Teknika 19 (3): 795-808

JURNAL TEKNIKA
ISSN: 0854-3143
e-ISSN: 2622-3481
Journal homepage: http://jurnal.polsri.ac.id/index.php/teknika
Journal Email: teknika@polsri.ac.id

Analisis Keamanan Informasi SIMRS dengan Metode Indeks KAMI dan OCTAVE Allegro

Suroso*[1], Wasilah[2]

[*1,2]Program Studi Magister Teknik Informatika, Institut Informatika Dan Bisnis Darmajaya, Bandar Lampung, Indonesia
*Email Penulis Korespondensi: suroso.2321211006@mail.darmajaya.ac.id

Abstrak

Keamanan informasi merupakan elemen krusial dalam mendukung operasional rumah sakit, khususnya pada Sistem Informasi Manajemen Rumah Sakit (SIM-RS) yang menangani data sensitif seperti informasi pasien dan data medis. Penelitian ini bertujuan mengevaluasi praktik keamanan informasi pada SIM-RS di Rumah Sakit XYZ dengan pendekatan gabungan antara Indeks Keamanan Informasi (KAMI) dan metode OCTAVE Allegro. Indeks KAMI digunakan untuk mengukur kematangan dan kesiapan manajemen keamanan informasi, sementara OCTAVE Allegro membantu dalam identifikasi, penilaian, dan prioritisasi risiko. Hasil evaluasi menunjukkan tingkat keamanan informasi berada dalam kategori "Cukup Baik" dengan skor 492. Namun, beberapa aspek seperti kategori Sistem Elektronik (skor 26) dan Pengelolaan Risiko (nilai 24) perlu ditingkatkan. Analisis risiko dengan OCTAVE Allegro mengidentifikasi beberapa risiko prioritas tinggi (kategori Mitigate) seperti kontrol akses, verifikasi data, backup rutin, dan perlindungan terhadap kebocoran data. Risiko Defer seperti penyalahgunaan hak akses dapat ditangani melalui kebijakan akses yang lebih selektif, sedangkan risiko Accept berdampak rendah cukup ditangani dengan pelatihan staf dan validasi input. Integrasi metode KAMI dan OCTAVE Allegro memberikan gambaran menyeluruh dalam memitigasi risiko serta memperkuat keamanan informasi di Rumah Sakit XYZ.

Kata kunci*—Keamanan Informasi, SIMRS, Indeks KAMI, OCTAVE Allegro*

Abstract

Information security is a crucial element in supporting hospital operations, especially within the Hospital Management Information System (HMIS), which handles sensitive data such as patient information and medical records. This study aims to evaluate information security practices in the HMIS of XYZ Hospital using a combined approach of the Information Security Index (KAMI) and the OCTAVE Allegro method. The KAMI Index is used to measure the maturity and readiness of information security management, while OCTAVE Allegro assists in identifying, assessing, and prioritizing security risks. The evaluation results indicate that the level of information security is categorized as "Fairly Good" with a score of 492. However, certain aspects, such as the Electronic System category (score of 26) and Risk Management (score of 24), require improvement. Risk analysis using OCTAVE Allegro identified several high-priority risks (Mitigate category), such as access control, data verification, routine backups, and protection

Received: June 7, 2025; Online Available: June 29, 2025

against data leakage. Defer risks, like access rights misuse, can be managed through more selective access policies, while low-impact Accept risks can be addressed with simple controls such as staff training and data input validation. The integration of the KAMI Index and OCTAVE Allegro provides a comprehensive overview for risk mitigation and enhances information security at XYZ Hospital.

Keywords— *Information Security, SIMRS, KAMI Index, OCTAVE Allegro*

1. PENDAHULUAN

Keamanan informasi merupakan mekanisme untuk menjaga kerahasiaan, konsistensi, ketepatan, dan ketersediaan aset informasi selama proses pengolahan, penyimpanan, dan transmisi [1]. Dalam era pemanfaatan teknologi informasi yang semakin luas, keamanan informasi menjadi hal krusial bagi organisasi atau instansi. Semakin banyak data yang dikelola, semakin besar pula risiko informasi tersebut rusak, hilang, atau terekspos ke pihak yang tidak berwenang. Rumah sakit, sebagai institusi yang menyediakan layanan kesehatan masyarakat, memanfaatkan teknologi informasi untuk mendukung kegiatan operasionalnya [2]. Data yang dikelola, seperti data pribadi pasien, informasi medis, hingga informasi keuangan, merupakan aset sensitif yang harus dilindungi. Serangan terhadap data medis tidak hanya mengancam privasi pasien tetapi juga dapat menghambat pengobatan, yang berpotensi membahayakan kesehatan dan kesejahteraan mereka [3].

Salah satu penerapan teknologi informasi yang signifikan di rumah sakit adalah Sistem Informasi Manajemen Rumah Sakit (SIM-RS). Sistem ini mendukung pengelolaan data secara terintegrasi, mempercepat pengambilan keputusan klinis dan manajerial, serta meningkatkan efisiensi operasional [4]. SIM-RS mencakup berbagai modul, seperti sistem informasi medis, laboratorium, radiologi, dan farmasi, yang semuanya bertujuan meningkatkan kualitas layanan kesehatan. Rumah Sakit XYZ telah mengadopsi SIM-RS untuk mendukung proses administrasi, manajemen informasi, hingga pengadaan barang secara efektif. Namun, penggunaan teknologi informasi ini juga menghadirkan tantangan berupa risiko keamanan, seperti peretasan, pencurian data, atau serangan *malware* [5]. Untuk itu, diperlukan audit keamanan sistem informasi guna memastikan perlindungan terhadap data sensitif dan keberlanjutan operasional rumah sakit.

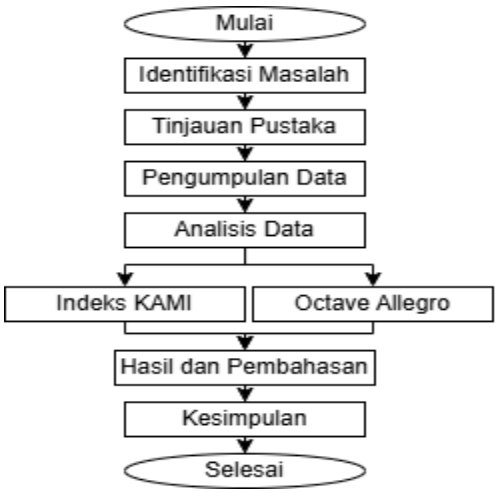
Berbagai penelitian telah dilakukan untuk mengevaluasi keamanan informasi menggunakan pendekatan yang berbeda. Penelitian oleh [5] mengevaluasi keamanan informasi di PT. Kano Teknologi Utama dengan Indeks KAMI versi 5.0 dan ISO/IEC 27001:2022 melalui pendekatan studi kasus, menghasilkan rekomendasi untuk meningkatkan keamanan informasi. Sedangkan [6] memanfaatkan metode OCTAVE Allegro dalam mengidentifikasi dan merancang mitigasi risiko pada aplikasi ujian online di SMA Semen Gresik, dengan fokus pada analisis aset informasi, ancaman, dan prioritas risiko. *OCTAVE Allegro* untuk mengkaji risiko pada sistem informasi akademik di perguruan tinggi, menghasilkan strategi perlindungan aset informasi kritis dan langkah mitigasi. Kemudian [7] menganalisis risiko keamanan informasi di RSUD Cengkareng menggunakan *OCTAVE Allegro*, mencakup identifikasi aset informasi, area masalah, skenario ancaman, hingga rekomendasi mitigasi risiko berdasarkan matriks risiko relatif. Terakhir, penelitian [8] mengevaluasi tingkat kematangan keamanan informasi di Tiyuh Pulung Kencana, Kabupaten Tulang Bawang Barat, menggunakan Indeks KAMI versi 4.2. Penelitian ini menemukan bahwa meskipun tingkat kematangan telah mencapai kategori 'baik', penguatan kebijakan dan prosedur tetap diperlukan untuk mencapai standar optimal.

Penelitian ini menggunakan pendekatan gabungan antara Indeks Keamanan Informasi (KAMI) dan *Octave Allegro*. Indeks KAMI, yang dikembangkan oleh Kementerian Komunikasi dan Informatika (Kominfo), dirancang untuk membantu instansi mengukur tingkat kematangan, kesiapan, dan kelengkapan manajemen keamanan informasi [9]. Dengan memberikan kerangka kerja yang jelas, Indeks KAMI mendukung penerapan keamanan informasi yang baik dan efektif [6]. Sementara itu, *Octave Allegro* adalah metode evaluasi risiko yang sistematis dan

komprehensif, dirancang untuk mengidentifikasi, menilai, dan memprioritaskan risiko keamanan informasi tanpa memerlukan keahlian mendalam dalam manajemen risiko [7].

Penelitian ini bertujuan untuk mengevaluasi praktik keamanan informasi yang diterapkan di Rumah Sakit XYZ. Dengan mengintegrasikan kedua metode tersebut, penelitian ini diharapkan dapat memberikan gambaran yang lebih holistik mengenai keamanan sistem informasi, memastikan perlindungan data pasien, dan menjaga keberlanjutan operasional rumah sakit dari potensi ancaman baik eksternal maupun internal.

2. METODE PENELITIAN



Gambar 1 Langkah Langkah Penelitian

Gambar 1 menyajikan langkah-langkah penelitian yang digunakan dalam penelitian ini supaya menghasilkan penelitian yang berkualitas.

2.1 Identifikasi Masalah

Pada tahap identifikasi Masalah, diidentifikasi berbagai permasalahan keamanan informasi pada SIM-RS di Rumah Sakit XYZ, seperti risiko pencurian data pasien, gangguan operasional akibat serangan malware, serta kelemahan dalam pengelolaan akses dan autentikasi.

2.2 Tinjauan Pustaka

Dalam tahap ini, dilakukan pengumpulan referensi dari berbagai literatur dan penelitian terdahulu yang relevan, termasuk pendekatan Indeks KAMI dan *Octave Allegro* dalam evaluasi keamanan informasi.

2.3 Pengumpulan Data

Dalam penelitian ini, data dikumpulkan melalui metode observasi, wawancara, dan penyebaran kuesioner kepada pegawai Rumah Sakit XYZ yang terlibat dalam pengelolaan SIM-RS. Namun, belum dijelaskan secara eksplisit mengenai jumlah responden, jabatan, maupun latar belakang profesional mereka. Untuk memperkuat validitas penelitian, penting untuk mencantumkan informasi berikut:

Dalam bagian metode, penting untuk dijelaskan bahwa responden merupakan bagian integral dari proses pengumpulan data kualitatif maupun kuantitatif. Oleh karena itu, penulis perlu mencantumkan:

1. Profil responden: jabatan, divisi, dan relevansi mereka terhadap pengelolaan SIM-RS.
2. Jumlah total partisipan, misalnya “sebanyak 12 orang yang terdiri dari 1 kepala bagian IT, 2 staf keamanan informasi, 3 operator sistem, dan 6 staf pengguna aplikasi SIM-RS”.

3. Penjelasan ini dapat memperjelas konteks evaluasi dan meningkatkan kepercayaan terhadap validitas temuan.

2.4 Analisis Data

Data yang telah dikumpulkan kemudian dianalisis untuk memahami kondisi dan potensi risiko keamanan informasi pada SIM-RS di Rumah Sakit XYZ dengan menggunakan metode Indeks KAMI dan *Octave Allegro*.

2.5 Metode Indeks KAMI dan Octave Allegro

Indeks KAMI digunakan untuk mengukur tingkat kematangan dan kesiapan manajemen keamanan informasi di rumah sakit [10]. *Octave Allegro* diterapkan untuk mengevaluasi dan memprioritaskan risiko keamanan informasi, dengan fokus pada identifikasi aset informasi kritis, ancaman, dan mitigasi risiko [11].

Metode Indeks KAMI digunakan untuk mengukur tingkat kematangan dan kesiapan keamanan informasi berdasarkan enam area utama: tata kelola, pengelolaan risiko, kerangka kerja, pengelolaan aset, teknologi, dan sistem elektronik. Setiap area dinilai menggunakan indikator yang diberi skor sesuai tingkat pemenuhannya. Hasil penilaian divisualisasikan dalam bentuk skor total dan radar chart untuk menunjukkan kondisi keamanan secara menyeluruh. Metode ini bersifat evaluatif dan bertujuan memberikan gambaran kelemahan yang perlu diperbaiki, bukan sebagai standar sertifikasi.

Sementara itu, *OCTAVE Allegro* digunakan untuk menganalisis risiko informasi secara sistematis. Tahapan utamanya meliputi identifikasi aset informasi kritis, area masalah, dan skenario ancaman, kemudian dilakukan penilaian risiko berdasarkan dampak terhadap reputasi, keuangan, produktivitas, kesehatan, dan aspek hukum. Setiap risiko dihitung skor relatifnya, lalu dikategorikan ke dalam pendekatan mitigasi: *Mitigate* (ditangani segera), *Defer* (ditunda), atau *Accept* (diterima). Metode ini menghasilkan rekomendasi keamanan yang terfokus, seperti kontrol akses, backup, dan pelatihan staf, sehingga memperkuat perlindungan terhadap data SIM-RS.

2.6 Hasil dan Pembahasan

Berdasarkan analisis dari kedua metode tersebut, hasil penelitian dirangkum untuk memberikan gambaran menyeluruh tentang kondisi keamanan informasi. Pembahasan mencakup rekomendasi untuk meningkatkan keamanan sistem informasi Penelitian diakhiri dengan menyajikan kesimpulan utama yang menjawab tujuan penelitian. Kesimpulan mencakup langkah-langkah penting untuk memastikan keamanan informasi pada SIM-RS di Rumah Sakit XYZ.

3. HASIL DAN PEMBAHASAN

Pada bagian ini disajikan hasil analisis keamanan informasi pada SIM-RS di Rumah Sakit XYZ menggunakan metode Indeks KAMI dan *Octave Allegro*. Analisis dengan Indeks KAMI mencakup 7 langkah penilaian, yaitu kategori sistem elektronik, tata kelola, pengelolaan risiko, kerangka kerja, pengelolaan aset, aspek teknologi, dan suplemen [12]. Pendekatan ini bertujuan untuk mengevaluasi tingkat kematangan dan kesiapan manajemen keamanan informasi rumah sakit.

Sementara itu, analisis dengan *Octave Allegro* dilakukan melalui 8 langkah sistematis, yang meliputi menetapkan kriteria pengukuran risiko, mengembangkan profil aset informasi, mengidentifikasi wadah aset informasi, mengidentifikasi kondisi dan situasi sistem kritis, mengidentifikasi skenario ancaman, mengidentifikasi risiko, menganalisis risiko, dan menentukan pendekatan mitigasi risiko [13]. Pendekatan ini dirancang untuk memberikan identifikasi risiko yang mendalam serta langkah mitigasi yang terfokus, sehingga dapat meningkatkan perlindungan terhadap data pasien dan keberlanjutan operasional rumah sakit.

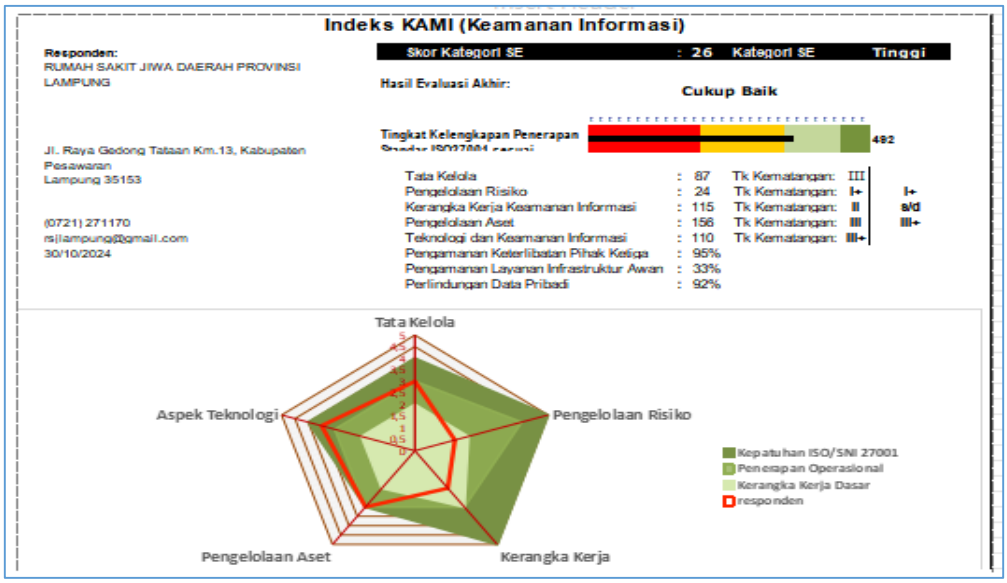
3.1. Indeks KAMI

Instrument penilaian Indeks KAMI 4.2. Instrument berupa Tabel Penilaian dan *Radar Chart* yang berisikan Skor Akhir Evaluasi dan Status Tingkat Kesiapan yang meliputi Tingkat Kematangan dan Tingkat Kelengkapan dan hasil keseluruhannya dapat ditemukan dalam Tabel 1.

Tabel 1. Nilai Untuk Tiap Area

Area Penilaian	Skor Evaluasi
Keamanan Sistem Elektronik	26
Tata Kelola Keamanan Informasi	87
Manajemen Risiko Keamanan Informasi	24
Kerangka Kerja Sistem Keamanan	115
Manajemen Aset Informasi	156
Teknologi dan Aspek Keamanan Teknis	110

Tampilan *dashboard* Indeks Keamanan Informasi (KAMI) menunjukkan hasil evaluasi terkait kesiapan dan pengelolaan keamanan informasi di Rumah Sakit XYZ. Berdasarkan *dashboard* ini, hasil evaluasi akhir menunjukkan skor 492 dengan kategori "Cukup Baik", yang berarti kondisi keamanan informasi di rumah sakit ini sudah cukup baik, namun masih ada beberapa aspek yang perlu diperbaiki, seperti terlihat pada Gambar 2.



Gambar 2 *Dashboard* Penilaian Indeks KAMI

Berikut adalah penjelasan dari tujuh kategori yang dievaluasi dalam tampilan tersebut:

a. Sistem Elektronik: Kategori ini menilai kesiapan dan keamanan sistem elektronik yang digunakan oleh organisasi, seperti *server*, database, dan infrastruktur digital lainnya [14]. Skor 26 dengan tingkat ketergantungan ‘Tinggi’ dan menunjukkan bahwa sistem elektronik membutuhkan perbaikan dan peningkatan dalam hal keamanan.
b. Tata Kelola Keamanan Informasi: Kategori ini mengevaluasi sejauh mana organisasi telah mengimplementasikan praktik tata kelola keamanan informasi, termasuk kebijakan, prosedur, dan manajemen yang ada [15]. Skor 87 menunjukkan bahwa tata kelola keamanan informasi pada SIM-RS di Rumah Sakit XYZ sudah cukup baik, meskipun masih memerlukan perbaikan untuk mencapai tingkat kesiapan yang lebih optimal.
c. Pengelolaan Risiko Keamanan Informasi: Kategori ini menilai pendekatan organisasi dalam mengidentifikasi, mengevaluasi, dan mengelola risiko terkait dengan keamanan informasi

[16]. Skor 24 menunjukkan bahwa manajemen risiko pada SIM-RS di Rumah Sakit XYZ masih memerlukan perhatian lebih.

d. Kerangka Kerja: menilai struktur, kebijakan, dan sistem yang diterapkan untuk menjaga keamanan informasi [17]. Skor 115 menunjukkan bahwa kerangka kerja keamanan informasi pada SIM-RS di Rumah Sakit XYZ sudah cukup terimplementasi dengan baik, meskipun masih ada ruang untuk penyempurnaan.
e. Pengelolaan Aset Informasi: Kategori ini mengevaluasi bagaimana organisasi mengelola aset informasi seperti data dan perangkat keras [18]. Skor 156 menunjukkan bahwa Area ini mendapatkan skor tertinggi, menunjukkan bahwa pengelolaan aset informasi, termasuk identifikasi dan perlindungannya, sudah dilakukan dengan cukup baik.
f. Teknologi dan Keamanan Informasi: Skor 110 menunjukkan bahwa teknologi dan aspek keamanannya telah cukup diperhatikan, tetapi masih ada kebutuhan untuk memperkuat implementasi teknologinya agar lebih sesuai dengan standar keamanan informasi.

Secara keseluruhan, hasil evaluasi menunjukkan bahwa pada SIM-RS di Rumah Sakit XYZ memiliki tingkat kesiapan keamanan informasi yang cukup baik, tetapi beberapa area, terutama pada kategori Sistem Elektronik dengan nilai skor 26 dan Pengelolaan Risiko dengan nilai skor 24, masih perlu diperbaiki untuk meningkatkan postur keamanan informasi secara keseluruhan.

3.2. Octave Alegro

Sebagaimana pengumpulan data dan informasi yang telah dilakukan pada penilaian menggunakan Indeks KAMI, data tersebut juga berasal dari responden yang sama. Namun, pada tahap ini, penilaian dilakukan dengan pendekatan *Octave Allegro* untuk memperdalam analisis risiko dan menyusun langkah mitigasi yang lebih terfokus [19].

Hasil penelitian ini menunjukkan bahwa tingkat keamanan informasi SIM-RS di Rumah Sakit XYZ berada pada kategori "Cukup Baik" dengan skor total Indeks KAMI sebesar 492. Temuan ini sejalan dengan studi yang dilakukan di RSUD Cengkareng [7] yang menggunakan metode OCTAVE Allegro dan juga menemukan sejumlah risiko tinggi terkait kontrol akses dan perlindungan data pasien. Sementara itu, studi di RS Benyamin Guluh Kolaka [18] dengan pendekatan Indeks KAMI menunjukkan skor yang lebih tinggi, namun tetap menyoroti kelemahan pada aspek tata kelola dan pengelolaan risiko. Hal ini menunjukkan bahwa meskipun rumah sakit telah menerapkan SIM-RS secara luas, isu keamanan informasi masih menjadi tantangan umum.

Perbedaan hasil antara rumah sakit satu dengan lainnya umumnya dipengaruhi oleh faktor seperti kesiapan infrastruktur TI, dukungan manajemen terhadap kebijakan keamanan, dan kapasitas sumber daya manusia di bidang IT. Misalnya, RS dengan unit TI yang terlatih dan adanya kebijakan keamanan formal cenderung memiliki skor kematangan yang lebih baik. Oleh karena itu, untuk meningkatkan generalisasi, studi lanjutan dapat melibatkan beberapa rumah sakit dengan karakteristik berbeda guna melihat pola risiko dan efektivitas mitigasi yang lebih luas.

3.2.1 Kriteria Pengukuran Resiko

Penulis menganalisis kriteria pengukuran risiko dengan menilai dampak area dan menetapkan skala utama. Identifikasi organizational drivers dilakukan untuk mengevaluasi dampak setiap area menggunakan Risk Measurement Criteria *Worksheet* [20]. Hasilnya ditampilkan pada Tabel 2.

Tabel 2 Kriteria Pengukuran Risiko

Prioritas	Area Dampak (Impact Area)
1	Keselamatan dan Kesehatan (Safety and Health)
2	Reputasi dan Kepercayaan Pengguna (Reputation & Trust)
3	Dampak Finansial (Financial Impact)

4	Produktivitas Operasional (Productivity)
5	Sanksi Hukum dan Denda (Fines and Legal Consequences)

3.2.2. Mengembangkan Profil Aset Informasi

Tabel 3 menyajikan data kuantitatif yang penting, namun masih memerlukan narasi pendukung agar pembaca dapat memahami konteks dan maknanya secara utuh. Misalnya, skor rendah pada kategori Sistem Elektronik (26) dalam Indeks KAMI perlu dijelaskan lebih lanjut. Apakah skor tersebut disebabkan oleh minimnya kontrol akses, kurangnya pembaruan perangkat keras, atau tidak adanya sistem pemantauan keamanan jaringan? Penjelasan ini penting untuk menghubungkan data dengan akar masalah dan solusi yang ditawarkan.

Selain itu, pada bagian analisis risiko menggunakan *OCTAVE Allegro*, skor risiko yang tinggi seperti pada isu hilangnya data akibat tidak adanya backup (skor 43) perlu dikaitkan secara langsung dengan potensi dampak terhadap layanan rumah sakit. Misalnya, narasi dapat menjelaskan bahwa kegagalan sistem akibat data hilang bisa mengganggu proses pendaftaran pasien atau akses rekam medis, sehingga berpengaruh pada pelayanan. Dengan menambahkan penjelasan hubungan antar item—misalnya antara skor Indeks KAMI yang rendah dengan risiko tinggi pada area terkait—pembaca akan lebih mudah memahami urgensi mitigasi dan arah rekomendasi yang diberikan.

.

Tabel 3 Profil Aset Informasi

Komponen	Deskripsi
Aset Informasi Kritis	Data Pengguna (User Data)
Alasan Pemilihan Aset	Pengguna diwajibkan melakukan proses login untuk dapat mengakses data di sistem aplikasi rumah sakit.
Deskripsi Aset	Terdiri dari informasi kredensial seperti nama pengguna (*username*), kata sandi (*password*), serta hak akses ke sistem aplikasi Rumah Sakit XYZ.
Pemilik Aset (Owner)	Unit Pengelola Sistem Informasi Rumah Sakit XYZ
Persyaratan Keamanan	
- *Kerahasiaan (Confidentiality)*	Akses hanya diberikan kepada staf yang memiliki otorisasi. Dikelola oleh Pengelola Sistem Informasi.
- *Integritas (Integrity)*	Hanya petugas berwenang yang diizinkan melihat dan memodifikasi data. Dikelola oleh Pengelola Sistem Informasi.
- *Ketersediaan (Availability)*	Aset ini wajib dapat diakses oleh staf operasional untuk keperluan kerja setiap saat (24/7). Dikelola oleh Pengelola Sarana dan Prasarana.
Persyaratan Keamanan Utama	Integritas merupakan aspek keamanan yang paling vital untuk aset informasi ini.

3.2.3. Mengidentifikasi Wadah Aset Informasi

Penulis mengidentifikasi wadah untuk penyimpanan dan pemrosesan, baik internal maupun eksternal, dengan mengelompokkan ke dalam tiga kategori: *Technical, Physical*, dan *People*. Hasilnya disajikan pada Tabel 4.

Tabel 4 Information *Asset Risk Environment* (*Technical*)

Kategori	**Deskripsi**	**Penanggung Jawab (Owner)**

Internal	Server web dan server basis data	Unit Pengelola Sistem Informasi Rumah Sakit XYZ
	Perangkat komputer dan laptop operasional	Unit Pengelola Sarana dan Prasarana Rumah Sakit XYZ
	Jaringan lokal (LAN)	Unit Pengelola Sistem Informasi Rumah Sakit XYZ
Eksternal	Penyedia layanan internet (ISP)	Pihak penyedia layanan eksternal (vendor)

3.2.4. Identifikasi Area Masalah

Tahap ini mengelompokkan aktivitas yang dapat merusak aset informasi rumah sakit untuk mengidentifikasi area masalah. Hasil analisis ditampilkan pada Tabel 5.

Tabel 5 Mengidentifikasi Area Masalah

No.	**Area Risiko (Area of Concern – Data User)**
1	Penyusupan ke sistem informasi melalui celah keamanan oleh pihak yang tidak dikenal, baik dari dalam maupun luar organisasi.
2	Penggunaan hak akses oleh individu yang tidak memiliki wewenang, sehingga berpotensi merusak atau mengekspos data pengguna.
3	Gangguan atau kerusakan terhadap data pengguna yang tersimpan dalam basis data rumah sakit.
4	Hilangnya data pengguna akibat ketiadaan proses pencadangan yang rutin dan sistematis.
5	Penyisipan atau perubahan informasi pengguna dengan data yang tidak valid atau palsu.
6	Kesalahan dalam memasukkan informasi pengguna ke dalam sistem rumah sakit yang dapat memicu kegagalan fungsi.
7	Terjadinya kebocoran data dari permintaan layanan yang diajukan oleh pengguna, sehingga dapat disalahgunakan oleh pihak tertentu.
8	Distribusi hak akses ke data permintaan layanan yang belum selesai diproses, menyebabkan gangguan terhadap sistem layanan.

3.2.5. Identifikasi Skenario Ancaman

Penulis mengidentifikasi *threat scenario* untuk fokus pada area tertentu dengan menggambarkan ancaman secara rinci terhadap aset informasi, Dengan hasil analisisnya ada pada Tabel 6.

Tabel 6 Identifikasi Skenario Ancaman

Elemen	Deskripsi
Aset Informasi	Data Pengguna (*User Data*)
Area Risiko	Pemanfaatan celah keamanan oleh pihak internal maupun eksternal yang tidak dikenal
1. Aktor (Actor)	Pengguna sistem, baik yang sah maupun tidak sah
2. Cara (Means)	Eksploitasi kelemahan pada server, database, atau modul aplikasi
3. Motivasi (Motives)	Dapat terjadi secara disengaja atau tidak disengaja
4. Dampak (Outcome)	✓ Pengungkapan informasi (*Disclosure*) ✓ Modifikasi data (*Modification*) ✓ Penghapusan data (*Destruction*) ✓ Gangguan sistem (*Interruption*)
5. Kebutuhan Keamanan	Penguatan sistem melalui peningkatan keamanan software, hardware, dan jaringan; serta pemantauan sistem secara berkala

6. Probabilitas	✓ Tinggi (*High*) ✓ Sedang (*Medium*) ✓ Rendah (*Low*)

3.2.6. Identifikasi Risiko

Identifikasi risiko dilakukan berdasarkan *threat scenario* yang berdampak pada Rumah Sakit XYZ, seperti tercantum dalam Tabel 7.

Tabel 7 Mengidentifikasi Risiko

No	Area Risiko	Dampak yang Ditimbulkan
1	Penyusupan melalui celah keamanan oleh pihak yang tidak dikenali, baik dari dalam maupun luar institusi	Modifikasi tidak sah terhadap informasi akibat celah sistem dapat menghasilkan data yang tidak akurat atau rusak, sehingga mengganggu operasional sistem informasi rumah sakit secara keseluruhan.
2	Penggunaan hak akses secara tidak sah terhadap informasi pengguna	Ancaman terhadap kerahasiaan data penting pengguna berpotensi menimbulkan penyebaran aset informasi krusial dan menghambat kelangsungan operasional rumah sakit. Selain itu, manipulasi data juga dapat terjadi.
3	Kerusakan pada data pengguna dalam sistem basis data rumah sakit	Gangguan terhadap integritas data akibat kerusakan ini dapat berdampak langsung pada kualitas dan keandalan informasi yang disimpan di rumah sakit.
4	Hilangnya informasi pengguna akibat tidak adanya sistem cadangan	Ketiadaan backup menyebabkan gangguan layanan serta potensi kerugian besar karena kehilangan data yang bersifat vital bagi operasional rumah sakit.
5	Pemalsuan isi data pengguna	Penyisipan informasi yang tidak valid dapat mengurangi tingkat kepercayaan pengguna terhadap pengelolaan informasi oleh pihak rumah sakit.
6	Kesalahan dalam entri data pengguna ke sistem	Input data yang tidak tepat bisa menimbulkan kesalahan sistem, menyebabkan gangguan layanan, serta menimbulkan kerugian bagi pengguna.
7	Terjadinya kebocoran informasi dari permintaan layanan pengguna	Kebocoran ini dapat dimanfaatkan oleh pihak yang tidak berwenang untuk melakukan penyalahgunaan, yang dapat merugikan baik pasien maupun pihak rumah sakit.
8	Distribusi akses ke permintaan layanan yang masih berjalan	Hak akses yang tersebar tanpa kontrol memicu gangguan terhadap proses layanan yang sedang berlangsung dan memperlambat kinerja sistem secara keseluruhan.

3.2.7. Analisis Risiko

Analisis risiko dilakukan dengan menghitung dampak dan skor risiko relatif berdasarkan prioritas dampak area. Dengan metode Octave Allegro, area dampak dikategorikan sebagai *Low* (1), *Medium* (2), dan *High* (3). Hasil perhitungan ditampilkan pada Tabel 8 dan Tabel 9.

Tabel 8 Penentuan Skor Impact Area

Kategori Dampak	Tingkat Prioritas	Skor Dampak: Rendah	Skor Dampak: Sedang	Skor Dampak: Tinggi
Reputasi & Kepercayaan Pelanggan	2	2	4	6
Kerugian Finansial	3	3	6	9

Penurunan Produktivitas	4	4	8	12
Dampak terhadap Kesehatan & Keselamatan	1	1	2	3
Sanksi Hukum & Denda	5	5	10	15

Tabel 9 Analisis Risiko

No	Area Risiko	Dampak (Consequences)	Skor Risiko Relatif
1	Penyalahgunaan celah dalam sistem keamanan oleh pihak tak dikenal, baik internal maupun eksternal	Modifikasi data yang tidak sah akibat kelemahan keamanan dapat menyebabkan ketidaksesuaian atau kerusakan informasi, yang berdampak pada terganggunya kinerja sistem informasi rumah sakit	**37**
2	Akses tidak sah terhadap data pengguna	Pelanggaran keamanan data pengguna berpotensi menyebarkan aset informasi penting dan mengganggu aktivitas operasional rumah sakit, serta memungkinkan manipulasi data yang membahayakan	**29**
3	Pemalsuan informasi pada data pengguna	Kerusakan pada data pengguna menyebabkan gangguan terhadap integritas informasi penting yang tersimpan di database rumah sakit	**40**
4	Hilangnya data akibat absennya sistem pencadangan	Ketidaktersediaan cadangan data menyebabkan terganggunya aktivitas rumah sakit dan menimbulkan kerugian signifikan akibat kehilangan data krusial	**43**
5	Kerusakan pada data pengguna dalam sistem database	Data yang rusak atau tidak valid dapat menurunkan kepercayaan pengguna terhadap sistem dan manajemen rumah sakit	**44**
6	Kesalahan penginputan data pengguna ke dalam sistem	Kesalahan saat memasukkan data dapat merugikan pengguna dan mengganggu kelancaran sistem informasi	**15**
7	Kebocoran data permintaan layanan	Informasi yang bocor dapat disalahgunakan oleh pihak tidak bertanggung jawab, mengakibatkan kerugian bagi pengguna maupun institusi	**36**
8	Distribusi hak akses terhadap layanan yang belum selesai diproses	Penyebaran hak akses menyebabkan terganggunya layanan yang sedang berlangsung dan memperlambat proses kerja sistem	**26**

3.2.8. Pendekatan Mitigasi

Penelitian ini menggunakan pendekatan mitigasi untuk menentukan status rekomendasi risiko berdasarkan relative risk score. Hasilnya dirangkum pada Tabel 10, Tabel 11, dan Tabel 12.

Tabel 10 Risk Relative Matrix

Rentang Skor Risiko	Kategori Risiko (POOL)	Pendekatan Penanganan
30–45	1	Risiko dikategorikan tinggi dan membutuhkan tindakan mitigasi segera.
16–29	2	Risiko tergolong sedang dan dapat ditangani di kemudian waktu sesuai prioritas.
0–15	3	Risiko rendah yang dapat diterima tanpa perlu intervensi langsung.

Tabel 11 Mitigasi

No	Area Risiko	Skor Risiko Relatif	Kategori Risiko	Strategi Penanganan
1	Eksploitasi celah sistem keamanan oleh pihak tidak dikenal, baik dari dalam maupun luar organisasi	37	1	Penanganan segera (*Mitigate*)
2	Penyalahgunaan hak akses terhadap data pengguna	29	2	Penundaan tindakan sambil menunggu evaluasi (*Defer*)
3	Pemalsuan data pengguna yang berdampak pada keakuratan informasi	40	1	Penanganan langsung diperlukan (*Mitigate*)
4	Kehilangan data pengguna akibat tidak adanya pencadangan sistem	43	1	Harus segera ditindaklanjuti (*Mitigate*)
5	Kerusakan data dalam database sistem rumah sakit	44	1	Tindakan mitigasi langsung diperlukan (*Mitigate*)
6	Kesalahan input data oleh pengguna sistem rumah sakit	15	3	Dapat diterima tanpa penanganan besar (*Accept*)
7	Kebocoran informasi dari permintaan layanan pengguna	36	1	Perlu ditangani secara aktif (*Mitigate*)
8	Penyebaran akses terhadap layanan yang masih dalam proses	26	2	Penanganan dapat ditunda dengan pengawasan (*Defer*)

Tabel 12 Kontrol dan Rekomendasi

No	Area Risiko	Rekomendasi	Deskripsi
1	Eksploitasi celah keamanan oleh pihak internal atau eksternal yang tidak terverifikasi	RA-3 Penilaian Risiko	Lakukan identifikasi serta dokumentasi potensi ancaman dan kelemahan yang ada dalam sistem, baik dari dalam maupun luar organisasi.
2	Penyalahgunaan hak akses data pengguna	PE-2 Kontrol Akses Fisik	Laksanakan pengawasan dan verifikasi berkala terhadap akses fisik terhadap data pengguna.

3	Manipulasi atau pemalsuan data pengguna	AC-4 Pengawasan Alur Informasi	Terapkan pemantauan dan audit terhadap aliran informasi pada data pengguna untuk memastikan keabsahan dan keamanannya.
4	Hilangnya data pengguna akibat tidak adanya sistem pencadangan	CP-2 Rencana Kontinjensi	Siapkan solusi alternatif atau cadangan untuk mengantisipasi risiko kehilangan data akibat gangguan atau serangan.
5	Kerusakan pada data pengguna dalam sistem database rumah sakit	CP-9 Cadangan Sistem Informasi	Terapkan mekanisme pencadangan data secara rutin untuk menjamin kerahasiaan, integritas, dan ketersediaan informasi.
6	Kesalahan entri data pengguna dalam sistem	IR-4 Penanganan Insiden	Lakukan validasi dan verifikasi ulang terhadap data yang diinput guna mencegah kesalahan yang merugikan pengguna atau sistem.
7	Kebocoran data dari permintaan layanan pengguna	IA-2 Identifikasi dan Otentikasi (Pengguna Organisasi)	Perbarui secara rutin kredensial pengguna seperti username dan password untuk menghindari penyalahgunaan.
8	Penyebaran akses terhadap permintaan layanan yang masih berjalan	—	Diperlukan kebijakan pembatasan hak akses untuk mencegah distribusi informasi yang tidak seharusnya dan menjaga kelancaran proses layanan.

4. KESIMPULAN

Penelitian ini menunjukkan bahwa tingkat keamanan informasi SIM-RS di Rumah Sakit XYZ berada pada kategori “Cukup Baik” berdasarkan skor Indeks KAMI sebesar 492, dengan kelemahan utama pada aspek Sistem Elektronik dan Pengelolaan Risiko. Melalui metode OCTAVE Allegro, diidentifikasi sejumlah risiko prioritas tinggi yang memerlukan tindakan mitigasi, seperti kontrol akses, backup data, dan perlindungan terhadap kebocoran informasi. Secara teoritis, penelitian ini berkontribusi dalam memperkaya literatur mengenai penerapan gabungan Indeks KAMI dan OCTAVE Allegro dalam konteks rumah sakit. Secara praktis, hasil penelitian ini memberikan panduan konkret bagi pengelola SIM-RS dalam memperkuat kebijakan dan implementasi keamanan informasi di lingkungan layanan kesehatan.

5. SARAN

Untuk penelitian selanjutnya, disarankan agar cakupan studi diperluas dengan melibatkan lebih dari satu rumah sakit guna memperoleh gambaran yang lebih komprehensif dan dapat digeneralisasi. Selain itu, penggunaan metode kombinasi lain seperti COBIT atau ISO/IEC 27001 dapat dipertimbangkan untuk membandingkan efektivitas kerangka kerja manajemen keamanan informasi. Penelitian mendatang juga sebaiknya menyertakan uji validitas dan reliabilitas instrumen secara kuantitatif, serta analisis statistik terhadap hubungan antar variabel risiko, agar hasil yang diperoleh lebih kuat secara metodologis dan relevan untuk pengambilan keputusan di sektor layanan kesehatan.

DAFTAR PUSTAKA

[1] D. Insan Khamil, G. Made Arya Sasmita, dan A. Agung Ngurah Hary Susila, "Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Kami 4.2 Dan ISO/IEC 27001:2013 (Studi Kasus: Diskominfo Kabupaten Gianyar)," 2022. [Daring]. Tersedia pada: http://jurnal.mdp.ac.id

[2] T. Rafiiqa dan U. Indahyanti, "Analisis Tingkat Keamanan Sistem Informasi Manajemen Rumah Sakit (E-HOS System) Menggunakan Metode OCTAVE," 2023.

[3] T. Rafiiqa dan U. Indahyanti, "Analysis of Hospital Management Information System Security Levels (E-HOS System) Using the OCTAVE Method [Analisis Tingkat Keamanan Sistem Informasi Manajemen Rumah Sakit (E-HOS System) Menggunakan Metode OCTAVE]."

[4] A. Kurniawan, F. Hafidz As Shidiq, dan L. Lazuardi, "PENYUSUNAN RENCANA STRATEGIS SISTEM INFORMASI DAN TEKNOLOGI INFORMASI DI RUMAH SAKIT JIWA GRHASIA DAERAH ISTIMEWA YOGYAKARTA," 2021.

[5] L. D. A. Jelita, M. N. Al Azam, dan A. Nugroho, "Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/EIC 27001:2022," *Jurnal SAINTEKOM*, vol. 14, no. 1, hlm. 84–94, Mar 2024, doi: 10.33020/saintekom.v14i1.623.

[6] R. Ramadhan dan M. Restu Alfiansyah, *Analisis dan Mitigasi Resiko Teknologi Informasi dan Keamanan Informasi Menggunakan Framework Octave Allegro (Studi Kasus : Perusahaan Percetakan Documedia)*. 2021.

[7] J. Wijaya, A. Megafitri, K. Khotimah, dan R. Astriratma, *Analisis dan Manajemen Risiko Keamanan Informasi pada Rumah Sakit Menggunakan Metode Octave Allegro (Studi Kasus: Rumah Sakit Umum Daerah Cengkareng)*. 2021.

[8] K. H. R dan M. S. Hasibuan, "Analisis Tingkat Kematangan Keamanan Informasi Menggunakan Indeks KAMI pada Tiyuh Pulung Kencana," *Journal of Digital Literacy and Volunteering*, vol. 2, no. 1, hlm. 31–37, Jan 2024, doi: 10.57119/litdig.v2i1.78.

[9] S. Nugroho dan T. Rochmadi, "Analysis of Information Security Readiness Using the Index KAMI," vol. 4, hlm. 881–886, 2024, doi: 10.51454/decode.v4i3.602.

[10] R. Dewantara dan B. Sugiantoro, "EVALUASI MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) PADA JARINGAN (STUDI KASUS : UIN SUNAN KALIJAGA YOGYAKARTA)," *Jurnal Teknologi Informasi dan Inlu Komputer*, vol. 8, no. 6, hlm. 1137–1148, 2021, doi: 10.25126/jtiik.202183123.

[11] B. S. Deva dan R. Jayadi, "Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro," *Jurnal Teknologi dan Informasi (JATI)*, vol. 12, no. 27, hlm. 12, 2022, doi: 10.34010/jati.v12i2.

[12] K. H. R dan M. S. Hasibuan, "Analisis Tingkat Kematangan Keamanan Informasi Menggunakan Indeks KAMI pada Tiyuh Pulung Kencana," *Journal of Digital Literacy and Volunteering*, vol. 2, no. 1, hlm. 31–37, Jan 2024, doi: 10.57119/litdig.v2i1.78.

[13] V. Gerardo dan A. N. Fajar, "Academic IS Risk Management using OCTAVE Allegro in Educational Institution," *Journal of Information Systems and Informatics*, vol. 4, no. 3, 2022, [Daring]. Tersedia pada: http://journal-isi.org/index.php/isiPublishedByDRPM-UBD

[14] I. Afrianto dan T. Suryana, "Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI-SNI ISO/IEC 27001:2009 Studi Kasus Perguruan Tinggi X," 2015.

[15] R. A. Putra, P. Gala, R. Sengkey, dan C. Punusingon, "Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI," *Jurnal Teknik Informatika*, vol. 15, no. 3, hlm. 189–198, 2020.

[16] D. Dwi Prasetyowati, I. Gamayanto, dan S. wibowo, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks KAMI Berdasarkan ISO/IEC 27001:2013 pada Politeknik Ilmu Pelayaran Semarang Evaluation of Information Security Management Using KAMI

Based on ISO / IEC 27001: 2013: The case of Politeknik Ilmu Pelayaran Semarang," *65 Journal of Information System*, vol. 4, no. 1, hlm. 65–75, 2019.

[17] G. Sekar Palupi, "Analisis Tingkat Keamanan Informasi Pada RSUD Dr. R. Sosodoro Djatikoesoemo Bojonegoro Menggunakan Indeks KAMI Berdasarkan ISO 27001:2013," 2024.

[18] K. Sari, N. Ningsi, N. Zainuddin, dan A. M. Sajiah, "Evaluation of Information Security at Benyamin Guluh Kolaka Hospital using the KAMI 4.2 Index with ISO 27001:2013," *Jurnal Media Informasi Teknologi*, vol. 1, no. 1, 2024.

[19] R. R. Saputra, E. Setiawan, dan A. Ambarwati, "Manajemen Risiko Teknologi Informasi Menggunakan Metode OCTAVE Allegro pada PT. Hakiki Donarta Surabaya," *Jurnal Sains, Teknologi dan Industri*, vol. 17, no. 1, hlm. 1–10, 2019.

[20] M. Iqbal, D. Arief Prambudi, dan I. D. A. S. P. Putu, "Penggunaan Indeks Keamanan Informasi (KAMI) 4.2 Sebagai Metode Evaluasi Kemanan Informasi Pada Dinas Komunikasi Dan Informatika Kota XYZ," *EQUIVA Journal of Mathematics & Information Technology*, vol. 2, no. 1, 2024.