JURNAL MULTI MEDIA DAN IT
VOL.09 NO.01 (2025), PP. 080-086
P-ISSN : 2548-9534 | E-ISSN : 2548-9550

Evaluasi Keamanan Informasi Sistem Informasi Manajemen RSUD KHZ Musthafa Menggunakan Indeks KAMI 5.0 Berbasis ISO/IEC 27001:2022

Rayhan Ramadhan [a], *Nur Widiyasono*[b], *Alam Rahmatullah* [c]

[a,b,c] *Universitas Siliwangi, Indonesia*

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima Redaksi: 22 Juni 2025
Revisi Akhir: 5 September 2025
Diterbitkan *Online*: 8 September 2025

KATA KUNCI

Evaluasi Risiko, Indeks KAMI 5.0, ISO/IEC 27001:2022, Keamanan Informasi

KORESPONDENSI

Rayhan Ramadhan
187006108@student.unsil.ac.id

ABSTRAK

RSUD Kyai Haji Zaenal Musthafa, rumah sakit tipe C yang diresmikan pada 22 Februari 2011, menyediakan layanan kesehatan dengan dukungan sistem pendaftaran *online*. Namun penggunaan sistem informasi digital memunculkan risiko keamanan siber. Untuk mengevaluasi tingkat keamanan sistem informasi manajemen rumah sakit tersebut, digunakan Indeks KAMI yang mengacu pada standar ISO 27001. Hasil penelitian menunjukkan bahwa SIMRS RSUD KHZ Musthafa memiliki sistem elektronik yang berkategorikan "Tinggi" dan kesiapan sertifikasi ISO 27001 “Tidak Layak” dengan skor akhir 520. Disarankan agar manajemen TI melakukan perbaikan kebijakan, khususnya dalam pengelolaan risiko keamanan informasi sesuai panduan Indeks KAMI 5.0. Penelitian ini menyoroti pentingnya penyusunan kebijakan risiko dan perencanaan strategi keamanan informasi terintegrasi. Kontribusi penelitian ini memberikan peta jalan awal implementasi kontrol keamanan berbasis ISO di sektor kesehatan daerah.

DOI: https://doi.org/10.46961/jommit.v9i1

1. PENDAHULUAN

Keamanan informasi merupakan upaya perlindungan terhadap akses, penggunaan, atau perusakan data yang tidak sah, dengan menjaga kerahasiaan, integritas, dan ketersediaan informasi [1]. Keamanan informasi menjadi hal penting untuk semua kalangan, baik individu, organisasi atau perusahaan dan negara, termasuk pada pihak yang berjalan pada bidang kesehatan. RSUD KHZ Musthafa adalah rumah sakit tipe C milik Pemkab Tasikmalaya yang menyediakan berbagai layanan medis dan fasilitas penunjang, termasuk sistem informasi dan layanan pendaftaran *online* berbasis BPJS dan asuransi lainnya.

Seiring meningkatnya pemanfaatan teknologi informasi, ancaman terhadap keamanan siber di sektor kesehatan pun meningkat, terutama selama pandemi COVID-19, yang menjadikan institusi kesehatan sebagai target utama serangan siber [2]. Diperlukan reformulasi kebijakan yang mencakup pelatihan karyawan terkait protokol keamanan siber, penerapan teknologi perlindungan tingkat lanjut, serta kolaborasi dengan para ahli di bidang terkait [3]. Faktor stres juga terbukti berkorelasi dengan lemahnya praktik keamanan siber [4]. Selain itu, belum banyak penelitian yang mengevaluasi kesiapan SIMRS tipe C di wilayah regional Indonesia menggunakan Indeks KAMI terbaru.

Untuk mengukur kesiapan institusi terhadap ancaman tersebut, Badan Siber dan Sandi Negara (BSSN) mengembangkan Indeks KAMI, sebuah alat evaluasi berbasis ISO/IEC 27001 dan regulasi perlindungan data. Institusi kesehatan dapat menerapkan langkah tepat dalam melindungi data pasien, keakurasian data dan penyesuaian pada standar keamanan informasi yang berlaku [5]. Penelitian ini bertujuan mengevaluasi tingkat keamanan informasi di RSUD KHZ Musthafa menggunakan Indeks KAMI 5.0 sesuai ISO/IEC

27001:2022, dengan fokus pada beberapa area strategis melalui kuesioner yang dijawab oleh tim manajemen TI rumah sakit.

2. TINJAUAN PUSTAKA

2.1. Keamanan Informasi

Keamanan informasi secara umum merupakan upaya untuk melindungi suatu informasi baik berbentuk fisik maupun non-fisik dari berbagai macam ancaman. Keamanan informasi dalam ranah digital memiliki 3 asas, yaitu *Confidentiality*, yaitu mempertahankan pembatasan yang sah terhadap akses dan pengungkapan informasi, termasuk cara untuk melindungi privasi pribadi dan informasi kepemilikan, *Integrity*, yaitu menjaga terhadap modifikasi atau penghancuran informasi yang tidak pantas dan memastikan informasi tersebut tidak dapat disangkal dan autentik, dan *Availability*, yaitu memastikan akses dan penggunaan informasi yang tepat waktu dan dapat diandalkan [6],

2.2. Evaluasi

Evaluasi berasal dari bahasa prancis "*évaluation*" yang berarti tindakan menilai atau menilai. Evaluasi merupakan sebuah proses penting dalam memberi kesimpulan yang didasarkan pada suatu penilaian [7]. Evaluasi ini dilakukan secara sistematis dan dirancang untuk membantu pengambilan keputusan yang lebih baik.

2.3. Sistem Informasi Manajemen Rumah Sakit (SIMRS)

Sistem Informasi Manajemen Rumah Sakit (SIMRS) adalah suatu sistem teknologi informasi komunikasi yang memproses dan mengintegrasikan seluruh alur proses pelayanan Rumah Sakit dalam bentuk jaringan koordinasi, pelaporan, dan prosedur administrasi untuk memperoleh informasi secara tepat dan akurat, dan merupakan bagian dari Sistem Informasi Kesehatan [8]. Sistem Informasi Kesehatan adalah seperangkat tatanan yang meliputi data, informasi, indikator, prosedur, teknologi, perangkat, dan sumber daya manusia yang saling berkaitan dan dikelola secara terpadu untuk mengarahkan tindakan atau keputusan yang berguna dalam mendukung pembangunan kesehatan [9].

2.4. Indeks KAMI

Indeks Keamanan Informasi (KAMI) merupakan aplikasi yang digunakan sebagai alat bantu untuk melakukan asesmen dan evaluasi tingkat kesiapan (Kelengkapan dan Kematangan) penerapan keamanan informasi [10]. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2022.

Indeks KAMI tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan kerangka kerja keamanan informasi kepada Pimpinan Instansi. Dengan adanya update pada SNI ISO/IEC 27001:2022, telah dilakukan revisi Indeks Keamanan Informasi (KAMI) dan dilakukan update dari Indeks KAMI versi 4.2 menjadi Indeks KAMI versi 5.0

2.5. ISO 27001:2022

ISO/IEC 27001 merupakan standar internasional yang digunakan dalam sistem manajemen keamanan informasi (*Information Security Management System* – ISMS), yang disusun dan diterbitkan oleh *International Organization for Standardization* (ISO) bersama dengan *International Electrotechnical Commission* (IEC). ISO/IEC 27001 bertujuan untuk menjamin perlindungan terhadap seluruh aspek keamanan informasi, yang mencakup unsur kerahasiaan, integritas, serta ketersediaan data [11]. ISO/IEC 27001:2022, resmi diterbitkan pada 25 Oktober 2022 untuk menanggapi tantangan global di bidang keamanan siber dan meningkatkan kepercayaan terhadap sistem digital [12].

2.6. Studi Komparatif

Studi sebelumnya menerapkan penggunaan Indeks KAMI versi 5.0 pada Sistem Informasi Manajemen Rumah Sakit (SIMRS) di RSUD Bali Mandara yang tergolong rumah sakit tipe B, dan memperoleh skor sebesar 177. Hasil ini mengindikasikan bahwa tingkat kesiapan terhadap sertifikasi ISO 27001 berada dalam kategori 'Tidak Memenuhi Syarat' [13]. Sementara itu, riset lain yang menggunakan Indeks KAMI versi 4.2 di RS Benyamin Guluh, sebuah rumah sakit tipe C yang berlokasi di Kabupaten Kolaka, menunjukkan bahwa tingkat kematangan serta kelengkapan sistem keamanan informasinya masih berada pada level II, yang juga diklasifikasikan sebagai 'Tidak Memenuhi Syarat'. Penelitian tersebut juga mengungkap adanya sejumlah gap yang belum sesuai dengan ketentuan dalam ISO 27001:2013." [14].

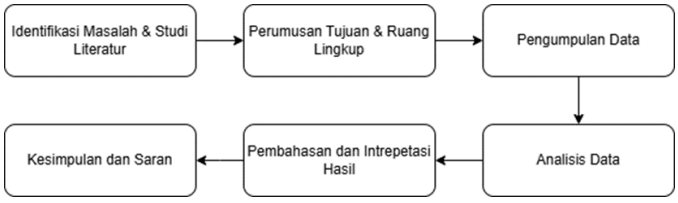
2.7. Landasan Teori

Penelitian ini didasarkan pada integrasi antara:

1. *Framework* ISO/IEC 27001:2022 sebagai standar global pengelolaan keamanan informasi.
2. *Framework* Indeks KAMI 5.0 sebagai instrumen nasional evaluasi kesiapan keamanan di institusi publik.
3. Kepatuhan terhadap UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, sebagai dasar hukum nasional.

3. KONSEP PERANCANGAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif, yaitu metode penelitian yang digunakan untuk mengamati, mendeskripsikan, dan menginterpretasikan fenomena secara alami dan mendalam, tanpa manipulasi terhadap variabel [15]. Penelitian ini tidak berfokus pada pengujian hipotesis statistik, melainkan pada eksplorasi, interpretasi, dan deskripsi terhadap situasi aktual terkait penerapan keamanan informasi pada Sistem Informasi Manajemen Rumah Sakit (SIMRS).



Gambar 1 Tahapan Penelitian Evaluasi Tingkat Keamanan

https://doi.org/10.46961/jommit.v9i1

Gambar 1 adalah tahapan penelitian yang dilakukan untuk mengevaluasi tingkat keamanan SIMRS di RSUD KHZ Musthafa. Tahapan pertama yaitu mengidentifikasi masalah terkait keamanan informasi dalam sistem manajemen rumah sakit melalui wawancara studi pendahuluan dengan managemen IT RSUD KHZ Musthafa, dan melakukan studi literatur dari jurnal, buku, standar keamanan informasi seperti ISO 27001, COBIT, NIST CSF, juga *framework* Indeks KAMI 5.0.

Proses selanjutnya ialah menentukan tujuan utama penelitian yaitu menganalisis dan mengevaluasi pemanfaatan Indeks KAMI 5.0 dalam mengevaluasi SIMRS dan menentukan ruang lingkup atau cakupan yang akan dievaluasi dan aspek keamanan yang diteliti yaitu:

Tahapan selanjutnya adalah pengumpulan data yang dilakukan dengan wawancara dan observasi kepada manajemen IT rumah sakit dengan memberikan daftar pertanyaan yang ada dalam *framework* Indeks KAMI 5.0 dimulai dengan mengkategorikan sistem elektronik sebagai tumpuan utama pengukuran tingkat keamanan informasi berdasarkan besar atau tidaknya sistem elektronik objek evaluasi Indeks KAMI, yang tertera pada gambar 2.

KATEGORI SISTEM ELEKTRONIK				
Rendah		**Skor Akhir**		**Status Kesiapan**
10	15	0	247	Tidak Layak
		248	443	Pemenuhan Kerangka Kerja Dasar
		444	760	Cukup Baik
		761	916	Baik
Tinggi		**Skor Akhir**		**Status Kesiapan**
16	34	0	387	Tidak Layak
		388	646	Pemenuhan Kerangka Kerja Dasar
		647	828	Cukup Baik
		829	916	Baik
Strategis		**Skor Akhir**		**Status Kesiapan**
35	50	0	472	Tidak Layak
		473	760	Pemenuhan Kerangka Kerja Dasar
		761	864	Cukup Baik
		865	916	Baik

Gambar 2 Kategori Sistem Elektronik

Pertanyaan selanjutnya mengenai 7 area lain dengan meminta tanggapan dari responden yaitu managemen IT RSUD mulai dari area yang terkait dengan bentuk kerangka kerja dasar keamanan informasi (label "1"), efektifitas dan konsistensi penerapannya (label "2"), dan kemampuan untuk selalu meningkatkan kinerja keamanan informasi (label "3"). Responden memberikan jawaban dengan kategori "Tidak Dilakukan", "Dalam Perencanaan", "Dalam Penerapan atau Diterapkan Sebagian", dan "Diterapkan secara menyeluruh" sesuai dengan keadaan atau kondisi keamanan sistem rumah sakit. Semua jawaban diberikan skor yang akan diproses oleh *framework* Indeks KAMI seperti pada gambar 3.

	Kategori Pengamanan		
Status Pengamanan	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan atau Diterapkan Sebagian	2	4	6
Diterapkan secara Menyeluruh	3	6	9

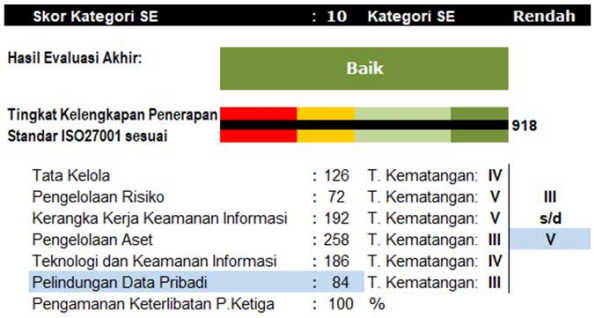
Gambar 3 Tabel penilaian

Proses selanjutnya yaitu analisis data dari jawaban yang sudah dikumpulkan dimasukkan pada *framework* Indeks KAMI yang akan menampilkan tingkat keamanan informasi melalui skor tiap area cakupan yang sudah dijawab yang dihitung seluruhnya oleh *framework*. Skor tiap area cakupan dikategorikan sesuai dengan kategori sistem elektronik dan didefinisikan sebagai:

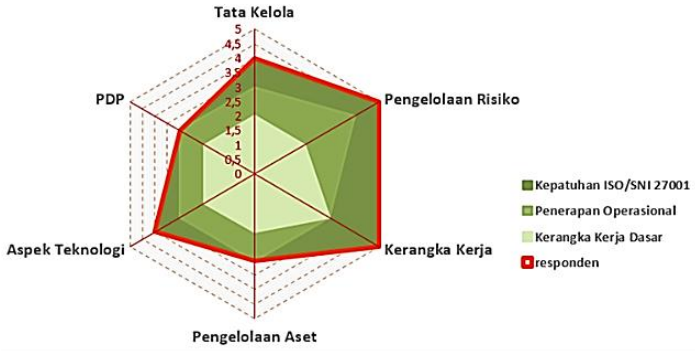
1. Tingkat I - Kondisi Awal
2. Tingkat II - Penerapan Kerangka Kerja Dasar
3. Tingkat III - Terdefinisi dan Konsisten
4. Tingkat IV - Terkelola dan Terukur
5. Tingkat V – Optimal

Tingkatan ini ditambah dengan tingkatan antara - I+, II+, III+, dan IV+, sehingga total terdapat 9 tingkatan kematangan.

Total skor dari semua cakupan area dihitung seluruhnya untuk menampilkan skor akhir yang mereprentasikan kesiapan sertifikasi ISO 27001 seperti pada gambar 4 dan diagram 6 sudut yang menampilkan visualisasi skor akhir pada gambar 5.



Gambar 4 Contoh hasil skor akhir



Gambar 5 Diagram Contoh hasil skor akhir

Tahapan selanjutnya yaitu Pembahasan dan intrepetasi hasil, dengan membahas hasil jawaban yang sudah dimasukkan pada diagram di *sheet dashboard framework* Indeks KAMI dan menintrepetasikan tampilan dari diagram hasil skor.

Proses terakhir yaitu kesimpulan dan saran pada proses tahapan yang terakhir ini dilakukan penyimpulan temuan utama evaluasi tingkat keamanan dan memberi saran untuk perbaikan dan pengembangan cakupan area yang nantinya enjadi bahan evaluasi managemen IT rumah sakit.

4. HASIL DAN PEMBAHASAN

4.1. Pengumpulan dan Analisis Data

Data yang sudah terkumpul dan terinput pada tabel pengisian di aplikasi Indeks KAMI akan dihitung sendiri oleh aplikasi excel tersebut dengan skor yang sudah ditentukan sesuai dengan jawaban yang terinput sesuai dengan gambar 3. Skor dari cakupan

https://doi.org/10.46961/jommit.v9i1

area 1 yaitu Kategori Sistem Elektronik menentukan tipe sistem elektronik yang digunakan beserta area skor yang menentukan penilaian akhir sesuai dengan Gambar 2. Untuk cakupan area 2 sampai 6, hasil dari skor kategori 1 dan 2 menentukan apakah skor dari jawaban kategori 3 valid atau tidak untuk dihitung. Cakupan area 7 hanya memiliki kategori 1 dan 2 saja sedangkan area 8 mempunyai rumus tersendiri. Semua diatur sesuai dengan pedoman dari *framework* Indeks KAMI.

Tabel 1 Skor Kategori Sistem Elektronik

Kategori	Jumlah	Point	Total
Rendah	4	1	4
Tinggi	5	2	10
Stragetis	1	5	5
Total skor			19

Hasil jawaban dari Kategori Sistem Elektronik menunjukkan skor 19 yang berarti SIMRS dari RSUD KHZ Musthafa memiliki kategori Tinggi dengan skor minimum 16, yang berarti sistem elektronik yang digunakan cukup besar dan penting untuk diamankan dari berbagai ancaman.

Tabel 2 Skor Tata Kelola Keamanan Informasi.

Status Pengamanan	Kategori			
	1	2	3	
Tidak Dilakukan	0	1	4	
Dalam Perencanaan	1	0	0	
Dalam Penerapan atau Diterapkan Sebagian	5	1	2	
Diterapkan secara Menyeluruh	2	6	0	
Tidak Berlaku/Relevan	0	0	0	
Total Skor	17	40	0	= 57

Hasil jawaban dari Tata Kelola Keamanan Informasi pada kategori 1 dan 2 menghasilkan skor 57, yang berarti belum mencapai skor minimum untuk validasi skor kategori 3.

Tabel 3 Tingkat Kematangan Tata Kelola Keamanan Informasi.

Status Pengamanan	Kategori			
	II	III	IV	
Tidak Dilakukan	0	1	4	
Dalam Perencanaan	1	0	0	
Dalam Penerapan atau Diterapkan Sebagian	5	1	2	
Diterapkan secara Menyeluruh	2	6	0	
Tidak Berlaku/Relevan	0	0	0	
Total Skor	41	0	0	= 41

Tingkat kematangan Tata Kelola Keamanan Informasi menghasilkan skor 41 yang bertingkat II yaitu penerapan kerangka kerja dasar.

Tabel 4 Skor Pengelolaan Risiko Keamanan Informasi.

Status Pengamanan	Kategori			
	1	2	3	
Tidak Dilakukan	4	2	1	
Dalam Perencanaan	3	0	0	
Dalam Penerapan atau Diterapkan Sebagian	2	2	1	
Diterapkan secara Menyeluruh	1	0	0	
Tidak Berlaku/Relevan	0	0	0	
Total Skor	10	8	0	= 18

Hasil jawaban dari Pengelolaan Risiko Keamanan Informasi pada kaegori 1 dan 2 menghasilkan skor 18, yang dimana belum mencapai skor minimum untuk validasi skor kategori 3.

Tabel 5 Tingkat Kematangan Pengelolaan Risiko Keamanan Informasi.

Status Pengamanan	Kategori			
	II	III	IV	
Tidak Dilakukan	4	2	1	
Dalam Perencanaan	3	0	0	
Dalam Penerapan atau Diterapkan Sebagian	2	2	1	
Diterapkan secara Menyeluruh	1	0	0	
Tidak Berlaku/Relevan	0	0	0	
Total Skor	10	0	0	= 10

Tingkat kematangan Pengelolaan Risiko Keamanan Informasi menghasilkan skor 10 dimana belum mencapai skor minimum tingkat kematangan II, yang menjadikan cakupan ini memiliki tingkat kematangan I yaitu kondisi awal.

Tabel 6 Skor Kerangka Kerja Keamanan Informasi.

Status Pengamanan	Kategori			
	1	2	3	
Tidak Dilakukan	2	4	5	
Dalam Perencanaan	4	1	1	
Dalam Penerapan atau Diterapkan Sebagian	2	4	1	
Diterapkan secara Menyeluruh	4	2	3	
Tidak Berlaku/Relevan	0	0	0	
Total Skor	20	30	0	= 50

Hasil Jawaban dari Kerangka Kerja Keamanan informasi menunjukan hasil skor 50 yang dimana belum mencapai skor minimum untuk validasi skor kategori 3.

Tabel 7 Tingkat Kematangan Kerangka Kerja Keamanan Informasi.

Status Pengamanan	Kategori				
	II	III	IV	V	
Tidak Dilakukan	1	8	1	2	
Dalam Perencanaan	4	1	0	0	
Dalam Penerapan atau Diterapkan Sebagian	2	4	0	0	
Diterapkan secara Menyeluruh	4	4	1	0	
Tidak Berlaku/Relevan	0	0	0	0	
Total Skor	22	0	0	0	= 22

Hasil skor tingkat kematangan Kerangka Kerja Keamanan Informasi ialah 22, yang menunjukkan belum mencapai tingkat

https://doi.org/10.46961/jommit.v9i1

kematangan II namun masuk dalam tingkat kematangan I+ kondisi awal

Tabel 8 Skor Pengelolaan Aset Informasi

Status Pengamanan	Kategori			
	1	2	3	
Tidak Dilakukan	2	1	3	
Dalam Perencanaan	0	1	0	
Dalam Penerapan atau Diterapkan Sebagian	4	2	1	
Diterapkan secara Menyeluruh	21	15	3	
Tidak Berlaku/Relevan	0	0	0	
Total Skor	71	100	0	= 171

Hasil skor dari jawaban Pengelolaan Aset Informasi menghasilkan nilai 171 yang dimana belum mencapai skor miminum validasi kategori 3.

Tabel 9 Tingkat Kematangan Pengelolaan Aset Informasi

Status Pengamanan	Kategori		
	II	III	
Tidak Dilakukan	2	1	
Dalam Perencanaan	0	1	
Dalam Penerapan atau Diterapkan Sebagian	5	2	
Diterapkan secara Menyeluruh	21	15	
Tidak Berlaku/Relevan	0	0	
Total Skor	95	0	= 95

Hasil skor tingkat kematangan Pengelolaan Aset Informasi menghasilkan nilai 95 yang menunjukan tingkat kematangan II yaitu penerapan kerangka kerja dasar.

Tabel 10 Skor Teknologi dan Keamanan Informasi

Status Pengamanan	Kategori			
	1	2	3	
Tidak Dilakukan	1	2	0	
Dalam Perencanaan	0	1	1	
Dalam Penerapan atau Diterapkan Sebagian	5	2	2	
Diterapkan secara Menyeluruh	8	10	3	
Tidak Berlaku/Relevan	0	0	0	
Total Skor	34	70	36	= 140

Hasil skor dari jawaban Teknologi dan Keamanan Informasi menghasilkan nilai 140. Pada area ini, kategori 3 sudah valid untuk terhitung namun pada pertanyaan nomor 6.35 memiliki kriteria nilai minimum, dan dari hasil skor diatas menunjukan belum mencapai skor minimum tersebut sehingga skor dari pertanyaan 6.35 belum valid.

Tabel 11 Tingkat Kematangan Teknologi dan Keamanan Informasi

Status Pengamanan	Kategori			
	II	III	IV	
Tidak Dilakukan	1	2	0	
Dalam Perencanaan	0	1	1	
Dalam Penerapan atau Diterapkan Sebagian	5	2	2	
Diterapkan secara Menyeluruh	8	13	0	
Tidak Berlaku/Relevan	0	0	0	
Total Skor	34	0	0	= 34

Hasil skor tingkat kematangan Teknologi dan Keamanan Informasi menghasilkan nilai 34 yang menunjukan tingkat kematangan II yaitu penerapan kerangka kerja dasar.

Tabel 12 Skor Perlindungan Data Pribadi

Status Pengamanan	Kategori		
	1	2	
Tidak Dilakukan	0	0	
Dalam Perencanaan	0	0	
Dalam Penerapan atau Diterapkan Sebagian	0	0	
Diterapkan secara Menyeluruh	4	12	
Tidak Berlaku/Relevan	0	0	
Total Skor	12	72	= 84

Hasil skor dari jawaban Perlindungan Data Pribadi menghasilkan nilai 84 dengan status pengamanan ditetapkan secara menyeluruh untuk semua pertanyaan.

Tabel 13 Skor Perlindungan Data Pribadi

Status Pengamanan	Kategori		
	II	III	
Tidak Dilakukan	0	0	
Dalam Perencanaan	0	0	
Dalam Penerapan atau Diterapkan Sebagian	0	0	
Diterapkan secara Menyeluruh	6	10	
Tidak Berlaku/Relevan	0	0	
Total Skor	24	60	= 84

Hasil skor tingkat kematangan II dan III menghasilkan nilai 63 yang menunjukan tingkat kematangan III yaitu terdefinisi dan konsisten.

https://doi.org/10.46961/jommit.v9i1

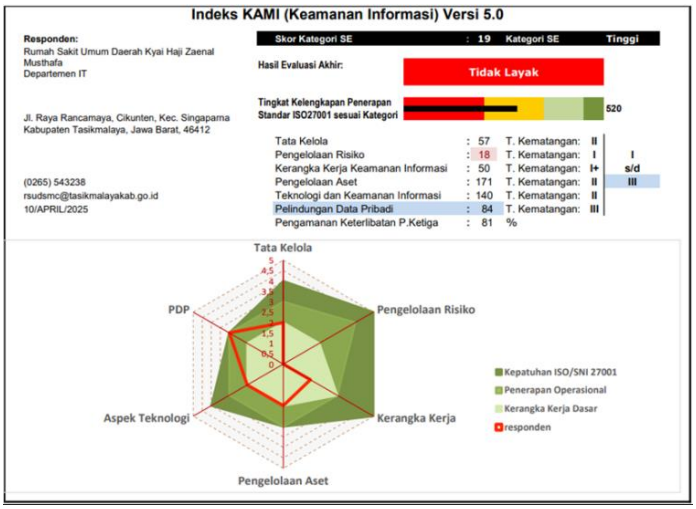
Tabel 14 Skor Suplemen

Status Pengamanan	Kategori 1
Tidak Dilakukan	5
Dalam Perencanaan	0
Dalam Penerapan atau Diterapkan Sebagian	0
Diterapkan secara Menyeluruh	22
Tidak Berlaku/Relevan	0
Total Skor	81%

Hasil skor Suplemen menunjukkan 81% dengan rumus:
Jumlah skor / (Jumlah pertanyaan*3) = 66 / 81 = 0,81481 = 81%
Cakupan area ini tidak memiliki tingkat kematangan, hanya persentase status keamanan.

4.2. Pembahasan dan Intrepetasi Hasil

Seluruh jawaban yang sudah diinput pada aplikasi excel Indeks KAMI akan menampilkan skor akhir pada bagan diagram *di sheet Dashboard*. Bagan menampilkan 3 bagian utama yaitu kategori SE, hasil evaluasi akhir, tingkat kelengkapan penerapan ISO27001 sesuai kategori dan tingkat kematangan sesuai kategori.



Gambar 6 Diagram hasil skor akhir

SIMRS di RSUD KHZ Musthafa memiliki sistem elektronik berkategori "Tinggi" dengan hasil evaluasi akhir "Tidak Layak". Walaupun pada rentang kelengkapan penerapan ISO 27001 mencapai baris kuning dengan skor 520, skor pada cakupan area Pengelolaan Resiko memiliki skor 18 dan tingkat kematangan I, yang merupakan skor rendah dan menyebabkan hasil evaluasi akhir yang seharusnya "Pemenuhan Kerangka Kerja Dasar" menjadi "Tidak Layak". Hal ini menjadi sorotan utama untuk mengkaji ulang dan memperbaiki sektor pada pengelolaan risiko keamanan informasi di RSUD KHZ Musthafa. Dari hasil pertanyaan pada cakupan area Pengelolaan Risiko, ada beberapa poin yang harus segera ditindak lanjuti berdasarkan status pengamanannya yang belum dilakukan sama sekali, yaitu:

1. Menetapkan penanggung jawab risiko khusus dalam manajemen risiko keamanan informasi, termasuk alur pelaporan yang dapat dieskalasikan hingga ke tingkat pimpinan.
2. Menyusun dan mendokumentasikan kerangka kerja risiko yang mencakup klasifikasi aset, tingkat ancaman, kemungkinan, serta dampaknya, dan dievaluasi secara berkala.
3. Menentukan ambang risiko yang dapat diterima sebagai dasar dalam pengambilan keputusan mitigasi.
4. Menyusun mitigasi risiko berbasis prioritas dengan penanggung jawab dan target waktu penyelesaian yang jelas, serta memastikan efektivitas penggunaan sumber daya dan dilakukan evaluasi berkala.

Namun di sisi lain, cakupan area Perlindungan Data Pribadi memiliki skor terbaik dengan skor 84 dan tingkat keamtangan III. Dikarenakan hasil dari evaluasi keamanan yang difasilitasi BSRE belum atau tidak diberikan dari pihak terkait dilansir oleh Kepala bagian IT RSUD KHZ Musthafa, evaluasi Indeks KAMI ini belum bisa dibandingkan dengan hasil evaluasi dari BSRE.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil dari penelitian yang telah dilakukan dapat dibuat kesimpulan, ialah:

1. SIMRS RSUD KHZ Musthafa memiliki sistem elektronik yang berkategori "Tinggi"
2. Hasil Evaluasi Akhir untuk kesiapan sertifikasi ISO 27001 untuk RSUD KHZ Musthafa "Tidak Layak" dengan skor akhir 520
3. Cakupan area dengan skor tertinggi adalah Perlindungan Data Pribadi dengan skor 84 dan tingkat kematangan III "Terdefinisi dan Konsisten", sedangkan skor terendah dimiliki oleh Pengelolaan Risiko dengan skor 18 dan tingkat kematangan I "Kondisi Awal."
4. Walaupun skor akhir sudah mencapai angka 520 dan masuk kotak kuning pada rentang kelengkapan penerapan ISO 27001, skor rendah dari cakupan area Pengelolaan Risiko menyebabkan hasil evaluasi akhir menjadi "Tidak Layak".

Penelitian ini menunjukkan bahwa SIMRS pada Rumah Sakit Umum Daerah KHZ Musthafa masih kurang dalam tingkat kesiapan pengamanan informasi. Hasi dari penelitian ini merekomendasikan agar pihak manajemen IT RSUD KHZ Musthafa mengkaji ulang dan memperbaiki atau menambahkan peraturan atau kebijakan pada sektor pengelolaan risiko keamanan informasi sesuai dengan pertanyaan yang ada pada Indeks KAMI 5.0 serta pada cakupan area lainnya yang masih memiliki skor rendah seperti area Kerangka Kerja Keamanan Informasi yang masih bertingkat kematangan I+ yaitu "Kondisi Awal".

Kekurangan dari penelitian ini adalah hasil dari evaluasi ini hanya sebatas gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi yang memenuhi aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2022. Harapan untuk penelitian selanjutnya bisa meneliti lebih dalam tingkat keamanan SIMRS dari RSUD KHZ Musthafa dan atau membantu dalam memperbaiki atau menambahkan tingkat keamanan tersebut.

https://doi.org/10.46961/jommit.v9i1

DAFTAR PUSTAKA

[1] M. E. Whitman and H. J. Mattord, *Principles of Information Security*, 6th ed. Boston, MA: Cengage Learning, 2018.

[2] Awaludin, W. Sulistyadi, and A. F. Chandra, "Analysis of Attacks and Cybersecurity in the Health Sector During a Pandemic COVID-19: Scoping Review," *Journal of Social Science*, vol. 4, pp. 62–70, 2023, doi: 10.46799/jss.v4i1.512.

[3] L. Wasserman and Y. Wasserman, "Hospital cybersecurity risks and gaps: Review (for the non-cyber professional)," 2022.

[4] M. A. Fauzi, P. Yeng, B. Yang, and D. Rachmayani, "Examining the Link between Stress Level and Cybersecurity Practices of Hospital Staff in Indonesia," in *Proc. ACM Int. Conf. Series*, 2021.

[5] W. S. Basri and A. L. A., "Risk Management in Information Systems: Applying ISO 31000:2018 and ISO/IEC 27001:2022 Controls at PMI's Central Clinic," *Int. J. Appl. Inf. Manag.*, vol. 4, pp. 1–13, 2018.

[6] M. Nieles, K. Dempsey, and V. Y. Pillitteri, *An Introduction to Information Security*. Gaithersburg, MD: NIST, 2017.

[7] T. Taqiyuddin, S. Supardi, and L. Lubna, "Evaluasi Formatif dan Sumatif dalam Pembelajaran Pendidikan Agama Islam," *J. Ilmiah Profesi Pendidikan*, vol. 9, pp. 1936–1942, 2024, doi: 10.29303/jipp.v9i3.2392.

[8] Kementerian Kesehatan Republik Indonesia, *Peraturan Menteri Kesehatan Republik Indonesia Nomor 82 Tahun 2013*, 2013.

[9] B. S. Nurwito et al., "Manfaat dan Efektivitas Penerapan Sistem Informasi pada Rumah Sakit Swasta dan Rumah Sakit Pemerintah," *Jurnal Manajemen Informasi Kesehatan Indonesia*, vol. 12, no. 2, 2022, doi: 10.33560/jmiki.v12i2.664.

[10] Badan Siber dan Sandi Negara (BSSN), "Indeks KAMI," [Online]. Available: https://www.bssn.go.id/indeks-kami/.

[11] R. Nur Akmal, D. Dwi Susilo, and E. Halma Rouf, "Evaluasi Keamanan Sistem Informasi Rumah Sakit: Metode Pengujian ISO 27001 di RS Khusus Mata Purwokerto," 2025.

[12] M. Malatji, "Management of enterprise cyber security: A review of ISO/IEC 27001:2022," in *Proc. Int. Conf. Cyber Manag. Eng. (CyMaEn)*, 2023.

[13] Nyoman, A. A. Wibawa, A. Agung, N. Hary Susila, and M. A. Pasirulloh, "Information Security Evaluation at Hospital Using Index KAMI 5.0 and Recommendations Based on ISO/IEC 27001:2022," *J. Inf. Syst. Informatics*, vol. 6, 2024, doi: 10.51519/journalisi.v6i4.949.

[14] K. Sari, N. Ningsi, N. Zainuddin, and A. M. Sajiah, "Evaluation of Information Security at Benyamin Guluh Kolaka Hospital using the KAMI 4.2 Index with ISO 27001:2013," *J. Media Informasi Teknologi*, vol. 1, 2024.

[15] Sugiyono, *Metode Penelitian dan Pengembangan: Pendekatan Kualitatif, Kuantitatif, dan R&D*. Bandung: Alfabeta, 2015.

https://doi.org/10.46961/jommit.v9i1