JSI : Jurnal Sistem Informasi *(E-Journal), VOL. 16, NO. 2, Oktober 2024*
ISSN Print : 2085-1588
ISSN Online :2355-4614
LINK: https://jsi.ejournal.unsri.ac.id/index.php/jsi/index

Penilaian Risiko Menggunakan Metode Analisa *Failure Mode And Effects Analysis* (FMEA) Dengan Standar ISO 27001 Pada Rumah Sakit

Nabilla Rizky Ananda, Tsabitha Daffa Putri Salsabila Ersa, Adelia Fitri Nabila, Nasywa Iqnatia Latifa, Enricco Rayhan Farrel, Laqma Dica Fitrani, Ari Cahaya Puspitaningrum
[1,2,3,4,5,6,7] Sistem Informasi, Fakultas Teknik & Desain, Universitas Hayam Wuruk Perbanas
e-mail: 202202021011@mhs.hayamwuruk.ac.id

Abstrak

Manajemen risiko adalah bidang penting yang menangani berbagai risiko yang dihadapi dalam operasi bisnis. Studi ini memeriksa penerapan Sistem Informasi Manajemen Rumah Sakit (SIMRS) di Rumah Sakit X untuk meningkatkan efisiensi operasional, akurasi data, dan keamanan informasi. SIMRS mendukung integrasi berbagai departemen rumah sakit, mengurangi kesalahan, dan meningkatkan koordinasi. Meskipun memiliki manfaat, praktik manajemen risiko saat ini di rumah sakit tidak sepenuhnya sesuai dengan standar ISO 27001, yang berpotensi mempengaruhi kerahasiaan, integritas, dan ketersediaan data. Penelitian ini Menggunakan Metode Failure Mode and Effects Analysis (FMEA) dan ISO 27001, hal ini dilakukan dengan mengidentifikasi risiko yang terkait dengan perangkat keras, perangkat lunak, sumber daya manusia, dan aset informasi. Hasil dari penelitian ini ditemukan 20 cause failure yang akan menyebabkan terjadinya risiko pada keamanan aset TI di Rumah sakit X. Terdapat 4 cause failure yang memiliki level tinggi dan diberikan rekomendasi sesuai dengan Annex yang ada pada ISO 27001:2013.

Kata Kunci: *Manajemen Risiko, Rumah Sakit, ISO 27001, Failure Mode and Effects (FMEA)*

Abstract

Risk management is an important area that addresses various risks faced in business operations. This study examines the implementation of the Hospital Management Information System (Hospital Information System or HIS, for brevity) at Hospital X to improve operational efficiency, data accuracy, and information security. The HIS supports the integration of various hospital departments, reduces errors, and improves coordination. Despite these benefits, current risk management practices in hospitals often fall short of full compliance with ISO 27001 standards, potentially impacting data confidentiality, integrity, and availability. This research employs the Failure Mode and Effects Analysis (FMEA) and ISO 27001 methodologies to identify hardware, software, human resources, and information assets risks. The research identified 20 potential causes of failure that could compromise the security of IT assets at Hospital X.

Keywords*: Risk Management, Hospital, ISO 27001, Failure Mode and Effects (FMEA)*

1. INTRODUCTION

Manajemen Risiko merupakan salah satu cabang keilmuan yang mempelajari tentang segala risiko yang dapat terjadi pada saat menjalankan suatu bisnis dalam sebuah perusahaan [1]. Banyak hal yang dibahas dalam topik tersebut, salah satunya yakni teknologi informasi. Penguatan teknologi informasi sangat penting karena sebagian besar bisnis tidak dapat terus beroperasi dengan sukses jika layanan teknologi informasinya tidak tersedia [2]. Penggunaan dari teknologi informasi telah masuk hampir ke seluruh aspek penunjang kehidupan, contohnya seperti aspek transportasi, kesehatan, lingkungan, pendidikan, terutama bisnis perusahaan [3]. Pada sebuah bisnis dalam segala bidang, teknologi informasi menjadi penunjang utama dalam menghadapi arus digitalisasi [4]. Dalam perjalanan mencapai tujuan, organisasi seringkali dihadapkan pada berbagai

rintangan, salah satunya adalah risiko yang terkait dengan teknologi informasi. Risiko ini dapat menghambat kelancaran operasional dan berakibat pada kegagalan dalam mencapai target [5]. Dalam mengidentifikasi manajemen risiko, perlu diperhatikan beberapa aset penting yaitu pertama identifikasi aset, dilanjutkan dengan identifikasi risiko, lalu mengidentifikasi ancaman (*Threat*), identifikasi kerentanan (*Vulnerability*) yang ada, identifikasi kemungkinan dari adanya ancaman dan kerentanan tersebut, Identifikasi tingkatan dari level risiko, serta menentukan dampak bisnis [6].

Seperti yang dijumpai pada salah satu instansi rumah sakit, yakni rumah sakit X. Pada rumah sakit X terdapat sebuah sistem yang dinamakan SIMRS untuk menunjang jalannya proses bisnis pada rumah sakit tersebut. SIMRS di rumah sakit X merupakan teknologi yang dapat mendukung operasional rumah sakit agar lebih efisien. Sistem ini memastikan data yang dimasukkan adalah akurat dan konsisten, yang sangat penting dalam pengelolaan rekam medis pasien yang harus selalu *up-to-date* dan dapat diandalkan. Dengan dilengkapi dengan fitur keamanan seperti enkripsi data dan kontrol akses berbasis peran untuk melindungi data pasien yang tidak sah.

Sistem ini memungkinkan integrasi antara berbagai departemen dalam rumah sakit X seperti UGD, laboratorium, farmasi, sehingga informasi pasien dapat diakses oleh semua departemen yang membutuhkan, mengurangi kesalahan dan meningkatkan koordinasi. Data yang terpusat memungkinkan, manajemen rumah sakit untuk menghasilkan laporan yang dibutuhkan untuk analisis kinerja pengambilan secara cepat akurat. Analisis data yang mendalam juga membantu dalam mengembangkan strategi yang lebih efektif, bukan hanya itu saja SIMRS juga dapat mengelola inventaris dan sumber daya rumah sakit X seperti obat-obatan, peralatan medis, dan bahan habis pakai memastikan bahwa semua kebutuhan operasional rumah sakit X dapat dipenuhi tepat waktu.

Penerapan SIMRS di rumah sakit X merupakan langkah maju dalam integrasi teknologi informasi di bidang kesehatan. Sistem ini membantu meningkatkan efisiensi operasional, akurasi data, keamanan informasi, integrasi lintas departemen, pelaporan, analisis, dan pengelolaan sumber daya rumah sakit. Namun, untuk memaksimalkan manfaat dari SIMRS, penting bagi manajemen rumah sakit untuk terus memantau dan mengelola risiko yang mungkin muncul seiring dengan penggunaan sistem ini. Dengan pendekatan manajemen risiko yang tepat, rumah sakit X dapat mengatasi tantangan yang ada dan terus meningkatkan kualitas layanan kepada pasien. Implementasi SIMRS menunjukkan bagaimana teknologi informasi dapat diintegrasikan dalam operasional rumah sakit untuk mendukung manajemen risiko dan meningkatkan kualitas layanan kesehatan secara keseluruhan.

Pengelolaan Risiko sesuai dengan ISO:27001 perlu diterapkan dengan tujuan agar penanganan risiko memenuhi standar [7]. Dalam pengelolaan risiko yang diterapkan pada rumah sakit X, belum memiliki tuntunan yang jelas dan tergolong berjalan mengikuti arahan untuk mengatasi risiko yang terjadi. Dalam berbagai aspek standar keamanan informasi, maka hal tersebut akan memiliki dampak pada informasi atau data yang tidak terjaga kerahasiaannya yang disebut sebagai *Confidentially*, informasi yang tidak utuh atau *Integrity* dan informasi yang tidak selalu tersedia yaitu *Availability* [8]. Hal-hal tersebut merupakan aspek utama dalam memahami beberapa standar keamanan informasi

agar dapat menerapkan standar yang baik untuk mengelola manajerial risiko dalam rumah sakit X.

2. RESEARCH METHOD

Dalam menyusun penelitian ini, kami menerapkan metode deskriptif dengan melakukan analisa mitigasi risiko sesuai dengan Annex ISO 27001 yang dilakukan dengan cara wawancara. ISO 27001 merupakan sebuah standar untuk menganalisa serta mitigasi risiko pada suatu perusahaan. Standar tersebut berkaitan dengan sistem keamanan informasi (SMKI) atau yang biasa disebut sebagai *Information Security Management System* (ISMS) yang memberikan sebuah panduan [9]. Penerapan ISO 27001 dalam mitigasi risiko bertujuan untuk memberikan panduan pada suatu perusahaan untuk mengelola, memahami, dan mengurangi risiko terkait dengan keamanan informasi yang dapat menjaga keberlangsungan proses bisnis yang sedang berjalan dan melindungi informasi sensitif yang dimiliki oleh perusahaan tersebut [7].

Tahap sebelum melakukan penilaian sesuai dengan standar ISO 27001, maka dilakukan penilaian sesuai dengan metode *Failure Mode and Effects Analysis* (FMEA). FMEA merupakan sebuah teknik penilaian yang digunakan dengan tujuan untuk meningkatkan keandalan, kelebihan dan keamanan suatu proses bisnis yang berlaku pada suatu perusahaan dengan cara mengidentifikasi apa saja potensi-potensi kegagalan atau sering disebut sebagai modus kegagalan pada proses bisnis tersebut [11]. Melalui FMEA, maka akan dapat menilai apa saja risiko yang dapat terjadi pada suatu bidang tertentu terutama yakni bidang IT [12]. Disamping kemajuan yang dirasakan jika menerapkan IT pada suatu perusahaan, terdapat pula kekurangan maupun risiko yang akan menjadi hambatan dalam realisasi sistem dalam kegiatan sehari-hari perusahaan.

2.1 Tahap Awal

2.1.1 Studi Pustaka

Pada penelitian ini, tim peneliti mempelajari terkait manajemen risiko melalui berbagai sumber ilmu pengetahuan. Tahap awal penerimaan teori terkait manajemen risiko yakni melalui mata kuliah pembelajaran. Sumber lainnya yaitu tim peneliti membaca berbagai jurnal dengan pembahasan sesuai dengan penelitian yang sedang dilakukan. Literasi lain juga digunakan seperti *e-book* yang diunggah pada internet. Tim peneliti mengumpulkan teori-teori tersebut dan menjadikannya sebagai penunjang utama terkait penyusunan jurnal penelitian ini.

2.2 Identifikasi Masalah

Pada penelitian ini, untuk tahap pengumpulan data yang dilakukan adalah dengan melakukan wawancara pada departemen IT SIMRS pada rumah sakit X. Proses wawancara dimulai dengan mengajukan beberapa pertanyaan terkait aset-aset yang dimiliki dan bagaimana cara pengelolaan yang dilakukan jika terjadi suatu risiko pada aset tersebut. Pertanyaan dijawab secara jelas oleh staf terkait, selain itu juga dijelaskan beberapa point penting yang diterapkan untuk mengelola risiko yang terjadi. Tetapi pada beberapa jawaban yang telah didapatkan, untuk pengelolaan manajerial risiko yang sudah diterapkan belum memenuhi standar yang ada pada ISO 27001.

Setelah mengajukan pertanyaan pada tahap wawancara, didapatkan hasil untuk aset-aset yang dimiliki di rumah sakit X. Aset tersebut dikelompokkan pada beberapa jenis seperti, *Hardware, Software,* Sumber Daya Manusia (SDM), dan Informasi. Pada Hardware terdapat aset seperti komputer, printer, CPU, Wifi, Server, dan beberapa aset lainnya. Untuk Software yang digunakan adalah menggunakan *software System Inhost* yang dijalankan pada SIMRS rumah sakit. Dalam hal Sumber Daya Manusia, terdapat 3 orang yakni Supervisor, dan 2 staf pendukung. Selanjutnya pada informasi terdapat data pasien, data karyawan, data farmasi, data keuangan, dan beberapa data lainnya. Pada hal-hal tersebut, terdapat beberapa risiko dan masing-masing sudah ditangani sesuai cara yang biasa diterapkan pada Rumah Sakit tersebut.

2.3 Tahap Analisa Risiko

risiko yang terdapat pada tiap aset memiliki cara penanganan yang berbeda-beda. risiko dapat lebih mudah untuk dianalisis sesuai dengan kelompok jenisnya masing-masing. Pada setiap jenis risiko, tentu saja memiliki standar dalam penanganan yang baik. Untuk standarisasi ISO 27001 yang seharusnya diterapkan, risiko tersebut ada yang sudah memenuhi dan masih terdapat yang belum memenuhi standar sesuai dengan ISO 27001. Maka dilihat dari hal tersebut, tim peneliti berniat untuk memberikan solusi dan mengarahkan manajerial risiko agar dapat sesuai dengan standar yang ada pada ISO 27001.

2.4 Tahap Pengelolaan Risiko dan Pemberian Rekomendasi

Sesuai dengan hasil dari wawancara yang telah dilakukan, untuk proses pengendalian dan pengelolaan risiko terkait dengan pengelolaan SIMRS di rumah Sakit X, maka dilakukan identifikasi penilaian *Failure Mode and Effects Analysis* (FMEA) dengan memperhatikan standar ISO 27001. Melalui metode tersebut, maka akan dapat terlihat bagaimana pengendalian risiko yang telah diterapkan. Apakah pengendalian tersebut sudah sesuai dengan standar ISO 27001. Dari hasil FMEA juga bisa diketahui tingkatan level risiko yang sedang dihadapi, serta rekomendasi untuk mitigasi risiko tersebut yang sesuai dengan standar ISO 27001.

3. RESULTS AND ANALYSIS

Dengan menggunakan metode yang telah dijelaskan diatas, maka diperoleh hasil analisa risiko pertama dengan menggunakan penilaian dari metode *Failure Mode and Effects Analysis* (FMEA) dan memperoleh hasil sesuai dengan tabel berikut:

Tabel 1**.** Tingkat RPN

RPN	Level risiko
200>	*Very High*
151-200	*High*
101-150	*Medium*
51-100	*Low*
0-50	*Very Low*

Tabel 2**.** Penilaian FMEA

No	Aset	Potensi risiko	Sev	Occ	Det	RPN	Level
1	Komputer	Komputer rusak	7	5	3	105	*High*
2	Printer Standart	Printer eror	6	4	3	72	*Medium*
3	Kabel	Kabel putus, arus listrik tidak stabil	8	4	2	64	*Medium*
4	Wifi	Wifi trobel dan eror, tidak bisa tersambung	7	3	3	63	*Medium*
5	Mouse	Mouse rusak	5	3	4	60	*Medium*
6	CPU	CPU rusak	8	5	2	80	*High*
7	Server	Server down	9	3	2	54	*Medium*
8	System Inhost	System down, system maintenance	8	2	3	48	*Medium*
9	Supervisor	Resign dari pekerjaan, cuti, human error	6	4	3	72	*Medium*
10	Staff	Resign dari pekerjaan, cuti, hanya 1 staff yang bertugas. Human error, staff belum menguasai SIMRS, kompetensi kurang, pemahaman terhadap software masih kurang mendalam.	7	5	2	70	*High*
11	Data Pasien	Kehilangan data dan kebocoran data	9	2	2	36	*Low*
12	Data Karyawan	Penyalahgunaan data karyawan	8	3	3	72	*Medium*
13	Data Kalim BPJS	Server BPJS down, system tidak dapat diakses	9	4	2	72	*Medium*
14	Data Keuangan	Manipulasi data keuangan	9	3	3	81	*High*
15	Data Pelayanan Pasien	Kesalahan input data dan tidak sesuai dengan keluhan	8	2	4	64	*Medium*
16	Data Pendaftaran	Server system sulit diakses, system penuh dan memerlukan waktu untuk mendaftar	7	3	3	63	*Medium*
17	Data Farmasi	Penyalahgunaan data obat	8	2	3	48	*Medium*
18	Data Pelayanan Rawat Inap	Kesalahan dalam pengisian dan pengelolaan data pasien rawat inap	8	3	3	72	*Medium*
19	Data Bagian Gudang	Kesalahan input data gudang	7	2	4	56	*Medium*
20	Penyedia Jasa Server	*Server down*	9	3	2	54	*Medium*

Berdasarkan pemetaan pada tabel 2, maka dapat dilihat bahwa risiko (*cause failure*) yang akan di mitigasi adalah risiko nomor 1, 6, 14, dan 20. Pada nomor tersebut

JSI : Jurnal Sistem Informasi *(E-Journal), VOL. 16, NO. 2, Oktober 2024*
ISSN Print : 2085-1588
ISSN Online :2355-4614
LINK: https://jsi.ejournal.unsri.ac.id/index.php/jsi/index

dipilih untuk di mitigasi karena memiliki Tingkat risiko yang tergolong tinggi. Mitigasi dilakukan sebagai Langkah penanganan untuk meminimalisir terjadinya risiko tersebut pada Perusahaan.

Tabel 3. Matrik Level

***Saverity*/Dampak**	***Very High***					
	High				**1, 6, 14, 20**	
	Moderate			**2, 3, 4, 5, 7, 8, 9, 12, 13, 15, 16, 17, 18, 19, 20**		
	Low		**11**			
	Very Low					
		Very Low	***Low***	***Moderate***	***High***	***Very High***
		***OCCURANCE*/KEMUNGKINAN**				

Dari penjelasan diatas dapat diketahui bahwa cause failure yang memerlukan penanganan adalah cause failure yang berada di kolom merah dan kuning yaitu cause failure nomor 1, 6, 14, 20. Dari hasil perhitungan RPN dan Matrik dapat dipetakan lagi dalam bentuk tabel untuk melihat kesesuaian dan memilih cause failure mana yang akan diprioritaskan dalam proses mitigasi atau ditangani untuk meminimalisir terjadinya risiko.

Tabel 4**.** Penilaian ISO 27001 diisi very high dan high

No	Jenis Aset	Nama Aset	Risk	Solusi	Annex	Kontrol
1	Hardware	Komputer	Komputer rusak	Diperbaiki dan membuat laporan	A.11.2.1	Peralatan harus ditempatkan dan dilindungi untuk mengurangi risiko ancaman dan bahaya lingkungan, serta peluang akses yang tidak sah
		CPU	CPU rusak	Diperbaiki dan Mengganti dengan komponen baru	A.11.2.1	Peralatan harus ditempatkan dan dilindungi untuk mengurangi

						risiko ancaman dan bahaya lingkungan, serta peluang akses yang tidak sah
2	People/SDM	Staff	Resign dari pekerjaan, cuti, hanya 1 staff yang bertugas. Human error, staff belum menguasai simrs, kompetensi kurang, pemahaman terhadap software masih kurang mendalam.	Melakukan koordinasi dan melihat manual book	A.7.2.1 A.7.2.2	Manajemen harus mewajibkan seluruh karyawan dan kontraktor untuk menerapkan keamanan informasi sesuai dengan kebijakan dan prosedur yang ditetapkan organisasi. Semua karyawan organisasi dan kontraktor harus menerima pendidikan dan pelatihan kesadaran yang sesuai serta pembaruan rutin dalam kebijakan dan prosedur organisasi yang relevan dengan tujuan sesuai pekerjaan mereka.
3	Informasi	Data Keuangan	Manipulasi data keuangan	Penerapan system audit internal, enkripsi data, dan akses terbatas	A.9.1.2 A.12.7.1	Pengguna hanya akan diberikan akses ke jaringan dan layanan jaringan yang

						secara khusus telah memiliki izin untuk dipergunakan. Persyaratan audit dan aktivitas yang melibatkan verifikasi sistem operasional harus direncanakan dan disepakati secara hati-hati untuk meminimalkan gangguan terhadap proses bisnis

4. CONCLUSION

Penelitian ini meninjau manajemen risiko di Rumah Sakit X melalui implementasi Sistem Informasi Manajemen Rumah Sakit (SIMRS). SIMRS meningkatkan efisiensi operasional, akurasi data, dan keamanan informasi, namun praktik manajemen risiko masih belum sesuai standar ISO 27001. Analisis FMEA mengkategorikan risiko berdasarkan keparahan, frekuensi kejadian, dan deteksi, menyoroti perlunya pemeliharaan rutin komputer dan sistem audit internal untuk data keuangan. Rekomendasi mencakup penerapan kontrol sesuai Annex ISO 27001, pembuatan manual book, koordinasi staf, serta pelaporan dan audit ketat. Implementasi ini diharapkan mengurangi risiko dan meningkatkan kualitas layanan, menekankan pentingnya manajemen risiko sesuai standar internasional untuk keberlanjutan dan keamanan operasional rumah sakit.

REFERENCES

[1] Suryaningsum, “Manajemen Resiko_tgl 27-10_Sri Suryaningsum 2,” *Manaj. Resiko*, pp. 9–215, 2010.

[2] L. D. Fitrani, “RISK ASSESMENT AND BUSINESS IMPACT ANALYSIS AS A BASIS FOR THE DRAFTING DISASTER RECOVERY PLAN AT UPT-TIK OF XYZ UNIVERSITY,” vol. 7, no. Idc, pp. 321–334, 2022.

[3] Tutik, N. Mutiah, and I. Rusi, “Analisis Dan Manajemen Risiko Keamanan Informasi Menggunakan Metode Failure Mode And Effects Analysis (FMEA) Dan ISO/IEC 27001:2013,” *Coding J. Komput. dan Apl.*, vol. 10, no. 02, pp. 249–261, 2022.

[4] D. A. Sunarta, "Kaum milenial di perkembangan ekonomi digital," *Econ. Bus. Manag. Int. ...*, vol. 5, no. 1, pp. 9–16, 2023, doi: 10.556442/eabmij.v5i01.

[5] Fitrani, "Risk Risk Assessment and Development of Access Control Information Security Governance Based on ISO/IEC 27001:2013 At XYZ University," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 2, pp. 891–907, 2022, doi: 10.35957/jatisi.v9i2.1643.

[6] R. I. A. Falach, L. Abdurrahman, and I. Santoso, "Octave Allegro Risk Analysis and Information Security Control Design in Hospital Management Information System Billing Module Using Octave Allegro," *e-Proceeding Eng.*, vol. 8, no. 2, pp. 2709–2722, 2021.

[7] I. Setiawan, A. R. Sekarini, R. Waluyo, and F. N. Afiana, "Manajemen Risiko Sistem Informasi Menggunakan ISO 31000 dan Standar Pengendalian ISO/EIC 27001 di Tripio Purwokerto," *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 20, no. 2, pp. 389–396, 2021, doi: 10.30812/matrik.v20i2.1093.

[8] M. Metode Blowfish Dengan Bahasa Pemrograman Java Mohamad Natsir, K. Kunci, K. Simetris, and A. Blowfish, "Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data Office," *Jurnal*, vol. 6, pp. 2089–5615, 2016.

[9] B. Panjaitan, L. Abdurrahman, and R. Mulyana, "Pengembangan Implementasi Sistem Manajemen Keamanan Informasi Berbasis Iso 27001:2013 Menggunakan Kontrol Annex: Studi Kasus Data Center Pt. Xyz," *e-Proceeding Eng.*, vol. 8, no. 2, pp. 2813–2825, 2021.

[10] M. Amirinnisa[1] and R. Bisma[2], "Analisis Penilaian Risiko Keamanan Informasi Berdasarkan Iso 27005 Untuk Persiapan Sertifikasi Iso 27001 pada Pemerintah Kota Madiun," *Jeisbi*, vol. 04, no. 04, pp. 47–58, 2023.

[11] A. Alijoyo, Q. B. Wijaya, and I. Jacob, "Failure Mode Effect Analysis Analisis Modus Kegagalan dan Dampak RISK EVALUATION RISK ANALYSIS: Consequences Probability Level of Risk," *Crms*, p. 19, 2020.

[12] M. H. Aiman and M. Nuruddin, "Analisis Kecacatan Produk Pada Mesin Pemotongan Dengan Menggunakan Metode FMEA di UD. Abdi Rakyat," *J. Tek. Ind. J. Has. Penelit. dan Karya Ilm. dalam Bid. Tek. Ind.*, vol. 9, no. 2, p. 577, 2023, doi: 10.24014/jti.v9i2.23835.