ANALISA MANAJEMEN RISIKO SISTEM INFORMASI MANAJEMEN RUMAH SAKIT (SIMRS) PADA RUMAH SAKIT XYZ MENGGUNAKAN ISO 31000

Louis Eberhard Hutagalung
PT. Pro-Int Dinamika
e-mail: louiseberhard86@gmail.com

Abstrak

Rumah Sakit merupakan sebuah instansi kesehatan yang merupakan pusat pelayanan kesehatan di mana orang sakit dapat ditampung dan diobati dengan baik. Rumah Sakit XYZ merupakan bagian dari jaringan pelayanan kesehatan *AHSA*, dimana pada tahun 1986 telah menggunakan aplikasi CLIPPER untuk penyimpanan data. Penelitian ini bertujuan untuk melakukan manajemen risiko Sistem Informasi Manajemen Rumah Sakit (SIMRS) pada Rumah Sakit XYZ. Dengan melakukan wawancara serta membagikan Kuesioner kepada bagian Mirsa sebagai pengelola IT pada Rumah Sakit. Dalam melakukan manajemen risiko, ISO 31000 diterapkan dan disesuaikan untuk semua jenis organisasi dengan memberikan struktur dan pedoman yang berlaku generik terhadap semua operasi yang terkait dengan manajemen risiko. Hasil dari penelitian ini menunjukkan bahwa terdapat 2 *risk level* tingkatan *high*, merupakan risiko berbahaya yang harus diatasi secepatnya, dan 13 *risk level* tingkatan *medium* yang merupakan risiko yang harus diperhatikan terus-menerus, sehingga setiap risiko harus dilakukan perlakuan risiko yang diharapkan dapat menjadi acuan dalam penanganan dan pemeliharaan terhadap Sistem Informasi di waktu yang akan datang.

Kata Kunci: Manajemen Risiko, Sistem Informasi Manajemen Rumah Sakit, ISO 31000

RISK MANAGEMENT ANALYSIS OF HOSPITAL MANAGEMENT INFORMATION SYSTEM (SIMRS) IN XYZ HOSPITAL USING ISO 31000

ABSTRACT

Hospital is a health institution which is a health service center where sick people can be accommodated and treated properly. XYZ Hospital is part of the AHSA health service network, which in 1986 used the CLIPPER application for data storage. This study aims to carry out risk management of the Hospital Management Information System (SIMRS) at the XYZ Hospital. By conducting interviews and distributing questionnaires to Mirsa's department as IT manager at the hospital. In carrying out risk management, ISO 31000 is applied and adapted for all types of organizations by providing a structure and guidelines that apply generically to all operations related to risk management. The results of this study indicate that there are 2 high level risk levels, which are dangerous risks that must be dealt with as soon as possible, and 13 medium level risks which are risks that must be considered continuously, so that each risk must be treated with risk which is expected to be a reference in handling and maintenance of Information Systems in the future.

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

1. Pendahuluan

Rumah Sakit merupakan sebuah instansi kesehatan yang merupakan pusat pelayanan kesehatan di mana orang sakit dapat ditampung dan diobati dengan baik. Dengan banyaknya kegiatan yang dilakukan oleh Rumah Sakit, maka semakin banyak data dan informasi yang akan tersimpan. Informasi yang ditampung merupakan seluruh kegiatan dalam organisasi sehingga informasi tersebut diharapkan dapat dikelola dengan baik agar tidak terjadi kehilangan data. Informasi digunakan oleh Rumah Sakit

sebagai alat pertimbangan dalam melakukan tindakan dalam bentuk medis maupun tindakan untuk kepentingan organisasi.

Pada zaman ini teknologi informasi sudah menjadi tumpuan dalam menjalankan organisasi karena banyaknya keuntungan yang didapatkan melalui teknologi, dan tantangan zaman yang membuat teknologi semakin lama semakit berkembang sehingga membuat organisasi harus siap untuk mengikuti perkembangan dan mengharapkan agar organisasi tersebut mendapatkan keuntungan yang signifikan. Dalam penggunaan teknologi informasi, Sistem Informasi Manajemen (SIM) merupakan suatu Sistem yang sudah sering ditemukan pada beberapa organisasi agar dapat produktifitas organisasi dapat lebih meningkat. SIMRS (Sistem Informasi Manajemen Rumah Sakit) merupakan salah satu contoh penggunaan sistem yang digunakan dalam Rumah Sakit untuk menunjang aktivitas-aktivitas Rumah Sakit dan mengelola data informasi terkait organisasi. Dengan digunakannya SIMRS diharapkan dapat mempermudah kinerja Rumah Sakit dan mempermudah kegiatan-kegiatan Operasional. SIMRS diharapkan akan mempermudah pegawai dalam mennyelesaikan pendataan serta permasalahan pasien yang datang.

Rumah Sakit XYZ merupakan instansi yang telah menggunakan SIMRS untuk menopang kinerja organisasi tersebut, dan penggunaan SIMRS sangat berpengaruh karena telah diaplikasikan pada setiap ruangan pada Rumah Sakit tersebut. Diharapkan dengan diterapkan pada setiap ruangan dapat memaksimalkan pelayanan kepada pasien yang datang, di mana pasien yang datang akan ditangani lebih cepat dan tidak perlu menggunakan metode manual dalam pencatatan data pasien tersebut. Namun dalam penggunaan teknologi informasi terdapat risiko-risiko yang tidak disadari akan berdampak buruk dan menghambat kinerja organisasi tersebut. Risiko dapat terjadi karena kesalahan manusia ataupun kesalahan dalam sistem [1]. Risiko dapat berdampak buruk bagi organisasi karena dapat menurunkan kualitas pelayanan dalam mencapai tujuan organisasi. Risiko harus sepatutnya diatasi agar teknologi informasi dapat berjalan dengan lancar dan tidak mengurangi kemungkinan kerugian. Dengan demikian dibutuhkan suatu pengelolaan terhadap risiko yang kemungkinan akan terjadi pada organisasi tersebut agar tidak mengalami kerugian.

Manajemen risiko merupakan suatu cara untuk mengelola risiko-risiko yang ada dalam organisasi, di mana ancaman yang terdapat dalam organisasi akan dianalisa dan kemudian akan diminimalisir sebaik mungkin. Dalam penggunaan SIMRS, dibutuhkan Manajemen Risiko yang dapat mengurangi kemungkinan permasalahan, sehingga sistem yang berjalan dengan baik. Dibutuhkan pemahaman yang baik tentang teknologi informasi yang digunakan agar pengelolaan melalui manajemen risiko dapat dijalankan dengan baik. Dalam melakukan manajemen risiko dibutuhkan sebuah penilaian risiko, di mana penilaian risiko digunakan untuk meningkatkan kinerja organisasi. *Framework* ISO 31000 merupakan suatu kerangka pengerjaan bagi organisasi agar dapat melakukan manajemen risiko. Dalam penulisan ini, peneliti akan menggunakan ISO 31000 dalam menganalisa manajemen risiko teknologi informasi pada Rumah Sakit XYZ. Alasan menggunakan ISO 31000 dalam penelitian ini adalah kerangka kerja yang terstruktur, teknik penanganan risiko yang efektif dan terbukti dalam penelitian [2] di mana *framework* ISO dapat mengidentifikasikan 12 jenis risiko yang 8 diantaranya tergolong risiko level tinggi (*High*), 3 level Sedang (*Medium*), dan 1 level Rendah (*Low*) serta melakukan Pengurangan Risiko (*Risk Reduction*) sesuai dengan masing-masing level risiko. Berdasarkan latar belakang penulisan, maka penulis tertarik untuk melakukan penelitian dengan judul **"**ANALISA MANAJEMEN RISIKO SISTEM INFORMASI MANAJEMEN RUMAH SAKIT (SIMRS) PADA RUMAH SAKIT XYZ MENGGUNAKAN ISO 31000".

2. Metode Penelitian

Dalam melakukan identifikasi masalah, penulis menggunakan metode kuantitatif dengan teknik pengumpulan data sebagai berikut:

1. Studi literatur
   Melakukan kajian secara relevan dan memiliki teori yang akan menjadi acuan dalam penelitian.
2. Observasi
   Melakukan pengamatan terhadap objek yang diteliti.
3. Kuesioner
   Teknik pengumpulan data dengan cara memberikan pertanyaan kepada responden.

4. ISO 31000
   Menurut [3] ISO 31000 merupakan standart yang di publikasikan oleh ISO yang mengatur pengelolaan risiko. ISO 31000-2009 memberikan panduan, kerangka kerja, dan proses untuk mengatur risiko. Standart ini dapat digunakan oleh berbagai organisasi untuk membantu meningkatkan kemungkinan (*likehood*) di dalam proses mencapai tujuan, meningkatkan performa di dalam mengidentifikasi peluang (*opportunity*) dan ancaman (*threat*) serta dilakukan untuk memanfaatkan sumber daya yang ada dalam menangani risiko (*risk treatment*).

Pengertian Rumah Sakit

Menurut [4] Rumah Sakit adalah suatu organisasi yang melibatkan tenaga medis profesional yang terorganisir baik dari sarana maupun prasarana kedokteran yang permanen, pelayanan kedokteran, asuhan keperawatan yang berkesinambungan diagnosis serta pengobatan penyakit yang diderita oleh pasien. Jadi dapat disimpulkan bahwa Rumah Sakit adalah sarana pertolongan pada orang yang terkena penyakit, dan akan dilayani oleh tenaga ahli di bidang Kesehatan di mana saran dan prasarana sudah lengkap.

Pengertian Manajemen Risiko

Menurut [5], manajemen risiko merupakan suatu usaha untuk mengetahui, menganalisis, serta mengendalikan risiko dalam setiap kegiatan organisasi dengan tujuan untuk memperoleh efektivitas dan efisiensi yang lebih tinggi. Sedangkan menurut Hanggraeni [6], manajemen risiko merupakan suatu rangkaian prosedur dan metodologi yang digunakan untuk mengidentifikasi, mengukur, memonitor dan mengontrol risiko yang timbul dari bisnis operasional organisasi. Jadi dapat dikatakan bahwa manajemen risiko adalah suatu metode yang digunakan dalam mengendalikan sebuah risiko yang ada pada organisasi sehingga dampak yang didapatkan berguna bagi organisasi.

Pengertian Sistem Informasi Manajemen Rumah Sakit

Dalam Undang-Undang Republik Indonesia Nomor 44 Tahun 2009 tentang Rumah Sakit dan Peraturan Menteri Kesehatan No.82 Tahun 2013 tentang Sistem Informasi Manajemen Rumah Sakit, dalam pasal 1 ayat 6 dikatakan bahwa SIMRS adalah sistem pengelolaan informasi seluruh kegiatan rumah sakit sehingga membantu setiap proses manajemennya untuk meningkatkan efisiensi, efektivitas, profesionalisme, kinerja, serta akses dalam pelayanan rumah sakit. Menurut [7] Teknologi informasi memiliki peran penting dalam pelayanan kesehatan saat ini. Di mana kualitas pengolahan informasi merupakan faktor penting bagi keberhasilan institusi pelayanan kesehatan. Sistem informasi yang baik dapat mendukung alur kerja klinis dengan berbagai cara yang akan memberikan kontribusi untuk perawatan pasien yang lebih baik. Menurut [8] Sistem informasi mempunyai 3 peranan penting dalam mendukung proses pelayanan kesehatan, yaitu: mendukung proses dan operasi pelayanan kesehatan, mendukung pengambilan keputusan staf dan manajamen serta mendukung berbagai strategi untuk keunggulan kompetitif.

Jadi dapat disimpulkan bahwa Sistem Informasi Manajemen Rumah Sakit merupakan suatu sarana teknologi informasi di mana penggunaannya dapat memaksimalkan kinerja Rumah Sakit sehingga pelayanan yang diberikan memuaskan bagi pasien.

Pengertian ISO 31000

ISO 31000 adalah suatu standar implementasi manajemen risiko yang diterbitkan oleh *International Organization for Standardization* pada tanggal 13 November 2009. Standar ini ditujukan untuk dapat diterapkan dan disesuaikan untuk semua jenis organisasi dengan memberikan struktur dan pedoman yang berlaku generik terhadap semua operasi yang terkait dengan manajemen risiko.

Tahapan ISO 31000

1. Komunikasi dan Konsultasi
   Komunikasi dan konsuultasi adalah suatu usaha agar stakeholder memahami berbagai macam risiko, agar keputusan yang diambil tidak merugikan organisasi. Dengan melakukan komunikasi dan konsultasi diharapkan dapat menambah kinerja manajemen risiko menjadi terencana dan lancar. Komunikasi dan konsultasi dilakukan dengan pemangku kepentingan agar organisasi dapat memberikan data yang dibutuhkan, serta penjelasan mengenai sistem yang akan diteliti.

2. Lingkup, konteks, dan kriteria
   Tujuan dalam menetapkan lingkup, konteks, dan kriteria adalah untuk mengidentifikasi dan merancang manajemen risiko yang sesuai dengan ruang lingkup organisasi tersebut.
3. Penilaian Risiko (Asesmen Risiko)
   Penilaian risko adalah proses melakukan identifikasi risiko, analisis risiko, dan evaluasi risiko. Dalam melakukan penilaian risiko, dibutuhkan data-data dan informasi akurat dan informasi yang ada dalam organisasi.

A. Identifikasi Risiko

Identifikasi risiko merupakan cara untuk mencari, menemukan dan menjelaskan secara rinci apa sajakah risiko yang menghambat sebuah organisasi. Dibutuhkan informasi yang benar agar mengidentifikasi risiko. Identifikasi risiko dapat dilakukan dengan cara melakukan wawancara kepada ahli di bidang Teknologi Informasi (Staff IT). Ada beberapa tahapan yang akan dilakukan dalam melakukan identifikasi risiko:

1. Mengidentifikasi Teknologi informasi dalam organisasi.
2. Menganalisis kemungkinan risiko yang akan muncul dalam teknologi informasi tersebut.
3. Mengidentifikasi dampak dari risiko

B. Analisis Risiko

Analisis risiko merupakan cara untuk mengidentifikasi risiko-risiko yang ada. Analisis risiko bertujuan untuk memberikan gambaran pada saat melakukan evaluasi risiko, agar metode risiko yang dilakukan dapat tepat sasaran. Digunakan tabel likehood untuk mengetahui seberapa sering risiko terjadi dalam satu waktu tertentu.

Tabel 1 *Likehood*

Likehood		Keterangan	Frekuensi
Rating	Kriteria		
1	*Rare*	Risiko hampir tidak pernah terjadi	>2 tahun
2	*Unlikely*	Risiko jarang terjadi	1-2 tahun
3	*Possible*	Risiko kadang-kadang terjadi	7-12 bulan/tahun
4	*Likely*	Risiko sering terjadi	4-6 bulan/tahun
5	*Certain*	Risiko Pasti terjadi	1-3 bulan/tahun

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

Tabel 2 *Impact*

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

C. Evaluasi Risiko

Evaluasi risiko adalah proses pengambilan keputusan dalam manajemen risiko. Evaluasi risiko memiliki peran dalam melakukan tindakan lebih lanjut atau tidak jika tidak dibutuhkan. Dalam tahap evaluasi risiko digunakan matriks risiko, yang berasal hasil dari analisis risiko, kemudian dimasukkan ke dalam matriks.

Tabel 3 Matriks Risiko

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

4. Perlakuan Risiko
   Tujuan dalam perlakukan risiko adalah untuk mempertimbangkan pilihan perlakukan risiko dan mengimplementasikan manajemen risiko, sehingga dapat mengendalikan risiko, mengurangi kemungkinan kerugian, dan meningkatkan kinerja organisasi. Menurut [9] organisasi memiliki pilihan dalam perlakuan risiko sebagai berikut:
   A. Mengubah kemungkinan
      Dilakukan untuk mencegah terjadinya risiko yang berdampak buruk pada perusahaan dan melaksanakan kemungkinan terjadinya risiko yang positif sehingga menjadi keuntungan bagi organisasi.
   B. Mengubah dampak
      Mengurangi kerugian yang dapat terjadi karena risiko yang belum dicegah, dan memaksimalkan manfaat dari risiko yang berdampak negatif pada organisasi.
   C. Mengubah kemungkinan dan dampak
      Melakukan pencegahan risiko yang berdampak negatif atau memicu terjadinya risiko yang berdampak positif, dan menyiapkan rencana cadangan sebagai antispasi jika semua kemungkin gagal.
5. Pemantauan dan Tinjauan
   Pemantauan dan tinjauan dilakukan untuk menjamin dan memastikan bahwa pelaksanaan proses risiko telah berhasil dilakukan. Pemantauan harus selalu dilakukan, dan meninjau hasil yang sudah dilakukan. Hasil pemantauan dan kaji ulang harus dimasukkan ke dalam aktivitas organisasi sebagai tolok ukur kinerja organisasi tersebut.
6. Pencatatan dan Pelaporan
   Setelah proses manajemen risiko selesai dilaksanakan, dibutuhkan sebuah pencatatan yang berguna sebagai catatan pelaksanaan kegiatan, menjadi bukti hukum jika ada permasalahan, dan sarana untuk pengetahuan, baik menjadi pengembangan knowledge management dalam perusahaan

Rumus yang digunakan

Dalam menghitung hasil kuesioner yang diberikan, peneliti menggunakan rumus Likert. Menurut untuk mengetahui presentasi jawaban dari setiap responden, rumus Likert dengan rumus sebagai berikut:

$$\% = \frac{f}{n} x100 \quad (1)$$

Dimana:
% = Index
f = Frekuensi pada kuesioner
n= Jumlah skor maksimum (Jumlah responden * Skor tertinggi)

3. Hasil Penelitian

Hasil penelitian merupakan hasil dari proses perumusan masalah dan metologi penelitian, dimana metode dan teknik analisis data yang digunakan pada objek penelitian yang diharapkan dapat menyelesaikan rumusan masalah, mencapai sebuah kesimpulan dan dapat dijadikan bahan acuan dalam memajukan organisasi tersebut.

Komunikasi dan Konsultasi

Tahap pertama yang dilakukan dalam analisis manajemen risiko menggunakan ISO 31000 adalah melakukan observasi dan wawancara kepada pihak yang terkait di Rumah Sakit XYZ, dimana penulis melakukan wawancara kepada Kepala Mirsa. Tahap ini dilakukan kepada bagian Mirsa untuk membahas izin dalam melakukan analisis manajemen risiko, sehingga apa yang akan diperoleh dapat dipertanggungjawabkan kepada pihak Rumah Sakit XYZ. Proses selanjutnya adalah melakukan komunikasi dan konsultasi, dimana akan dilakukan penampungan informasi dan menanyakan pendapat mengenai risiko penggunaan SIMRS dan cara pengelolaan, sehingga dapat menjadi pertimbangan dalam mengambil keputusan pengelolaan manajemen risiko.

Lingkup, Konteks, dan Kriteria

Tujuan dilakukan penelitian ini adalah untuk menganalisa manajemen risiko Teknologi Informasi pada Rumah Sakit XYZ, dimana objek penelitian SIMRS yang merupakan sistem informasi manajemen pada Rumah Sakit XYZ yang dikelola oleh bagian Mirsa, dimana risiko yang ada merupakan risiko dari penggunaan SIMRS. Adapun konteks pada SIMRS adalah sebagai berikut:

A. Software
Software yang digunakan berbasis website berbasis *local area*, yang digunakan dalam pengimputan data yang sesuai dengan bagian masing-masing.

B. Informasi
Informasi merupakan data-data yang telah diimput, dan akan disimpan untuk kepentingan organisasi dan dapat digunakan untuk pengambilan keputusan dalam proses bisnis. Data-data yang dimasukkan berupa data pengguna, data keuangan, dan data pasien masuk

C. Infrastruktur
Infrastruktur yang digunakan dalam menjalankan SIMRS antara lain *Hardware*, *operation system*, *database*, mikrotik, jaringan dan fasilitas-fasilitas yang dapat mendukung penggunaan SIMRS.

D. Pengguna
Merupakan peran penting dalam menjalankan Teknologi Informasi. Keahlian dalam penggunaan dan profesionalitas dibutuhkan untuk menjalankan sistem, sehingga dapat mendukung kinerja organisasi tersebut.

Assesmen Risiko (Penilaian Risiko)

Penilaian risko adalah proses melakukan identifikasi risiko, analisis risiko, dan evaluasi risiko. Dalam melakukan penilaian risiko, dibutuhkan data-data dan informasi akurat dan informasi yang ada dalam organisasi.

A. Identifikasi Risiko

1. Identifikasi Aset
   Identifikasi asset merupakan cara pengumpulan terkait aset yang terkait pada penggunaan SIMRS

Tabel 4 Identifikasi Aset

	Aset Pada SIMRS Rumah Sakit XYZ
Data	Data Pasien
	Data Transaksi
	Data Dokter
Sistem	SIMRS
	Jaringan
	Mikrotik
	UTP
	Server
Hardware	CPU
	Monitor
	Printer

2. Identifikasi Kemungkinan Risiko
   Setelah melakukan identifikasi aset terhadap SIMRS, hal yang selanjutnya dilakukan adalah melakukan Identifikasi Kemungkinan Risiko yang terdiri dari beberapa faktor yang meliputi manusia, sistem, manusia, serta infrastruktur terkait penggunaan SIMRS.

Tabel 5 Identifikasi Kemungkinan Risiko

ID	Risiko
R01	Data Hilang
R02	Kegagalan Pengimputan data
R03	SIMRS tidak dapat dijalankan
R04	Jaringan Lambat
R05	Tidak Mendapatkan *IP Address*
R06	Koneksi putus-putus
R07	Data Tidak Sesuai
R08	UPS tidak dapat menyimpan daya
R09	*Human error*
R10	Tidak Mengetahui cara pengoperasian SIMRS
R11	*Hang* pada Komputer
R12	Virus
R13	Kerusakan *Hardware*
R14	Tidak bisa melakukan *booting* komputer
R15	Mati Listrik

3. Identifikasi Dampak Risiko

   Setelah melakukan identifikasi kemungkinan risiko pada SIMRS, selanjutnya dilakukan identifikasi dampak risiko dimana akan mengidentifikasi dampak yang akan ditimbulkan oleh kemungkinan risiko yang terjadi pada SIMRS.

Tabel 6 Identifikasi Dampak Risiko

ID	Risiko	Dampak
R01	Data Hilang	Tidak dapat melihat data yang tersimpan sebelumnya
R02	Kegagalan Pengimputan data	Tidak dapat memasukkan data secara *on time*
R03	Sistem *Crash*	Sistem tidak dapat dijalankan
R04	Jaringan Lambat	Pengimputan data memakan waktu yang lama
R05	Tidak Mendapatkan *IP Address*	Tidak bisa mengakses SIMRS
R06	Data Tidak Sesuai	Menghambat proses pengimputan
R07	UPS tidak dapat menyimpan daya	Tidak dapat melakukan *backup* data
R08	*Human error*	Menghambat Pemrosesan SIMRS
R09	Tidak Mengetahui cara pengoperasian SIMRS	Tidak dapat menjalankan SIMRS
R10	*Hang* pada Komputer	Mengganggu Proses SIMRS
R11	Virus	Tidak dapat menjalankan komputer
R12	Kerusakan *Hardware*	Tidak dapat menjalankan beberapa fungsi komputer
R13	Tidak bisa melakukan *booting* komputer	Tidak dapat menjalankan komputer
R14	Mati Listrik	Aktivitas penggunaan SIMRS akan terhenti

4. Analisis Risiko
Setelah melakukan tahap identifikasi risiko, selanjutnya melakukan analisis risiko. Analisis risiko bertujuan untuk untuk mengidentifikasi risiko-risiko yang ada. Dilakukan penilaian terhadap risiko-risiko yang sudah terindentifikasi berdasarkan kemungkinan (*likehood*) dan dampak (*impact*) yang akan ditimbulkan.

Tabel 7 Analisis Risiko

ID	Risiko	% Likehood	Likehood	% Impact	Impact
R01	Data Hilang	38%	2	48%	3
R02	Kegagalan Pengimputan data	52%	3	56%	3
R03	Sistem *Crash*	36%	2	60%	4
R04	Jaringan Lambat	64%	4	56%	3
R05	Tidak Mendapatkan *IP Address*	68%	4	44%	3
R06	Data Tidak Sesuai	44%	3	44%	3
R07	UPS tidak dapat menyimpan daya	40%	3	52%	3
R08	*Human error*	52%	3	48%	3
R09	Tidak Mengetahui cara pengoperasian SIMRS	40%	3	40%	3
R10	*Hang* pada Komputer	52%	3	52%	3
R11	Virus	52%	3	72%	4
R12	Kerusakan *Hardware*	60%	4	56%	3
R13	Tidak bisa melakukan *booting* komputer	52%	3	52%	3
R14	Mati Listrik	44%	3	76%	4

5. Evaluasi Risiko
Tahap akhir dalam melakukan assesmen risiko adalah evaluasi risiko yang merupakan tahap proses pengambilan keputusan dalam manajemen risiko. Hasil dari evaluasi risiko akan menentukan keputusan dalam menangani risiko tersebut. Risiko yang sudah ditemukan akan dibedakan menjadi 3 *risk level* yaitu *low, medium,* dan *high* dan proses sebelumnya akan disesuaikan dengan matriks risiko.

Tabel 8 Matriks Evaluasi Risiko

Likehood						
Certain	*5*	Medium	Medium	High	High	High
Likely	*4*	Medium	Medium	R04,R05,R13	High	High
Possible	*3*	Low	Medium	R02,R06,R07,R08 ,R09,R10,RR11, R14	R12, R15	High
Unlikely	*2*	Low	Low	R01	R03	Medium
Rare	*1*	Low	Low	Low	Medium	Medium
		1	*2*	*3*	*4*	*5*
	Impact	*Insignificant*	*Minor*	*Moderate*	*Major*	*Catasthropic*

Setelah melakukan evaluasi risiko dengan memasukkan risiko ke dalam tabel matriks evaluasi risiko berdasarkan kemungkinan (*likehood*) dan dampak (*impact*), kemudian akan dijelaskan 15 kemungkinan risiko yang sesuai dengan *risk level* tiap masing-masing risiko.

Tabel 9 *Risk Level* Kemungkinan Risiko

ID	Risiko	Likehood	Impact	*Risk Level*
R012	Virus	3	4	High
R15	Mati Listrik	3	4	High
R02	Kegagalan pengimputan data	2	4	Medium
R07	Data Tidak Sesuai	3	3	Medium
R08	UPS tidak dapat menyimpan daya	3	3	Medium
R09	*Human error*	3	3	Medium
R10	Tidak Mengetahui cara pengoperasian SIMRS	3	3	Medium
R11	*Hang* pada Komputer	3	3	Medium
R14	Tidak bisa melakukan *booting* komputer	3	3	Medium
R01	Data Hilang	2	3	Medium
R03	Sistem *Crash*	2	4	Medium
R04	Jaringan Lambat	4	3	Medium
R05	Tidak Mendapatkan *IP Address*	4	3	Medium
R13	Kerusakan *Hardware*	4	3	Medium

Pada tabel 9 merupakan hasil dari evaluasi risiko dimana hasil dari penggolongan identifikasi aset (data, sistem, *Hardware*) dimana terdapat 2 (virus, mati listrik) merupakan *risk level* tingkatan *high*, dan terdapat 13 (kegagalan pengimputan data, koneksi putus-putus, data tidak sesuai, UPS tidak dapat menyimpan daya, *human error*, tidak mengetahui cara pengoperasian SIMRS, *hang* pada komputer, tidak bisa melakukan booting pada komputer, data hilang, sistem *crash*, jaringan lambat, tidak mendapatkan *IP address*, kerusakan *hardware*) merupakan *risk level* tingkatan *medium*.

Perlakuan Risiko

Setelah melakkukan assesmen risiko, tahap selanjutnya yaitu perlakuan risiko. Perlakuan risiko digunakan untuk memberikan pemilihan perlakuan risiko sesuai yang dibutuhkan oleh organisasi. Dalam tahap ini penulis memberikan saran perlakuan risiko untuk setiap kemungkinan risiko pada SIMRS. Diharapkan saran tersebut dapat mengurangi setiap kemungkinan yang ada dan kemungkinan yang akan mengganggu proses penggunaan SIMRS.

Tabel 10 Perlakuan Risiko

ID	Risiko	*Risk Level*	Perlakuan Risiko
R012	Virus	High	1. Melakukan pemindaian virus menggunakan antivirus yang sudah disediakan dalam komputer. 2. Melakukan update antivirus secara berkala.
R15	Mati Listrik	High	Menyediakan Genset yang dapat melakukan *cover* di seluruh bagian.
R02	Kegagalan pengimputan data	Medium	1. Memeriksa apakah jaringan terhubung atau tidak. 2. Mematikan firewall agar terhubung dengan l*ocal network*.
R07	Data Tidak Sesuai	Medium	Melakukan pengecekan ulang sebelum melakukan pengimputan data.
R08	UPS tidak dapat menyimpan daya	Medium	1. Melakukan pemeriksaan secara rutin penyimpanan daya. 2. Memiliki cadangan jika UPS yang digunakan sedang rusak.
R09	*Human error*	Medium	1. Melakukan pembagian tugas sesuai dengan bagian masing-masing. 2. Memberikan instruksi penggunaan Komputer yang baik.

R10	Tidak Mengetahui cara pengoperasian SIMRS	Medium	Melakukan sosialisasi penggunaan SIMRS kepada karyawan yang terlibat penggunaan sistem tersebut.
R11	*Hang* pada Komputer	Medium	1. Melakukan perawatan komputer secara berkala. 2. Melakukan pembaruan perangkat yang sudah termakan usia.
R14	Tidak bisa melakukan *booting* komputer	Medium	1. Melakukan pembersihan pada 2.Melakukan pengecekan terhadap komponen CPU.
R01	Data Hilang	Medium	1. Melakukan *backup* data. 2. Memeriksa beberapa *bug* yang ada dalam sistem.
R03	Sistem *Crash*	Medium	Memeriksa penggunaan port untuk sistem tersebut, apakah terpakai atau bentrok dengan sistem lain.
R04	Jaringan Lambat	Medium	1. Memeriksa aktivitas server, dan mematikan proses yang tidak berhunbungan dengan sistem. 2. Melakukan pembatasan penggunaan jaringan kepada yang membutuhkan saja.
R05	Tidak Mendapatkan *IP address*	Medium	1. Melakukan intstalasi update pada driver Ethernet secara teratur. 2. Mengganti Perangkat yang sudah lama.
R13	Kerusakan *Hardware*	Medium	1. Memberikan pengarahan kepada pegawai tentang cara penggunaan komputer dengan baik. 2. Melakukan perawatan komputer secara berkala.

Pencatatan dan Pelaporan

Pencatatan dan pelaporan dilakukan setelah adanya hasil perlakuan risiko, dimana kritik dan saran yang diberikan untuk dilakukan pada SIMRS. Hasil dari implementasi manajemen risiko SIMRS diamati oleh bagian Mirsa Rumah Sakit XYZ. Seluruh kegiatan yang dilakukan oleh peneliti melibatkan seluruh staff bagian Mirsa yang terkait dengan pengelolaan SIMRS.

Pencatatan dan pelaporan diberikan kepada pihak Rumah Sakit dimana penulis melakukan komunikasi dan melaporkan terkait kemungkinan risiko yang berpotensi menghambat proses SIMRS, dan memberikan saran yang dapat dilakukan oleh organisasi untuk meminimalisir kemungkinan yang akan terjadi suatu saat nanti.

4. Kesimpulan dan Saran

Kesimpulan

Berdasarkan hasil analisa yang dilakukan pada dengan menggunakan *framework* ISO 31000 pada Rumah Sakit XYZ, maka didapatkan kesimpulan sebagai berikut:

1. Dalam melakukan manajemen risiko, dilakukan tahap demi tahap sesuai dengan pedoman ISO 31000 yang dimulai dari komunikasi dan konsultasi yang dilaksanakan berdasarkan data dari pihak yang bersangkutan. Lalu menetapkan lingkup, konteks dan kriteria yang akan dianalisa. Kemudian melakukan assesmen risiko yang terdiri dari 3 tahapan yang akan menjelaskan hasil yang didapatkan, dan kemudian melakukan perlakuan risiko yang memberikan saran untuk mengatasi risiko tersebut. Setelah melakukan perlakuan risiko dilakukan pencatatan dan pelaporan yang akan diberikan kepada pihak organisasi untuk menjadi bahan pertimbangan dalam menangani risiko yang ada dalam organisasi tersebut.
2. Hasil dari assesmen risiko didapatkan risiko berupa 2 *risk level* tingkatan *high* (virus, mati listrik) dan terdapat 13 *risk level* tingkatan *medium* (kegagalan pengimputan data, koneksi putus-putus, data tidak sesuai, UPS tidak dapat menyimpan daya, *human error*, tidak mengetahui cara pengoperasian SIMRS, *hang* pada komputer, tidak bisa melakukan booting pada komputer, data hilang, sistem *crash*, jaringan lambat, tidak mendapatkan *IP address*,

kerusakan *hardware*). Diharapkan dengan diberikan saran melalui perlakuan risiko diharapkan dapat mencegah kemungkinan-kemungkinan risiko yang akan datang selanjutnya.

Saran

Peneliti telah menyelesaikan proses Manajemen Risiko sesuai dengan metode ISO 31000:2018. Penelitian ini melibatkan staff IT pada Rumah Sakit XYZ agar proses manajemen risiko berjalan dengan baik. Penulis mengetahui bahwa banyak kekurangan yang dimiliki, sehingga penulis memiliki saran sebagai berikut:

1. Dalam melakukan konteks kriteria, diharapkan dapat dianalisis secara menyeluruh, baik dari konteks eksternal maupun internal, agar mengetahui seberapa besar kontribusi *stakeholder* dalam menjalankan SIMRS.
2. Implementasi manajemen risiko dapat dilakukan pada beberapa bagian dikarenakan Rumah Sakit XYZ memiliki 3 teknologi informasi yang belum dilakukan manajemen risiko sehingga dapat diimplementasikan untuk meningkatkan kualitas organisasi tersebut.

5. Referensi

[1] H. Purba, "Rekomendasi Pengembangan IT Governance Menggunakan Analytical Hierarchy Process pada Institusi Pendidikan (Studi Kasus: Universitas Advent Indonesia)," *TeIKa,* vol. 03, no. 1, pp. 1-10, 2010.

[2] F. A. Alvian, M. H. S. and P. Z. B. , "Manajemen risiko pada laboratorium integrasi universitas islam negeri sunan ampel surabaya menggunakan iso 31000," *JURNAL MANAJEMEN,* pp. 56-67, 2020.

[3] S. Agustinus, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Program HRMS," *J. RESTI (Rekayasa Sistem dan Teknologi Informasi,* vol. Vol. 1, p. No. 3, 2017.

[4] Ilma, "Analisis Statistik Asuhan Kesehatan Pasien Rawat Inap di Rumah Sakit Bhayangkara Padang," *Jurnal Kesehatan Medika Saintika,* 2020.

[5] H. Darmawi, Manajemen Risiko: Edisi 2, Jakarta: Sinar Grafika Offset, 2016.

[6] S. E. S. O. T. and S. S. , "Peran Business Continuity Plan dan Contingency Plan Dalam Meminimalisir Risiko Teknologi Informasi Pada Industri Asuransi," *Jurnal Asuransi dan Manajemen Risiko,* p. 42–52, 2013.

[7] Ammenwerth E, Ehlers F, Hirsch B and Gratl G, "HIS-Monitor: an approach to assess the quality of information processing in hospitals," *International journal of medical informatics,* 2006.

[8] J. O. Brien, Introduction to information Systems, The McRraw-Hill Companies. Inc, 2005.

[9] L. J. Susilo and V. R. Kaho, Manajemen Risiko ISO 31000:2018, Grasindo, 2018.

[10] S. Metode Penelitian Kuantitatif Kualitatif dan R&D, Bandung: Alfabeta, 2012.