JURNAL ILMIAH SISTEM INFORMASI (JUSI)
VOL 4, No. 3, November 2025, pp. 944 - 958
p-ISSN : 2803-1507 (media cetak) | e-ISSN : 2803-1531 (media online)
Link Publikasi: https://ejurnal.provisi.ac.id/index.php/JUISI/issue/view/151

Enhancing Information Security and Risk Governance in Hospital Electronic Medical Record Systems

Evva Choirotul Mahfazza[1], Yusuf Amrozi[2], Faris Muslihul Amin[3]
[1,2,3] Fakultas Sains dan Teknologi, Universitas Islam Negeri Sunan Ampel Surbaya
Jl. Ahmad Yani No. 117, 60237, Jemur Wonosari, Kec. Wonocolo, Surabaya, Jawa Timur, Indonesia
e-mail: evvamahfazza31@gmail.com*[1]; yusuf.amrozi@uinsby.ac.id[2]; faris@uinsby.ac.id[3]

ARTICLE INFO

Article History:

Received: 20-09-2025
Revised: 20-10-2025
Accepted: 11-11-2025
Published: 30-11-2025

ABSTRACT

This study aims to analyse risk management in hospital medical records information systems using the ISO 31000:2018 framework. Electronic medical records play a critical role in storing and managing sensitive patient data, requiring a structured risk management approach to identify, evaluate, and control potential threats. The research method used was a descriptive qualitative approach, using observation and interviews with information technology staff and medical records managers. The results revealed 11 key risks, divided into three categories: high, medium, and low. High risks were primarily related to the lack of system protection against cyber threats. This study concluded that implementing ISO 31000:2018 can help hospitals develop more effective risk mitigation strategies, thereby supporting the security, integrity, and availability of patient data.

Keywords: *Risk Management, Electronic Medical Records, ISO 31000:2018, Information Security.*

Abstrak

Penelitian ini bertujuan untuk menganalisis manajemen risiko pada sistem informasi rekam medis rumah sakit dengan menggunakan kerangka kerja ISO 31000:2018. Rekam medis elektronik berperan penting dalam penyimpanan dan pengelolaan data pasien yang bersifat sensitif, sehingga diperlukan pendekatan manajemen risiko yang terstruktur untuk mengidentifikasi, mengevaluasi, dan mengendalikan potensi ancaman. Metode penelitian yang digunakan adalah deskriptif kualitatif dengan teknik observasi dan wawancara terhadap staf teknologi informasi serta pengelola rekam medis. Hasil penelitian menunjukkan adanya 11 risiko utama yang terbagi dalam tiga kategori, yaitu risiko tinggi, sedang, dan rendah. Risiko dengan tingkat tinggi terutama terkait dengan kurangnya perlindungan sistem terhadap ancaman siber. Penelitian ini menyimpulkan bahwa penerapan ISO 31000:2018 dapat membantu rumah sakit dalam menyusun strategi mitigasi risiko yang lebih efektif, sehingga mendukung keamanan, integritas, dan ketersediaan data pasien.

Kata Kunci: *Manajemen Risiko, Rekam Medis Elektronik, ISO 31000:2018, Keamanan Informasi.*

1. PENDAHULUAN

Perkembangan *teknologi informasi* telah memberikan dampak signifikan terhadap sektor kesehatan, terutama dalam upaya peningkatan mutu layanan dan efisiensi operasional rumah sakit [1], [2], [3]. Salah satu inovasi yang banyak diadopsi adalah Sistem Informasi Rekam Medis Elektronik (SIRME) [4]. Melalui sistem ini, tenaga medis dapat mengakses riwayat kesehatan pasien, hasil pemeriksaan laboratorium, hingga tindakan medis secara efisien dan aman. Implementasi SIRME dinilai mampu mempercepat proses pengambilan

DOI: https://doi.org/10.51903/00wfhv86

p-ISSN : 2803-1507 e-ISSN : 2803-1531

keputusan klinis dan mengurangi kesalahan pencatatan yang sering terjadi pada sistem berbasis kertas [5]. Oleh karena itu, penerapan SIRME menjadi bagian penting dari transformasi digital di sektor kesehatan yang berorientasi pada peningkatan kualitas layanan dan keselamatan pasien.

Fenomena di lapangan menunjukkan bahwa penerapan SIRME di berbagai rumah sakit di Indonesia masih menghadapi sejumlah tantangan, baik dari sisi teknis, keamanan informasi, maupun kapasitas sumber daya manusia. Menurut [6] rumah sakit masih belum memiliki sistem rekam medis yang sepenuhnya terintegrasi dengan standar keamanan data pasien. Kondisi ini meningkatkan potensi terjadinya gangguan operasional, kebocoran data, hingga kerusakan sistem. Data medis pasien tergolong sebagai informasi sensitif yang harus dijaga kerahasiaannya; kebocoran informasi dapat menimbulkan dampak hukum, etika, serta menurunkan tingkat kepercayaan masyarakat terhadap institusi kesehatan [7]. Oleh karena itu, dibutuhkan pendekatan manajemen risiko yang sistematis untuk menjaga keberlanjutan, keamanan, dan keandalan sistem informasi di lingkungan rumah sakit.

Dalam konteks pengelolaan risiko, *International Organization for Standardization* (ISO) telah mengembangkan standar internasional ISO 31000 yang memberikan prinsip, kerangka kerja, serta pedoman dalam manajemen risiko secara terstruktur dan terintegrasi [8]. ISO 31000:2018 menekankan pentingnya proses identifikasi, analisis, evaluasi, serta mitigasi risiko secara menyeluruh agar organisasi dapat mengantisipasi potensi ancaman dan meminimalisir dampak negatif terhadap operasi [9]. Penerapan standar ini sangat relevan bagi pengelolaan SIRME karena mampu mengatur langkah-langkah sistematis dalam mengidentifikasi dan menanggulangi risiko yang berkaitan dengan keamanan data, integritas sistem, serta kontinuitas layanan medis. Dengan menerapkan prinsip-prinsip ISO 31000, rumah sakit dapat meningkatkan ketahanan sistem informasi terhadap ancaman siber, kesalahan teknis, maupun kegagalan operasional yang dapat menghambat pelayanan kesehatan [10].

Berbagai penelitian terdahulu telah membahas penerapan manajemen risiko berbasis ISO 31000 pada sektor kesehatan. [11] menekankan bahwa SIRME memiliki peran strategis dalam meningkatkan efisiensi pelayanan, namun juga memerlukan manajemen risiko yang kuat agar sistem tetap berfungsi optimal. [12] mengidentifikasi bahwa aspek keamanan informasi menjadi komponen risiko utama dalam sistem informasi rumah sakit. [13] menunjukkan bahwa penerapan ISO 31000 mampu meningkatkan kesiapan organisasi dalam menghadapi ancaman terhadap sistem informasi kesehatan melalui pendekatan proaktif dan berbasis konteks organisasi. Penelitian lain [14] menyoroti pentingnya integrasi antara kebijakan keamanan informasi dengan kerangka manajemen risiko agar sistem dapat memberikan perlindungan menyeluruh terhadap data pasien. Meskipun demikian, sebagian besar penelitian tersebut masih berfokus pada aspek konseptual, tanpa membahas secara mendalam bagaimana implementasi ISO 31000 diterapkan dalam konteks pengelolaan risiko Teknologi Informasi (TI) di sistem rekam medis elektronik.

Gap analysis dari berbagai penelitian sebelumnya menunjukkan masih adanya kekurangan dalam penerapan ISO 31000 pada sistem informasi kesehatan, khususnya dalam konteks pengelolaan risiko TI secara komprehensif dan terukur. Sebagian besar penelitian hanya menyoroti risiko pada aspek teknis atau keamanan informasi, tanpa memperhatikan keterkaitan dengan faktor organisasi, kebijakan, serta kesiapan sumber daya manusia. Selain itu, belum banyak kajian yang secara spesifik mengkaji bagaimana penerapan ISO 31000:2018 dapat digunakan untuk mengevaluasi dan memperkuat manajemen risiko pada sistem rekam medis elektronik rumah sakit di Indonesia. Oleh karena itu, penelitian ini difokuskan untuk menganalisis penerapan ISO 31000:2018 dalam mengidentifikasi, menilai, serta mengendalikan risiko pada Sistem Informasi Rekam Medis Elektronik di rumah sakit.

Tujuan penelitian ini adalah untuk mengevaluasi efektivitas penerapan ISO 31000:2018 dalam mengelola risiko pada SIRME, dengan fokus pada aspek keamanan informasi, keandalan sistem, dan kesiapan sumber daya manusia. Penelitian ini juga bertujuan untuk memberikan rekomendasi strategis bagi pihak manajemen rumah sakit dalam memperkuat tata kelola risiko sistem informasi agar selaras dengan prinsip keberlanjutan dan keselamatan pasien. Melalui analisis risiko berbasis ISO 31000, diharapkan dapat diperoleh pemahaman yang lebih mendalam mengenai potensi risiko yang dihadapi oleh SIRME serta langkah mitigasi yang paling tepat untuk mengurangi dampaknya terhadap operasional rumah sakit. Penguatan pemahaman terhadap konteks organisasi juga dibutuhkan agar proses identifikasi dan penilaian risiko dapat dilakukan secara lebih akurat.

Dari sisi akademis, penelitian ini memiliki kontribusi dalam memperkaya literatur di bidang sistem informasi kesehatan dan manajemen risiko TI. Penelitian ini tidak hanya memberikan nilai teoritis, tetapi juga

p-ISSN : 2803-1507 e-ISSN : 2803-1531

menawarkan kontribusi praktis bagi pengambil kebijakan, pengembang sistem, dan manajemen rumah sakit dalam merancang strategi mitigasi risiko yang efektif dan terukur. Dengan demikian, hasil penelitian ini diharapkan dapat menjadi acuan bagi institusi kesehatan dalam meningkatkan tata kelola dan keamanan sistem informasi yang berkelanjutan serta mendukung terciptanya pelayanan kesehatan yang profesional dan terpercaya [14]. Pengembangan strategi tersebut memerlukan pemahaman yang komprehensif mengenai kebutuhan operasional rumah sakit agar implementasinya dapat berjalan sesuai konteks layanan.

Kebaruan penelitian ini terletak pada fokus analisisnya terhadap integrasi antara aspek keamanan informasi dan tata kelola risiko (*risk governance*) menggunakan ISO 31000:2018, serta penekanan pada faktor sumber daya manusia sebagai elemen kunci dalam pengelolaan risiko TI pada sistem rekam medis elektronik. Pendekatan ini memperluas kajian sebelumnya yang umumnya hanya menyoroti risiko teknis atau keamanan data tanpa mempertimbangkan keterkaitan antar faktor organisasi dan SDM [15]. Analisis mendalam terhadap peran SDM diperlukan untuk memahami bagaimana kompetensi dan kesiapan personel mempengaruhi efektivitas pengendalian risiko. Pemahaman tersebut juga membantu organisasi dalam merancang program penguatan kapasitas yang relevan dengan kebutuhan operasional sistem informasi kesehatan.

2. TINJAUAN PUSTAKA

Penelitian terkait Sistem Informasi Rekam Medis Elektronik (SIRME) atau *Electronic Medical Record* (EMR) menunjukkan bahwa teknologi ini telah banyak dimanfaatkan untuk meningkatkan kualitas manajemen data kesehatan di berbagai fasilitas pelayanan kesehatan. Studi terdahulu [16] membahas bagaimana SIRME mendukung pengelolaan, penyimpanan, dan penyajian informasi medis secara digital guna menunjang proses layanan klinis. Temuan [17] turut menunjukkan bahwa penerapan EMR berdampak pada peningkatan efisiensi layanan, penurunan kesalahan pencatatan, dan percepatan proses diagnosis serta pengambilan keputusan. Selain itu, penelitian lain [18] menyoroti peran SIRME dalam integrasi data antarunit pelayanan, mulai dari pendaftaran pasien hingga pencatatan tindakan medis, sehingga membentuk alur pelayanan yang lebih efektif dan berfokus pada kebutuhan pasien.

Sejalan dengan kebutuhan pengelolaan informasi yang semakin kompleks dalam sistem kesehatan digital, berbagai penelitian juga menekankan pentingnya manajemen risiko dalam mendukung keberlangsungan operasional. Model proses manajemen risiko seperti pada Gambar 1 digunakan untuk mengidentifikasi, menganalisis, dan mengevaluasi risiko secara sistematis. Literartur [19] menjelaskan bahwa tahapan cakupan, konteks, dan kriteria menjadi dasar dalam menentukan ruang lingkup serta parameter risiko sebelum proses penilaian dilakukan. Penelitian terdahulu membahas bagaimana identifikasi, analisis, dan evaluasi risiko membantu organisasi memahami sumber ancaman dan potensi dampaknya terhadap proses layanan. Selain itu, perlakuan risiko melalui pengendalian, pengurangan, transfer, atau penerimaan dijelaskan sebagai strategi mitigasi yang umum digunakan. [20], [21] menekankan pentingnya komunikasi, konsultasi, pemantauan, dan peninjauan berkala untuk memastikan efektivitas penerapan manajemen risiko, sedangkan dokumentasi risiko disebutkan sebagai elemen yang mendukung pembelajaran organisasi.

p-ISSN : 2803-1507 e-ISSN : 2803-1531



Gambar 1. Manajemen risiko untuk mengidentifikasi, menganalisis, dan mengevaluasi risiko secara sistematis

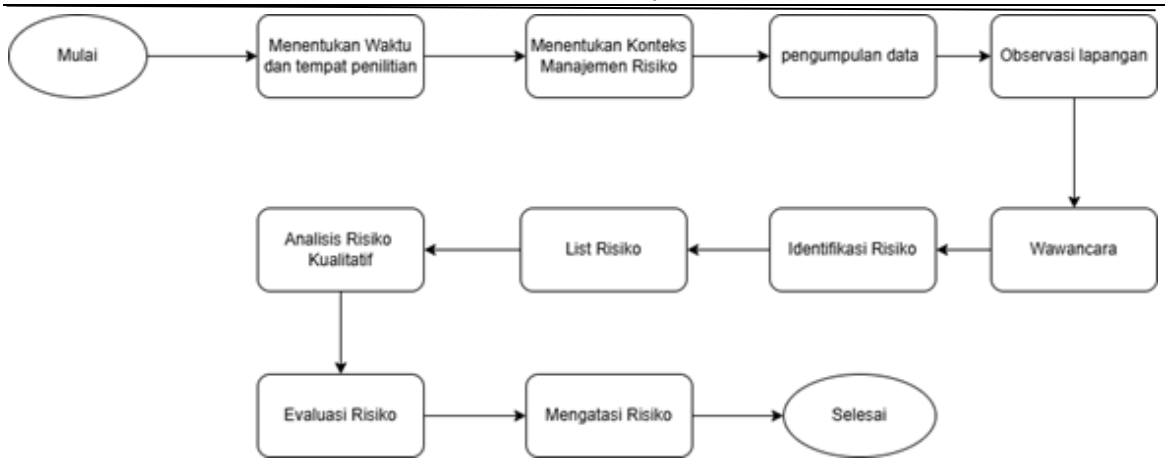
Penguatan manajemen risiko tersebut kemudian banyak dikaitkan dengan penerapan standar ISO 31000:2018 yang memberikan kerangka kerja sistematis bagi organisasi, termasuk sektor kesehatan. Penelitian dalam [22] menjelaskan bahwa ISO 31000 dapat digunakan untuk mengidentifikasi, menganalisis, dan mengendalikan risiko secara terstruktur. Studi lain [23] menguraikan integrasi prinsip-prinsip ISO 31000 dalam proses pengambilan keputusan dan tata kelola risiko organisasi. Dalam konteks fasilitas kesehatan, penelitian [24] menunjukkan bahwa penerapan standar ini membantu organisasi meningkatkan kesiapan menghadapi ancaman seperti kebocoran data, gangguan sistem, maupun kesalahan manusia. Penelitian lebih lanjut [25], menyoroti peningkatan ketahanan sistem informasi terhadap risiko siber, sedangkan [26] membahas pentingnya integrasi kebijakan keamanan informasi dalam manajemen risiko agar keberlanjutan operasional tetap terjaga. [27] menemukan bahwa aspek teknis dan keamanan data merupakan komponen yang paling rentan dalam operasional sistem informasi kesehatan, sehingga menuntut penerapan manajemen risiko yang lebih komprehensif.

Kebutuhan akan manajemen risiko yang kuat pada sistem informasi kesehatan juga berkaitan erat dengan isu keamanan informasi, khususnya pada pengelolaan SIRME. Berbagai penelitian menunjukkan bahwa perlindungan data pasien merupakan salah satu tantangan utama dalam transformasi digital layanan kesehatan. Studi terdahulu menekankan pentingnya kontrol keamanan yang menjaga kerahasiaan, integritas, dan ketersediaan data, mengingat ancaman dapat berkembang dari serangan siber, kesalahan pengguna, maupun kelemahan pengendalian akses. Penelitian dalam [28] menunjukkan bahwa keberhasilan perlindungan data sangat dipengaruhi oleh kebijakan keamanan yang kuat, peningkatan kesadaran pengguna, serta pemantauan sistem secara berkelanjutan. Literatur juga menyoroti perlunya mekanisme pengamanan yang adaptif karena risiko keamanan informasi terus berubah seiring perkembangan teknologi dan pola serangan digital. Penelitian-penelitian tersebut menekankan bahwa penguatan tata kelola keamanan informasi menjadi bagian penting agar SIRME dapat berfungsi dengan aman dan tetap mendukung kualitas layanan kesehatan.

3. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan analisis deskriptif untuk menggambarkan proses, kondisi, dan konteks yang berkaitan dengan penerapan sistem informasi kesehatan di lingkungan rumah sakit. Pendekatan ini memungkinkan peneliti mengidentifikasi pola serta karakteristik penelitian secara sistematis berdasarkan data yang dikumpulkan dari observasi dan interaksi dengan lingkungan penelitian. Informasi yang diperoleh dari proses tersebut membantu peneliti menyusun pemahaman awal mengenai alur metodologis yang akan diterapkan. Alur umum pelaksanaan penelitian dapat dilihat sebagaimana ditunjukkan pada Gambar 2.

p-ISSN : 2803-1507 e-ISSN : 2803-1531



Gambar 2. Alur metode penelitian yang digunakan

Pada Gambar 2 menjelaskan metode penelitian penggunaan analisis deskriptif dalam penelitian ini terbukti sangat bermanfaat dalam memahami dan mengartikulasikan secara komprehensif kondisi yang ada dalam lingkup, lokasi, dan kumpulan tertentu [29]. Dalam penelitian ini, data dikumpulkan dengan observasi pada staf IT dan bagian Rekam Medis Rumah Sakit. Data yang diperoleh melalui observasi tersebut memberikan gambaran mengenai pola kerja serta mekanisme pengelolaan informasi di lingkungan rumah sakit. Pendekatan ini membantu peneliti menilai bagaimana proses operasional berlangsung dan bagaimana data diproses oleh staf terkait.

Saat melaksanakan evaluasi risiko, penelitian ini menggunakan pendekatan khusus yang dikenal dengan *ISO 31000:2018*. Pemanfaatan metode ini bertujuan untuk membangun kerangka atau perspektif terstruktur yang diturunkan dari sudut pandang peneliti, dengan mempertimbangkan masukan dari pemangku kepentingan terkait. Kerangka kerja ini mencakup identifikasi potensi risiko yang mungkin terjadi di lingkungan, serta penerapan langkah-langkah untuk memitigasi atau mencegah risiko tersebut. Pendekatan ini juga memungkinkan peneliti memahami hubungan antara karakteristik organisasi dan munculnya risiko dalam pengelolaan informasi.

Setelah seluruh data berhasil dikumpulkan, peneliti menerapkan metode penilaian risiko untuk menganalisis dan menafsirkan informasi yang ada, dengan tujuan mengungkap berbagai risiko yang mungkin sedang terjadi, berpotensi terjadi di masa mendatang, atau pernah terjadi sebelumnya. Tahapan ini mencakup analisis terhadap seberapa sering risiko dapat muncul dan seberapa besar dampak yang ditimbulkannya. Melalui proses ini, peneliti berupaya merumuskan langkah-langkah untuk meminimalkan kemungkinan terjadinya risiko atau mencegahnya agar tidak terjadi di kemudian hari. Analisis tersebut juga memberikan pemahaman mengenai prioritas pengendalian yang perlu diterapkan agar setiap risiko dapat ditangani sesuai tingkat urgensinya.

4. HASIL DAN PEMBAHASAN

4.1. *Konteks*

Berdasarkan hasil observasi dan identifikasi awal terhadap sistem rekam medis elektronik di Rumah Sakit Bojonegoro, ditemukan bahwa sistem tersebut menyimpan berbagai data sensitif pasien, termasuk riwayat penyakit, hasil laboratorium, dan data identitas pribadi. Kompleksitas sistem informasi yang tinggi memunculkan berbagai potensi risiko, seperti gangguan operasional akibat pemadaman listrik, serangan *malware* yang mengancam kerahasiaan data, serta potensi *human error* dalam proses input data. Kondisi tersebut menggambarkan perlunya penguatan mekanisme pengendalian internal agar potensi gangguan dapat dipetakan secara lebih komprehensif. Setiap potensi risiko yang muncul menunjukkan bahwa sistem memiliki ketergantungan tinggi pada aspek teknis maupun sumber daya manusia yang terlibat dalam pengoperasiannya.

Dengan mengacu pada kerangka kerja ISO 31000:2018, proses manajemen risiko dimulai dari penetapan konteks organisasi, identifikasi aset dan kerentanannya, hingga analisis dan evaluasi risiko. Salah satu temuan penting adalah kurangnya sistem *backup* data yang terintegrasi secara otomatis, yang dapat menyebabkan kehilangan data saat terjadi kerusakan sistem. Selain itu, masih terdapat beberapa titik lemah dalam sistem

p-ISSN : 2803-1507 e-ISSN : 2803-1531

keamanan jaringan yang belum dilengkapi dengan *firewall* atau deteksi intrusi yang memadai. Temuan tersebut menunjukkan perlunya pemetaan ulang terhadap kelengkapan kontrol keamanan yang saat ini digunakan untuk mendukung keberlangsungan operasional sistem.

4.2. *Kriteria*

Dalam ISO 31000:2018, kriteria manajemen risiko adalah parameter yang digunakan untuk mengevaluasi dan menilai sejauh mana suatu risiko dapat diterima atau harus ditindaklanjuti. Kriteria ini meliputi kemungkinan (likelihood) terjadinya suatu risiko, serta dampaknya (consequence) terhadap tujuan organisasi, termasuk aspek finansial, operasional, dan reputasi. Tingkat risiko kemudian dihitung berdasarkan kombinasi dari kemungkinan dan dampak, yang biasanya digambarkan dalam bentuk matriks risiko untuk mempermudah proses penilaian dan prioritisasi. Selain itu, kriteria juga mempertimbangkan batas penerimaan risiko (risk acceptance), kesesuaian dengan tujuan organisasi, dan kepatuhan terhadap regulasi yang berlaku. Kriteria-kriteria ini penting untuk memastikan bahwa proses pengelolaan risiko di organisasi, seperti rumah sakit, berjalan secara sistematis dan sesuai standar [30].

4.3. *Penilaian Risiko*

Penetapan penilaian risiko merupakan bagian penting dari proses manajemen risiko yang meliputi identifikasi risiko dan evaluasi risiko. Pada bagian ini dibahas hasil penilaian risiko yang telah dilakukan pada aplikasi rekam medis berdasarkan hasil observasi dengan pihak pengelola. Proses tersebut memberikan gambaran mengenai bagaimana risiko muncul dalam kegiatan operasional harian serta bagaimana risiko tersebut dapat berdampak pada keberlangsungan layanan. Informasi yang diperoleh dari tahapan ini memberikan dasar bagi peneliti untuk memahami karakteristik ancaman yang mungkin memengaruhi sistem informasi rumah sakit.

4.3.1. *Identifikasi Risiko*

Berdasarkan hasil wawancara, diketahui bahwa proses identifikasi risiko di bagian Rekam Medis Rumah Sakit dilakukan dengan “melihat situasi atau kendala secara manual” tanpa menggunakan metode khusus atau alat bantu. Identifikasi risiko biasanya dilakukan saat terjadi masalah sehingga tidak ada mekanisme pemantauan risiko yang bersifat preventif. Kondisi ini menunjukkan bahwa identifikasi risiko belum berjalan secara sistematis atau terdokumentasi dengan baik. Pendekatan tersebut juga menandakan bahwa pemahaman mengenai pengelolaan risiko masih terbatas pada penyelesaian masalah setelah risiko muncul.

4.3.2. *Identifikasi Aset*

Proses identifikasi aset dilakukan dengan mengumpulkan informasi secara menyeluruh terkait semua aset yang terlibat dalam penggunaan sistem rekam medis, baik perangkat keras maupun perangkat lunak. Aset yang diidentifikasi mencakup data pasien, data transaksi, server, jaringan, hingga aplikasi khusus yang mendukung operasional rumah sakit. Informasi aset tersebut dideskripsikan secara rinci, termasuk lokasi fisik, nilai, fungsi, dan pihak yang bertanggung jawab, guna menunjang evaluasi risiko yang efektif. Penjelasan mengenai aset-aset tersebut dapat dilihat secara lebih jelas sebagaimana ditunjukkan pada Tabel 1.

Tabel 1. Identifikasi Aset

Aset pada Sistem Rekam Medis	
SDM	Staf
	Admin
Data	Data Pasien
	Data Dokter
Sistem	Sistem Rekam Medis
	Jaringan
	UTP
	Server
Hardware	CPU

Berdasarkan sumber kategori dan aset dalam Table 1 Sistem Rekam Medis Rumah Sakit (mencakup berbagai jenis data dan perangkat yang mendukung operasional sistem. Aset-aset tersebut diklasifikasikan ke dalam beberapa tipe seperti data pasien, data transaksi, data dokter, serta komponen sistem seperti Sistem Rekam Medis, jaringan, dan perangkat keras (*hardware*) seperti CPU. Identifikasi terhadap kategori dan aset ini sangat penting untuk memastikan setiap komponen yang terlibat dalam pengelolaan Sistem Rekam Medis

p-ISSN : 2803-1507 e-ISSN : 2803-1531

mendapatkan perlindungan risiko yang tepat dan menyeluruh [30]. Informasi tersebut juga membantu peneliti menilai tingkat ketergantungan sistem terhadap setiap jenis aset untuk mendukung kesinambungan layanan.

Proses identifikasi aset lanjutan dilakukan untuk memperoleh gambaran lebih rinci mengenai semua komponen yang berpotensi menimbulkan risiko dalam sistem rekam medis. Analisis ini mencakup aset dari kategori SDM, sistem, dan data, serta risiko yang terkait dengan masing-masing aset. Setiap aset dianalisis dari sisi kelemahan operasional, keamanan, dan prosedur pengelolaan yang saat ini diterapkan. Hasil identifikasi rinci tersebut dirangkum dalam Tabel 2, yang menunjukkan deskripsi dan potensi risiko dari masing-masing aset yang telah teridentifikasi.

Tabel 2. Deskripsi Identifikasi Aset

Kode Aset	Kategori	Nama Aset	Deskripsi
R01	SDM (Manusia)	Input Data Pasien	Kesalahan input data pasien oleh staf medis yang belum memahami sistem, koreksi dilakukan manual.
R02		Privasi Data	Risiko kebocoran data medis oleh pegawai karena kelalaian atau kurangnya pengetahuan tentang keamanan data.
R03		Pemahaman Kebijakan	Tidak adanya pelatihan rutin untuk memastikan pegawai memahami kebijakan keamanan informasi.
R04	Sistem	Sistem Rekam Medis	Sistem sering mengalami *error*, menyebabkan gangguan dalam operasional.
R05		Jaringan/*Server*	Downtime sistem tercatat tinggi dan belum tersedia sistem cadangan yang andal.
R06		*Backup* Data	Prosedur pemulihan data tidak terdokumentasi dengan baik dan belum diuji secara berkala.
R07		Antivirus/Firewall	Sistem belum dilindungi secara optimal oleh antivirus atau firewall yang diperbarui.
R08		Hak Akses Pengguna	Beberapa pengguna memiliki akses penuh yang tidak sesuai dengan peran dan tanggung jawabnya.
R09		Monitoring Sistem	Monitoring performa dan keamanan sistem belum dilakukan secara rutin.
R10	Data	Audit Keamanan Informasi	Belum pernah dilakukan audit keamanan sistem informasi secara berkala.
R11		Enkripsi Data	Sistem belum menerapkan enkripsi pada data yang disimpan atau dikirimkan melalui jaringan.

Proses observasi dan identifikasi aset juga dilengkapi dengan pengumpulan data melalui wawancara dan pertanyaan terstruktur kepada pihak TI. Pendekatan ini digunakan untuk memperoleh pemahaman mendalam mengenai praktik pengelolaan aset, prosedur keamanan, dan risiko yang terkait dengan sistem rekam medis. Informasi yang diperoleh menunjukkan adanya potensi risiko yang muncul akibat kombinasi kelemahan sistem, prosedur, dan perilaku pengguna. Ringkasan pertanyaan dan hasil observasi terhadap pengelolaan aset dapat dilihat pada Tabel 3.

Pada Tabel 3 dijelaskan isi pertanyaan wawancara terhadap pihak terkait yaitu esalahan input data pasien masih sering terjadi, terutama pada shift malam atau ketika staf baru mengoperasikan sistem. Insiden kebocoran data medis juga pernah terjadi, misalnya ketika seorang karyawan membagikan data pasien melalui grup WhatsApp tanpa enkripsi. Dari sisi kebijakan, pelatihan keamanan informasi belum pernah dijadikan program rutin, hanya disampaikan secara lisan saat briefing atau ketika ada kebijakan baru. Sistem rekam medis sendiri mengalami error sekitar 2–3 kali per bulan, dan downtime tercatat 1–2 jam setiap bulannya akibat gangguan listrik atau jaringan. Untuk pemulihan data, backup hanya dilakukan manual setiap minggu dengan hard disk eksternal, belum otomatis, dan tidak terenkripsi.

Perlindungan sistem juga belum memadai karena hanya menggunakan antivirus gratis dan firewall standar. Terkait hak akses, meskipun sudah terdata siapa yang bisa mengakses, tetapi belum ada sistem log audit untuk memastikan pengawasan lebih baik. Monitoring sistem pun masih bersifat reaktif, baru dilakukan setelah ada keluhan pengguna, karena belum tersedia dashboard real-time. Audit keamanan informasi belum pernah dilakukan, sehingga tidak ada laporan perkembangan atau kelemahan sistem secara menyeluruh. Selain itu, enkripsi data belum direncanakan dalam waktu dekat karena keterbatasan anggaran dan SDM.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Tabel 3. Pertanyaan untuk Bagian TI Rekam Medis

No	Pertanyaan	Hasil Observasi
1.	Seberapa sering terjadi kesalahan input data pasien, dan bagaimana proses koreksinya?	Kesalahan input data masih terjadi, terutama saat shift malam atau ketika staf baru mengoperasikan sistem.
2.	Pernahkah terjadi insiden kebocoran data medis?	Pernah, karena salah satu karyawan ada yang membagikan data pasien lewat grup *Whatsapp* tanpa enkripsi
3	Bagaimana memastikan pegawai memahami kebijakan ini? Apakah ada pelatihan berkala atau belum	Pelatihan keamanan informasi belum menjadi program wajib atau berkala. Informasi hanya disampaikan secara lisan dalam briefing atau ketika ada kebijakan baru.
4	Seberapa sering sistem mengalami error?	Error biasanya terjadi 2–3 kali dalam sebulan
5	Apakah ada catatan frekuensi downtime dan Apakah ada sistem cadangan (redundancy)	Downtime tercatat sekitar 1–2 jam per bulan, biasanya karena pemadaman listrik atau gangguan jaringan.
6	Bagaimana prosedur pemulihan jika data hilang?	ackup dilakukan secara manual setiap minggu oleh staf IT menggunakan hard disk eksternal, tetapi belum otomatis dan belum terenkripsi.
7	Apakah sistem dilindungi dengan antivirus/firewall?	Saat ini sistem menggunakan antivirus gratis dan firewall standar jadi kurang memadai.
8	Siapa saja yang memiliki akses penuh ke data?	Belum ada sistem log audit, tapi sudah terdata siapa saja yang bisa mengakses.
9	Apakah dilakukan monitoring sistem secara rutin?	Monitoring dilakukan secara reaktif, yaitu setelah ada keluhan dari pengguna. Belum ada dashboard pemantauan performa real-time.
10	Apakah pernah dilakukan audit keamanan sistem?	Tidak ada laporan audit terdokumentasi, sehingga sulit menilai perkembangan dan kelemahan sistem secara menyeluruh.
11	Apakah ada rencana mengimplementasikan enkripsi?	Saat ini belum ada rencana jangka pendek untuk enkripsi karena keterbatasan anggaran dan SDM.

4.3.3. *Kemungkinan dan Dampak Risiko*

Analisis risiko dilakukan untuk menilai kemungkinan munculnya risiko dan dampaknya terhadap operasional sistem rekam medis. Proses ini mencakup identifikasi faktor-faktor yang berpotensi menimbulkan gangguan, baik yang berasal dari SDM, sistem, maupun data. Penilaian ini bertujuan untuk memberikan gambaran yang lebih rinci mengenai aspek-aspek yang memerlukan pengendalian dan perhatian khusus dalam pengelolaan risiko. Hasil identifikasi kemungkinan risiko dan dampaknya terhadap sistem dapat dilihat pada Tabel 4.

Tabel 4. Identifikasi kemungkinan risiko dan dampaknya terhadap sistem

Faktor	ID	Kemungkinan Risiko
SDM	R01	Staf medis salah menginput data pasien akibat kurang pemahaman sistem.
	R02	Pegawai membocorkan data medis karena kelalaian atau ketidaktahuan akan privasi data.
	R03	Pegawai belum dilatih terkait kebijakan keamanan informasi rekam medis.
SISTEM	R04	Sistem mengalami error dan menurunkan efisiensi pelayanan medis.
	R05	SIRS tidak dapat diakses saat dibutuhkan (downtime).
	R06	Ada backup tetapi terkadang juga down, menyebabkan potensi kehilangan data penting.
	R07	Sistem tidak memiliki antivirus/firewall yang memadai.
	R08	Hak akses pengguna tidak dibatasi secara ketat sesuai peran.
	R09	Tidak dilakukan monitoring rutin atas performa dan keamanan sistem.
Data	R10	Tidak ada audit keamanan sistem informasi secara berkala.
	R11	Tidak ada enkripsi data saat penyimpanan atau pengiriman.

Berdasarkan hasil identifikasi pada Tabel 4, terdapat sebelas potensi risiko utama yang dikelompokkan ke dalam tiga faktor penyebab, yaitu SDM, sistem, dan data. Pada aspek SDM, risiko muncul akibat kurangnya pemahaman staf terhadap sistem, kelalaian dalam menjaga kerahasiaan data medis, serta minimnya pelatihan terkait kebijakan keamanan informasi. Faktor sistem menunjukkan risiko seperti error aplikasi, gangguan akses (*downtime*), kegagalan *backup*, ketiadaan antivirus atau firewall, pembatasan hak akses yang lemah, serta kurangnya monitoring performa dan keamanan. Sementara itu, faktor data meliputi ketiadaan audit keamanan dan belum diterapkannya enkripsi data.

Kondisi ini menunjukkan bahwa risiko tidak hanya berasal dari aspek teknis, tetapi juga dari perilaku dan kompetensi pengguna sistem. Interaksi antara kelemahan sistem dan kelalaian manusia dapat memperbesar peluang terjadinya insiden keamanan informasi. Tanpa upaya mitigasi yang terencana, potensi kerugian dari insiden keamanan bisa meningkat secara signifikan. Oleh karena itu, dibutuhkan strategi mitigasi terpadu yang mencakup peningkatan infrastruktur keamanan, pelatihan SDM, dan penerapan kebijakan perlindungan data secara konsisten untuk menjaga keandalan dan keberlanjutan sistem rekam medis elektronik.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Dampak dari risiko yang teridentifikasi pada Sistem Informasi Rekam Medis Elektronik mencerminkan konsekuensi terhadap keselamatan pasien, integritas data, dan keberlanjutan operasional rumah sakit. Faktor risiko yang berasal dari kesalahan manusia maupun gangguan sistem dapat menimbulkan berbagai masalah, seperti keterlambatan pelayanan, kehilangan data penting, hingga ancaman hukum terkait pelanggaran privasi. Dampak ini menunjukkan perlunya penguatan pengendalian internal dan prosedur keamanan yang berlapis (*layered security*), serta pengawasan rutin untuk meminimalkan potensi kerugian. Rincian dampak risiko berdasarkan masing-masing aset dan faktor dapat dilihat pada Tabel 5.

Tabel 5. Dampak risiko berdasarkan masing-masing aset dan faktor

ID	Dampak
R01	Kesalahan diagnosis, pengobatan tidak tepat, membahayakan pasien.
R02	Tuntutan hukum, hilangnya kepercayaan pasien, pelanggaran privasi.
R03	Tingkat kesalahan tinggi, sistem mudah disalahgunakan.
R04	Pelayanan terhambat, keterlambatan layanan pasien.
R05	Pasien tidak tertangani cepat, risiko nyawa.
R06	Kehilangan data penting secara permanen.
R07	Peretasan, manipulasi data pasien, ancaman ransomware.
R08	Penyalahgunaan data oleh pengguna yang tidak berwenang.
R09	Masalah tidak terdeteksi dini, kerusakan sistem berlanjut.
R10	Tidak sesuai regulasi, sanksi dari regulator.
R11	Data dapat disadap saat dikirim atau dicuri dari penyimpanan

Berdasarkan Tabel 5, dampak risiko pada Sistem Informasi Rekam Medis Elektronik mencakup konsekuensi serius baik terhadap keselamatan pasien maupun integritas data. Risiko yang berasal dari kesalahan manusia dan gangguan sistem dapat menyebabkan keterlambatan layanan, kehilangan data penting, hingga ancaman hukum akibat pelanggaran privasi. Dampak tersebut menegaskan pentingnya penerapan keamanan berlapis dan pengawasan rutin untuk mencegah kerusakan sistem serta menjaga kepercayaan publik terhadap layanan kesehatan digital. Selain itu, faktor eksternal seperti serangan *siber* dan kegagalan perangkat keras juga berpotensi memperparah gangguan operasional pada sistem ini.

4.3.4. *Analisis Risiko*

Proses analisis risiko memerlukan pemahaman awal mengenai parameter yang digunakan untuk menilai tingkat kemungkinan terjadinya suatu risiko. Informasi mengenai tingkat kemungkinan ini membantu evaluator menilai seberapa sering suatu peristiwa berpotensi muncul dalam konteks operasional. Parameter tersebut disusun secara bertingkat agar proses identifikasi dapat dilakukan secara sistematis dan konsisten. Setiap level dirancang untuk menggambarkan kondisi nyata berdasarkan periode kemunculan risiko dalam aktivitas organisasi, sebagaimana ditunjukkan pada Tabel 6.

Tabel 6. Kriteria Risiko dalam aktivitas organisasi

Level	Deskripsi	Frekuensi
1	Rare	Hampir tidak mungkin terjadi (lebih dari 2 tahun)
2	Unlikely	Kemungkinan kecil terjadi (1–2 tahun)
3	Possible	Mungkin terjadi (7–12 bulan)
4	Likely	Kemungkinan besar terjadi (4–6 bulan)
5	Certain	Hampir pasti terjadi (1–3 bulan)

Pada Tabel 6 setelah risiko teridentifikasi, langkah selanjutnya adalah melakukan analisis risiko untuk menentukan tingkat risiko berdasarkan kriteria *likelihood* (kemungkinan terjadinya risiko) dan *impact* (dampak jika risiko terjadi). Penentuan tingkat risiko ini diperlukan agar setiap potensi ancaman dapat diklasifikasikan secara lebih terukur sesuai karakteristiknya. Proses tersebut membantu organisasi memahami urgensi penanganan risiko berdasarkan kombinasi kemungkinan dan dampak. Informasi ini juga berfungsi sebagai dasar dalam menyusun langkah mitigasi yang lebih terarah. Berikut adalah kriteria yang digunakan dalam analisis risiko.

Penilaian *impact* diperlukan untuk mengetahui seberapa besar pengaruh yang mungkin timbul apabila suatu risiko benar-benar terjadi. Kategori *impact* disusun untuk memberikan gambaran yang jelas mengenai tingkat gangguan yang dapat memengaruhi keberlangsungan layanan. Penyusunan kategori ini juga membantu evaluator menentukan prioritas risiko berdasarkan skala dampaknya terhadap proses bisnis. Struktur penilaian ini memberikan acuan objektif dalam menilai tingkat keparahan risiko, seperti yang diperlihatkan pada Tabel 7.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Tabel 7. tingkat keparahan risiko

Level	Deskripsi	Keterangan
1	Tidak Signifikan	Tidak menghambat aktivitas pelayanan
2	Kurang Signifikan	Aktivitas pelayanan sedikit terhambat, namun aktivitas inti tidak terganggu
3	Cukup Signifikan	Menyebabkan gangguan pada proses bisnis, sehingga sebagian aktivitas terhambat
4	Signifikan	Menghambat hampir seluruh aktivitas pelayanan
5	Sangat Signifikan	Aktivitas pelayanan berhenti karena proses bisnis mengalami gangguan total

Pada Tabel 7 dijelaskan kriteria *impact* dari tidak signifikan, kurang signifikan, cukup signifikan, signifikan, dan sangat signifikan. Kategori tersebut digunakan untuk memberikan penilaian yang konsisten terhadap dampak yang mungkin terjadi pada proses pelayanan. Setiap tingkat dampak disusun untuk menggambarkan seberapa besar gangguan yang dapat dialami organisasi dalam kondisi tertentu. Pemahaman mengenai kategori ini membantu evaluator menilai prioritas penanganan risiko secara lebih objektif.

Tahap penilaian risiko dilakukan untuk menggabungkan nilai *likelihood* dan *impact* sehingga menghasilkan tingkat risiko komprehensif pada setiap faktor yang telah teridentifikasi. Tahap ini memungkinkan organisasi memahami area yang memiliki potensi gangguan tertinggi dalam sistem informasi rekam medis. Proses penilaian juga membantu menyusun prioritas mitigasi berdasarkan kombinasi skor yang diperoleh dari masing-masing risiko. Hasil penggabungan kedua parameter tersebut disajikan secara terstruktur sebagaimana terdapat pada Tabel 8.

Tabel 8. Hasil Penilaian Risiko

ID	Kemungkinan Risiko	Likelihood	Impact
R01	Staf medis salah menginput data pasien akibat kurang pemahaman sistem.	2	2
R02	Pegawai membocorkan data medis karena kelalaian atau ketidaktahuan akan privasi data.	3	4
R03	Pegawai belum dilatih terkait kebijakan keamanan informasi rekam medis.	2	3
R04	Sistem mengalami error dan menurunkan efisiensi pelayanan medis.	1	3
R05	SIRS tidak dapat diakses saat dibutuhkan (downtime).	2	2
R06	Tidak tersedia backup data rekam medis, menyebabkan potensi kehilangan data penting.	2	4
R07	Sistem tidak memiliki antivirus/firewall yang memadai.	4	5
R08	Hak akses pengguna tidak dibatasi secara ketat sesuai peran.	3	3
R09	Tidak dilakukan monitoring rutin atas performa dan keamanan sistem.	2	4
R010	Tidak ada audit keamanan sistem informasi secara berkala.	2	2
R11	Tidak ada enkripsi data saat penyimpanan atau pengiriman.	2	3

Berdasarkan hasil pada Tabel 8, penilaian risiko terhadap Sistem Informasi Rekam Medis menunjukkan bahwa tingkat kemungkinan (*likelihood*) dan dampak (*impact*) bervariasi antar faktor. Risiko dengan nilai tertinggi terdapat pada R07, yaitu ketiadaan antivirus atau firewall yang memadai dengan skor kemungkinan 4 dan dampak 5, yang berpotensi besar terhadap ancaman siber dan kehilangan data pasien. Risiko lainnya dengan dampak tinggi mencakup R06 terkait ketiadaan *backup* data dan R09 mengenai kurangnya monitoring sistem, keduanya memiliki potensi menimbulkan gangguan operasional dan kehilangan informasi penting. Sementara risiko seperti R01, R04, dan R010 tergolong sedang karena memiliki nilai kemungkinan dan dampak relatif rendah. Secara keseluruhan, hasil ini menggambarkan bahwa ancaman terbesar terhadap sistem berasal dari kelemahan keamanan teknis dan kurangnya kontrol operasional, sehingga diperlukan *Risk Treatment* berupa peningkatan perlindungan sistem, audit keamanan berkala, dan optimalisasi prosedur pengelolaan data.

4.4. *Evaluasi Risiko*

Proses evaluasi risiko dilakukan untuk memetakan tingkat prioritas risiko berdasarkan hasil analisis sebelumnya sehingga setiap risiko dapat ditangani sesuai tingkat urgensinya. Tahapan ini memanfaatkan hubungan antara nilai *likelihood* dan *impact* yang telah diperoleh pada proses analisis risiko. Metode evaluasi digunakan untuk melihat posisi risiko pada level rendah, sedang, atau tinggi dalam konteks operasional sistem rekam medis. Gambaran pemetaan risiko tersebut disajikan melalui matriks evaluasi sebagaimana ditunjukkan pada Tabel 9.

Berdasarkan Tabel 9 analisis evaluasi risiko dilakukan untuk menentukan prioritas penanganan risiko berdasarkan tingkat risiko yang telah dianalisis. Dalam evaluasi risiko, digunakan matriks evaluasi risiko untuk memetakan risiko berdasarkan *likelihood* dan *impact*. Penilaian ini memberikan gambaran mengenai

p-ISSN : 2803-1507 e-ISSN : 2803-1531

posisi setiap risiko dalam tingkatan tertentu sesuai pengaruh dan peluang terjadinya. Informasi tersebut menjadi dasar untuk melakukan klasifikasi risiko yang lebih terarah.

Tabel 9. Matriks Evaluasi Risiko

Likelihood/Impact	1 (Tidak Signifikan)	2 (Kurang Signifikan)	3 (Cukup Signifikan)	4 (Signifikan)	5 (Sangat Signifikan)
5 (Certain)	Medium	High	High	Extreme	Extreme
4 (Likely)	Medium	Medium	High	High	Extreme
3 (Possible)	Low	Medium	Medium	High	High
2 (Unlikely)	Low	Low	Medium	Medium	High
1 (Rare)	Low	Low	Low	Medium	Medium

Tahap berikutnya memerlukan pemetaan risiko secara lebih rinci untuk mengetahui letak setiap risiko dalam matriks evaluasi berdasarkan kombinasi nilai *likelihood* dan *impact*. Proses pemetaan ini membantu menilai tingkat keseriusan risiko berdasarkan posisi masing-masing risiko dalam matriks. Selain itu, pemetaan ini memudahkan penentuan tindakan lanjutan karena setiap risiko berada pada kategori yang dapat diidentifikasi secara visual. Pemetaan rinci tersebut disajikan sebagaimana terlihat pada Tabel 10.

Tabel 10. Matrix Evaluasi Berdasarkan Likelihood dan Impact

Likelihood / Impact	1 (Tidak Signifikan)	2 (Kurang Signifikan)	3 (Cukup Signifikan)	4 (Signifikan)	5 (Sangat Signifikan)
5 (*Certain*)					
4 (*Likely*)					R07
3 (*Possible*)			R08	R02	
2 (*Unlikely*)		R01, R05, R010	R03, R11	R06, R09	
1 (*Rare*)			R04		

Berdasarkan hasil observasi dan penilaian risiko, risiko-risiko pada Sistem Rekam Medis dipetakan seperti Tabel 10. Hasil pemetaan tersebut menunjukkan perbedaan tingkat urgensi antar risiko berdasarkan kombinasi nilai kemungkinan dan dampaknya. Posisi risiko pada matriks membantu menentukan prioritas perlakuan yang harus dilakukan agar risiko yang lebih tinggi dapat segera ditangani. Informasi ini menjadi dasar untuk melanjutkan proses klasifikasi tingkat risiko pada tahap berikutnya.

4.4.1. *Klasifikasi Tingkat Risiko*

Klasifikasi risiko dilakukan untuk mengelompokkan setiap risiko ke dalam tingkatan tertentu berdasarkan hasil pemetaan pada matriks evaluasi. Tahapan ini membantu memastikan bahwa penanganan risiko dapat dilakukan secara terukur dan sesuai dengan tingkat ancaman yang dihadapi oleh sistem rekam medis. Setiap kategori risiko mencerminkan sejauh mana risiko tersebut dapat memengaruhi operasional apabila tidak ditangani. Rincian klasifikasi tingkat risiko disajikan pada Tabel 11.

Tabel 11. Klasifikasi Risiko

ID	Kemungkinan Risiko	Likelihood	Impact	Level Risiko
R07	Sistem tidak memiliki antivirus/firewall yang memadai.	4	5	Tinggi
R02	Pegawai membocorkan data medis karena kelalaian atau ketidaktahuan akan privasi data.	3	4	Sedang
R03	Pegawai belum dilatih terkait kebijakan keamanan informasi rekam medis.	2	3	Sedang
R06	Tidak tersedia backup data rekam medis, menyebabkan potensi kehilangan data penting.	2	4	Sedang
R08	Hak akses pengguna tidak dibatasi secara ketat sesuai peran	4	4	Sedang
R09	Hak akses pengguna tidak dibatasi secara ketat sesuai peran.	2	4	Sedang
R11	Tidak ada enkripsi data saat penyimpanan atau pengiriman.	2	3	Sedang
R01	Staf medis salah memasukkan input data pasien akibat kurang pemahaman sistem.	2	2	Rendah
R04	Sistem mengalami *error* dan menurunkan efisiensi pelayanan medis.	1	3	Rendah
R05	SIRS tidak dapat diakses saat dibutuhkan (*downtime*)	2	2	Rendah
R10	Tidak ada audit keamanan sistem informasi secara berkala.	2	2	Rendah

Pada tahap selanjutnya dilakukan proses evaluasi terhadap potensi risiko yang sudah dianalisis sebelumnya. Berdasarkan hasil analisis tersebut, peneliti menyusun matriks penilaian yang mengacu pada kerangka kerja ISO 31000:2018 untuk memudahkan proses evaluasi risiko. Matriks penilaian ini dibagi menjadi tiga kategori tingkatan, yaitu tingkat tinggi, menengah, dan rendah. Dengan menggunakan bagan ini, peneliti dapat memperkirakan besarnya probabilitas terjadinya risiko serta dampak yang mungkin ditimbulkan.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

4.4.2. *Perlakuan Risiko*

Berdasarkan hasil evaluasi risiko pada Tabel 12 dilakukan perencanaan strategi perlakuan risiko untuk menangani risiko-risiko yang telah teridentifikasi (Berliana & Tanamaah, 2021). Pendekatan ini dipilih karena setiap metode mampu memberikan kontribusi berbeda dalam mengendalikan risiko operasional yang muncul dalam proses pengelolaan data rekam medis. Perencanaan strategi tersebut mempertimbangkan karakteristik risiko yang bervariasi sehingga diperlukan penyesuaian tindakan pada setiap kategori risiko. Pemilihan strategi juga memanfaatkan acuan praktik *risk management* yang umum diterapkan dalam sistem informasi kesehatan. Strategi ini mengacu pada empat pendekatan utama, yaitu:

Tabel 12. Perlakuan Risiko

No.	Strategi	Penjelasan
1	Avoid	Menghindari aktivitas atau kondisi yang dapat memicu timbulnya risiko.
2	Reduce	Mengurangi kemungkinan terjadinya risiko atau dampaknya melalui tindakan preventif atau protektif.
3	Sharing	Mentransfer risiko kepada pihak lain, misalnya melalui kerja sama teknis atau asuransi.
4	Accept	Menerima risiko sebagaimana adanya jika dianggap tidak signifikan atau biaya penanganannya terlalu tinggi.

Berdasarkan Observasi dengan pihak terkait serta hasil evaluasi, berikut adalah rekomendasi perlakuan risiko untuk Sistem Rekam Medis Rumah Sakit Aisyiyah Bojonegoro. Identifikasi risiko dilakukan dengan menggabungkan temuan lapangan dan informasi teknis dari pihak pengelola sistem sehingga menghasilkan gambaran risiko yang komprehensif. Proses penilaian tersebut memberikan dasar untuk menentukan tindakan mitigasi yang tepat sesuai tingkat urgensi masing-masing risiko. Klasifikasi risiko yang telah disusun juga membantu dalam menentukan prioritas penanganan agar sumber daya dapat digunakan secara efektif. Dijelaskan di Tabel 13.

Tabel 13. Hasil Perlakuan Risiko

ID	Deskripsi Risiko	Risk Level	Tindakan Risiko	Tindakan Risiko
R07	Sistem tidak memiliki antivirus/firewall yang memadai.	Tinggi	Reduce	-Pasang antivirus danfirewall enterprise - Audit keamanan berkala
R02	Pegawai membocorkan data medis karena kelalaian atau ketidaktahuan akan privasi data.	Sedang	Reduce	- Pelatihan keamanan data berkala - Penandatanganan NDA - Monitoring aktivitas pengguna
R03	Pegawai belum dilatih terkait kebijakan keamanan informasi rekam medis.	Sedang	Reduce	- Pelatihan onboarding - Modul pelatihan interaktif dalam sistem - Supervisi awal saat penggunaan
R06	Tidak tersedia backup data rekam medis, menyebabkan potensi kehilangan data penting.	Sedang	Reduce	- Terapkan backup harian otomatis - Simpan backup di server terpisah/cloud - Uji pemulihan data
R08	Hak akses pengguna tidak dibatasi secara ketat sesuai peran	Sedang	Reduce	- Terapkan kontrol akses berbasis peran (RBAC) - Audit log akses pengguna secara rutin
R09	Hak akses pengguna tidak dibatasi secara ketat sesuai peran.	Sedang	Reduce	- Buat SOP pemeliharaan sistem - Jadwalkan maintenance reguler - Dokumentasi hasil monitoring
R11	Tidak ada enkripsi data saat penyimpanan atau pengiriman.	Sedang	Reduce	- Definisikan hak akses tiap jabatan - Audit otorisasi pengguna tiap bulan
R01	Staf medis salah menginput data pasien akibat kurang pemahaman sistem.	Rendah	Reduce	-Sediakan panduan pengguna - Buat menu bantuan/interaktif - Fitur user-friendly
R04	Sistem mengalami error dan menurunkan efisiensi pelayanan medis.	Rendah	Reduce	- Debug dan uji sistem berkala - Terapkan version control - Laporkan error secara sistematis
R05	SIRS tidak dapat diakses saat dibutuhkan (downtime);	Rendah	Reduce	- Perbaiki server uptime - Redundansi server (failover system) - Monitoring status server 24/7
R10	Tidak ada audit keamanan sistem informasi secara berkala.	Rendah	Reduce	- Perbaiki server uptime - Redundansi server (failover system) - Monitoring status server 24/7

Berdasarkan hasil observasi dan evaluasi bersama pihak terkait, Tabel 13 menampilkan rekomendasi *Risk* Treatment terhadap risiko yang teridentifikasi pada Sistem Informasi Rekam Medis. Risiko dengan tingkat tinggi terdapat pada R07, yaitu ketiadaan antivirus atau firewall, yang direkomendasikan untuk dikurangi melalui pemasangan sistem keamanan enterprise dan audit berkala. Risiko dengan tingkat sedang, seperti

p-ISSN : 2803-1507 e-ISSN : 2803-1531

R02, R03, R06, R08, R09, dan R11, dapat diminimalkan melalui pelatihan keamanan data, penerapan kontrol akses berbasis peran (RBAC), implementasi backup otomatis harian, enkripsi data, serta pengawasan aktivitas pengguna. Sementara itu, risiko dengan tingkat rendah seperti R01, R04, R05, dan R10 disarankan untuk ditangani dengan peningkatan kualitas sistem melalui panduan pengguna, debugging rutin, peningkatan uptime server, dan dokumentasi hasil pemeliharaan. Secara keseluruhan, strategi perlakuan risiko ini berfokus pada pendekatan Reduce, yaitu pengurangan potensi ancaman melalui kombinasi tindakan teknis, kebijakan keamanan, dan penguatan kompetensi SDM agar sistem rekam medis lebih aman, andal, dan berkelanjutan.

5. DISKUSI

Hasil penelitian menunjukkan bahwa risiko tertinggi pada SIRME terutama berasal dari aspek keamanan teknis seperti ketiadaan *firewall*, antivirus yang tidak memadai, dan tidak diterapkannya enkripsi data, sebagaimana juga ditekankan dalam kajian [12], [27] mengenai kerentanan infrastruktur digital kesehatan. Temuan ini memperlihatkan bahwa kondisi keamanan sistem di rumah sakit masih berada pada level yang rentan, yang konsisten dengan temuan risiko siber dalam sektor layanan kesehatan. Identifikasi 11 risiko memperlihatkan bahwa kelemahan teknis berpotensi memperbesar peluang terjadinya serangan siber serta kegagalan sistem yang memengaruhi mutu layanan. Pola risiko ini memperkuat bukti literatur bahwa komponen teknis menjadi salah satu sumber ancaman dominan dalam pengelolaan sistem informasi medis.

Analisis risiko pada faktor SDM menunjukkan bahwa kurangnya pelatihan, lemahnya kepatuhan terhadap kebijakan keamanan informasi, dan potensi *human error* memiliki peran signifikan dalam meningkatkan peluang insiden. Temuan ini selaras dengan pembahasan [15] tentang pentingnya kompetensi manusia dalam menjaga keamanan informasi, namun hasil penelitian ini menunjukkan tingkat ketergantungan yang lebih tinggi karena tidak adanya pelatihan rutin yang terstandardisasi. Ketidaksiapan SDM dalam menjaga kerahasiaan data memperluas gambaran risiko yang dicatat pada penelitian [28], terutama terkait kesadaran keamanan dan perilaku pengguna. Kondisi tersebut mengindikasikan bahwa risiko pada aspek SDM dapat memperburuk dampak risiko teknis ketika tidak dikendalikan secara sistematis.

Risiko operasional seperti *downtime*, kegagalan *backup*, dan ketiadaan *monitoring* real-time menunjukkan bahwa infrastruktur sistem belum mendukung kebutuhan operasional yang berkelanjutan. Situasi ini sejalan dengan uraian pada [22] yang menekankan pentingnya penguatan manajemen risiko operasional dalam kerangka ISO 31000, namun penelitian ini memperlihatkan bahwa kelemahan operasional tidak hanya berdampak pada efisiensi, tetapi juga berpotensi menimbulkan gangguan pada layanan medis kritis. Beberapa risiko seperti kegagalan *backup* dan lemahnya pembatasan hak akses menunjukkan adanya celah tata kelola yang belum diidentifikasi secara mendalam dalam penelitian terdahulu. Temuan ini memperlihatkan hubungan yang erat antara risiko operasional dan risiko keamanan, sehingga keduanya harus dianalisis dalam kerangka tata kelola risiko yang terintegrasi.

Penelitian ini berkontribusi dengan memberikan gambaran empiris mengenai bagaimana risiko teknis, operasional, dan perilaku pengguna saling berinteraksi dalam konteks rumah sakit, meskipun penelitian memiliki keterbatasan seperti ruang lingkup yang hanya mencakup satu institusi dan metode analisis yang bersifat deskriptif. Keterbatasan tersebut membatasi generalisasi hasil, terutama terhadap rumah sakit dengan tingkat digitalisasi berbeda, sebagaimana juga disinggung dalam literatur bahwa karakteristik organisasi memengaruhi tingkat risiko [19]. Selain itu, tidak digunakannya pendekatan kuantitatif atau model probabilistik menyebabkan gambaran tingkat risiko belum sepenuhnya terukur secara numerik. Meskipun demikian, hasil penelitian tetap memberikan landasan empiris yang relevan untuk penguatan kebijakan keamanan dan tata kelola risiko di sektor kesehatan.

6. KESIMPULAN DAN SARAN

6.1. *Kesimpulan*

Berdasarkan hasil analisis risiko terhadap pengelolaan Sistem Informasi Rekam Medis di rumah sakit menggunakan pendekatan ISO 31000:2018, dapat disimpulkan bahwa terdapat 11 potensi risiko yang berhasil diidentifikasi dan diklasifikasikan ke dalam tiga tingkatan, yaitu tinggi, sedang, dan rendah. Risiko dengan kategori tinggi berkaitan dengan ancaman keamanan siber seperti serangan virus dan peretasan, yang berpotensi mengganggu integritas dan kerahasiaan data pasien. Risiko tingkat sedang sebagian besar berkaitan dengan keterbatasan kompetensi sumber daya manusia, kurang optimalnya implementasi SOP,

p-ISSN : 2803-1507 e-ISSN : 2803-1531

serta kelemahan dalam pengelolaan data. Sementara itu, risiko dengan tingkat rendah meliputi kendala teknis operasional dan ketidakteraturan akses sistem yang perlu dimonitor secara berkala.

Secara konseptual, penelitian ini menunjukkan bahwa interaksi antara faktor manusia dan infrastruktur teknologi merupakan sumber risiko yang saling memengaruhi. Keterbatasan kompetensi pegawai dapat memperbesar peluang kesalahan operasional, sedangkan kelemahan sistem dapat menurunkan efektivitas kinerja pengguna. Oleh karena itu, penerapan manajemen risiko yang efektif tidak dapat dilakukan secara parsial, tetapi harus mengintegrasikan aspek teknis, organisasi, dan perilaku manusia dalam satu kerangka tata kelola risiko yang berkelanjutan. Hasil penelitian ini menegaskan pentingnya peningkatan keamanan sistem, pelatihan rutin bagi pegawai, serta evaluasi kebijakan keamanan informasi untuk menciptakan sistem rekam medis elektronik yang aman, andal, dan mendukung mutu pelayanan kesehatan digital.

6.2. *Saran*

Berdasarkan temuan penelitian ini, direkomendasikan agar Rumah Sakit Bojonegoro meningkatkan keamanan informasi dengan menerapkan manajemen risiko secara berkelanjutan sesuai kerangka kerja ISO 31000:2018. Upaya penguatan dapat dilakukan melalui pembaruan sistem keamanan, pemasangan firewall dan antivirus terbaru, serta pelaksanaan audit keamanan secara berkala untuk mencegah potensi serangan siber. Selain itu, peningkatan kapasitas dan kompetensi sumber daya manusia perlu menjadi perhatian utama guna mengurangi risiko kesalahan operasional. Dari sisi akademis, penelitian berikutnya disarankan untuk mengombinasikan pendekatan ISO/IEC 27001 agar cakupan analisis keamanan informasi menjadi lebih luas dan mendalam. Sementara itu, secara metodologis, penelitian lanjutan dapat menggunakan pendekatan kuantitatif atau model penilaian risiko berbasis probabilitas untuk menghasilkan hasil yang lebih objektif dan terukur.

DAFTAR PUSTAKA

[1] G. E. Myeong and K. S. Ram, "Blockchain Based Zero Knowledge Proof Protocol For Privacy Preserving Healthcare Data Sharing," *J. Technol. Informatics Eng.*, vol. 4, no. 1, pp. 171–189, Apr. 2025, doi: 10.51903/jtie.v4i1.296.

[2] A. A. Ashofi and M. Migunani, "The Impact of Data Security, Ease of Use, and Access Speed on User Trust in Mobile Banking Applications," *J. Manag. Informatics*, vol. 2, no. 3, pp. 104–117, May 2023, doi: 10.51903/jmi.v2i3.148.

[3] A. Zainudin, A. P. Hadi, and A. Priyadi, "Sistem Informasi Persediaan Obat Berbasis Web di Rumah Sakit Bina Kasih," *J. Ilm. Sist. Inf.*, vol. 3, no. 3, pp. 30–34, Jan. 2024, doi: 10.51903/2xwvpm83.

[4] C. Pekkari, B. Lund, T. Davidson, A. Naimi-Akbar, A. Marcusson, and C. K. Weiner, "Cost Analysis of Orthognathic Surgery: Outpatient Care versus Inpatient Care," *Int. J. Oral Maxillofac. Surg.*, vol. 53, no. 10, pp. 829–835, Oct. 2024, doi: 10.1016/j.ijom.2024.02.005.

[5] E. Yudianti and M. Arini, "Penerapan Healthcare Failure Mode and Effect Analysis (HFMEA) pada Implementasi Rekam Medis Elektronik," *J. Kesehat. Vokasional*, vol. 9, no. 1, pp. 61–75, Feb. 2024, doi: 10.22146/jkesvo.88541.

[6] F. A. Reegu *et al.*, "Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System," *Sustainability*, vol. 15, no. 8, p. 6337, Apr. 2023, doi: 10.3390/su15086337.

[7] K. Mohan, P. Kitsos, S. M. Williamson, and V. Prybutok, "Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven Healthcare," *Appl. Sci.*, vol. 14, no. 2, p. 675, Jan. 2024, doi: 10.3390/app14020675.

[8] S. H. Björnsdottir, P. Jensson, S. E. Thorsteinsson, I. M. Dokas, and R. J. De Boer, "Benchmarking ISO Risk Management Systems to Assess Efficacy and Help Identify Hidden Organizational Risk," *Sustainability*, vol. 14, no. 9, p. 4937, Apr. 2022, doi: 10.3390/su14094937.

[9] L. Purwanti, I. Triyuwono, G. Maski, D. Pusposari, A. Prakoso, and M. Ibrahim, "The Impact of ISO 31000 Adoption on the Performance of Banking Companies in Indonesia," *Cogent Bus. Manag.*, vol. 12, no. 1, p. 2507222, Dec. 2025, doi: 10.1080/23311975.2025.2507222.

[10] A. Sermhattakit and P. Sae-Lim, "Key Risks and Mitigation Strategies in Enterprise Risk Management

for Private Hospitals: A Mixed-Method Study," *Inq. (United States)*, vol. 62, pp. 1–13, Jan. 2025, doi: 10.1177/00469580251347132.

[11] N. Watted *et al.*, "The Complexity of Skeletal Transverse Dimension: From Diagnosis, Management, and Treatment Strategies to the Application of Collaborative Cross (CC) Mouse Model," *J. Funct. Morphol. Kinesiol.*, vol. 9, no. 1, p. 51, Mar. 2024, doi: 10.3390/jfmk9010051.

[12] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber Security: State of the Art, Challenges and Future Directions," *Cyber Secur. Appl.*, vol. 2, p. 100031, Jan. 2024, doi: 10.1016/j.csa.2023.100031.

[13] H. M. Melaku, "Context-Based and Adaptive Cybersecurity Risk Management Framework," *Risks*, vol. 11, no. 6, p. 101, May 2023, doi: 10.3390/risks11060101.

[14] B. Alamri, K. Crowley, and I. Richardson, "Cybersecurity Risk Management Framework for Blockchain Identity Management Systems in Health IoT," *Sensors*, vol. 23, no. 1, p. 218, Dec. 2022, doi: 10.3390/s23010218.

[15] A. Pollini *et al.*, "Leveraging Human Factors in Cybersecurity: an Integrated Methodological Approach," *Cogn. Technol. Work*, vol. 24, no. 2, pp. 371–390, Jun. 2021, doi: 10.1007/s10111-021-00683-y.

[16] I. Pouliezou, A. P. Gravia, and M. Vasoglou, "Digital Model in Orthodontics: Is It Really Necessary for Every Treatment Procedure? A Scoping Review," *Oral*, vol. 4, no. 2, pp. 243–262, Jun. 2024, doi: 10.3390/oral4020020.

[17] A. Azadi and F. J. García-Peñalvo, "Aligning EMR Structure with Treatment Cycles: Enhancing Data Management and CDSS Functionality," *Appl. Sci.*, vol. 15, no. 10, p. 5273, May 2025, doi: 10.3390/app15105273.

[18] Z. A. Maizura, S. K. Citra, and T. Purwaningrum, "Penerapan Aplikasi SATUSEHAT SDMK Bagi SDM Dinas Kesehatan Kabupaten Ponorogo," *Karya Nyata J. Pengabdi. Kpd. Masy.*, vol. 2, no. 1, pp. 73–86, Jan. 2025, doi: 10.62951/karyanyata.v2i1.1024.

[19] J. V. Barraza de la Paz, L. A. Rodríguez-Picón, V. Morales-Rocha, and S. V. Torres-Argüelles, "A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0," *Systems*, vol. 11, no. 5, p. 218, Apr. 2023, doi: 10.3390/systems11050218.

[20] S. M. H. S. ; Falcão, M. J. ; De Almeida, S. M. H. S. Rezvani, M. João, F. Silva, and N. Marques De Almeida, "The Risk-Informed Asset-Centric (RIACT) Urban Resilience Enhancement Process: An Outline and Pilot-Case Demonstrator for Earthquake Risk Mitigation in Portuguese Municipalities," *Appl. Sci.*, vol. 14, no. 2, p. 634, Jan. 2024, doi: 10.3390/app14020634.

[21] S. Ngwenya, N. S. Mashau, S. E. Mhlongo, and A. N. Traoré, "A Systematic Review of the Risk Management Frameworks for Potentially Toxic Chemical Elements," *Toxicol. Ind. Health*, vol. 39, no. 12, pp. 679–686, Dec. 2023, doi: 10.1177/0748233723120909.

[22] S. H. Björnsdóttir, P. Jensson, R. J. de Boer, and S. E. Thorsteinsson, "The Importance of Risk Management: What is Missing in ISO Standards?," *Risk Anal.*, vol. 42, no. 4, pp. 659–691, Apr. 2022, doi: 10.1111/risa.13803.

[23] L. Ispas, C. Mironeasa, and A. Silvestri, "Risk-Based Approach in the Implementation of Integrated Management Systems: A Systematic Literature Review," *Sustainability*, vol. 15, no. 13, p. 10251, Jun. 2023, doi: 10.3390/su151310251.

[24] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations," *Sensors*, vol. 23, no. 15, p. 6666, Jul. 2023, doi: 10.3390/s23156666.

[25] M. F. Safitra, M. Lubis, and H. Fakhrurroja, "Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity," *Sustainability*, vol. 15, no. 18, p. 13369, Sep. 2023, doi: 10.3390/su151813369.

[26] K. T. Kosmowski, E. Piesik, J. Piesik, and M. Śliwiński, "Integrated Functional Safety and

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Cybersecurity Evaluation in a Framework for Business Continuity Management," *Energies*, vol. 15, no. 10, p. 3610, May 2022, doi: 10.3390/en15103610.

[27] Z. Wenhua, F. Qamar, T. A. N. Abdali, R. Hassan, S. T. A. Jafri, and Q. N. Nguyen, "Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends," *Electronics*, vol. 12, no. 3, p. 546, Jan. 2023, doi: 10.3390/electronics12030546.

[28] A. Mishra, Y. I. Alzoubi, A. Q. Gill, and M. J. Anwar, "Cybersecurity Enterprises Policies: A Comparative Study," *Sensors*, vol. 22, no. 2, p. 538, Jan. 2022, doi: 10.3390/s22020538.

[29] Q. Aini, D. Manongga, U. Rahardja, I. Sembiring, and Y. M. Li, "Understanding Behavioral Intention to Use of Air Quality Monitoring Solutions with Emphasis on Technology Readiness," *Int. J. Human–Computer Interact.*, vol. 41, no. 8, pp. 5079–5099, 2025, doi: 10.1080/10447318.2024.2357860.

[30] D. M. Lengyel, T. A. Mazzuchi, and W. E. Vesely, "Establishing Risk Matrix Standard Criteria for Use in the Continuous Risk Management Process," *J. Sp. Saf. Eng.*, vol. 10, no. 3, pp. 276–283, Sep. 2023, doi: 10.1016/j.jsse.2023.05.001.