama pada aspek pengelolaan aset dan mitigasi ancaman[4].

Berbagai pendekatan telah diterapkan dalam mengevaluasi keamanan informasi akademik, seperti metode Failure Mode and Effect Analysis (FMEA)[5], audit berbasis framework COBIT 5[6], serta pemanfaatan indeks evaluatif seperti KAMI versi 4.2[4]. Selain itu, adopsi alat bantu audit seperti Computer-Assisted Audit Tools and Techniques (CAATTs) dinilai mampu meningkatkan efisiensi proses evaluasi keamanan[7]. Untuk mendukung perbaikan berkelanjutan, siklus manajemen mutu Plan-Do-Check-Act (PDCA) juga banyak digunakan sebagai pendekatan sistematis dalam evaluasi keamanan informasi yang sesuai dengan prinsip ISO[2],[6].

Penelitian ini secara spesifik bertujuan untuk mengevaluasi sistem keamanan informasi akademik pada salah satu perguruan tinggi swasta di Indonesia dengan mengacu pada standar ISO/IEC 27001:2022 dan menggunakan pendekatan PDCA sebagai kerangka evaluasi. Evaluasi dilakukan melalui identifikasi aset, penilaian risiko, audit kesesuaian terhadap 93 kontrol ISO, analisis kesenjangan, dan penyusunan rekomendasi pengendalian keamanan. Fokus utama dari ruang lingkup penelitian ini adalah sistem informasi akademik sebagai objek evaluasi, dengan batasan pada aspek keamanan informasi digital dan pengelolaan risikonya.

Berdasarkan kajian literatur, diketahui bahwa ancaman siber dalam sektor pendidikan di Indonesia terus meningkat seiring adopsi teknologi informasi, namun upaya mitigasi terhadap risiko tersebut belum dilakukan secara menyeluruh[8],[9]. Oleh karena itu, penting dilakukan analisis keamanan yang menyeluruh dan terstruktur terhadap sistem akademik dengan mengacu pada standar internasional. Harapannya, penelitian ini dapat memberikan gambaran tingkat kesiapan keamanan sistem informasi akademik, mengidentifikasi celah implementasi, serta menghasilkan rekomendasi kontrol keamanan yang relevan bagi institusi pendidikan di Indonesia[10].

LANDASAN TEORI

ISO/IEC 27001:2022

ISO/IEC 27001 merupakan standar global yang mengatur persyaratan dalam penerapan sistem manajemen keamanan informasi (SMKI). Standar ini mencakup kebijakan keamanan informasi, perencanaan penilaian risiko, kontrol teknis dan prosedural, serta audit dan tinjauan manajemen secara berkala[3]. Penerapan membantu organisasi mengelola dan melindungi aset informasi secara sistematis[5].

Audit Keamanan Informasi

Audit keamanan informasi adalah proses sistematis untuk menilai kesesuaian kebijakan dan kontrol keamanan terhadap standar seperti ISO/IEC 27001. Beberapa penelitian menunjukkan bahwa banyak institusi pendidikan di Indonesia masih memiliki tingkat audit internal yang rendah, serta kurangnya dokumentasi formal dan minimnya evaluasi berkala[3][11]. Audit juga dapat diintegrasikan dengan kerangka kerja lain seperti COBIT untuk meningkatkan tata kelola TI[12][13].

Implementasi ISO/IEC27001

Berbagai studi meneliti kesiapan institusi pendidikan dalam mengadopsi ISO/IEC 27001. Beberapa menggunakan pendekatan ISO/IEC 27005 dan FMEA untuk mengevaluasi risiko informasi[11][6]. Temuan menunjukkan adanya kelemahan dalam identifikasi aset, kontrol risiko, dan dukungan manajemen[5][14]. Penyesuaian kebijakan keamanan dengan kondisi lokal dan dokumentasi formal juga menjadi faktor penting dalam keberhasilan implementasi[11]

Faktor Penentu Keberhasilan Keamanan Informasi

Keamanan informasi tidak hanya bergantung pada teknologi, tetapi juga pada proses bisnis, kebijakan internal, dan peran sumber daya manusia[15]. Praktik manajemen layanan TI seperti ITIL dapat mendukung keberlanjutan kontrol keamanan[16]. Keterlibatan manajemen, pelatihan staf, serta budaya keamanan turut memengaruhi efektivitas implementasi standar keamanan.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode audit sistem informasi berdasarkan kerang kerja ISO 27001:2022[11]. Tahapan penelitian ini mengikuti pendekatan PDCA (Plan-Do-Check-Act) yang digunakan untuk mengevaluasi keamanan sistem informasi.

Tahap *Plan*

Tahap *plan* merupakan fase awal dalam evaluasi, yaitu dengan menyusun kerangka kerja evaluasi dan menetapkan ruang lingkup sistem yang akan dianalisis. Fokus evaluasi diarahkan pada delapan klausul utama ISO/IEC 27001:2022 yang relevan dengan lingkungan sistem informasi akademik, yaitu:

1. Kebijakan keamanan informasi (5.2)
2. Manajemen risiko (6.1.2)
3. Kontrol operasional (8.1, 8.2)
4. Pemantauan dan evaluasi (9.1, 9.3)
5. Perbaikan berkelanjutan (10.2)

Berikut tabel aset informasi yang telah diidentifikasi

Tabel 1. Aset Informasi

Aset utama	Aset pendukung
Database akademik	*Labtop/PC*
Website Akademik	Sistem operasi
Server hosting	UPS
Data mahasiswa dan dosen	*Switch*/*router* jaringan
Akun admin sistem	*Firewall*

Do

Tahap ini mencakup proses evaluasi lapangan, yang melibatkan pengumpulan data dan penilaian risiko, meliputi:Wawancara mendalam dan observasi langsung pada pengelolaan sistem informasi akademik, Analisis dokumen pendukung, kebijakan, dan arsip teknis yang berkaitan, Identifikasi ancaman dan kerentanan terhadap aset informasi, Penilaian risiko dilakukan dengan metode Confidentiality-Integrity-Availability (CIA) dan pendekatan kualitatif berdasarkan tingkat dampak dan kemungkinan ancaman. Pada tahap ini penulis menentukan nilai CIA aset informasi untuk menentukan Tingkat prioritas aset.

Tabel 2. Nilai CIA Aset Informasi

Nama Aset	C	I	A	Nilai
Database akademik	4	3	4	11
Website Akademik	2	3	3	8
Server hosting	3	4	4	11
Data mahasiswa dan dosen	4	3	3	10
Akun admin sistem	4	4	3	11
Laptop/PC	2	4	3	9
Sistem operasi	3	4	4	11
UPS	1	2	4	7
Switch/*router* jaringan	2	3	4	9
Firewall	3	4	4	11

Seluruh proses evaluasi dirangkum dalam alur kerangka evaluasi yang menggambarkan tahapan mulai identifikasi aset hingga penyusunan rekomendasi kontrol keamanan.

Gambar 1. Kerangka Evaluasi

Check

Tahapan ini bertujuan untuk menilai sejauh mana implementasi kontrol keamanan telah sesuai dengan standar ISO/IEC 27001:2022. Penilaian dilakukan dengan menggunakan checklist audit yang telah disusun mengacu pada delapan klausul utama ISO/IEC 27001:2022. Masing-masing klausul dinilai berdasarkan tiga kategori:

Y = sesuai

T = tidak sesuai

P = Partial

Evaluasi dilakukan berdasarkan bukti dokumentasi, observasi sistem, dan konfirmasi dari pihak pengelola sistem informasi. Hasil dari tahap ini

menjadi dasar untuk melakukan analisis kesenjangan (gap analysis) antara praktik yang berjalan dengan standar keamanan yang ditetapkan.

Act

Berdasarkan hasil analisis kesesuaian dan temuan gap, disusun rekomendasi peningkatan kontrol keamanan informasi. Rekomendasi tersebut disesuaikan dengan referensi kontrol keamanan pada Annex A ISO/IEC 27001:2022, yang mencakup: Penetapan kebijakan keamanan informasi. Prosedur manajemen keamanan risiko, Mekanisme audit internal dan evaluasi berkala, Program peningkatan kesadaran keamanan informasi, Rencana tindakan korektif untuk setiap klausul yang belum sesuai.

HASIL DAN PEMBAHASAN

Penilaian Risiko Aset Informasi

Tahap awal dalam proses evaluasi keamanan informasi adalah melakukan identifikasi aset dan penilaian Tingkat risikonya. Penilaian ini penting untuk mengetahui sejauh mana setiap aset informasi memiliki potensi kerentanan dan dampak terhadap keberlangsungan layanan sistem informasi akademik di STMIK Jayakarta.

Tabel 3. Tingkat Risiko Aset

Nama aset	CIA	D	A	R
Database akademik	11	h	l	m
Website akademik	8	m	m	m
Server hosting	11	h	m	h
Data mahasiswa dan dosen	10	h	m	h
Akun admin sistem	11	h	m	h
labtop /PC	9	m	m	m
Sistem operasi	11	h	m	h
UPS	7	m	m	m
Switch/router jaringan	9	m	l	m
Firewall	11	h	m	h

Keterangan:
D = Dampak
A = Ancaman
R = Risiko
(h= high, m= medium, l= low)

Dari hasil perhitungan risiko diatas, dilakukan rekapitulasi untuk mengetahui distribusi Tingkat risiko keseluruhan pada sistem informasi akademik

Tabel 4. Rekapitulasi Tingkat Risiko

Kategori aset	Jumlah aset	Risiko tinggi	Risiko sedang
Aset utama	5	3	2
Aset pendukung	5	2	3
Total	10	5	5

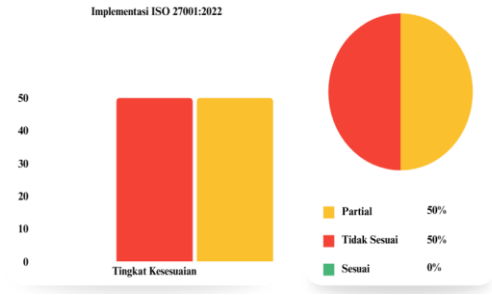
Hasil Audit Kesesuaian Terhadap ISO 27001:2022

Tabel 5. Kesesuaian Terhadap ISO 27001:2022

Kontrol ISO 27001	Status			Temuan
	Y	N	P	
5.2 Kebijakan keamanan informasi		✓		Tidak ada dokumen kebijakan formal dan belum tersosialisasi.
6.1.2 Perencanaan		✓		Belum tersedia dokumen risk

penilaian risiko				assessment dan risk treatment plan.
8.1 Pengendalian operasional			✓	Pengendalian dilakukan, tapi dokumentasi formal belum lengkap.
8.2 Penanganan risiko			✓	Penanganan risiko dilakukan, tapi belum terdokumentasi resmi.
9.1 Monitoring dan evaluasi			✓	Monitoring dilakukan, tetapi tidak ada pengukuran & analisis formal.
9.2 Audit internal		✓		Audit keamanan belum pernah dilakukan secara formal.
9.3 Tinjauan manajemen		✓		Tidak ditemukan bukti rapat manajemen rutin terkait keamanan.
10.2 Perbaikan berkelanjutan			✓	Tindakan perbaikan bersifat reaktif, tidak ada dokumentasi formal.

Berdasarkan tabel evaluasi kesesuaian terhadap ISO/IEC 27001:2022 terdapat empat klausul tidak sesuai dengan standar dan empat klausul partial (sesuai sebagian).



Gambar 2. Kesesuaian Kontrol Keamanan Berdasarkan Audit ISO 27001:2022

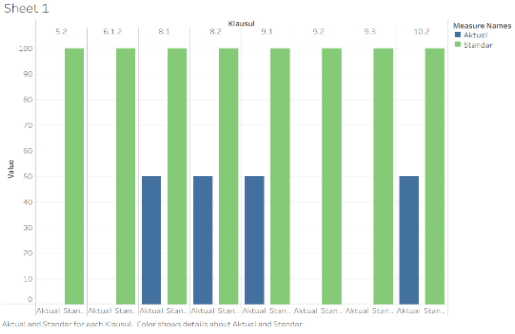
Berdasarkan temuan audit, dilakukan analisis kesenjangan antara kondisi aktual dan ketentuan ISO/IEC 27001:2022.

Tabel 6. Evaluasi gap implementasi keamanan informasi terhadap ISO 27001:2022

Kontrol ISO 27001	**Gap**
5.2 Kebijakan keamanan informasi	Tidak tersedia dokumen kebijakan keamanan formal yang mencakup prinsip, cakupan, dan tanggung jawab.
6.1.2 Perencanaan penilaian risiko	Belum ada metode atau dokumentasi resmi untuk menilai risiko.
8.1 Pengendalian operasional	Kontrol dilakukan, namun belum terdokumentasi secara formal dan standardisasi masih kurang.
8.2 Penanganan risiko	Penanganan risiko tidak terdokumentasi dan belum dilakukan secara rutin.
9.1 Monitoring dan evaluasi	Monitoring dilakukan, tetapi tanpa pengukuran formal dan dokumentasi evaluasi.
9.2 Audit internal	Audit keamanan informasi belum pernah dilakukan, tidak ada bukti laporan audit.
9.3 Tinjauan	Tidak ada bukti tinjauan

manajemen	SMKI oleh manajemen puncak secara berkala.
10.2 Perbaikan berkelanjutan	Perbaikan hanya bersifat reaktif dan belum terdokumentasi dalam sistem perbaikan berkelanjutan.

Berdasarkan hasil analisis pada Tabel 5, berikut disajikan diagram batang yang menggambarkan tingkat kesenjangan implementasi keamanan informasi pada masing-masing klausul ISO/IEC 27001:2022.



Gambar 3. Diagram Gap Implementasi perklausul ISO/IEC 27001:2022

Mayoritas gap ditemukan pada aspek dokumentasi dan pemantauan keamanan, yang menunjukkan perlunya perbaikan kebijakan formal, penilaian risiko, dan pelaksanaan audit internal. Sebagai tindak lanjut dari hasil gap analysis, disusun rekomendasi kontrol keamanan berdasarkan Annex A ISO/IEC 27001. Rekomendasi ini bertujuan sebagai dasar perbaikan yang sistematis dan terukur.

Tabel 7. Rekomendasi kontrol keamanan

Klausul	**Kontrol keamanan (Annex A)**	**Rekomendasi implementasi**
5.2	A.5.1.1	Buat dokumen kebijakan formal dan sosialisasikan ke seluruh unit
6.1.2	A.6.1.2, A.6.1.3	Gunakan template ISO 27005 dan buat risk register
8.1	A.8.2.1	Susun prosedur operasional standar (SOP) dan dokumentasi mitigasi
8.2	A.6.1.3	Buat SOP penilaian risiko tiap semester dan simpan sebagai arsip berkala
9.1	A.8.16.1	Gunakan tools SIEM dan susun laporan evaluasi berkala
9.2	A.18.2.1, A.18.2.2	Susun program audit tahunan dan pelatihan auditor
9.3	A.18.1.1, A.18.1.2	Jadwalkan rapat tinjauan dan simpan notulen sebagai bukti
10.2	A.10.1.1	Terapkan analisis akar masalah dan corrective action

Rekomendasi kontrol keamanan disusun berdasarkan temuan evaluasi terhadap klausul ISO/IEC 27001:2022 dan Annex A. Kontrol mencakup penyusunan kebijakan, manajemen risiko, dokumentasi prosedur, audit internal, serta tindakan korektif untuk

meningkatkan efektivitas sistem keamanan informasi.

KESIMPULAN

Berdasarkan hasil evaluasi terhadap sistem informasi akademik di STMIK Jayakarta menggunakan kerangka ISO/IEC 27001:2022, diperoleh temuan bahwa 5 dari 10 aset informasi tergolong dalam kategori risiko tinggi. Kondisi ini menandakan pentingnya penguatan pengelolaan aset informasi melalui penerapan kontrol keamanan yang lebih efektif dan terstruktur.

Audit kesesuaian terhadap klausul ISO/IEC 27001:2022 menunjukkan ketidaksesuaian pada klausul 5.2, 6.1.2, 9.2, dan 9.3, yang sebagian besar disebabkan oleh belum optimalnya dokumentasi kebijakan, proses audit internal, dan evaluasi manajemen secara berkala. Hal ini mengindikasikan perlunya penyempurnaan dalam siklus manajemen keamanan informasi secara menyeluruh.

Sebagai tindak lanjut, disusun rekomendasi kontrol keamanan berdasarkan Annex A ISO/IEC 27001:2022 yang mencakup penguatan kebijakan formal, peningkatan pelaksanaan audit internal, perencanaan mitigasi risiko, serta pengembangan program evaluasi berkelanjutan. Pendekatan ini sejalan dengan prinsip-prinsip tata kelola keamanan informasi yang menekankan pada keberlangsungan, integritas, dan akuntabilitas sistem.

Oleh karena itu, temuan ini diharapkan menjadi acuan dalam merumuskan strategi penguatan sistem informasi akademik secara komprehensif dan berkesinambungan, mengacu pada praktik terbaik standar internasional.

DAFTAR PUSTAKA

[1]Sinaga R., and Taan F., "*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.*

[2]Meitarice S., Febyana L., Fitriansyah A., and Kurniawan R,, "*Risk Management Analysis of Information Security in an Academic Information System at a Public University in Indonesia : Implementation of ISO / IEC 27005 : 2018 and ISO / IEC 27001 : 2013 Security Controls*," vol. 2, no. July, pp. 58–75, 2024, doi: *10.30996/jitcs.12099*.

[3]Intan Mafiana A., Hanum L., Ilmi H. M., and Febriliani S., "*Implementasi Manajemen*

Keamanan Informasi Berbasis Iso 27001 Pada Sistem Informasi Akademik," J. Digit. Bus. Innov. Manag., vol. 2, no. 2, pp. 139–163, 2023, doi: *10.26740/jdbim.v2i2.57580*.

[4]Jenny M. S., Shofa R. N., and Rahmatulloh A., "*Analisis Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 4.2 Pada Sistem Informasi Akademik (SIMAK) Universitas Siliwangi*," pp. 73–80, 2024, [Online]. Available: *http://www.jurnal.umk.ac.id/site ch*

[5]Kusnandar A., Rochim A. F., and Gunawan V., "*Pengukuran Tingkat Risiko dan Keamanan Informasi Menggunakan Metode FMEA Berbasis ISO / IEC 27001 pada Instansi XYZ untuk Keamanan Sistem Informasi*," vol. 04, 2024, doi: *10.21456/vol14iss4pp375-384.*

[6]Titan T. P. Y., Maharani Vani, and Maulana N. D., "*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.

[7]Nasrah H., Muda I., and Kesuma S. A., "*Computer Assisted Audit Tools and Techniques Adoption: A Systematic Literature Review*," Int. J. Soc. Serv. Res., vol. 3, no. 3, pp. 630–638, 2023, doi: *10.46799/ijssr.v3i3.301.*

[8]Irawan Ade,Fadholi W. H. N., Erikamaretha Zahwa, and Sinlae Fried, "*Tantangan dan Strategi Manajemen Keamanan Siber di Indonesia berbasis IoT*," J. Zetroem, vol. 6, no. 1, pp. 114–119, 2024, doi: *10.36526/ztr.v6i1.3376.*

[9]Ilmu Komputer J., Informasi S., and Informatika T., "*Tinjauan Implementasi National Institute of Standards and Technology (Nist) Dalam Meningkatkan Keamanan Jaringan Dengan Cybersecurity Framework (Csf) : Studi Kasus Smkn4 Bandar Lampung*," vol. 3, no. 1, pp. 2964–4763, 2024.

[10]Akmal R. N., Susilo D. D., and Rouf E. H., "*Evaluasi Keamanan Sistem Informasi Rumah Sakit : Metode Pengujian ISO 27001 di RS Khusus Mata Purwokerto*," vol. 6, no. 1, pp. 560–569, 2025.

[11]Ardius E. and Syamsuar D., "*Assessment Risk Terhadap Penggunaan Sistem Informasi Akademik Universitas Ea Menggunakan*

Metode Iso 27001," J. Teknol. Inf. Mura, vol. 15, no. 1, pp. 1–13, 2023, *doi: 10.32767/jti.v15i1.1948.*

[12]Vatresia A., Tambunan P. N., and Erlanshari A., "*Audit Sistem Informasi pada Sistem Manajemen Layanan Satu Atap (SIMANTAP) Menggunakan Kerangka COBIT 5.0 (Studi Kasus: Bank Indonesia Provinsi Bengkulu)*," J. Teknol. Inf. dan Ilmu Komput., vol. 9, no. 5, pp. 1029–1036, 2022, doi: *10.25126/jtiik.2022945792.*

[13]Nurul Wahidah R., Lutfiyana N., Fitria Ramadanti V., Septiyo P., and Drefiyanto R., "*Audit Sistem Informasi Absensi Mesin Fingerprint Pada PT. Metal Castindo Industritama Dengan Menggunakan Framework Cobit 5*," J. Sist. Inf., vol. 11, no. 2, pp. 51–57, 2022, doi: *10.51998/jsi.v11i2.482.*

[14]Agustika F., Siregar S., Obara D., and Paramarta V., "*Telaah Teknologi Informasi Dan Sistem Informasi Dalam Organisasi Dengan Lingkungan*," J. Bisnis Kolega, vol. 9, no. 1, pp. 24–33, 2023, doi: *10.57249/jbk.v9i1.104*.

[15]Nuraeni F., Setiawan R., Nurhakim W., and Mubarok M. S., "*Sistem Informasi Akademik Berbasis Mobile Apps Sebagai Media Informasi Akademik Online*," J. Algoritm., vol. 18, no. 2, pp. 358–366, 2022, doi: *10.33364/algoritma/v.18-2.951.*

[16]Riyadi Y., Wahidin M., and Elanda A., "*Systematic Literature Review Implementasi Service Operation Dalam Kerangka Kerja Information Technology Infrastructure Library (ITIL) di Indonesia: Tren Penelitian, Manfaat dan Tantangan*," J. Interkom J. Publ. Ilm. Bid. Teknol. Inf. dan Komun., vol. 17, no. 2, pp. 81–97, 2022, doi: *10.35969/interkom.v17i2.232*.