ANALISIS MANAJEMEN RISIKO PADA SISTEM INFORMASI MANAJEMEN RUMAH SAKIT(SIMRS) DENGAN ISO 31000 DAN NIST 800-30 DI RSUD H. OK ARYA ZULKARNAIN

Tika Aulia Rahmi, Muhammad Ikhwani, Muthmainnah
Sistem Informasi, Universitas Malikussaleh
Jalan Batam, Blang Pulo, Muara satu – Lhokseumawe – Aceh (24352), Indonesia
tika.210180148@mhs.unimal.ac.id

ABSTRAK

Sistem Informasi Manajemen Rumah Sakit (SIMRS) merupakan sistem terintegrasi yang mendukung pelayanan, administrasi, dan pengelolaan data di rumah sakit. Namun, penerapannya tidak terlepas dari berbagai risiko yang dapat memengaruhi operasional dan keamanan informasi. Penelitian ini bertujuan untuk menganalisis manajemen risiko pada SIMRS di RSUD H. Ok Arya Zulkarnain dengan menggabungkan dua kerangka kerja, yaitu ISO 31000 dan NIST 800-30. ISO 31000 digunakan untuk identifikasi risiko secara umum, sedangkan NIST 800-30 berfokus pada aspek keamanan informasi dengan dukungan pengujian sistem menggunakan aplikasi Acunetix. Hasil penelitian menunjukkan terdapat 15 risiko yang diklasifikasikan ke dalam 3 tingkat, yaitu 5 risiko tergolong tinggi *(high),* 8 risiko berada di tingkat sedang (*medium)* dan *2* risiko berada pada kategori rendah (*low*). Risiko tertinggi meliputi *human error* (kesalahan dalam mengoperasikan sistem), kurang baiknya kualitas jaringan, listrik padam, terserang virus atau *malware* pada *software* dan penyalahgunaan hak akses. Langkah-langkah mitigasi disusun berdasarkan hasil analisis risiko dan rekomendasi kontrol sesuai prinsip ISO 31000 dan NIST 800-30. Penelitian ini memberikan kontribusi dalam penyusunan strategi pengendalian risiko SIMRS secara terstruktur dan aplikatif untuk mendukung keberlangsungan sistem informasi manajemen rumah sakit.

Kata kunci : *Manajemen Risiko, Sistem Informasi Manajemen rumah Sakit (SIMRS), ISO 31000, NIST 800-30*

1. PENDAHULUAN

Pertumbuhan teknologi informasi kini menjadi faktor penting bagi perusahaan dalam mendukung kelangsungan dan kesuksesan proses bisnisnya. Teknologi informasi berperan signifikan dalam membantu perusahaan meningkatkan kualitas produk dan layanan, mengoptimalkan anggaran operasional, serta memaksimalkan kinerja untuk dapat bertahan dan bersaing di tengah persaingan yang semakin ketat di dunia bisnis saat ini. Pemanfaatan teknologi informasi berkembang dengan sangat cepat dan telah diterapkan di berbagai bidang, termasuk pendidikan, bisnis, dan kesehatan. Dalam sektor medis, penggunaan teknologi informasi menjadi salah satu faktor penting yang mendukung operasional pelayanan di rumah sakit [1]. Rumah sakit sebagai salah satu fasilitas pelayanan kesehatan memiliki peran sangat strategis dalam upaya mempercepat derajat kesehatan masyarakat Indonesia [2].Seiring dengan banyaknya aktivitas yang dilakukan, jumlah data dan informasi yang harus disimpan juga semakin meningkat. Informasi yang dikumpulkan mencakup seluruh kegiatan dalam organisasi, sehingga penting untuk mengelolanya dengan baik agar tidak terjadi kehilangan data. Rumah sakit memanfaatkan informasi ini sebagai dasar pertimbangan dalam mengambil keputusan medis maupun untuk kepentingan organisasi [3]. Oleh karena itu, rumah sakit mengadopsi teknologi, seperti Sistem Informasi Manajemen Rumah Sakit (SIMRS).

Sistem Informasi Manajemen Rumah Sakit (SIMRS) merupakan salah satu subsistem yang ada di rumah sakit, yang mengelola semua informasi terkait dengan pengguna, sesuai dengan peran masing-masing. Sistem Informasi Manajemen Rumah Sakit (SIMRS) memiliki peranan krusial dalam mendukung seluruh proses di rumah sakit melalui penggunaan teknologi informasi [4]. Penerapan SIMRS sangat diperlukan untuk mengintegrasikan semua layanan yang ada di rumah sakit. SIMRS modern dirancang dengan komprehensif dan terintegrasi, berfungsi untuk mengelola proses administratif, keuangan, serta aspek klinis rumah sakit. Sistem ini menjadi fokus utama dalam menyediakan informasi yang diperlukan untuk perawatan pasien dan menjalin integrasi dengan lembaga eksternal, seperti jaminan kesehatan dan fasilitas pelayanan kesehatan lainnya, yang terlibat dalam pertukaran informasi [5]. SIMRS yang mengikuti standar nasional ini dikeluarkan berdasarkan regulasi yang relevan, yaitu Peraturan Kementerian Kesehatan Indonesia Nomor 82 Tahun 2013 tentang Sistem Manajemen Rumah Sakit. Peraturan tersebut mengatur bahwa setiap rumah sakit di Indonesia diwajibkan untuk menyelenggarakan, melaksanakan, serta mengelola dan mengembangkan SIMRS [6].

Rumah Sakit Umum Daerah (RSUD) H. Ok Arya Zulkarnain telah melaksanakan penerapan Sistem Informasi Manajemen Rumah Sakit (SIMRS) secara bertahap. Dengan adanya sistem ini, diharapkan pengelolaan data menjadi lebih efisien, kesalahan manual dapat diminimalkan, dan penanganan pasien dapat dilakukan dengan lebih cepat. Namun, dalam implementasi SIMRS di RSUD

H. Ok Arya Zulkarnain menghadirkan sejumlah tantangan, seperti terbatasnya jumlah staf yang terampil dalam menggunakan sistem ini, ketidakstabilan jaringan internet, serta ancaman terhadap keamanan informasi, termasuk risiko kebocoran data pasien.

Dikarenakan kompleksitas yang ada, analisis mendalam terhadap risiko sistem informasi ini masih sangat diperlukan. Oleh karena itu, analisis manajemen risiko SIMRS di RSUD H. Ok Arya Zulkarnain menjadi penting untuk memastikan sistem berfungsi secara optimal dan tidak mengganggu pelayanan kesehatan. Penelitian ini akan menggunakan dua metode, yaitu ISO 31000 untuk identifikasi risiko secara umum, dan NIST 800-30 yang berfokus pada aspek keamanan informasi. Kombinasi kedua metode ini memungkinkan identifikasi dan pengelolaan risiko secara menyeluruh, baik dari sisi operasional maupun keamanan data, guna mendukung pelayanan kesehatan yang lebih baik.

2. TINJAUAN PUSTAKA

2.1. Teknlogi Informasi

Teknologi Informasi (TI) merupakan sekumpulan alat, perangkat, dan proses yang digunakan untuk menciptakan, mengelola, menyimpan, dan berbagi informasi. Teknologi informasi memberikan keuntungan besar pada setiap organisasi dengan memudahkan pengambilan keputusan serta memperlancar aktivitas operasional dan proses bisnis sehari-hari [7]. Teknologi informasi dalam penempatannya sangat penting bagi suatu lembaga atau institusi untuk mendukung pencapaian rencana strategis. Untuk mencapai tujuan visi, misi dan tujuan perusahaan atau institusi [8].

2.2. Sistem Informasi Manajemen Rumah Sakit (SIMRS)

SIMRS adalah suatu sistem teknologi informasi komunikasi yang memproses dan mengintegrasikan seluruh alur proses pelayanan rumah sakit untuk memperoleh informasi secara tepat dan akurat. Sistem Manajemen Rumah Sakit (SIMRS) merupakan himpunan atau kegiatan dan prosedur yang terorganisasikan dan saling berkaitan serta saling ketergantungan dan dirancang sesuai dengan rencana dalam usaha menyajikan informasi yang akurat dan tepat waktu. Sistem ini berguna menunjang proses fungsi-fungsi manajemen dan pengambilan keputusan dalam memberikan pelayanan kesehatan di rumah sakit [3].

2.3. Manajemen risiko

Manajemen risiko adalah pendekatan terstruktur untuk mengelola ketidakpastian yang terkait dengan ancaman. Proses ini mencakup penilaian risiko, yang berfungsi untuk menentukan tingkat dan prioritas risiko atau ancaman yang dihadapi. Strategi pengelolaan risiko dapat mencakup beberapa langkah, seperti mengalihkan risiko ke pihak lain, menghindari risiko, mengurangi dampak negatifnya, atau menerima sebagian risiko tertentu. Dalam konteks teknologi informasi, manajemen risiko menjadi hal krusial bagi perusahaan karena dampaknya yang signifikan terhadap operasional perusahaan [9].

2.4. ISO 31000

ISO 31000 adalah standar internasional untuk implementasi manajemen risiko yang diterbitkan oleh *International Organization for Standardization* pada 13 November 2009. Standar ini dirancang agar fleksibel dan dapat diterapkan pada berbagai jenis organisasi dengan menyediakan struktur dan pedoman umum untuk semua operasi yang terkait dengan manajemen risiko. Tahapan ISO 31000 [3].

2.5. NIST 800-30

NIST 800-30 adalah kerangka kerja yang dirancang oleh *National Institute of Standards and Technology* (NIST), sesuai mandat dari *Computer Security Act of* 1987 dan *Information Technology Management Reform Act of* 1996. Dokumen ini menyediakan panduan dasar untuk mengembangkan program manajemen risiko yang efektif, serta memberikan definisi dan pedoman praktis dalam menilai dan mengurangi risiko dalam sistem TI. Tujuan utama dari kerangka kerja ini adalah membantu organisasi menciptakan sistem TI yang lebih andal dengan tingkat risiko yang dapat diterima. Selain itu, kerangka ini membantu memilih kontrol keamanan yang sesuai dengan anggaran organisasi [10].

2.6. Kombinasi ISO 31000 Dan NIST 800-30

Tahapan	ISO 31000	NIST 800-30	Kombinasi
Menetapkan Konteks	Pentingnya memahami konteks organisasi, keterlibatan pemangku kepentingan menggunakan ISO 31000.	Relevansi NIST 800-30 dalam mengidentifikasi batasan dari sistem informasi dengan identifikasi bersamaan dengan sumber daya dan informasi.	Mendefinisikan Ruang Lingkup, Konteks, Kriteria, Karakterisasi Sistem.
Identifikasi Risiko	Cari risiko, gunakan berbagai teknik untuk menemukan sebanyak mungkin risiko. Pikirkan tentang apa yang mungkin terjadi, mengapa, dan bagaimana	Identifikasi Sumber Ancaman, Identifikasi Kerentanan.	Identifikasi Ancaman, Identifikasi Kerentanan, Identifikasi Risiko.
Analisis Risiko	Menyajikan kerangka kerja yang disediakan oleh ISO 31000 untuk menganalisis risiko secara rinci, dengan mempertimbangkan kuantitatif dan kualitatif	Memanfaatkan metode analisis risiko NIST SP 800-30 untuk menilai risiko yang terkait dengan informasi dan keamanan siber.	Menentukan *likelihood* dan *impact*.
Evaluasi Risiko	Menerapkan proses evaluasi ISO 31000 untuk menentukan signifikansi risiko yang teridentifikasi	Menggabungkan pedoman evaluasi risiko NIST 800-30 untuk menilai risiko dalam konteks teknologi informasi dan keamanan siber	Penentuan tingkat risiko keamanan informasi.
Perlakuan Risiko	Membahas integrasi pendekatan penanganan risiko ISO 31000 (penghindaran, mitigasi dan berbagi)	Menekankan pentingnya menyelaraskan strategi penanganan risiko dengan rencana respons insiden dan rencana pemulihan bencana	Perlakuan Risiko / Mitigasi Risiko.
Pemantauan dan Peninjauan	Menjelaskan pentingnya pemantauan dan peninjauan, pendekatan manajemen risiko terpadu untuk memastikan efektivitas dan kesesuaian untuk implementasi.	Melibatkan manajemen tingkat atas dan pemangku kepentingan dalam proses pemantauan dan peninjauan.	Pemantauan dan Tinjauan, Dokumentasi Hasil,

Gambar 1. Integrasi ISO 31000 dan NIST 800-30

Proses manajemen risiko akan mengacu pada standar ISO 31000, yang diadopsi untuk disesuaikan

dengan sistem tata kelola e-government di Indonesia. Untuk mengidentifikasi secara lebih spesifik kemampuan teknologi informasi, terutama dalam aspek keamanan informasi, akan mengintegrasikannya dengan pedoman dari NIST 800-30, seperti yang ditunjukkan dalam gambar 1 [11].

a. Menetapkan Konteks
   Tahap ini menekankan pentingnya memahami konteks organisasi, melibatkan pemangku kepentingan, serta mendefinisikan ruang lingkup, kriteria, dan karakterisasi sistem.
b. Identifiksi Risiko
   Dilakukan untuk menemukan risiko yang mungkin memengaruhi sistem, mengidentifikasi ancaman eksternal dan internal, serta kelemahan atau kerentanan dalam sistem.
c. Analisis Risiko
   Analisis risiko bertujuan untuk memahami risiko yang telah diidentifikasi dan menyediakan dasar untuk evaluasi lebih lanjut. Tahapan ini menggunakan tabel *likelihood* untuk menentukan frekuensi terjadinya risiko dalam periode tertentu, sehingga membantu memastikan metode pengelolaan risiko tepat sasaran.

Tabel 1. *Likelihood*

Rating	**Kriteria**	**Tingkat Kejadian**	**Jumlah Frekuensi Kemungkinan Terjadi dalam 1 Tahun**
1	*Rare*	Hampir Tidak Terjadi	X < 2 kali
2	*Unlikely*	Jarang	2 ≤ X ≤ 5 kali
3	*Possible*	Kadang-kadang Terjadi	6 ≤ X ≤ 9 kali
4	*Likely*	Sering Terjadi	10 ≤ X ≤ 12 kali
5	*Certain*	Hampir sering Terjadi	> 12 kali

Setelah itu digunakan tabel *impact* yang merupakan dampak yang akan terjadi, jika kemungkinan risiko tersebut terjadi.

Tabel 2. *Impact*

Rating	**Kriteria**	**Keterangan**
1	*Insignificant*	Tidak mengganggu aktivitas perusahaan
2	*Minor*	Aktivitas perusahaan sedikit terhambat namun aktivitas inti perusahaan tidak terganggu.
3	*Moderate*	Menyebabkan gangguan pada proses bisnis sehingga sebagian jalannya aktivitas perusahaan terhambat
4	*Major*	Menghambat hampir seluruh aktivitas perusahaan
5	*Insignificant*	Aktivitas perusahaan berhenti karena proses bisnis mengalami gangguan total

d. Evaluasi Risiko
   Evaluasi risiko adalah tahap pengambilan keputusan dalam manajemen risiko untuk menentukan apakah diperlukan tindakan lebih lanjut. Proses ini menggunakan matriks risiko, yang disusun berdasarkan hasil analisis risiko, untuk menentukan tingkat prioritas dan perlakuan yang sesuai.

Likelihood						
	Certain	5	Medium	Medium	High	High	High
	Likely	4	Medium	Medium	Medium	High	High
	Possible	3	Low	Medium	Medium	High	High
	Unlikely	2	Low	Low	Medium	Medium	Medium
	Rare	1	Low	Low	Low	Medium	Medium
	Impact		1	2	3	4	5
			Insignificant	Minor	Moderate	Major	Catasthropic

Gambar 2. Matriks Risiko

e. Perlakuan Risiko
   Perlakuan risiko dilakukan untuk mengelola risiko sesuai dengan evaluasi, melalui langkah-langkah seperti mitigasi. Perlakuan risiko memastikan bahwa ancaman terhadap sistem dapat diminimalkan atau dihilangkan, sehingga operasional tetap berjalan lancar dan tujuan organisasi tercapai. Hasilnya yaitu rekomendasi control untuk mengurangi kemungkinan atau dampak risiko.

2.7. Acunetix

Acunetix merupakan sebuah alat yang banyak digunakan oleh para pengembang *website* untuk dapat melihat keamanan pada sebuah *website* yang digunakan. Aplikasi ini akan melakukan pemindaian pada *website* yang ingin diketahui sejauh mana keamanan yang telah dijalankan pada *website*. Dengan menggunakan aplikasi ini, pengembang dapat memperbaiki kelemahan dalam *website* yang digunakan untuk mengurangi kelemahan dalam keamanan sebuah situs *website* [12].

2.8. Penelitian Terdahulu

Penelitian oleh Dwi Erlangga, dkk tahun 2024 membahas penerapan manajemen risiko pada SIMRS di Rumah Sakit XYZ Pekanbaru dengan pendekatan ISO 31000. Penelitian ini menemukan 10 jenis risiko, terdiri dari 2 risiko tinggi seperti kebakaran dan listrik padam, serta 8 risiko sedang termasuk gangguan server, human error, dan kerusakan data. Analisis dilakukan melalui tahapan identifikasi, penilaian, hingga perlakuan risiko menggunakan RACI Chart untuk pembagian tanggung jawab. Hasilnya menekankan pentingnya pengelolaan risiko tinggi agar operasional SIMRS tetap berjalan optimal [13].

Penelitian oleh Muhammad Salmon Hardani, dkk tahun 2022 mengkaji manajemen risiko keamanan informasi pada Sistem Informasi SIMS di instansi pemerintah dengan menggunakan pendekatan NIST 800-30. Melalui identifikasi ancaman dan kerentanan menggunakan alat bantu seperti Acunetix,

ditemukan 14 kerentanan, termasuk SQL Injection dan Cross Site Scripting. Hasil analisis risiko menghasilkan 6 risiko tinggi, 13 sedang, dan 1 rendah. Penelitian ini juga menyarankan pengendalian risiko melalui pembaruan antivirus, backup server, serta peningkatan sistem keamanan guna menekan risiko ke level yang dapat diterima organisasi [14].

Penelitian oleh Irfan Erfian Nurdin dan Benfano Soewito tahun 2024 merancang kerangka manajemen risiko TI terintegrasi untuk sistem pemerintahan elektronik di Kementerian XYZ dengan menggabungkan ISO 31000 dan NIST SP 800-30. Penelitian ini menghasilkan matriks prioritas risiko, serta rencana penanganan insiden dan pemulihan bencana. Risiko utama yang diidentifikasi meliputi kebijakan internal yang tidak diperbarui dan serangan siber seperti SQL injection dan web defacement. Dari hasil analisis, ditemukan 1 risiko sangat tinggi, 4 tinggi, 7 sedang, 14 rendah, dan 6 sangat rendah. Penelitian ini menekankan pentingnya integrasi hasil manajemen risiko ke dalam tata kelola TI agar selaras dengan kebijakan pemerintah dan tangguh terhadap ancaman digital [11].

3. METODE PENELITIAN

Adapun penjelasan dari setiap tahap adalah sebagai berikut:

a. Identifikasi Masalah
   Peneliti merumuskan permasalahan yang sedang dikaji pada topik penelitian.
b. Studi Literatur
   Studi literatur dilakukan dengan mengumpulkan informasi dari sumber-sumber terdokumentasi yang relevan, seperti panduan ISO 31000 dan NIST 800-30.
c. Penentuan Subjek Penelitian (Pemangku Kepentingan)
   Tabel RACI Chart (Responsibility Assignment Matrix) digunakan untuk mengidentifikasi peran dan tanggung jawab berbagai pemangku kepentingan dalam aktivitas yang terkait dengan SIMRS di RSUD H. Ok Arya Zulkarnain.

Gambar 3. Tahapan Peneitian

Tabel 3. RACI Chart

Peranan Aktivitas	Kepala IT	Admin SIMRS	Pj Pendaftaran	Pj Administrasi
Meneliti dan mengurus SIMRS	A	R/I	C	C
Mengoperasikan SIMRS	A	R	R	R
Menyimpulkan dan memberi izin serta bertanggung jawab atas pekerjaan staff	R/A	C/I		
Memelihara sistem, jaringan, server dan memberikan rekomendasi untuk perbaikan	A/I	C	C	C

a. Pengumpulan Data
   Data dikumpulkan melalui observasi langsung terhadap penggunaan SIMRS dan wawancara terstruktur dengan pemangku kepentingan. Pertanyaan wawancara dirancang untuk menggali persepsi risiko, potensi ancaman, serta kelemahan sistem dari sisi teknis maupun operasional.
b. Analisis Risiko
   Hasil wawancara dan observasi dianalisis untuk menentukan tingkat risiko berdasarkan kombinasi nilai *likelihood* (kemungkinan) dan *impact* (dampak). Selanjutnya, risiko dipetakan dalam matriks risiko untuk dikategorikan ke dalam tingkat rendah (*low*), sedang (*medium*), atau tinggi (*high*).
c. Perlakuan Risiko
   Berdasarkan hasil analisis, disusun rekomendasi kontrol untuk mengurangi dan mengelola risiko. Rekomendasi ini mengacu pada prinsip dari ISO 31000 dan kontrol keamanan dari NIST 800-30, dengan tujuan menjaga kelangsungan dan keamanan SIMRS secara menyeluruh.

4. HASIL DAN PEMBAHASAN

4.1. Penetapan Konteks

Adapun konteks pada SIMRS adalah sebagai berikut:

a. Software
   Software yang digunakan berbasis *website* yang dapat diakses di mana saja selama terhubung ke

internet. Software digunakan untuk pengimputan data yang sesuai dengan bagian masing-masing.

b. Informasi
Informasi merupakan data-data yang telah diimput, dan akan disimpan untuk kepentingan rumah sakit dan dapat digunakan untuk pengambilan keputusan dalam proses bisnis. Data-data yang dimasukkan berupa data pegawai, data tenaga medis, data pasien, data rekam medis, data administrasi, data laboratorium dan radiologi.

c. Infrastruktur
Infrastruktur yang digunakan dalam menjalankan SIMRS antara lain Hardware (komputer, leptop, server, printer, perangkat jaringan), *website* SIMRS, database dan fasilitas-fasilitas yang dapat mendukung penggunaan SIMRS.

d. Pengguna
Pengguna merupakan peran penting dalam menjalankan Teknologi Informasi. Pengguna terdiri dari dokter, perawat, staf administrasi, staf keuangan, rekam medis, apoteker, petugas laboratoium yang menggunakan SIMRS dalam operasional sehari hari dan tenaga ahli SIMRS yang bertanggung jawab terhadap pengelolaan, pemeliharaan, dan pengembangan SIMRS.

4.2. Identifikasi Risiko

Pada dasarnya risiko akan terjadi apabila terdapat ancaman dan kerentanan pada suatu sistem. Dari hasil wawancara menunjukkan beberapa ancaman dan celah pada SIMRS.

4.3. Identifikasi Ancaman

Bentuk ancaman yang terjadi dikelompokkan bedasarkan tiga faktor, yaitu alam atau lingkungan, manusia, dan sistem atau infrastruktur. Dari hasil wawancara terdapat beberapa ancaman yang berhasil diidentifikasi, berikut hasilnya dapat dilihat pada tabel berikut:

Tabel 4. Identifikasi Kemungkinan Ancaman

Faktor	ID	Kemungkinan Ancaman
Alam atau Lingkungan	A1	Petir
	A2	Kebakaran
Manusia	M1	*Human error* (kesalahan dalam mengoperasikan sistem)
	M2	Penyalahgunaan hak akses
	M3	Pencurian perangkat keras
Sistem dan Infrastruktur	S1	Kerusakan *hardware*
	S2	Listrik padam
	S3	Kurang baiknya kualitas jaringan
	S4	*Server down*
	S5	*Overload* sistem
	S6	Terserang virus atau *malware* pada *software*
	S7	*Data corruput*

Pada tahap indentifikasi ancaman terdapat 12 kemungkinan resiko yang berasal dari ketiga faktor yaitu alam atau lingkungan, manusia, Sistem atau infrastruktur yang dapat mengancam proses kinerja SIMRS. Setelah itu identifikasi penyebab dan dampak apa saja yang akan muncul dari kemungkinan ancaman, dapat dilihat pada tabel berikut.

Tabel 5. Identifikasi Penyebab dan Dampak Ancaman

ID	Penyebab Utama	Dampak Risiko
A1	Bencana alam (cuaca ekstrem)	Kerusakan perangkat SIMRS dan gangguan jaringan komunikasi
A2	Korsleting listrik atau instalasi tidak aman	Kerusakan perangkat SIMRS dan gangguan layanan rumah sakit
M1	Kurangnya pelatihan SDM	Kesalahan input data pasien, potensi kesalahan diagnosa
M2	Akses tidak sesuai fungsi atau lupa logout	Kebocoran dan kerusakan integritas data pasien
M3	Keamanan fisik lemah dan kelalaian staf	Kehilangan perangkat penting, gangguan operasional SIMRS
S1	Usia perangkat tua dan kurang pemeliharaan	SIMRS tidak optimal, keterlambatan pelayanan pasien
S2	Gangguan pasokan listrik	SIMRS tidak dapat digunakan, akses terganggu
S3	Monitoring jaringan minim	Pelayanan lambat, input data terhambat
S4	Tidak ada pemeliharaan atau koordinasi vendor rendah	SIMRS tidak dapat diakses, pelayanan terganggu
S5	Infrastruktur TI tidak memadai	Sistem lambat, gangguan akses data penting
S6	Serangan virus atau kerusakan sistem	Data hilang/tidak akurat, kesulitan pengambilan keputusan
S7	Keamanan sistem lemah dan kesadaran pengguna rendah	Sistem rusak, layanan terhenti, data sensitif dicuri

Berdasarkan hasil identifikasi terhadap ancaman, penyebab dan dampak risiko yang telah dijelaskan. SIMRS memiliki potensi risiko yang berasal dari berbagai sumber, baik dari faktor alam, manusia, maupun sistem atau infrastruktur.

4.4. Identifikasi Kerentanan

Dalam melakukan analisis risiko, identifikasi kerentanan juga termasuk analisis pada sistem TI. Hal ini bertujuan untuk menemukan celah-celah kerentanan yang mungkin saja dapat dimanfaatkan oleh pihak lain untuk merugikan SIMRS yang ada. Untuk melakukan identifikasi kerentanan pada SIMRS, diperlukan bantuan *tool penetration testing* yaitu aplikasi Acunetix. Acunetix merupakan sebuah alat yang banyak digunakan oleh para pengembang *website* untuk dapat melihat keamanan pada sebuah *website* yang digunakan.

Aplikasi ini akan melakukan pemindaian pada *website* yang ingin diketahui sejauh mana keamanan yang telah dijalankan pada *website* [12]. Metode pentest dilakukan untuk melihat simulasi hasil serangan yang mungkin terjadi oleh attacker pada SIMRS yang ada untuk menemukan kelemahan sistem tersebut.

Tabel 6. Identifikasi Kerentanan SIMRS dengan aplikasi Acunetix

ID	Nama Kerentanan	Level Acunetix
K1	Cross-Site Request Forgery (CSRF)	Medium
K2	Link rusak dalam sistem	Low
K3	Header Content-Type tidak ditetapkan	Low

Pada tahap indentifikasi kerentanan dengan menggunakan aplikasi acunetix terdapat 3 kerentanan yang dapat mengancam proses kinerja SIMRS. Dari hasil tersebut dapat dikatakan bahwa level kerentanan dari SIMS berada pada level medium. Kerentanan yang sudah teridentifikasi pada tabel 3 memiliki dampak risiko yang dapat dilihat pada table 4.

Tabel 7. Identifikasi Penyebab dan Dampak Kerentanan

ID	Level Acunetix	Penyebab Utama	Dampak Risiko
K1	*Medium*	Tidak adanya token anti-CSRF pada form HTML	Aksi ilegal dapat dilakukan tanpa sepengetahuan pengguna
K2	*Low*	Sumber daya dihapus/dipindahkan atau kesalahan URL	Gangguan akses fitur SIMRS dan kebingungan pengguna
K3	*Low*	*Server* tidak mengatur header secara tepat, memungkinkan *MIME sniffing*	Risiko eksekusi skrip berbahaya, membuka celah serangan *XSS* atau injeksi

Dari hasil identifikasi kerentanan pada SIMRS yang diperoleh melalui pengujian menggunakan aplikasi Acunetix, diketahui bahwa terdapat beberapa kelemahan sistem yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Setiap kerentanan memiliki penyebab dan potensi dampak yang signifikan terhadap keamanan data dan layanan sistem.

4.5. Analisis Risiko

Setelah melakukan identifikasi kemungkinan resiko dan dampaknya, selanjutnya masuk pada proses analisis resiko. Pada tahap ini di lakukan analisis tehadap kemungkinan resiko yang sebelumnya sudah di identifikasi, pada tahap ini terdapat dua tabel yaitu *Likelihood* dan *Impact* yang menjadi acuan untuk tahap analisis resiko.

Tabel 8. Daftar Pemangku Kepentingan SIMRS

ID	Jabatan
N1	Kepala IT
N2	Admin SIMRS
N3	PJ Pendaftaran
N4	PJ Administrasi

Pemangku kepentingan yang terlibat dalam pengelolaan dan operasional SIMRS memiliki peran penting. Penilaian risiko dilakukan dengan melibatkan mereka secara langsung melalui wawancara yang mencakup tingkat kemungkinan (*likelihood*) dan dampak (*impact*) dari masing-masing risiko.

4.6. *Likelihood*

Likelihood (tingkat kemungkinan) menggambarkan frekuensi atau probabilitas terjadinya suatu risiko. Setiap narasumber memberikan skor untuk masing-masing risiko dengan skala penilaian dari 1 sampai 5. Skor yang diperoleh dari masing-masing narasumber selanjutnya dirata-ratakan untuk menentukan tingkat kemungkinan (*likelihood*) dari setiap risiko.

Tabel 9. Perolehan Rating *Likelihood*

ID	***Likelihood* (1 - 5)**			
	N1	**N2**	**N3**	**N4**
A1	2	1	1	2
A2	1	1	1	1
M1	4	3	3	3
M2	3	2	3	2
M3	2	3	3	2
S1	3	2	3	3
S2	3	3	3	2
S3	3	4	3	4
S4	1	2	2	1
S5	3	3	4	2
S6	3	2	2	3
S7	2	2	2	3
K1	3	2	3	2
K2	1	2	1	2
K3	1	2	1	2

Nilai *likelihood* dinilai dalam rentang skala 1 sampai 5, di mana skor 1 menunjukkan kemungkinan yang sangat rendah (hampir tidak terjadi), dan skor 5 menunjukkan kemungkinan yang sangat tinggi (hampir sering terjadi).

4.7. *Impact*

Impact menggambarkan sejauh mana kerugian atau gangguan yang dapat ditimbulkan oleh suatu risiko apabila benar-benar terjadi pada sistem SIMRS. Setiap narasumber memberikan skor untuk masing-masing risiko dengan skala penilaian dari 1 sampai 5. Skor yang diperoleh dari masing-masing narasumber selanjutnya dirata-ratakan untuk menentukan tingkat dampak (*impact*) dari setiap risiko.

Tabel 10. Perolehan Rating *Impact*

ID	*Impact* (1 - 5)			
	N1	N2	N3	N4
A1	3	4	4	3
A2	5	4	5	4
M1	5	4	4	4
M2	4	3	3	4
M3	3	3	2	2
S1	2	3	2	3
S2	4	5	4	5
S3	4	4	3	4
S4	5	5	4	5
S5	2	3	2	3
S6	4	5	4	4
S7	4	3	3	3
K1	2	3	2	2
K2	2	1	1	2
K3	2	2	1	2

Skor *impact* dinilai dalam rentang skala 1 sampai 5, di mana skor 1 menunjukkan dampak yang sangat kecil atau tidak signifikan, sedangkan skor 5 menunjukkan dampak yang sangat besar atau kritis terhadap keberlangsungan SIMRS.

Hasil pemeringkatan risiko dapat diputuskan menggunakan dua faktor, yaitu faktor kelompok kemungkinan terjadinya risiko (*likelihood*), dan faktor dampak akibat terjadinya risiko (*impact*) tersebut. Berikut adalah tabel hasil nilai prioritas risiko (RPN):

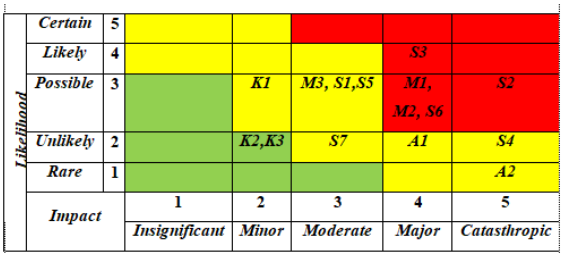
Tabel 11. Hasil Nilai Prioritas Risiko (RPN)

ID	*Likelihood*	*Impact*	RPN
A1	1,5	3,5	5,25
A2	1	4,5	4,5
M1	3,25	4,25	13,8125
M2	2,5	3,5	8,75
M3	2,5	2,5	6,25
S1	2,75	2,5	6,875
S2	2,75	4,5	12,375
S3	3,5	3,75	13,125
S4	1,5	4,75	7,125
S5	3	2,5	7,5
S6	2,5	4,25	10,625
S7	2,25	3,25	7,3125
K1	2,5	2,25	5,625
K2	1,5	1,5	2,25
K3	1,5	1,75	2,625

Nilai *Risk Priority Number (RPN)* diperoleh dari hasil perkalian antara nilai *likelihood* dan *impact* yang masing-masing merupakan rata-rata dari skor yang diberikan oleh empat narasumber. Risiko dengan nilai RPN yang tinggi menunjukkan bahwa risiko tersebut memiliki kemungkinan terjadi yang cukup besar dan dampaknya signifikan terhadap keberlangsungan operasional SIMRS.

4.8. Evaluasi Risiko

Proses penilaian risiko ini berupa tingkatan risiko berdasarkan matriks risiko yang ada dan dikategorikan menjadi tiga tingkatan. Tingkat suatu kategori risiko ditentukan berdasarkan kriteria nilai prioritas risiko: Tingkat 1 Low (rendah), Tingkat 2 Medium (sedang), dan Tingkat 3 High (tinggi). Tujuan penilaian risiko adalah untuk membantu mengambil keputusan berdasarkan hasil analisis risiko.



Gambar 4. Hasil Matriks Risiko

Berdasarkan proses penilaian risiko, dapat diputuskan risiko mana yang membutuhkan penanganan dan upaya mana yang perlu menjadi prioritas untuk mencegah terjadinya risiko tersebut. Hasil dari penilaian risiko ini akan diproses lebih lanjut pada langkah berikutnya.

Tabel 12. Pemeringkatan Risiko Berdasarkan RPN

Risk Level	ID	Nama Risiko	RPN
High	M1	Human error (kesalahan dalam sistem)	13,8125
	S3	Kurang baiknya kualitas jaringan	13,125
	S2	Listrik padam	12,375
	S6	Terserang virus atau malware pada software	10,625
	M2	Penyalahgunaan hak akses	8,75
Medium	S5	Overload sistem	7,5
	S7	Data corruput	7,3125
	S4	Server down	7,125
	S1	Kerusakan hardware	6,875
	M3	Pencurian perangkat keras	6,25
	K1	Cross-Site Request Forgery (CSRF)	5,625
	A1	Petir	5,25
	A2	Kebakaran	4,5
Low	K3	Header content-type tidak ditetapkan	2,625
	K2	Link rusak dalam sistem	2,25

4.9. Perlakuan Risiko

Pada tahap ini, dapat diputuskan tindakan apa saja yang berpotensi meminimalisir terjadinya risiko pada SIMRS. Menentukan keputusan strategi terkait upaya penanganan risiko adalah langkah tepat yang perlu dilakukan agar berbagai risiko dapat dicegah sekaligus meninimalisir kerusakan akibatnya. Maka rekomendasi control yang diusulkan untuk di terapkan ke Rumah Sakit H. Ok Arya Zulkarnain dapat ditampilkan pada Tabel berikut :

Tabel 13. Rekomendasi Kontrol

ID	Risiko Utama	Level	Rekomendasi Kontrol
M1	Human error	High	Melakukan pelatihan rutin bagi seluruh pengguna SIMRS dan sediakan layanan helpdesk untuk bantuan cepat.
S3	Kualitas jaringan buruk	High	Menggunakan koneksi cadangan dengan fitur failover otomatis dan pisahkan jaringan SIMRS dari publik.
S2	Listrik padam	High	Menyiapkan genset sebagai cadangan utama agar operasional SIMRS tetap berjalan saat listrik padam.
S6	Serangan virus/malware	High	Mengaktifkan antivirus di seluruh perangkat dan lakukan pembaruan secara berkala untuk mencegah infeksi.
M2	Penyalahgunaan hak akses	High	Menerapkan akun personal, ganti sandi berkala, dan kontrol hak akses sesuai tugas pengguna.
S5	Overload sistem	Medium	Meningkatkan kapasitas server, jaringan, dan perangkat untuk menangani beban tinggi tanpa menurunkan performa.
S7	Data corrupt	Medium	Melakukan pencadangan data secara berkala dan simpan di lokasi terpisah atau cloud.
S4	Server down	Medium	Mengoptimalkan konfigurasi server, gunakan server cadangan, dan terapkan load balancing untuk distribusi beban.
S1	Kerusakan hardware	Medium	Melakukan pemeliharaan perangkat secara rutin dan sediakan perangkat cadangan untuk penggantian cepat.
M3	Pencurian perangkat keras	Medium	memasang CCTV di area strategis dan perkuat keamanan ruang server serta perangkat utama SIMRS.
K1	Cross-Site Request Forgery (CSRF)	Medium	mengimplementasikan token anti-CSRF pada form dan validasi HTTP header asal permintaan.
A1	Petir	Medium	memasang penangkal petir eksternal serta gunakan UPS dan surge protector pada perangkat kritikal.
A2	Kebakaran	Medium	Menyediakan APAR dan sistem alarm kebakaran otomatis di ruang server dan periksa rutin kelayakannya.
K3	Header Content-Type tidak ditetapkan	Low	memastikan server mengatur header dengan tepat sesuai konten untuk mencegah eksploitasi browser.
K2	Link rusak dalam sistem	Low	Melakukan audit berkala terhadap link dalam sistem dan segera perbaiki agar tidak mengganggu akses layanan.

Tabel di atas menunjukkan rekomendasi kontrol yang dapat diterapkan untuk mengurangi tingkat risiko pada setiap ancaman dan kerentanan yang telah diidentifikasi. Rekomendasi ini disesuaikan dengan tingkat risiko (*Risk Level*) masing-masing dan bertujuan untuk meminimalkan dampak serta kemungkinan terjadinya insiden yang dapat mengganggu operasional SIMRS.

5. KESIMPULAN DAN SARAN

Analisis Manajemen Pada Risiko SIMRS Dengan ISO 31000 & NIST 800-30 Di RSUD H. Ok Arya Zulkarnain dilakukan secara terstruktur dengan mengintegrasikan tahapan dari kedua kerangka kerja. ISO 31000 digunakan untuk manajemen risiko scara umum, NIST 800-30 memperkuat analisis keamanan informasi. Identifikasi risiko melalui wawancara, observasi, dan pengujian menggunakan aplikasi Acunetix yang menemukan 15 risiko yaitu, 5 risiko dengan tingakatan tinggi (high) adalah human error, kurang baiknya kualitas jaringan, listrik padam, terserang virus atau malware pada software dan penyalahgunaan hak akses. 8 risiko dengan tingkatan sedang (medium) adalah overload sistem, data corrupt, server down, kerusakan hardware, pencurian perangkat keras, cross site request forgenry (CSRF), petir dan kebakaran. 2 risiko dengan tingkatan rendah (low) adalah header content-type yang tidak ditetapkan dan link rusak dalam sistem. Langkah-langkah mitigasi dalam mengurangi risiko SIMRS berdasarkan kerangka kerja ISO 31000 dan NIST 800-30 disusun berdasarkan hasil evaluasi risiko dan ditujukan untuk menurunkan tingkat kemungkinan maupun dampak dari setiap risiko. Beberapa langkah mitigasi yang disarankan antara lain, yaitu pemasangan antivirus dan firewall untuk mencegah serangan siber, pelatihan berkala kepada staf untuk meminimalisir kesalahan pengguna, penguatan sistem otorisasi dan pembatasan hak akses, peningkatan infrastruktur jaringan dan penyediaan cadangan daya seperti UPS serta penerapan sistem backup data dan pemeliharaan server secara rutin.

Keterbatasan penelitian ini belum mengkaji secara kuantitatif biaya penerapan kontrol risiko yang direkomendasikan. Padahal efektivitas kontrol tidak hanya bergantung pada seberapa besar risiko dapat dikurangi, tetapi juga pada sejauh mana pengeluaran yang diperlukan dapat diterima dan dipertanggungjawabkan. Oleh karena itu, penelitian selanjutnya disarankan menyertakan analisis *cost-benefit* untuk menilai kelayakan dan efisiensi setiap mitigasi. Analisis ini akan membantu memperkirakan perbandingan antara besarnya biaya yang harus dikeluarkan dengan potensi kerugian yang dapat dihindari. Pendekatan ini akan memperkuat pengambilan keputusan berbasis anggaran dan memperluas arah strategis investasi keamanan SIMRS secara berkelanjutan.

DAFTAR PUSTAKA

[1] M. S. Lubis and M. A. Pratama, "Peran Teknologi Informasi dalamPeningkatan Kualitas Pelayanan Kesehatan," *J. Pendidik. Tambusai*, vol. 9, no. 1, pp. 8052–8060, 2025.

[2] Z. Ardian, Z. Yunizar, R. P. Fhonna, M. Ikhwani, and A. Fazillah, "Perancangan Sistem Informasi Pendataan Kamar Di Rumah Sakit Umum Daerah Tgk Chik Ditiro Sigli Berbasis Web," *J. Informatics Comput. Sci.*, vol. 9, no. 1, p. 15, 2023, doi: 10.33143/jics.v9i1.2937.

[3] L. E. Hutagalung, "Analisa Manajemen Risiko Sistem Informasi Manajemen Rumah Sakit (Simrs) Pada Rumah Sakit Xyz Menggunakan Iso 31000," *TeIKa*, vol. 12, no. 01, pp. 23–33, 2022, doi: 10.36342/teika.v12i01.2820.

[4] Maya Saufinah Pane, Nirmaya Fanisya, Silvi Roma Rizkina, Yesy Prinkawati Nasution, and Dewi Agustina, "Sistem Informasi Manajemen Rumah Sakit (SIMRS) Untuk Meningkatkan Mutu Pelayanan Kesehatan Di Indonesia," *Detect. J. Inov. Ris. Ilmu Kesehat.*, vol. 1, no. 3, pp. 01–14, 2023, doi: 10.55606/detector.v1i3.1980.

[5] S. Rusli, "Implementasi Sistem Informasi Manajemen Rumah Sakit Dalam Pengolahan Data Rumah Sakit," *JKM (Jurnal Kesehat. Masyarakat) Cendekia Utama*, vol. 10, no. 2, p. 158, 2022, doi: 10.31596/jkm.v10i2.1036.

[6] A. Mariza, L. Abdurahman, and I. Santosa, "Analisis Risiko Dan Kontrol Pada SIMRS Gudang Obat Berdasarkan ISO 31000 (Studi Kasus: Rumah Sakit Khusus Ibu Dan Anak Kota Bandung)," *e-Proceeding Eng.*, vol. 7, no. 2, pp. 6984–6992, 2020.

[7] A. M. A. Saputra, L. P. I. Kharisma, A. A. Rizal, M. I. Burhan, and N. W. Purnawati, *TEKNOLOGI INFORMASI: Peranan TI dalam berbagai bidang*. PT. Sonpedia Publishing Indonesia, 2023.

[8] M. Muthmainnah, S. Safwandi, M. Jannah, and V. Ilhadi, "Evaluasi Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 5 Proses Dss03 Dan Mea01 Di Universitas X," *Sisfo J. Ilm. Sist. Inf.*, vol. 5, no. 1, pp. 1–12, 2021, doi: 10.29103/sisfo.v5i1.4848.

[9] A.Royyan, "Konsep Manajemen Risiko," *J. Penelit. Ilmu Ekon. dan Keuang. Syariah*, vol. 1, no. 3, pp. 130–137, 2023, doi: 10.59059/jupiekes.v1i3.322.

[10] I. Putu Jovano, I. R. Padiku, and B. Ahaliki, "Analisis Manajemen Risiko dan Keamanan Sistem Informasi Akademik Terpadu (SIAT) Universitas Negeri Gorontalo Menggunakan Framework NIST SP 800-30," *J. Syst. Inf. Technol.*, vol. 5, no. 1, pp. 135–144, 2025.

[11] I. E. Nurdin and B. Soewito, "Development of an Integrated It Risk Management Framework for Electronic-Based Government Systems: a Case Study of the Xyz Ministry," *Indones. Interdiscip. J. Sharia Econ.*, vol. 7, no. 1, pp. 1331–1353, 2024.

[12] S. Sandy and H. H. Solihin, "Audit Keamanan dan Manajemen Risiko pada e-Learning Universitas Sangga Buana," *J. Manaj. Inform.*, vol. 11, no. 1, pp. 1–14, 2021, doi: 10.34010/jamika.v11i1.3641.

[13] D. Erlangga, "Manajemen Risiko SIMRS Unit Rekam Medis Di Rumah Sakit Al-Ihsan Menggunakan ISO 31000:2018," *e-Proceeding Eng.*, vol. 10, no. 3, pp. 3222–3230, 2023.

[14] M. S. Hardani and K. Ramli, "Perancangan Manajemen Risiko Keamanan Sistem Informasi Manajemen Sumber Daya dan Perangkat Pos dan Informatika (SIMS) Menggunakan Metode NIST 800-30," *JURIKOM (Jurnal Ris. Komputer)*, vol. 9, no. 3, p. 591, 2022, doi: 10.30865/jurikom.v9i3.4181.