KAJIAN LITERATUR SISTEMATIS: AUDIT SISTEM INFORMASI DAN KEAMANAN INFORMASI BERBASIS ISO/IEC 27001:2022 DALAM SEKTOR PEMERINTAHAN

SYSTEMATIC LITERATURE REVIEW: ISO/IEC 27001-BASED INFORMATION SYSTEM AND INFORMATION SECURITY AUDIT IN THE INDONESIAN GOVERNMENT SECTOR

Adinda Wira Zahra Tsabitah[1*]
*E-mail: 22082010231@student.upnjatim.ac.id

[1]Sistem Informasi, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jawa Timur

Abstrak

Perkembangan transformasi digital dalam sektor pemerintahan menuntut adanya pengelolaan keamanan informasi yang lebih sistematis dan terstandar. Dalam konteks tersebut, audit sistem informasi berbasis ISO/IEC 27001:2022 menjadi penting untuk menilai kesesuaian pengendalian, efektivitas perlindungan aset informasi, serta kesiapan instansi pemerintah dalam menghadapi risiko keamanan informasi. Penelitian ini bertujuan untuk mengkaji secara sistematis berbagai penelitian terdahulu mengenai audit sistem informasi dan keamanan informasi berbasis ISO/IEC 27001:2022 dalam sektor pemerintahan. Metode yang digunakan adalah systematic literature review dengan pendekatan PRISMA melalui tahapan identifikasi, penyaringan, uji kelayakan, dan penetapan artikel terpilih. Data dianalisis secara tematik untuk mengidentifikasi pola penerapan, aspek keamanan informasi yang dominan dibahas, serta tantangan utama dalam implementasinya. Hasil kajian diharapkan menunjukkan bahwa penerapan ISO/IEC 27001:2022 pada sektor pemerintahan berfokus pada penguatan tata kelola keamanan informasi, manajemen risiko, kontrol akses, serta evaluasi kepatuhan dan kesiapan organisasi. Selain itu, tantangan yang diperkirakan paling sering muncul meliputi keterbatasan sumber daya manusia, belum optimalnya kebijakan internal, dan perbedaan tingkat kematangan keamanan informasi antarinstansi. Penelitian ini menyimpulkan bahwa audit sistem informasi berbasis ISO/IEC 27001:2022 memiliki peran penting dalam mendukung penguatan keamanan informasi di sektor pemerintahan dan dapat menjadi dasar bagi pengembangan kebijakan serta penelitian lanjutan.

Kata kunci**:** *Audit Sistem Informasi, Keamanan Informasi, Iso/Iec 27001:2022, Sektor Pemerintahan, Systematic Literature Review.*

Abstract

The development of digital transformation in the government sector demands more systematic and standardized information security management. In this context, ISO/IEC 27001:2022-based information system audits are crucial for assessing the suitability of controls, the effectiveness of information asset protection, and the readiness of government agencies to address information security risks. This study aims to systematically review previous studies on ISO/IEC 27001:2022-based information system audits and information security in the government sector. The method used is a systematic literature review with the PRISMA approach through the stages of identification, screening, due diligence, and determination of selected articles. Data are analyzed thematically to identify implementation patterns, the dominant information security aspects discussed, and the main challenges in its implementation. The results of the study are expected to show that the implementation of ISO/IEC 27001:2022 in the government sector

focuses on strengthening information security governance, risk management, access control, and evaluating compliance and organizational readiness. In addition, the most frequently encountered challenges include limited human resources, suboptimal internal policies, and differences in information security maturity levels between agencies. This study concludes that ISO/IEC 27001:2022-based information system audits have an important role in supporting the strengthening of information security in the government sector and can serve as a basis for policy development and further research.
***Keywords**: Information Systems Audit, Information Security, Iso/Iec 27001:2022, Government Sector, Systematic Literature Review,*

1. PENDAHULUAN

Perkembangan teknologi informasi mendorong sektor pemerintahan melakukan transformasi digital dalam layanan publik, administrasi, pengelolaan data, komunikasi, dan pengambilan keputusan. Perubahan ini membuat layanan menjadi lebih cepat, terbuka, dan efisien. Namun, penggunaan sistem elektronik juga meningkatkan risiko keamanan informasi, seperti kebocoran data, penyalahgunaan akses, perubahan data tanpa izin, gangguan layanan, dan menurunnya kepercayaan publik.

Instansi pemerintahan mengelola data penting, seperti data kependudukan, keuangan, layanan publik, kebijakan, arsip digital, dan data internal organisasi. Karena itu, keamanan informasi perlu dikelola secara serius melalui prinsip confidentiality, integrity, dan availability. Salah satu standar yang dapat digunakan adalah ISO/IEC 27001:2022, yaitu standar Sistem Manajemen Keamanan Informasi yang menekankan pengelolaan risiko, perlindungan aset informasi, serta evaluasi kontrol keamanan secara sistematis [1].

Audit sistem informasi berbasis ISO/IEC 27001:2022 penting untuk menilai kesiapan instansi pemerintah dalam menerapkan kebijakan, prosedur, kontrol keamanan, dan pengelolaan risiko informasi. Penelitian ini dilakukan untuk mengkaji secara sistematis penelitian terdahulu terkait audit sistem informasi dan keamanan informasi pada sektor pemerintahan. Kajian ini diharapkan dapat menunjukkan pola penerapan audit, aspek keamanan yang paling banyak dibahas, tantangan implementasi, serta framework atau tools pendukung yang digunakan.

2. METODOLOGI

Metode yang digunakan dalam penelitian ini adalah Systematic Literature Review atau SLR. Metode ini digunakan untuk mengidentifikasi, menyeleksi, mengevaluasi, dan mensintesis penelitian terdahulu yang relevan dengan topik audit sistem informasi dan keamanan informasi berbasis ISO/IEC 27001:2022 dalam sektor pemerintahan. Pendekatan yang digunakan dalam proses seleksi artikel mengacu pada alur PRISMA, yaitu identifikasi, penyaringan, uji kelayakan, dan penetapan artikel yang digunakan dalam kajian [2].

SLR dipilih karena metode ini mampu memberikan pemahaman yang sistematis mengenai perkembangan penelitian terdahulu. Melalui metode ini, peneliti dapat mengetahui pola penerapan ISO/IEC 27001 dalam audit sistem informasi, aspek keamanan informasi yang paling sering dibahas, tantangan implementasi, serta framework atau tools lain yang mendukung proses audit.

2.1 Research Question

Pertanyaan penelitian atau research question dalam penelitian ini disusun untuk mengarahkan proses analisis literatur. Adapun pertanyaan penelitian yang digunakan adalah sebagai berikut:

Table 1. Tabel Pertanyaan RQ

RQ	Pertanyaan

RQ1	Bagaimana penerapan audit sistem informasi berbasis ISO/IEC 27001 dalam sektor pemerintahan berdasarkan studi literatur?
RQ2	Aspek keamanan informasi apa saja yang paling sering dibahas dalam penelitian mengenai ISO/IEC 27001 pada sektor pemerintahan?
RQ3	Apa tantangan utama dalam penerapan audit sistem informasi dan keamanan informasi berbasis ISO/IEC 27001 dalam sektor pemerintahan?
RQ4	Framework atau tools lain apa yang digunakan selama penerapan audit?

2.2 Inclusion and Exclusion Criteria

Kriteria inklusi dan eksklusi digunakan untuk menentukan artikel yang layak dianalisis. Kriteria ini bertujuan agar artikel yang digunakan sesuai dengan fokus penelitian.

Table 2. Tabel Kriteria Artikel

No	Kriteria	Tipe
1	Artikel membahas audit sistem informasi, keamanan informasi, manajemen risiko, atau SMKI	Inclusion
2	Artikel menggunakan atau membahas ISO/IEC 27001, terutama ISO/IEC 27001:2022	Inclusion
3	Artikel berkaitan dengan sektor pemerintahan, layanan publik, atau organisasi yang relevan sebagai pembanding implementasi	Inclusion
4	Artikel berupa jurnal, prosiding, atau artikel ilmiah yang dapat diakses	Inclusion
5	Artikel tidak membahas keamanan informasi, audit sistem informasi, atau ISO/IEC 27001	Exclusion
6	Artikel tidak memiliki abstrak, metode, atau hasil yang dapat dianalisis	Exclusion
7	Artikel yang bersifat duplikat tidak dijadikan dasar utama sintesis, tetapi tetap dicatat apabila masuk dalam kumpulan literatur awal	Exclusion

2.3 Tahapan PRISMA

Tahapan PRISMA dalam penelitian ini dilakukan untuk menata proses seleksi artikel secara sistematis [3]. Artikel yang digunakan merupakan artikel yang telah dikumpulkan sebelumnya oleh peneliti dan kemudian disaring berdasarkan relevansi topik.

Table 3. Tahapan Seleksi Artikel Berdasarkan PRISMA

Tahapan	Jumlah Artikel	Keterangan
Identifikasi	100	Artikel awal yang dikumpulkan berdasarkan topik ISO/IEC 27001, audit sistem informasi, dan keamanan informasi
Penyaringan	31	Artikel disaring berdasarkan judul dan abstrak

Tahapan	Jumlah Artikel	Keterangan
Uji kelayakan	31	Artikel dinilai berdasarkan kesesuaian dengan RQ dan ketersediaan informasi hasil penelitian
Artikel digunakan	31	Artikel digunakan sebagai dasar sintesis tematik

Berdasarkan proses tersebut, sebanyak 31 artikel digunakan dalam penelitian ini. Artikel yang digunakan mencakup penelitian tentang ISO/IEC 27001:2022, ISO/IEC 27001:2013, Indeks KAMI, ISO/IEC 27005, ISO/IEC 27002, COBIT, NIST, FMEA, OCTAVE, dan beberapa pendekatan pendukung lain. Artikel yang masih menggunakan ISO/IEC 27001:2013 tetap dipertimbangkan karena memiliki relevansi dengan proses audit, evaluasi kesiapan SMKI, dan transisi menuju ISO/IEC 27001:2022.

2.4 Quality Assessment

Quality assessment dilakukan untuk menilai kelayakan artikel yang digunakan dalam kajian ini. Penilaian dilakukan berdasarkan tiga pertanyaan utama:

Table 3. Tabel Quality Assessment

QA	Pertanyaan
QA1	Apakah artikel membahas audit sistem informasi, keamanan informasi, atau manajemen risiko?
QA2	Apakah artikel membahas ISO/IEC 27001 atau framework yang berkaitan dengan keamanan informasi?
QA3	Apakah artikel relevan dengan sektor pemerintahan, layanan publik, atau konteks implementasi keamanan informasi yang dapat dijadikan pembanding?

Setiap artikel diberi nilai sebagai berikut:
1. Nilai 1 diberikan apabila artikel memenuhi kriteria.
2. Nilai 0,5 diberikan apabila artikel memenuhi sebagian kriteria.
3. Nilai 0 diberikan apabila artikel tidak memenuhi kriteria.

Table 4. Tabel Hasil Quality Assessment

No	Judul	Fokus Artikel	Tahun	QA1	QA2	QA3	Total
1	Implementasi ISO 27001:2022 dalam Manajemen Risiko Keamanan Informasi	Implementasi ISO 27001:2022 dalam manajemen risiko keamanan informasi	2025	1	1	1	3
2	Penerapan ISO/IEC 27001:2022 dalam Tata Kelola Keamanan Sistem Informasi	Penerapan ISO/IEC 27001:2022 dalam tata kelola keamanan sistem informasi	2024	1	1	0,5	2,5
3	Peran Sistem Informasi dalam Meningkatkan Kualitas Audit Keuangan Pemerintah Daerah	Peran sistem informasi dalam meningkatkan kualitas audit keuangan pemerintah daerah	2024	1	0,5	1	2,5

No	Judul	Fokus Artikel	Tahun	QA1	QA2	QA3	Total
4	Preparation of Information Security Risk Management Based on ISO/IEC 27001:2022 at Diskominfo West Java Province	Manajemen risiko keamanan informasi berbasis ISO/IEC 27001:2022 pada Diskominfo Jawa Barat	2025	1	1	1	3
5	Analisis Kesenjangan SMKI sebagai Persiapan Sertifikasi ISO/IEC 27001:2013 pada Institusi Pemerintah	Gap analysis SMKI untuk sertifikasi ISO/IEC 27001 pada institusi pemerintah	2021	1	1	1	3
6	Assessing Information Security Management Using ISO 27001:2013	Penilaian manajemen keamanan informasi menggunakan ISO 27001:2013	2024	1	1	0,5	2,5
7	Penerapan SMKI ISO 27001 pada Perpusnas RI	Penerapan SMKI ISO 27001 pada Perpusnas RI	2024	1	1	1	3
8	Analisis Keamanan Informasi Menggunakan Aplikasi Indeks KAMI pada Sekretariat DPRD Kabupaten Jombang	Analisis keamanan informasi menggunakan Indeks KAMI pada Sekretariat DPRD	2023	1	1	1	3
9	Analisis Risiko Keamanan Informasi Website Repository Digital Library Menggunakan ISO/IEC 27001 & 27002	Analisis risiko keamanan informasi website repository menggunakan ISO 27001 dan 27002	2024	1	1	0,5	2,5
10	Lanjutan artikel Repository Digital Library	Audit keamanan repository digital library berbasis ISO 27001 dan 27002	2024	1	1	0,5	2,5
11	Evaluasi SMKI Berdasarkan Indeks KAMI v4.2 pada Dinas XYZ Provinsi Jawa Tengah	Evaluasi SMKI berdasarkan Indeks KAMI pada Dinas XYZ Jawa Tengah	2023	1	1	1	3
12	Duplikat Assessing Information Security Management Using ISO 27001:2013	Assessing information security management using ISO 27001:2013	2024	1	1	0,5	2,5
13	Penilaian Tingkat Kesiapan Keamanan Informasi pada Dinas Kominfo Kabupaten XYZ	Penilaian kesiapan keamanan informasi pada Dinas Kominfo Kabupaten XYZ	2023	1	1	1	3

No	Judul	Fokus Artikel	Tahun	QA1	QA2	QA3	Total
	dengan Indeks KAMI 4.2						
14	Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27001 pada PT BPR Jatim	Audit keamanan sistem informasi berdasarkan ISO 27001 pada sektor perbankan daerah	2024	1	1	0,5	2,5
15	Analisis dan Manajemen Risiko Keamanan Informasi Menggunakan FMEA dan ISO/IEC 27001:2013 pada Diskominfo Sambas	Manajemen risiko keamanan informasi menggunakan FMEA dan ISO 27001 pada Diskominfo Sambas	2022	1	1	1	3
16	Analisis Manajemen Risiko Keamanan SIAM Poltekkes Kemenkes Riau	Manajemen risiko keamanan informasi SIAM Poltekkes Kemenkes Riau	2024	1	1	1	3
17	Analisis Risiko Aset TI Menggunakan OCTAVE dan FMEA Berbasis ISO 27001:2022	Risiko aset TI menggunakan OCTAVE dan FMEA berbasis ISO 27001:2022	2024	1	1	0,5	2,5
18	SMKI dengan Standar ISO/IEC 27001 dan ISO/IEC 27002 pada PT Jasa Marga	SMKI dengan ISO 27001 dan ISO 27002 pada PT Jasa Marga	2024	1	1	0,5	2,5
19	Audit Sistem Keamanan Informasi Menggunakan ISO 27001 pada SMKN 1 Pugung	Audit keamanan sistem informasi berdasarkan ISO 27001 pada lembaga pendidikan	2024	1	1	0,5	2,5
20	Evaluasi Risiko Keamanan Informasi Diskominfo Provinsi XYZ Menggunakan Indeks KAMI dan ISO 27005:2011	Evaluasi risiko keamanan informasi Diskominfo Provinsi XYZ	2022	1	1	1	3
21	Audit Keamanan Sistem Informasi Puskesmas dengan ISO/IEC 27001:2013 dan COBIT 5	Audit keamanan sistem informasi Puskesmas dengan ISO 27001 dan COBIT 5	2024	1	1	1	3
22	Pengukuran Tingkat Risiko dan Keamanan Informasi Menggunakan	Pengukuran tingkat risiko dan keamanan informasi	2024	1	1	0,5	2,5

No	Judul	Fokus Artikel	Tahun	QA1	QA2	QA3	Total
	FMEA Berbasis ISO/IEC 27001 pada Instansi XYZ	menggunakan FMEA berbasis ISO 27001					
23	Audit Keamanan Website Layanan Publik Mengacu ISO/IEC 27001: PeduliLindungi	Audit keamanan website layanan publik mengacu ISO/IEC 27001	2024	1	1	1	3
24	Kematangan Risiko Keamanan Informasi Layanan TI Menggunakan NIST dan ISO 27001 pada Bapenda Jawa Tengah	Kematangan risiko keamanan informasi layanan TI Bapenda Jawa Tengah	2024	1	1	1	3
25	Manajemen Risiko Keamanan Informasi Menggunakan ISO/IEC 27005 pada Diskominfo Sidoarjo	Manajemen risiko keamanan informasi menggunakan ISO 27005 pada Diskominfo Sidoarjo	2025	1	1	1	3
26	Evaluasi Keamanan Informasi SMA N 1 Sentolo Berdasarkan Indeks KAMI ISO/IEC 27001:2013	Evaluasi keamanan informasi sekolah berdasarkan Indeks KAMI ISO 27001	2024	1	1	0,5	2,5
27	ISO 27001 sebagai Metode Alternatif Perancangan Tata Kelola Keamanan Informasi di Arsip Nasional RI	ISO 27001 sebagai metode tata kelola keamanan informasi Arsip Nasional RI	2017	1	1	1	3
28	SMKI di PT Surveyor Indonesia Cabang Surabaya: Penerapan ISO 27001:2013	SMKI di PT Surveyor Indonesia dengan ISO 27001:2013	2024	1	1	0,5	2,5
29	Manajemen Risiko Keamanan Informasi ISO 27001:2022 Studi Kasus KPU	Manajemen risiko keamanan informasi ISO 27001:2022 pada KPU	2024	1	1	1	3
30	Duplikat: Implementasi ISO 27001:2022 dalam Manajemen Risiko Keamanan Informasi	Implementasi ISO 27001:2022 dalam manajemen risiko keamanan informasi	2025	1	1	1	3
31	Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks KAMI 4.2 dan ISO/IEC 27001:2013 pada Diskominfo Gianyar	Evaluasi kesiapan keamanan informasi menggunakan Indeks KAMI dan ISO 27001 pada Diskominfo Gianyar	2022	1	1	1	3

3. HASIL DAN PEMBAHASAN

Berdasarkan hasil telaah terhadap 31 artikel, penelitian mengenai audit sistem informasi dan keamanan informasi berbasis ISO/IEC 27001 banyak membahas penerapan standar ini dalam konteks instansi pemerintahan, terutama Dinas Komunikasi dan Informatika. Artikel yang dianalisis umumnya menggunakan ISO/IEC 27001 sebagai acuan untuk menilai kesiapan, kematangan, kepatuhan, serta efektivitas Sistem Manajemen Keamanan Informasi. Selain itu, beberapa penelitian juga menggunakan framework pendukung seperti Indeks KAMI, ISO/IEC 27005, ISO/IEC 27002, COBIT, NIST, FMEA, OCTAVE, RACI, dan PDCA.
Secara umum, artikel yang dikaji menunjukkan bahwa audit sistem informasi berbasis ISO/IEC 27001 tidak hanya digunakan untuk menilai aspek teknis keamanan, tetapi juga untuk mengevaluasi tata kelola, kebijakan, dokumentasi, manajemen risiko, pengendalian akses, dan kesiapan organisasi dalam menghadapi ancaman keamanan informasi.

3.1 RQ1: Penerapan Audit Sistem Informasi Berbasis ISO/IEC 27001 dalam Sektor Pemerintahan

Penerapan audit sistem informasi berbasis ISO/IEC 27001 dalam sektor pemerintahan umumnya dilakukan melalui tahapan identifikasi aset, identifikasi risiko, analisis risiko, evaluasi kontrol, penilaian kesenjangan, dan penyusunan rekomendasi perbaikan. ISO/IEC 27001 digunakan sebagai standar untuk menilai apakah instansi telah memiliki kebijakan, prosedur, kontrol keamanan, dan proses evaluasi yang sesuai dengan kebutuhan perlindungan informasi.
Beberapa penelitian menunjukkan bahwa audit dilakukan untuk mengetahui tingkat kesiapan instansi menuju penerapan atau sertifikasi ISO/IEC 27001. Misalnya, penelitian pada Diskominfo Kota Madiun menggunakan gap analysis untuk mengukur pemenuhan persyaratan ISO/IEC 27001. Hasilnya menunjukkan bahwa audit dapat membantu instansi mengetahui aspek yang sudah memenuhi standar dan aspek yang masih perlu diperbaiki.
Pada penelitian lain, ISO/IEC 27001:2022 digunakan untuk mendukung manajemen risiko keamanan informasi. Proses audit dilakukan dengan menilai risiko seperti serangan siber, bug aplikasi, kerusakan perangkat keras, kelemahan kontrol akses, dan rendahnya kompetensi sumber daya manusia. Dengan demikian, penerapan audit berbasis ISO/IEC 27001 dalam sektor pemerintahan berfungsi sebagai alat evaluasi, pengendalian risiko, dan dasar penyusunan perbaikan keamanan informasi.

3.2 RQ2: Aspek Keamanan Informasi yang Paling Sering Dibahas

Aspek keamanan informasi yang paling sering dibahas dalam artikel adalah confidentiality, integrity, dan availability. Ketiga aspek ini menjadi dasar utama dalam perlindungan informasi pemerintahan. Confidentiality berkaitan dengan perlindungan data agar hanya dapat diakses oleh pihak yang berwenang. Integrity berkaitan dengan keutuhan dan keakuratan data. Availability berkaitan dengan ketersediaan sistem dan layanan ketika dibutuhkan.
Selain ketiga aspek tersebut, penelitian terdahulu juga banyak membahas manajemen risiko, kontrol akses, pengelolaan aset informasi, keamanan fisik, keamanan jaringan, manajemen insiden, monitoring, logging, backup data, dan kepatuhan terhadap regulasi. Aspek manajemen risiko menjadi salah satu pembahasan dominan karena ISO/IEC 27001 menggunakan pendekatan berbasis risiko dalam pengelolaan keamanan informasi.
Dengan demikian, aspek keamanan informasi dalam sektor pemerintahan tidak hanya terbatas pada perlindungan sistem secara teknis, tetapi juga mencakup tata kelola, kebijakan, sumber daya manusia, dokumentasi, dan proses evaluasi berkelanjutan.

3.3 RQ3: Tantangan Utama dalam Penerapan Audit dan Keamanan Informasi Berbasis ISO/IEC 27001

Tantangan utama dalam penerapan audit sistem informasi dan keamanan informasi berbasis ISO/IEC 27001 adalah keterbatasan sumber daya manusia. Banyak instansi pemerintah belum memiliki pegawai yang secara khusus memahami audit sistem informasi, manajemen risiko, dan standar keamanan informasi. Kondisi ini berdampak pada kurang optimalnya proses identifikasi risiko, penyusunan dokumen, dan penerapan kontrol keamanan.

Tantangan berikutnya adalah rendahnya kesadaran keamanan informasi. Beberapa penelitian menunjukkan bahwa human error masih menjadi penyebab risiko keamanan, seperti kelalaian dalam menjaga akun, penggunaan kata sandi lemah, kurangnya kepatuhan terhadap prosedur, dan minimnya pemahaman pegawai terhadap kebijakan keamanan informasi.

Selain itu, tantangan lain yang sering ditemukan adalah belum lengkapnya dokumentasi, keterbatasan anggaran, infrastruktur yang belum memadai, kebijakan internal yang belum optimal, serta perbedaan tingkat kematangan keamanan informasi antarinstansi. Ancaman siber yang terus berkembang, seperti phishing, malware, web defacement, ransomware, dan akses tidak sah, juga menjadi faktor yang memperkuat kebutuhan audit dan evaluasi berkala.

3.4 RQ4: Framework atau Tools Lain yang Digunakan Selama Penerapan Audit

Hasil kajian menunjukkan bahwa ISO/IEC 27001 sering digunakan bersama framework atau tools lain. Framework yang paling banyak digunakan adalah Indeks KAMI, terutama pada instansi pemerintah di Indonesia. Indeks KAMI digunakan untuk menilai tingkat kesiapan keamanan informasi berdasarkan beberapa area, seperti tata kelola, pengelolaan risiko, kerangka kerja keamanan, pengelolaan aset, teknologi, dan peran sistem elektronik.

Selain Indeks KAMI, beberapa penelitian menggunakan ISO/IEC 27005 untuk manajemen risiko keamanan informasi dan ISO/IEC 27002 sebagai panduan kontrol keamanan. COBIT digunakan untuk menilai tata kelola TI, sedangkan NIST digunakan untuk memperkuat pengelolaan risiko dan kontrol keamanan siber. Beberapa penelitian juga menggunakan FMEA dan OCTAVE untuk mengidentifikasi serta memprioritaskan risiko.

Tools teknis seperti SSL Labs, VirusTotal, dan OWASP Scanner juga ditemukan dalam penelitian yang berfokus pada audit keamanan website atau layanan publik berbasis web. Dengan demikian, penggunaan ISO/IEC 27001 akan lebih kuat apabila dikombinasikan dengan framework pendukung sesuai kebutuhan audit.

3.4 Hasil Temuan

Berdasarkan hasil analisis, ISO/IEC 27001:2022 memiliki peran penting dalam audit sistem informasi sektor pemerintahan. Standar ini membantu instansi menilai kesiapan keamanan informasi, mengidentifikasi risiko, mengevaluasi kontrol, dan menyusun rekomendasi perbaikan. Dalam praktiknya, penerapan ISO/IEC 27001 perlu didukung oleh kebijakan internal, kompetensi sumber daya manusia, dokumentasi yang lengkap, serta evaluasi berkelanjutan.

Temuan juga menunjukkan bahwa sektor pemerintahan masih menghadapi tantangan dalam penerapan keamanan informasi, terutama pada aspek SDM, awareness, dokumentasi, anggaran, dan kematangan tata kelola. Oleh karena itu, audit sistem informasi berbasis ISO/IEC 27001:2022 dapat menjadi dasar penting untuk memperkuat perlindungan data, meningkatkan kepatuhan, dan menjaga kepercayaan publik terhadap layanan digital pemerintah.

4. KESIMPULAN DAN SARAN

Berdasarkan hasil Systematic Literature Review terhadap 31 artikel, dapat disimpulkan bahwa audit sistem informasi berbasis ISO/IEC 27001:2022 memiliki peran penting dalam mendukung

keamanan informasi sektor pemerintahan. Audit ini digunakan untuk menilai kesiapan organisasi, mengevaluasi kontrol keamanan, mengidentifikasi risiko, serta memberikan rekomendasi perbaikan terhadap Sistem Manajemen Keamanan Informasi.

Aspek keamanan informasi yang paling sering dibahas adalah kerahasiaan, integritas, ketersediaan, manajemen risiko, kontrol akses, pengelolaan aset, keamanan jaringan, keamanan fisik, dan manajemen insiden. Tantangan utama yang ditemukan meliputi keterbatasan sumber daya manusia, rendahnya kesadaran keamanan informasi, dokumentasi yang belum lengkap, keterbatasan anggaran, serta perbedaan tingkat kematangan keamanan informasi antarinstansi.

Selain ISO/IEC 27001, beberapa framework dan tools lain juga digunakan untuk mendukung proses audit, seperti Indeks KAMI, ISO/IEC 27005, ISO/IEC 27002, COBIT, NIST, FMEA, OCTAVE, RACI, PDCA, SSL Labs, VirusTotal, dan OWASP Scanner. Penggunaan framework pendukung tersebut dapat memperkuat proses audit karena masing-masing memiliki fungsi yang berbeda dalam penilaian kesiapan, manajemen risiko, tata kelola TI, maupun pengujian teknis.

Saran untuk penelitian selanjutnya adalah melakukan kajian yang lebih spesifik pada satu jenis instansi pemerintahan, misalnya Diskominfo, Bapenda, KPU, atau instansi pelayanan publik lainnya. Penelitian berikutnya juga dapat membandingkan tingkat kesiapan ISO/IEC 27001:2022 antarinstansi agar diperoleh gambaran yang lebih jelas mengenai kematangan keamanan informasi di sektor pemerintahan.

5. DAFTAR RUJUKAN

[1] P. Sundari and W. Wella, “SNI ISO/IEC 27001 dan Indeks KAMI: Manajemen Risiko PUSDATIN (PUPR),” Ultima InfoSys Jurnal Ilmu Sistem Informasi, pp. 35–42, Jun. 2021, doi: 10.31937/si.v12i1.1701.

[2] Maulana, R. (2025). Systematic Literature Review: Implementasi ISO/IEC 27001 dalam Penguatan Keamanan Informasi di Indonesia. JIMT: Jurnal Informatika, Multimedia Dan Teknik, 1(2), 196–201. https://doi.org/10.71456/jimt/v1i2.1340

[3] E. Wiraspanggi, “Systematic Literature Review Dengan Metode Prisma: Integritas Fungsi Manajemen Sumber Daya Manusia Sebagai Instrumen Pengambilan Keputusan Organisasi Yang Efektif,” Journal of Science Education and Management Business, vol. 4, no. 3, pp. 819–836, Nov. 2025, doi: 10.62357/joseamb.v4i3.847.