ANALISIS RISIKO DAN KONTROL PADA SIMRS REKAM MEDIS BERDASARKAN ISO 31000

(STUDI KASUS: RUMAH SAKIT KHUSUS IBU DAN ANAK KOTA BANDUNG)

Alya Lathifa Dinar[1], Lukman Abdurahman[2], Iqbal Santosa[3]
[123]Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[1]alyalatifa@student.telkomuniversity.ac.id, [2]abdural@telkomuniversity.ac.id,
[3]iqbals@telkomuniversity.ac.id

The Mother and Child Hospital (RSKIA) is one of the hospitals managed by the Bandung city government. The government issued a regulation requiring that every hospital implement the Hospital Management Information System (SIMRS), RSKIA has carried out these government regulations since 2014. RSKIA built SIMRS without a third party.
Hospital agencies engaged in the field of health services such as RSKIA must be able to implement risk management governance properly and wisely. Based on the initial implementation of SIMRS in RSKIA, the hospital has never conducted a risk analysis of the risks that might occur in SIMRS.
To support this solution ISO 31000: 2018 becomes a method for analyzing risk management and can help RSKIA can continue to develop services in the health sector to maintain the quality of service for its patients. After conducting an analysis according to ISO 31000: 2018 standards then make recommendations and controls based on NIST 800-53 standards and Department of Defense Instruction 8500.3

Keywords : Risk Management, Hospital Management Information System, ISO 31000, Hospital.

Abstrak- Rumah Sakit Khusus Ibu dan Anak (RSKIA) merupakan salah satu rumah sakit yang dikelola oleh pemerintah kota Bandung. Pemerintah mengeluarkan peraturan yang mengharuskan bahwa setiap rumah sakit melakukan implementasi terhadap Sistem Informasi Manajemen Rumah Sakit (SIMRS), RSKIA sudah melakukan aturan pemerintah tersebut sejak tahun 2014. RSKIA membangun SIMRS tanpa adanya pihak ketiga.
Instansi rumah sakit yang bergerak pada bidang pelayanan kesehatan seperti RSKIA harus mampu menerapkan tata kelola manajemen risiko dengan baik dan bijak. Berdasarkan dari awal pengimplementasian SIMRS pada RSKIA, rumah sakit belum pernah melakukan analisis risiko terhadap risiko yang mungkin akan terjadi pada SIMRS.
Untuk mendukung solusi tersebut ISO 31000:2018 menjadi metode untuk menganalisis manajemen risiko dan dapat membantu RSKIA dapat terus melakukan pengembangan pelayanan di bidang kesehatan untuk menjaga kualitas pelayanan terhadap pasiennya. Setelah dilakukannya analisis sesuai standar ISO 31000:2018 lalu melakukan rekomendasi dan kontrol yang berdasarkan dengan standar NIST 800-53 dan *Department of Defense Instruction* 8500.3

Kata kunci: Manajemen Risiko, Sistem Informasi Manajemen Rumah Sakit, ISO 31000, Rumah Sakit.

1. Pendahuluan

1.1. Latar Belakang

Teknologi informasi sudah digunakan di berbagai perindustrian di Indonesia, salah satunya pada dunia kesehatan khususnya di rumah sakit. Teknologi informasi yang digunakan oleh dunia kesehatan ialah Sistem Manajemen Rumah Sakit (SIMRS). Penggunaan SIMRS dalam dunia kesehatan berguna untuk membantu seluruh kegiatan proses bisnis di rumah sakit. SIMRS yang berbasis standar nasional ini dikeluarkan berdasarkan regulasi yang terkait yakni peraturan Kementerian Kesehatan Indonesia nomor 82 tahun 2013 tentang Sistem Manajemen Rumah Sakit, yang membahas mengenai ketentuan bahwa setiap rumah sakit di Indonesia wajib menyelenggarakan, melaksanakan pengelolaan dan pengembangan SIMRS pada rumah sakit.
Rumah Sakit Khusus Ibu dan Anak Bandung (RSKIA), merupakan sebuah instansi perawatan yang di kelola oleh pemerintahan kota Bandung. RSKIA ialah sebuah instansi kesehatan yang pelayanannya disediakan oleh dokter spesialis, perawat dan tenaga ahli kesehatan lainnya. Dalam menjalankan proses bisnisnya, RSKIA ini menggunakan sistem informasi terkomputerisasi, RSKIA sudah mengimplementasikan SIMRS terhitung sejak tahun 2014. Implementasi SIMRS yang dilakukan oleh RSKIA secara bertahap hingga saat ini.
RSKIA memiliki unit IT untuk mengatur segala urusan yang berhubungan dengan IT di rumah sakit. Unit IT di RSKIA telah menerapkan risiko yang pernah terjadi selama SIMRS berjalan. Walaupun RSKIA telah melakukan manajemen risiko tidak mentupi kemungkinan bahwa akan adanya risiko lain, sementara

risiko yang teridentifikasi hanya risiko yang sudah pernah terjadi.

Salah satu cara untuk memitigasi sebuah risiko yang terjadi agar tidak menghambatnya tujuan organisasi ialah dengan mengidentifikasi dan menganalisis risiko tersebut. Identifikasi dan analisis risiko berguna untuk mempersiapkan instansi terhadap risiko yang akan terjadi, dan instansi sudah siap dan dapat memintigasi dampak yang terkait dari risiko yang terjadi.

Risiko yang ditimbulkan dapat dilakukan dengan menerapkan pengukuran terhadap risiko yang timbul pada SIMRS agar RSKIA dapat meminimalisirkan risiko yang timbul. Hasil dari pengukuran risiko yang dilakukan pengukuran dapat mengetahui besaran dampak dari risiko dan kerentanan dari data aset yang terkait yang dinilai penting oleh instansi yang lalu dapat diterapkan kontrol yang tepat terhadap skala priorita yang tertinggi.

Rekam Medis adalah salah satu aset komponen yang paling penting untuk rumah sakit. Rekam medis mencakup semua kegiatan pelayanan yang terjadi di rumah sakit, rekam medis juga sebagai modul yang menyimpan data semua pasien di rumah sakit. Dengan tidak adanya rekam medis, maka rumah sakit tidak dapat menerapkan pelayanan kesehatan terhadap pasien. Oleh karena itu aset yang terkait dengan rekam medis pada SIMRS sangatlah penting, sehingga harus dijaga dari risiko yang mungkin berdampak besar terhadap instansi jika tidak ada penaganan yang tepat.

Pada penelitian ini menggunakan ISO 31000:2018 sebagai acuan dalam menganalisis manajemen risiko, dan identifikasi risiko dengan menggunakan *Generic Risk Scenarios* Cobit5.

Penerapan pengelolaan risiko berbasis ISO 31000:2018 ini sangat penting karena menurut Susilo (2018:22), "proses pengelolaan risiko yang berulang akan membantu organisasi untuk menetapkan strategi, mencapai sasaran, dan mengambil keputusan dengan pertimbangan yang matang."

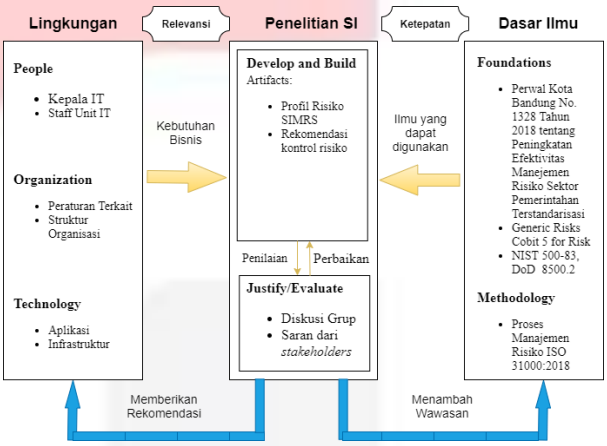
Dengan dilakukannya penelitian ini diharapkan RSKIA dapat mengelola aset dengan lebih baik.

2. Metode Penelitian

Model Konseptual merupakan kerangkat berpikir yang utuh dalam rangka penyederhanaan masalah dengan metode dan sistematika yang terstruktur. Metode ini mengacu pada ISO 31000:2018 sebagai acuan standar dalam melakukan analisis manajemen risiko. Diharapkan dengan adanya model konseptual ini dapat memberikan gambaran yang dapat membantu penelitian.. Framework penelitian untuk Sistem Informasi (SI) diilustrasikan seperti gambar 1.

Berikut penjelasan dari model konseptual tersebut.

1. Lingkungan penelitian dilakukan pada RSKIA Bandung, ruang lingkup yang dijadikan sebagai penelitian ialah Unit IT RSKIA. RSKIA sendiri sudah mengimplementasikan SIMRS selama kurang lebih 6 tahun terhitung dimulai dari tahun 2015. RSKIA pernah melakukan identfikasi risiko yang pernah terjadi, namun tidak melakukan identifikasi terhadap kemungkinan risiko yang lain yang mungkin akan terjadi nantinya.
2. Dasar hukum yang digunakan untuk mendukung penelitian ini adalah Perwal Kota Bandung No. 1328 Tahun 2018 Tentang Peningkatan Efektivitas Manajemen Risiko Sektor Pemerintahan Terstandarisasi. Kerangka kerja ISO 31000:2018 digunakan sebagai metodologi penelitian dan General Risk Scenario Cobit 5 for risk sebagai model. Sedangkan kontrol yang digunakan adalah NIST 800-53.
3. Hasil dari penelitian ini adalah artefak berupa profil risiko hardware SIMRS dan rekomendasi kontrol yang sesuai berdasarkan NIST 800-53.



Gambar 1 Model Konseptual

Data yang digunakan yaitu terdapat dua jenis data, data primer dan sekunder. Data primer merupakan sumber data penelitian yang diperoleh secara langsung dari sumbernya, metode yang dilakukan oleh penulis kepada pihak terkait RSKIA dengan melakukan wawancara secara langsung dan melalui wawancara online, pengambilan data ini bertujuan untuk sebagai bahan acuan melakukan proses penilaian risiko. Data sekunder adalah sumber data penelitian yang diperoleh melalui media perantara atau tidak langsung, metode yang digunakan penulis untuk proses data skunder ini ialah melalui sumber literatur yang disediakan, media dan internet. Data skunder yang dibutuhkan meliputi ISO 31000:2018, Data Lengkap RSKIA, dan framework yang di pakai yaitu NIST 800-53 dan DoD 8500.2. Lalu setalah semua data sudah dikumpulkan data akan diolah menggunakan standar ISO 3100-:2018, tahapan proses awal yang dilakukan adalah mengidentifikasi risiko, yang kedua menganalisis risiko berdasarkan penyebab dan dampak yang sudah teridentifikasi yang kemungkinan terjadi, setelah itu diberikan evaluasi risiko. Dan yang terakhir diberi penanganan yang sesuai terhadap risiko yang berdampak besar. Lalu penanganan tersebut diberikan kontrol untuk melakukan penanganan terhadap risiko yang mungkin terjadi.

3. Pembahasan

3.1 Tahap Pendefinisian Ruang Lingkup, Konteks dan Kriteria

3.1.1 Pendefinisian Ruang Lingkup 3.1.1.1 Profil RSKIA

3.1.1.1 Profil RSKIA

RSKIA merupakan salah satu rumah sakit di Bandung yang menggunakan SIMRS sebagai sistem pada rumah sakit. RSKIA yang beralamatkan di Jl. Astana Anyar No.224, Nyengseret, Kec. Astanaanyar, Kota Bandung, Jawa Barat 40242. RSKIA Bandung adalah salah satu rumah sakit yang dibangun oleh pemerintahan kota Bandung yang berdasarkan Peraturan Daerah Kota Bandung No. 14 Tahun 2009 tentang Pembentukan dan susunan Organisasi RSKIA. Sebelum menjadi RSKIA merupakan Rumah Sakit Bersalin Astana Anyar Kota Bandung dibawah Dinas Kesehatan Kota Bandung sesuai Perda No. 06 Tahun 2001 sebagai Lembaga Teknis daerah, dengan tugas pokok melaksanakan kewenangan dalam bidang pelayanan Kesehatan Ibu dan Anak. SIMRS digunakan pada sistem di RSKIA sebagai teknologi informasi yang mengatur sistem pada rumah sakit.

3.1.1.2 Visi, Misi. Dan Nilai RSKIA

Visi

Menjadi Rumah Sakit rujukan pelayanan kesehatan Ibu dan Anak yang Unggul, Mudah dan Nyaman

Misi

1. Menyelenggarakan pelayanan kesehatan yang lengkap, terpadu, unggul dan bermutu kelas dunia
2. Membangun kolaborasi dan jejaring dengan berbagai pihak
3. Mengembangkan sumber daya manusia yang profesional, berakhlak mulia dan berdaya saing tinggi

3.1.2 Identifikasi Konteks Organisasi

Penetapan konteks risiko dilakukan agar konteks apa saja yang digunakan sebagai acuan penelitian terhadap organisasi yang menjadi konteks objek penelitian dan dapat dipahami. Tabel mengenai konteks risiko penelitian dapat dilihat pada tabel 1.

3.1.3 Penetapan Kriteria Risiko

Penetapan kriteria risiko adalah untuk mengukur skala seberapa besar kemungkinan dan dampak yang akan dijadikan rujukan untuk menilai besaran risiko dan menentukan prioritas risiko. Acuan kriteria risiko yang digunakan adalah Peraturan Wali Kota Bandung Nomor 1328 Tahun 2018, pada regulasi tersebut terdapat kriteria kemunginan risiko pada tabel 2, kriteria dampak pada tabel 3, dan matriks risiko pada tabel 4. Kriteria kemungkinan adalah ukuran mengenai seberapa mungkin risiko tersebut akan terjadi. Kriteria dampak adalah ukuran terhadap besaran dampak risiko tersebut dapat mempengaruhi organisasi.

Tabel 1 Konteks Internal dan Eksternal

Konteks	Komponen	Dokumen
Internal	*stakeholder* internal	Sakit pada RSKIA Kota Bandung
		SK Direktur RSKIA Kota Bandung Nomor 445/46.1/SK/RSKIA/III /2016 Tentang Access Level Security Data dan Informasi pada RSKIA Kota Bandung
		SK Direktur Nomor 445/8/SK/RSKIA/I/2018 Tanggal 15 Januari 2018 tentang Kebijakan Manajemen dan Informasi di RS Khusus Ibu dan Anak Kota Bandung
		Peraturan Direktur RS Khusus Ibu dan Anak Kota Bandung Nomor: 445/2.15/SK/RSKIA/I/2019 Tentang Peraturan Internal Rumah Sakit *(Hospital By Laws)* RS Khusus Ibu dan Anak Kota Bandung
	Komitmen kontraktual	Sumpah/Janji sebagai Tenaga Kerja Kesehatan
Eksternal	Persyaratan hukum dan peraturan	Peraturan Menteri Kesehatan Republik Indonesia Nomor 82 Tahun 2013 Tentang Sistem Informasi Manajemen Rumah Sakit
		Peraturan Walikota Bandung Nomor 1338 tahun 2017 Tentang Tata Kelola Teknologi Informasi dan Komunikasi
		Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
		Peraturan Wali Kota Bandung Nomor 1328 Tahun 2018 tentang Peningkatan Efektivitas Manajemen Risiko Sektor Pemerintahan Terstandarisasi
	Hubungan dengan *stakeholder* eksternal	Perjanjian dengan Pihak Ketiga

Tabel 1 Kriteria Kemungkinan

Tingkat	Kriteria
Hampir Tidak Terjadi	Kemungkinan terjadinya < 2 kali dalam 5 tahun.
	Persentase kemungkinan terjadinya < 5% dari volume transaksi dalam 1 periode.
Jarang Terjadi	Kemungkinan terjadinya 2-10 kali dalam 5 tahun.
	Persentase kemungkinan terjadinya 5-10% dari volume transaksi dalam 1 periode.
Kadang-kadang Terjadi	Kemungkinan terjadinya 10-18 kali dalam 5 tahun.
	Persentase kemungkinan terjadinya 10-20% dari volume transaksi dalam 1 periode.
Sering Terjadi	Kemungkinan terjadinya 18-26 kali dalam 5 tahun.
	Persentase kemungkinan terjadinya 20-50% dari volume transaksi dalam 1 periode.
Hampir Pasti Terjadi	Kemungkinan terjadinya > 26 kali dalam 5 tahun.
	Persentase kemungkinan terjadinya > 50% dari volume transaksi dalam 1 periode.

Tabel 2 Kriteria Dampak

Level Dampak	Area Dampak	
Tidak Signifikan (1)	Kerugian Negara	Jumlah kerugian negara ≤ Rp10 Juta
	Penurunan reputasi	Keluhan Stakeholder secara langsung lisan/tertulis ke Perangkat Daerah jumlahnya ≤ 3 dalam satu periode
	Penurunan Kinerja	Pencapaian target kinerja ≥ 100%
	Gangguan Terhadap Layanan Perangkat Daerah	Pelayanan tertunda ≤ 1 hari
	Tuntutan Hukum	Jumlah tuntutan hukum ≤ 5 kali dalam satu periode
Minor (2)	Kerugian Negara	Jumlah kerugian negara lebih dari Rp10 Juta s.d Rp50 Juta
	Penurunan reputasi	Keluhan Stakeholder secara langsung lisan/tertulis ke Perangkat Daerah jumlahnya lebih dari 3 dalam satu periode
	Penurunan Kinerja	Pencapaian target kinerja di atas 80% s.d 100%
	Gangguan Terhadap Layanan Perangkat Daerah	Pelayanan tertunda di atas 1 hari s.d 5 hari
	Tuntutan Hukum	Jumlah tuntutan hukum di atas 5 kali s.d 15 kali dalam satu periode
Moderat (3)	Kerugian Negara	Jumlah kerugian negara lebih dari Rp50 Juta s.d Rp100 Juta
	Penurunan reputasi	Pemberitaan negatif di media massa lokal
	Penurunan Kinerja	Pencapaian target kinerja di atas 50% s.d 80%
	Gangguan Terhadap Layanan Perangkat Daerah	Pelayanan tertunda di atas 5 hari s.d 15 hari
	Tuntutan Hukum	Jumlah tuntutan hukum di atas 15 kali s.d 30 kali dalam satu periode
Signifikan (4)	Kerugian Negara	Jumlah kerugian negara lebih dari Rp100 Juta s.d Rp500 Juta
	Penurunan reputasi	Pemberitaan negatif di media massa nasional
	Penurunan Kinerja	Pencapaian target kinerja di atas 25% s.d 50%
	Gangguan Terhadap Layanan Perangkat Daerah	Pelayanan tertunda di atas 15 hari s.d 30 hari
	Tuntutan Hukum	Jumlah tuntutan hukum di atas 30 kali s.d 50 kali dalam satu periode
Sangat Signifikan (5)	Kerugian Negara	Jumlah kerugian negara lebih dari Rp500 Juta
	Penurunan reputasi	Pemberitaan negatif di media massa internasional
	Penurunan Kinerja	Pencapaian target kinerja ≤ 25%

Level Dampak	Area Dampak	
	Gangguan Terhadap Layanan Perangkat Daerah	Pelayanan tertunda lebih dari 30 hari
	Tuntutan Hukum	Jumlah tuntutan hukum lebih dari 50 kali dalam satu periode

Untuk matriks risiko akan dijelaskan pada matrisk dibawah ini

Level Risiko dapat ditentukan berdasarkan dari 2 hal yaitu level kemungkinan terjadinya risiko dan leve dampak risiko. Keduanya harus dijadikan sebagai ukuran untuk perhitungan secara Bersama untuk penentuan level risiko. Pada matrik ini level kemungkinan terjadinya risiko, level dampak dan level risikp masing masing menggunakan lima skala level, seperti gambar 3. [3].

Gambar 1 Matriks Risiko

Matriks Analisis Risiko 5x5		evel Dampak				
		1	2	3	4	5
		Tidak Signifikan	Minor	Moderat	Signifikan	Sangat Signifikan
Level Kemungkinan	5 Hampir Pasti terjadi	9	16	20	23	25
	4 Sering terjadi	6	13	18	22	24
	3 Kadang Terjadi	4	11	15	19	21
	2 Jarang terjadi	2	7	12	14	17
	1 Hampir Tidak Terjadi	1	3	5	8	10

Gambar 3 Level Risiko

Level Risiko		Besaran Risiko	Keterangan Warna
1	Sangat Rendah	1 s.d 3	Hijau Tua
2	Rendah	4 s.d 8	Hijau
3	Sedang	9 s.d 17	Kuning
4	Tinggi	18 s.d 22	Jingga
5	Sangat Tinggi	23 s.d 25	Merah

Selera risiko adalah sebagai acuan apakah risiko harus diberikan penanganan atau tidak, pada tabel berikut akan dijelaskan ukuran untuk menentukan besaran risiko yang ditangani.

Tabel 4 Selera Risiko

No.	Kategori Risiko	Perwal	Besaran Risiko yang Harus Ditangani
1	Pembangunan dan pemeliharaan portfolio	Risiko Reputasi	≥ 7
		Risiko Strategis	
2	Programme and Project Lifecycle	Risiko pembiayaan	≥ 11
		Risiko Belanja	
		Risiko Strategi	
		Risiko Operasional	
3	IT Investment Decision Making	Risiko Pendapatan	≥ 9
		Risiko Belanja	
		Risiko Strategis	
4	IT Expertise and Skill	Risiko Operasional	≥ 15
5	Staff Operation / Human Error	Risiko Fraud	≥ 6
		Risiko Kepatuhan	
6	Information	Risiko Fraud	≥ 9
		Risiko Kepatuhan	
		Risiko Operasional	
7	Arsitektur	Risiko Strategis	≥ 14
		Risiko Pendapatan	
8	Infrastructure	Risiko Operasional	≥ 7
		Risiko Strategis	
9	Software	Risiko Strategis	≥ 11
		Risiko Operasional	
		Risiko Pendapatan	
10	Business Ownership of IT	Risiko Strategis	≥ 11

		Risiko Operasional	
		Risiko Belanja	
11	Supplier Selection	Risiko Operasional	≥ 11
		Risiko Pembiyaan	
		Risiko Kepatuhan	
12	Regulatory Compliance	Risiko Kepatuhan	≥ 9
		Risiko Strategis	
13	Geopolitical	Risiko Operasional	≥ 12
		Risiko Pendapatan	
14	Infrastructure Theft or Destruction	Risiko Fraud	≥ 9
		Risiko Opersional	
		Risiko Pendapatan	
		Risiko Kepatuhan	
15	Malware	Risiko Operasional	≥ 10
16	Logical Attacks	Risiko Operasional	≥ 10
17	Industrial Action	Risko Operasional	≥ 12
		Risiko Pendapatam	
18	Environmental	Risiko Operasi	≥ 10
19	Acts of Nature	Risiko Operasional	≥ 12
		Risiko Pendapatan	
20	Inovation	Risiko Strategis	≥ 9

3.2 Tahapan Penliaian Risiko

3.2.1 Identifikasi Risiko

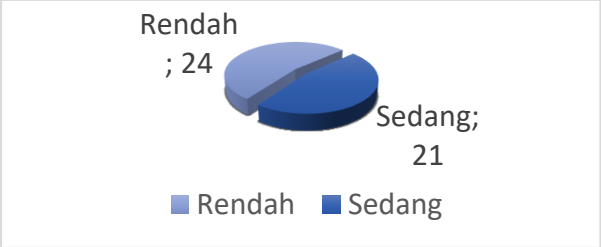
Proses pada penelitian ini pertama kali dilakukannya dengan Identifikasi Risiko, identifikasi risiko dilakukan untuk mengetahui penyebab dan dampak risiko yang mungkin akan terjadi. Identifikasi dilakukan sesuai dengan proses yang berkaitan dengan SIMRS Rekam Medis yang dapat dilihat pada tabel. Risiko yang teridentifikasi dari 11 proses pada SIMRS Rekam Medis dan 6 kategori risiko dari Cobbit 5 for risk dan 10 jenis risiko.

Tabel 5 Identifikasi Risiko

Kategori Risiko	Proses	Risiko
Infrastructure	Mengakses web server SIMRS pada modul rekam medis	Adanya kegagalan teknis / utility secara berkala
	Login user pengguna aplikasi SIMRS	
	Input pendaftaran Pasien	
	Menentukan Jenis Perawatan Pada Pasien: Rawat Inap dan Rawat Jalan	
	Penyimpanan data pasien sesuai dengan jenis riwayat proses rekam medis terhadap pasien	
	Input jenis Tindakan pelayanan kepada pasien	
	Cetak barcode sesuai dengan identitas No. RM Pasien	
	Mengirim data tagihan kepada pasien	Sistem tidak dapat menghandle banyaknya transaski saat volume user meningkat
Staff Operation/ Human Error	Mengakses web server SIMRS pada modul rekam medis	Adanya kesalahan input Informasi oleh staff TI atau pengguna sistem TI
	Login user pengguna aplikasi SIMRS	
	Input pendaftaran Pasien	
	Pemeriksaan Identitas Pasien	
	Menentukan Jenis Perawatan	

	Pada Pasien: Rawat Inap dan Rawat Jalan	
	Mengirim tagihan pasien ke kasir	
	Input data pasien untuk admisi terhadap jenis rawat inap	
	Cetak barcode sesuai dengan identitas No. RM Pasien	
	Penyimpanan data pasien sesuai dengan jenis riwayat proses rekam medis terhadap pasien	
Acts of Nature	Mengakses web server SIMRS pada modul rekam medis	Kerusakan akibat bencana alam seperti kebakaran, gempa bumi, tsunami
Information	Input pendaftaran Pasien	Data sensitif hilang / tereskpose, disebabkan serangan logis (logical attack)
	Pemeriksaan Identitas Pasien	
	Cetak barcode sesuai dengan identitas No. RM Pasien	Database corrupt, menyebabkan data tidak dapat diakses
Logical Attacks	Login user pengguna aplikasi SIMRS	Adanya kerusakan pada website (deface)
	Input pendaftaran Pasien	

Selanjutnya Ketika identifikasi risiko sudah ditetapkan dilakukannya analisis risiko terhadap penelitian dengan mengukur seberapa besar dampak yang mungin terjadi, hasil analisis dapat dijelaskan pada gambar



Evaluasi risiko diberikan kepada risiko yang sudah diberikan analisis, fungsi evaluasi risiko adalah untuk menentukan risiko mana saja yang harus diberi penanganan. Berikut akan dijelaskan pada gambar ini

4. Rekomendasi dan Kontrol

4.1 Penetapan Kontrol

Kontrol yang diberikan untuk risiko yang diberi penanganan sudah sesuai dengan aturan pada selera risiko. Penetapan kontrol ini menggunakan NIST 800-53 dan DoD 8500.2, kontrol yang diberikan dapat dilihat pada tabel 6 ini

Tabel 6 Penetapan Kontrol

No.	Proses	Risiko	Judul Kontrol	Standar
1	Pemeriksaan Identitas Pasien	Database corrupt, menyebabkan data tidak dapat diakses	CODB-3 Data backup Procedures	Department of Defense Instruction 8500.3
	Cetak Barcode Sesuai dengan No RM Pasien			

2.	Login user penggguna aplikasi SIMRS	Adanya kerusakan pada website (deface)	DCSS-2 System State Changes	
	Input pendaftaran Pasien			
3.	Mengakses web server SIMRS	Adanya kesalahan input Informasi oleh staff TI atau pengguna sistem TI	SI-10 Information input validation	NIST 800-53
	Login User Pengguna Aplikasi			
	Pemeriksaan Identitas Pasien			
	Input Jenis Tindakan Pelayanan Pasien			
	Cetak barcode sesuai dengan identitas No. RM Pasien			
	Penyimpanan Data Pasien Sesuai Dengan Riwayat Rekam Medis Pasien			
4	Input pendaftaran Pasien	Adanya kegagalan teknis / utility secara berkala	MA-1 System Maintenance Policy and Procedure	

4.2 Pernacangan Rekomendasi

Berdasarkan kontrol yang ditetapkan terhadap risiko yang diberi penanganan penulis membuat rancangan rekomendasi untuk risiko risiko yang belum mempunyai kontrol dan risiko yang harus diberi peningkatan, dijelaskan pada tabel 7

Tabel 7 Perancangan Rekomendasi

Judul Kontrol	Rekomendasi		
	People	*Process*	*Technology*
CODB-3 Data backup Procedures	Peningkatan Ketrampilan	-	-
DCSS-2 System State Changes	-	Revisi SPO Mengenai Pengelolaan Website (aspek proses)	-
SI-10 Information input validation	Peningkatan Keterampilan	-	-
MA-1 System Maintenance Policy and Procedure	-	SPO Tentang Kegagalan Infrastruktur yang akan menggunggu sistem layanan SIMRS (aspek proses)	-

4.2.1 Rekomendasi Aspek *People*

Rekomendasi Aspek *People* yang ditulis penulis ditabel ini sesuai dengan peranacangan rekomendasi yang penulis berikan, berikut tabel 8 perancangan rekomendasi aspek *people*.

Tabel 8 Rekomendasi Aspek People

No.	Kontrol	Judul Pelatihan	Deskripsi
1			Melatih kemampuan staff

	CODB-3 Data backup Procedures	Pelatihan Proses Backup Data Pada SIMRS	IT dalam bidang Backup Data pada SIMRS dengan melakukannya pelatihan tentang backup data.
2	SI-10 Information input validation	Pelatihan Pengunaan SIMRS	Melatih kemampuan user pengguna SIMRS agar dapat melakukan input data dengan benar.

4.2.2 Rekomendasi Aspek *Process*

Rekomendasi pada aspek *process* berupa revisi SPO yang sudah pernah ada dan membuat SPO baru sebagai rekomendasi. Berikut dijelaskan pada tabel 9

Tabel 9. Rekomendasi Aspek Process

No.	Kontrol	Rekomendasi	Deskripsi
1	DCSS-2 System State Changes	Revisi SPO Mengenai Pengelolaan Website	Menambah isi dari SPO Pengelolaan Website
2	MA-1 System Maintenance Policy and Procedure	SPO Tentang Kegagalan Infrastruktur yang akan mengganggu sistem layanan SIMRS	Membuat SPO untuk mengatasi kegagalan sistem layanan SIMRS

5. Penutup

5.1 Kesimpulan

Berdasarkan hasil penelitian analisis risiko yang dilakukan pada tugas akhir ini, dapat disimpulkan bahwa:

1. Pada tahapan awal dalam menganalisis risiko menggunakan ISO 31000 sebagai penetapan lingkup objek penelitian pada RSKIA, dilanjutkan dengan ditentukannya konteks internal dan eskternal, lalu ditetapkannya penetapan kriteria risiko yang berdasarkan Perwal nomor 1328 tahun 2018. Tahap selanjutnya pada penelitian ini adalah identifikasi risiko yang mungkin terjadi pada SIMRS Rekam Medis, Risiko yang teridentifikasi kemudian dilanjutkan dengan tahap analisis risiko yang berpacu dengan level kemungkinan dan level dampak. Setelah itu risiko diberikan evaluasi untuk menentukan risiko yang akan diberikan penanganan dan kontrol.

Pemberian evaluasi dan pengelolaannya dilakukan sesuai dengan risiko yang melewati atau setara dengan selera risiko yang sudah didefinisikan sebelumnya. Terdapat dua jenis penanganan pada risiko yang terjadi yaitu mitigasi dan transfer. Risiko yang diberi penanganan mitigasi adalah:

- Database corrupt, menyebabkan data tidak dapat diakses
- Adanya kerusakan pada website (deface)
- Adanya kesalahan input Informasi oleh staff TI atau pengguna sistem TI

Risiko diatas diberikan mitigasi sebagai penanganannya karena memiliki level dampak yang besar sehingga perlu diberikan kontrol agar mengurangi dampak yang akan terjadi. Selain penanganan mitigasi ada penanganan transfer , penanganan ini diberikan karena pihak RSKIA tidak dapat mengntrol risikonya dan membutuhkan pihak yang ahli untuk melakukan penanganan, risiko dengan penanganan tersebut adalah risiko adanya kegagalan teknis / utility secara berkala, seperti telcom.

Risiko yang sudah di evaluasi dan diberikan kontrok yang berdasarkan standar NIST 800-53 dan DoD 8500.2. Kontrol dari NIST 800-53 yang digunakan adalah CODB-3 Data backup Procedures, DCSS-2 System State Changes, SI-10 Information input validation, MA-1 System Maintenance Policy and Procedure.

5.2 Saran

Saran bagi RSKIA terhadap penelitian ini adalah :

1. Dalam melakukan proses terhadap setiap kegiatan pelayanan medis perlu dilakukan pengolahan risiko untuk mengetahui potensi yang mungkin akan terjadi pada setiap proses kegiatan pelayan medis di SIMRS.

Serta melakukan pengumpulan data mengenai risiko yang sudah pernah terjadi di Rekam Medis SIMRS.

2. Perlu dilakukannya pengolahaan risiko terhadap proses kegiatan pelayanan medis, dan perencanaan mengenai *risk assessment* secara keseluruhan pada Rekam Medis.

Saran untuk penelitian berikutnya:

1.Untuk penelitian selanjutnya diharapkan menggunakan atau menambahan metode dengan ISO yang berbeda agar penelitian selanjutnya lebih luas cakupannya terhadap manajemen risiko.

Daftar Pustaka

[1] L. J. Susilo dan D. Novita, Governance, risk management and compliance : executive's guide to risk governance and risk oversight, Jakarta: Grasindo, 2018.

[2] Wali Kota Bandung Provinsi Jawa Barat, PERATURAN WALI KOTA BANDUNG NOMOR 1328 TAHUN 2018 TENTANG PENINGKATAN EFEKTIVITAS MANAJEMEN RISIKO SEKTOR PEMERINTAHAN TERSTANDARISASI, Bandung: Sekretaris Daerah Kota Bandung, 2018.

[3] ISACA, COBIT 5 for Risk, ISACA, 2013, pp. 67-74.

[4] U.S. Department of Commerce, National Institute of Standards and Technology Special Publication 800-52 Revision 4, 2013.

[5] US Department of Defense Instruction Number 8500.2, Information Assurance (IA) Implementation, 2003.

[6] I. ISO 31000, ISO 31000:2018 Risk management — Guidelines, Switzerland: ISO Organization, 2018.

[7] Santosa, I., & R., Y. (2019). Analisis Risiko dan Kontrol Perlindungan Data Pribadi pada Sistem Informasi Administrasi Kependudukan. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*.