ANALISIS RISIKO DAN KONTROL PADA SIMRS GUDANG OBAT BERDASARKAN ISO 31000

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

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

Abstract- The Mother and Child Hospital (RSKIA) in Bandung is a hospital under the auspices of the government. Since the issuance of government regulations that require every hospital to use the Hospital Management Information System (SIMRS), RSKIA has implemented SIMRS since 2014. The risk analysis assessment is intended so that various risks in hospital information technology can be minimized and overcome. So that the city of Bandung RSKIA can continue to develop human resource management and improve the quality of service to patients, risk analysis is carried out using ISO 31000: 2018 which results in 5 risks above risk appetite. The risk is then given control using the NIST 800-53 standard and DoD 8500.2 which are then given recommendations from the personnel, process and technology aspects..

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

Abstrak- Rumah Sakit Khusus Ibu dan Anak (RSKIA) kota Bandung merupakan rumah sakit di bawah naungan pemerintah. Sejak dikeluarkannya peraturan pemerintah yang mengharuskan setiap rumah sakit menggunakan Sistem Informasi Manajemen Rumah Sakit (SIMRS), RSKIA sudah mengimplementasikan SIMRS sejak tahun 2014. Penilaian analisis risiko dimaksudkan agar berbagai risiko pada teknologi informasi rumah sakit dapat diminimalisir dan teratasi. Agar RSKIA kota Bandung dapat terus melakukan pengembangan terhadap manajemen sumber daya manusia dan melakukan peningkatan kualitas pelayanan kepada pasien maka dilakukannya analisis manajemen risiko menggunakan ISO 31000:2018 yang menghasilkan 5 risiko di atas selera risiko. Risiko tersebut kemudian diberikan kontrol menggunakan standar NIST 800-53 dan DoD 8500.2 yang selanjutnya diberikan rekomendasi dari aspek personil, proses, dan teknologi.

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

1. Pendahuluan

1.1. Latar Belakang

Teknologi informasi saat ini sudah banyak diterapkan di hampir seluruh sektor di Indonesia, seperti perbankan, industri, dan juga kesehatan. Salah satu contoh penggunaan teknologi informasi pada dunia kesehatan adalah Sistem Informasi Manajemen Rumah Sakit (SIMRS). Penggunaan sistem berbasis elektronik sangat membantu dalam menjalan proses bisnis yang lebih efisien dan terintegrasi. Namun, tidak dapat menutup kemungkinan selama penggunaan dan implementasi sistem tersebut adanya beberapa risiko yang dapat mengganggu proses bisnis yang terjadi di suatu instansi. Terdapat regulasi terkait yakni peraturan Menteri Kesehatan Republik Indonesia nomor 82 tahun 20013 tentang Sistem Informasi Manajemen Rumah Sakit yang mewajibkan setiap rumah sakit menyelenggarakan, melaksanakan pengelolaan dan pengembangan SIMRS.

Rumah Sakit Khusus Ibu dan Anak (RSKIA) kota Bandung, merupakan sebuah instansi pemerintahan yang bergerak dibidang kesehatan. RSKIA menggunakan sistem informasi terintegrasi dalam melaksanakan proses bisnisnya. RSKIA sudah mengimplementasikan SIMRS sejak tahun 2014 dengan menerapkannya secara bertahap hingga saat ini. Unit IT RSKIA sudah menerapkan manajemen risiko terhadap risiko yang pernah terjadi pada SIMRS. Walaupun RSKIA sudah pernah melakukan manajemen risiko, tetap tidak menutup kemungkinan bahwa akan adanya risiko lain terlebih lagi risiko yang diidentifikasi hanya risiko yang pernah terjadi saja.

Salah satu cara pencegahan agar risiko tidak menjadi suatu hal yang dapat menghambat instansi atau organisasi dalam mencapai tujuannya adalah dengan mengidentifikasi risiko dan menganalisis risiko – risiko tersebut. Guna dilakukannya identifikasi dan analisis risiko agar jika risiko tersebut timbul dikemudian hari maka instansi tersebut sudah siap dan dapat memitigasi risiko tersebut. Pengukuran terhadap risiko yang mungkin terjadi dimaksudkan agar RSKIA dapat mengatasi dan meminimalisir dampak yang ditimbulkan terhadap SIMRS. Hasil pengukuran dapat diketahui seberapa besar dampak dari risiko dan kerentanan dari tiap proses yang dinilai serius, untuk diterpakan kontrol yang tepat terhadap prioritas yang paling besar.

Gudang obat merupakan salah satu modul yang penting, stok obat dan semua transaksi dari dan untuk supplier menggunakan SIMRS gudang obat. Jika tidak ada modul ini maka pendataan obat dilakukan secara manual yang berdampak dengan tidak akuratnya data obat dan dapat menghambat pelayanan rumah sakit.

Penelitian tentang SIMRS sudah pernah dilakukan beberapa kali tetapi tidak ada yang berfokus pada manajemen risiko SIMRS gudang obat. Penelitian ini menggunakan ISO 31000:2018 sebagai pedoman dalam melaksanakan analisis manajemen risiko, dan acuan pengidentifikasian risiko menggunakan Generic Risk Scenarios Cobit 5. Pengelolaan risiko berbasis ISO 31000:2018 sangat penting karena sejalan dengan Susilo (2018:22), "proses pengelolaan risiko yang berulang akan membantu organisasi untuk menetapkan strategi, mencapai sasaran, dan mengambil keputusan dengan pertimbangan yang matang" **[1]**.

Banyak standar lain yang dapat menjadi acuan dalam penerapan manajemen risiko. Standar ISO 31000 telah diadopsi oleh Indonesia sebagai Standar Nasional Indonesia atau SNI ISO 31000. Pada survei nasional yang dilakukan pada tahun 2018, ISO 31000 adalah standar yang digunakan paling luas di perusahaan dengan persentase sebesar 67,5% diikuti standar COSO ERM dengan persentase 15% **[2]**.

Hasil lain dari survei juga menyatakan bahwa "Sebanyak 57,4% dari industri keuangan dan asuransi, 68,4% industri aktivitas jasa lainnya dan 78,8% dari industri pengolahan menggunakan ISO 31000 sebagai standar manajemen risiko." Maka dari ini penggunaan standar ISO 31000 dirasa merupakan standar terbaik untuk melakukan penilaian risiko **[2]**.

2. Metode Penelitian

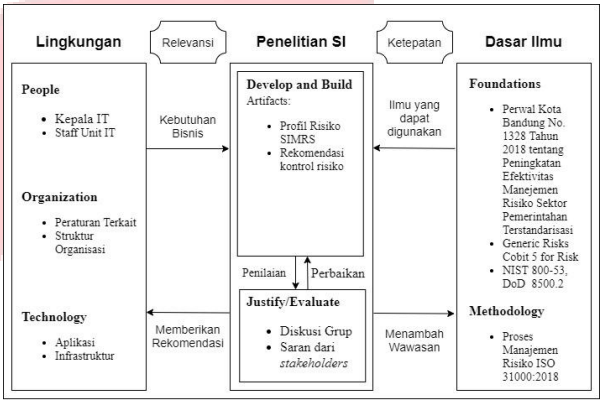
Model konseptual merupakan kerangka berpikir yang utuh dalam rangka penyederhanaan masalah dengan metode dan sistematika yang terstruktur. Metode ini mengacu pada ISO 31000:2018 sebagai acuan standar dalam melakukan analisis manajemen risiko. Diharapkan dengan adanya model konseptual ini dapat memberikan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

Berikut penjelasan dari model konseptual tersebut.

1. Penelitian dilakukan di RSKIA kota Bandung yang sudah mengimplementasikan SIMRS sejak 2014 yang sudah pernah melakukan identifikasi risiko yang pernah terjadi saja tetapi tidak melakukan penilaian risiko dan kontrol risiko terhadap risiko yang mungkin akan terjadi pada masa mendatang.

2. Dasar hukum yang digunakan untuk mendukung penelitian ini adalah Peraturan Wali Kota (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 Generic Risk Scenario Cobit 5 for risk sebagai model. Sedangkan kontrol yang digunakan adalah NIST 800-53 atau DoD 8500.2.

3. Hasil dari penelitian ini adalah artefak berupa profil risiko SIMRS gudang obat dan rekomendasi kontrol yang sesuai berdasarkan NIST 800-53 dan DoD 8500.2.



Gambar 1 Model Konseptual

Terdapat dua jenis data yang digunakan yaitu data primer dan sekunder. Data primer merupakan data yang dikumpulkan atau didapatkan secara langsung dari objek penelitian dengan menggunakan metode wawancara kepada pihak terkait. Pengambilan data ini bertujuan sebagai bahan melakukan proses penilaian risiko. Pengambilan data primer dilakukan dengan metode wawancara. Data sekunder adalah data yang diperoleh melalui sumber yang sudah disediakan oleh liteatur, media, maupun dari objek penelitian. Data sekunder yang dibutuhkan adalah ISO 31000:2018, Profil, Visi dan Misi dan Struktur Organisasi RSKIA, NIST 800-53 dan DoD 8500.2. Selanjutnya data yang sudah dikumpulkan diolah menggunakan standar ISO 31000:2018. Proses awal yang dilakukan adalah mengidentifikasi risiko, lalu menganalisis risiko yang sudah teridentifikasi penyebab dan dampak apa yang akan terjadi, setelah itu mengevaluasi risiko tersebut. Selanjutnya akan dilakukan penanganan risiko, pada proses ini risiko diberikan penanganan yang sesuai. Setelah risiko diberikan penanganan pada tahap sebelumnya, risiko diberikan rekomendasi kontrol berdasarkan standar NIST 800-53 atau DoD 8500.2. Kontrol dipilih dan diberikan pada risiko yang tepat.

3. Pembahasan

3.1 Tahap Pendefinisian Ruang Lingkup, Konteks dan Kriteria

3.1.1 Pendefinisian Ruang Lingkup

3.1.1.1 Profil RSKIA

RSKIA adalah rumah sakit Pemerintah Kota Bandung berdasarkan Peraturan Daerah Kota Bandung No. 14 Tahun 2009 tentang Pembentukan dan Susunan

Organisasi RSKIA Kota Bandung. Sebelum menjadi RSKIA kota Bandung, rumah sakit ini merupakan Rumah Sakit Bersalin Astanaanyar Kota Bandung berada di bawah 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.

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 organisasi yang menjadi objek penelitian dapat dipahami. Tabel mengenai konteks risiko dapat dilihat pada tabel 1.

3.1.3 Penetapan Kriteria Risiko
Kriteria risiko adalah skala seberapa besar kemungkinan dan dampak yang menjadi rujukan untuk menilai besaran risiko dan prioritas risiko. Acuan kriteria risiko yang digunakan adalah Peraturan Wali Kota Bandung Nomor 1328 Tahun 2018[8]. Terdapat kriteria kemungkinan risiko pada tabel 2, kriteria dampak pada tabel 3, dan matriks risiko pada tabel 4. Kriteria kemungkinan adalah ukuran seberapa mungkin risiko tersebut akan terjadi. Kriteria dampak adalah ukuran seberapa besar dampak risiko tersebut akan mempengaruhi organisasi.

Tabel 1 Konteks Internal dan Eksternal

Konteks	Komponen	Dokumen
Internal	Visi, misi, strategi, sasaran, dan kebijakan	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
	Struktur organisasi, peran dan tanggung jawab	
	Kemampuan (sumber daya & pengetahuan), hubungan dengan	SK Direktur RSKIA Kota Bandung Nomor 445/46.5/SK/RSKIA/III/2018 Tentang Pembentukan Tim Sistem Informasi Manajemen Rumah
	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 2 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 3 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%
	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 dipresentasikan pada matriks berikut ini.

Level Risiko ditentukan berdasarkan atas dua hal yaitu level kemungkinan terjadinya risiko dan level dampak risiko. Keduanya harus dikombinasikan dan diperhitungkan secara bersamaan dalam penentuan level risiko. Level kemungkinan terjadinya risiko, level dampak dan level risiko masing-masing menggunakan lima skala tingkatan (level) seperti pada gambar 3 [3].

Matriks Analisis Risiko 5x5			Level 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 2 Matriks 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

Gambar 3 Level Risiko

Selera risiko adalah sebagai acuan apakah risiko tersebut perlu ditangani atau tidak. Tabel penetapan selera risiko yang akan digunakan terdapat pada tabel 4.

Tabel 4 Selera Risiko

Kategori Risiko TI	Kategori Risiko (Pada Perwal 1328 th.2018)	Besaran Risiko yang Harus Ditangani
Pembangunan dan pemeliharaan portofolio	Risiko Reputasi	≥ 7
	Risiko Strategis	
Programme and Project Lifecycle	Risiko Pembiayaan	≥ 11
	Risiko Belanja	
	Risiko Strategis	
	Risiko Operasional	
IT Investment Decision Making	Risiko Pendapatan	≥ 9
	Risiko Belanja	
	Risiko Strategis	
IT Expertise and Skill	Risiko Operasional	≥ 15
Staff Operation / Human Error	Risiko Fraud	≥ 6
	Risiko Kepatuhan	
Information	Risiko Kepatuhan	≥ 9
	Risiko Fraud	
	Risiko Operasional	
Arsitektur	Risiko Strategis	≥ 14
	Risiko Pendapatan	
Infrastructure	Risiko Operasional	≥ 7
	Risiko Strategis	
Software	Risiko Strategis	≥ 11
	Risiko Operasional	
	Risiko Pendapatan	
Business Ownership of IT	Risiko Strategis	≥ 11
	Risiko Operasional	
	Risiko Belanja	
Supplier Selection	Risiko Operasi	≥ 11
	Risiko Pembiayaan	
	Risiko Kepatuhan	
Regulatory Compliance	Risiko Strategis	≥ 9
	Risiko Kepatuhan	
Geopolitical	Risiko Operasional	≥ 12
	Risiko Pendapatan	
Infrastructure Theft or Destruction	Risiko Fraud	≥ 9
	Risiko Operasional	
	Risiko Pendapatan	

Kategori Risiko TI	Kategori Risiko (Pada Perwal 1328 th.2018)	Besaran Risiko yang Harus Ditangani
	Risiko Kepatuhan	
Malware	Risiko Operasional	≥ 15
Logical Attacks	Risiko Operasional	≥ 15
Industrial Action	Risiko Pendapatan	≥ 12
	Risiko Operasional	
Environmental	Risiko Operasional	≥ 15
Acts of Nature	Risiko Pendapatan	≥ 12
	Risiko Operasional	
Inovation	Risiko Strategis	≥ 9

3.2 Tahap Penilaian Risiko

3.2.1 Identifikasi Risiko

Proses yang dilakukan pertama kali saat akan melakukan penilaian risiko adalah mengidentifikasi risiko yang ada dan akan terjadi pada organisasi. Identifikasi risiko dilakukan untuk mengetahui penyebab dan dampak apa yang akan terjadi jika risiko tersebut terjadi di organisasi. Identifikasi dilakukan berdasarkan proses dari SIMRS gudang obat yang dapat dilihat pada tabel

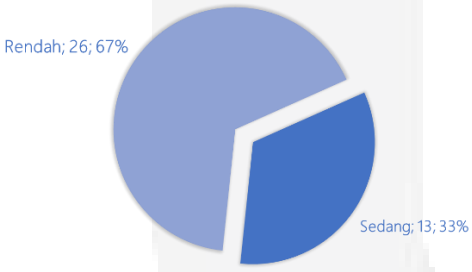
Risiko yang teridentifikasi dari 8 proses pada SIMRS Gudang Obat terdiri dari 5 kategori risiko dengan 11 jenis risiko.

Tabel 5 Identifikasi Risiko

Kategori Risiko	Proses	Risiko
Logical Attcaks	Login Gudang Obat	Pengguna yang tidak berwenang mencoba untuk masuk ke sistem
Staff Operation / Human Error	Login Gudang Obat	Adanya kesalahan input data oleh staf TI atau pengguna sistem TI
	Input Obat Masuk	
	Input Obat Keluar	
	Return Obat/ BHMP dari Warehouse	
	Input BHP Ruangan	
Information	Input Obat Masuk	Database corrupt, menyebabkan data tidak dapat diakses
		Database corrupt, menyebabkan data tidak dapat diakses
	Input Obat Keluar	Data yang berhubungan dengan penggunaan obat dimodifikasi dengan sengaja
	Return Obat/ BHMP dari Warehouse	Database corrupt, menyebabkan data tidak dapat diakses
	Rekap Transaksi	Database corrupt, menyebabkan data tidak dapat diakses
		Data yang berhubungan dengan informasi obat dimodifikasi dengan sengaja
		Data sensitif hilang / tereskpose, disebabkan serangan logis (logical attack)
	Cetak Dokumen	Database corrupt, menyebabkan data tidak dapat diakses
	Data Stok Obat	Database corrupt, menyebabkan data tidak dapat diakses
	Input BHP Ruangan	Database corrupt, menyebabkan data tidak dapat diakses
Infrastructure	Input Obat Masuk	Adanya kegagalan teknis / utility secara berkala seperti listrik dan telekom
	Input Obat Keluar	
	Return Obat/ BHMP dari Warehouse	

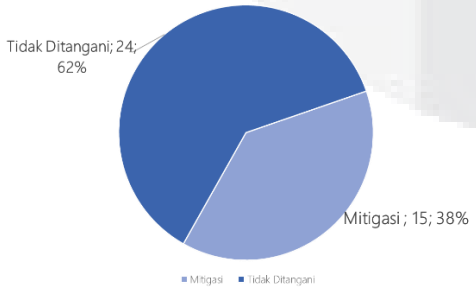
Kategori Risiko	Proses	Risiko
	Rekap Transaksi	
	Cetak Dokumen	
	Data Stok Obat	
	Input BHP Ruangan	
Software	Input Obat Masuk	1. Adanya glitch (error dalam program) saat software sudah di operational-kan 2. User tidak dapat menggunakan dan mengeksploitasi software baru
	Input Obat Keluar	
	Return Obat/ BHMP dari Warehouse	
	Rekap Transaksi	
	Cetak Dokumen	
	Data Stok Obat	
	Input BHP Ruangan	

Tahapan selanjutnya setelah risiko teridentifikasi adalah melakukan analisis risiko, berapa besar kemungkinan risiko itu akan terjadi dan seberapa besar dampak yang akan disebabkan oleh risiko tersebut. Hasil dari analisis tersebut terdapat pada gambar



Gambar 4 Analisis Risiko

Evaluasi Risiko adalah proses menentukan apakah risiko tersebut diberikan penanganan atau tidak. Risiko yang diberikan penanganan adalah risiko mana saja yang mempunyai besaran risiko sama atau lebih besar dari selera risiko.



Gambar 5 Evaluasi Risiko

4. Rekomendasi dan Kontrol

4.1. Penetapan Kontrol

Kontrol diberikan pada risiko yang melewati atau sama dengan batas selera risiko. NIST 800-53 atau DoD 8500.2 adalah kontrol yang digunakan pada penelitian ini. Kontrol yang diberikan dapat dilihat pada tabel 6.

Tabel 6 Penetapan Kontrol

Proses	Risiko	Judul Kontrol	Standar
Login Gudang Obat	Pengguna yang tidak berwenang mencoba untuk masuk ke sistem	SI-4 *Information System Monitoring*	NIST 800-53
Input Obat Masuk	Adanya kesalahan input Informasi oleh staff TI atau pengguna sistem TI	SI-10 *Information input validation*	NIST 800-53
Input Obat Keluar			
Input BPH Ruangan			
Return Obat/ BHMP dari Warehouse			
Rekap Transaksi	Data sensitif hilang / tereskpose, disebabkan serangan logis (logical attack)	RA-5 *Vulnerability Scanning*	NIST 800-53
Data Stok Obat			
Rekap Transaksi	Database corrupt, menyebabkan data tidak dapat diakses	CODB-3 *Data backup Procedures*	DoD 8500.2
Data Stok Obat			
Input Obat Masuk	Adanya kegagalan teknis / utility secara berkala (listrik,telecomn)	MA-1 *System Maintenance Policy and Procedures*	NIST 800-53
Input Obat Keluar			
Return Obat/ BHMP dari Warehouse			
Rekap Transaksi			
Cetak Dokumen			
Data Stok Obat			

4.2 Perancangan Rekomendasi

Berdasarkan kontrol yang sudah diberikan di atas maka penulis memberikan rekomendasi untuk risiko – risiko yang belum mempunyai kontrol dan risiko yang perlu diberikan peningkatan kontrol pada tabel 7.

Tabel 7 Perancangan Rekomendasi

Kontrol	Aspek	Rekomendasi
SI-4 Information System Monitoring	Process	Menyusun SPO User SIMRS
SI-10 Information input validation	Process	Menyusun SPO Input Data
RA-5 Vulnerability Scanning	People	Peningkatkan Kompetensi SDM
	Process	Menyusun SPO Vulnerability Scanning
	Technology	Implementasi Tools Vulnerability Scanning,
CODB-3 Data backup Procedures	Process	1. Revisi SPO Backup Data SIMRS 2. Revisi SPO Cara Backup Data
MA-1 System Maintenance Policy and Procedures	Process	Menyusun SPO Listrik Padam

4.2.1 Rekomendasi Aspek People

Pada perancangan rekomendasi aspek people, penulis memberikan rekomendasi peningkatan kompetensi dan penambahan deskripsi kerja. Berikut adalah tabel perancangan rekomendasi aspek people.

Tabel 8 Rekomendasi Aspek People

Kontrol	Judul Pelaihan	Deskripsi
RA-5 *Vulnerability Scanning*	Pelatihan *skill tools vulnerability scanning*	Meningkatkan kompetensi staf IT dengan melakukan pelatihan *tools vulnerability scanning*

4.2.2 Rekomendasi Aspek Process

Rekomendasi pada aspek process ini penulis mengajukan penyusunan SPO baru dan revisi SPO. Rekomendasi dapat dilihat pada tabel 9.

Tabel 9 Rekomendasi Aspek Process

Kontrol	Rekomendasi	Deskripsi
SI-4 *Information System Monitoring*	SPO *User* SIMRS	Membuat SPO yang mengatur user pada SIMRS
SI-10 *Information input validation*	SPO Input Data	Membuat SPO yang mengatur tentang penginputan data
RA-5 *Vulnerability Scanning*	SPO *Vulnerability Scanning*	Membuat SPO untuk memonitor kerentanan
CODB-3 *Data backup Procedures*	. Revisi SPO *Backup* Data SIMRS	Menambah isi dari SPO *Backup* Data SIMRS
	Revisi SPO Cara *Backup* Data	Menambah isi dari SPO Cara *Backup* Data
MA-1 *System Maintenance Policy and Procedures*	SPO Listrik Padam	Menyusun SPO yang berisi prosedur saat listrik padam

4.2.2 Rekomendasi Aspek Technology

Rekomendasi pada aspek teknologi ini penulis mengajukan implementasi tools vulnerability scanning pada tabel 10. Adapula rekomendasi tools pada tabel 11.

Tabel 10 Rekomendasi Aspek Technology

Kontrol	Rekomendasi	Deskripsi
RA-5 Vulnerability Scanning	Implementasi Tools *Vulnerability Scanning*,	Alat yang berfungsi sebagai pendeteksi celah kemamanan.

Tabel 11 Rekomendasi Tools

Rekomendasi Tools	Fitur
SolarWinds Network Configuration Manager	1. Otomatisasi jaringan 2. Kepatuhan jaringan 3. Cadangan konfigurasi 4. Wawasan Jaringan untuk Cisco ASA dan Cisco Nexus 5. Integrasi dengan Network Performance Monitor
Netsparker	1. Otomatis memindai semua jenis aplikasi web HTML5, Web 2.0 dan Aplikasi Halaman Tunggal (SPA) 2. Kerentanan secara otomatis diberikan tingkat keparahan 3. Menggunakan teknologi ScanningTM Berbasis Bukti

Rekomendasi Tools	Fitur
Acunetix	1. Teknologi Acusensor 2. Industri yang paling canggih dan mendalam dalam SQL injection dan pengujian Cross site scripting. 3. Mendukung HTML5 penuh dengan Acunetix DeepScan Teknologi 4. Dapat mendeteksi kerentanan Blind XSS dengan layanan AcuMonitor 5. Dapat mendeteksi otomatis kerentanan XSS berbasis DOM

5. Penutup

5.1. Kesimpulan

Berdasarkan penelitian yang sudah dilakukan, berikut merupakan kesimpulan yang dapat diambil:

1. Tahap pertama dalam menganalisis risiko menggunakan standar ISO 31000 adalah penetapan lingkup objek penelitian yaitu RSKIA, dilanjutkan dengan konteks internal dan eksternal lalu penetapan kriteria risiko berdasarkan Perwal nomor 1328 tahun 2018. Tahap selanjutnya adalah mengidentifikasi risiko apa saja yang mungkin terjadi pada SIMRS gudang obat. Risiko yang teridentifikasi sebanyak 12 risiko yang lalu dianalisis level kemungkinan dan dampak. Setelah itu risiko dievaluasi untuk menentukan risiko apa saja yang diberikan penanganan dan kontrol.
2. Pengelolaan dan pemberian evaluasi dilakukan berdasarkan risiko yang melewati atau setara dengan selera risiko yang sudah didefinisikan sebelumnya. Terdapat dua jenis penanganan yang diberikan yaitu mitigasi dan transfer. Risiko yang diberikan penanganan mitigasi adalah:
   - Pengguna yang tidak berwenang mencoba untuk masuk ke system,
   - Adanya kesalahan input Informasi oleh staff TI atau pengguna sistem TI
   - Database corrupt, menyebabkan data tidak dapat diakses
   - Data sensitif hilang / tereskpose, disebabkan serangan logis (logical attack)

   Risiko diatas diberikan penanganan mitigasi karena mempunyai level dampak yang besar sehingga harus diberikan kontrol untuk mengurangi dampak yang akan terjadi.Selain mitigasi, penanganan lain yang diberikan adalah transfer. Penanganan ini diberikan karena pihak RSKIA tidak bisa mengontrol risiko sehingga diberikan pada pihak yang lebih ahli. Risiko dengan penanganan transfer adalah kegagalan teknis / utility secara berkala seperti telecomm.
3. Risiko yang sudah dievaluasi selanjutnya diberikan kontrol berdasarkan standar NIST 800-53 dan DoD 8500.2. Kontrol dari NIST 800-53 yang digunakan adalah SI-4 Information System Monitoring, SI-10 Information input validation, RA-5 Vulnerability Scanning, dan CP-8 Telecommunications Services. Sedangkan kontrol yang dipilih dari DoD 8500.2 adalah CODB-3 Data backup Procedures. Tiap kontrol diberikan rekomendasi berdasarkan aspek people, process, dan technology.

6.2. Saran

Saran bagi RSKIA kota Bandung terkait penelitian ini adalah:

1. Meningkatkan kesadaran terkait risiko yang mungkin akan terjadi pada semua modul yang terdapat di SIMRS
2. Melakukan implementasi rekomendasi yang telah diberikan agar risiko terkait dapat ditangai sehingga level kemungkinan dan dampak yang terjadi akan berkurang

Saran yang diberikan untuk penelitian ini guna mengembangkan penelitian selanjutnya adalah:

1. Melakukan implementasi proses yang terdapat pada ISO S31000 secara menyeluruh

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] CRMS Indonesia, “Survei Nasional Manajemen Risiko,” PT. Cipta Raya Mekar Sahitya, Jakarta, 2018.

[3] 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.

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

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

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

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