e-ISBN 978-623-93343-3-8
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 20 April 2021

Manajemen Risiko Sistem Informasi Rumah Sakit (Studi Kasus : Rumah Sakit EMC Tangerang)

Anisah Dzakiyyah [1], Medina Nurul Zahra [2], Nuraini Azizi Rachim [3], Siti Khofifah Munjiyanti [4], Kraugusteelianan, S.Kom., M.Kom. [5]
Program Studi Sistem Informasi / Fakultas Ilmu Komputer
Universitas Pembangunan Nasional Veteran Jakarta
Jl. Rs. Fatmawati Raya, Pondok Labu, Kec. Cilandak, Jakarta Selatan, DKI Jakarta, 12450
anisahdzakiyyah@upnvj.ac.id [1], medinanz@upnvj.ac.id [2], nurainiar@upnvj.ac.id [3], sitikm@upnvj.ac.id [4], kraugusteeliana@upnvj.ac.id [5]

Abstrak. Rumah sakit merupakan sebuah tempat pelayanan masyarakat dalam hal kesehatan yang dapat memberikan sebuah diagnosa serta perawatan medis. Rumah Sakit EMC Tangerang merupakan salah satu anggota dari EMC Group dengan tujuan melayani secara pesat kebutuhan pelayanan kesehatan yang unggul dan terpercaya. Di era dengan kemajuan teknologi seperti saat ini, sistem serta aset TI pada rumah sakit merupakan hal krusial guna menyediakan informasi yang dibutuhkan. Dalam penerapan sistem informasi rumah sakit tersebut muncul risiko yang mengancam keberlangsungannya. Kegagalan organisasi dalam menilai sumber ancaman risiko menjadi salah satu penyebab yang mengancam keberlangsungan sistem informasi rumah sakit. Risiko dapat berasal dari sumber daya manusianya, sistem atau infrastrukturnya, ataupun dapat berasal dari faktor alam dan lingkungan yang dapat mengakibatkan terganggunya sistem informasi rumah sakit atau bahkan terhentinya layanan pada sistem informasi rumah sakit tersebut. Tujuan dari dilakukannya penelitian ini adalah untuk mengetahui risiko-risiko yang dapat terjadi pada sistem informasi Rumah Sakit EMC Tangerang dengan cara melakukan penilaian risiko, mitigasi risiko, evaluasi risiko, serta memberikan rekomendasi-rekomendasi guna meminimalisir risiko-risiko yang dapat mengancam keberlangsungan sistem informasi Rumah Sakit EMC Tangerang.

Kata Kunci: Sistem Informasi, Rumah Sakit, Manajemen Risiko, Penilaian Risiko.

1 Pendahuluan

Saat ini peranan teknologi informasi begitu besar pada hampir setiap aspek kehidupan manusia, salah satunya yakni pada aspek bisnis. Hampir semua instansi atau perusahaan saat ini menggunakan teknologi informasi sebagai alat utama untuk menjalankan aktivitas pengelolaan bisnisnya. Hal ini dikarenakan penggunaan teknologi informasi pada sebuah instansi akan membuat proses bisnis pada instansi tersebut menjadi lebih cepat karena telah ada integrasi data dan beberapa aktivitas bisnis telah dilakukan otomatis dengan bantuan teknologi informasi tersebut. Selain itu penggunaan teknologi informasi di instansi akan membuat aktivitas pengolahan data menjadi informasi yang bermanfaat bagi instansi menjadi lebih mudah dan cepat, sehingga instansi akan memberikan layanan yang cepat dan baik kepada pelanggan.

Penggunaan teknologi informasi pada instansi kesehatan juga merupakan suatu hal yang penting dikarenakan teknologi informasi dapat membantu rumah sakit dalam memberikan pelayanan yang optimal kepada pasien. Hal ini dikarenakan teknologi informasi dapat membantu pihak rumah sakit dalam memproses data seputar pasien dengan lebih cepat yang nantikan akan mempengaruhi tingkat kecepatan rumah sakit dalam memberikan penanganan yang utuh terhadap pasien. Akan tetapi, ketika sebuah instansi menggunakan teknologi informasi untuk menjalankan proses bisnis utamanya maka tidak luput dari berbagai risiko-risiko yang dapat mengancam keberlangsungan proses bisnis pada instansi itu sendiri. Sehingga aktivitas pengelolaan terhadap berbagai risiko yang dapat muncul ini menjadi hal yang sangat penting untuk diperhatikan. Salah satu hal yang dapat dilakukan instansi dalam mengelola segala risiko yang dapat terjadi ialah dengan melakukan upaya pengukuran terhadap berbagai risiko yang dapat timbul dari penggunaan teknologi informasi tersebut.

Rumah Sakit EMC Tangerang merupakan salah satu rumah sakit yang telah menggunakan teknologi informasi dalam memberikan layanan kesehatan kepada pasien melalui website https://www.emc.id/id/hospitals/emc-tangerang. Melalui website tersebut para pasien dapat membuat appointment untuk pemeriksaan, melihat daftar appointment, melihat daftar dokter beserta jadwal praktiknya, mengetahui layanan dan promo yang disediakan pihak rumah sakit EMC Tangerang serta pasien juga dapat mengetahui informasi kesehatan terbaru melalui website EMC Tangerang. Sistem informasi ini memiliki peranan penting dalam menunjang aktivitas pelayanan awal kepada pasien EMC Tangerang sehingga risiko-risiko yang dapat terjadi pada website harus dapat dikelola

dengan baik oleh pihak rumah sakit EMC Tangerang sehingga pelayanan yang diberikan kepada pasien dapat terus dilakukan dengan optimal.

Berdasarkan penjelasan di atas, maka penelitian ini bertujuan untuk mengukur risiko sistem informasi Rumah Sakit EMC Tangerang dengan judul "Manajemen Risiko Sistem Informasi Rumah Sakit (Studi Kasus : EMC Tangerang)". Hasil penelitian ini diharapkan dapat memberikan informasi kepada pihak rumah sakit dalam memahami, menilai dan mengambil tindakan pengendalian terhadap risiko-risiko yang dapat timbul dari penggunaan teknologi informasi sebagai bagian dari proses bisnis utama rumah sakit. Sehingga pihak rumah sakit dapat meningkatkan tingkat keberhasilan dan mengurangi tingkat kegagalan penggunaan teknologi informasi untuk mencapai tujuan organisasi.

2 Permasalahan

Berdasarkan latar belakang masalah yang telah dikemukakan di atas, berikut dituliskan permasalahan yang dapat dirumuskan dalam penulisan penelitian ini : (1) Meninjau dan mengetahui identifikasi aset, ancaman, dan kerentanan yang dimiliki dan dihadapi oleh Rumah Sakit EMC Tangerang dalam menjalankan bisnisnya; (2) Meninjau bentuk analisis kontrol sebagai tindakan preventif untuk mengantisipasi dan menghentikan kejadian yang tidak diinginkan yang terjadi pada Rumah Sakit EMC Tangerang; (3) Meninjau penetapan prioritas keamanan informasi sebagai bentuk penanggulangan risiko yang mungkin terjadi pada Rumah Sakit EMC Tangerang berdasarkan kemungkinan insiden yang terjadi dan dampaknya; dan (4) Membuat analisis dan perencanaan bentuk rekomendasi kontrol dan mitigasi risiko terhadap proses penilaian risiko untuk mendukung manajemen membuat keputusan yang tepat dalam mengimplementasikan manajemen risiko.

3 Tinjauan Pustaka

3.1 Risiko

Risiko adalah suatu yang memberikan pengaruh ketidakpastian dalam mencapai tujuan [1]. Risiko dapat juga diartikan sebagai sebuah potensi untuk terjadinya sesuatu hal yang negatif atau merugikan, seperti potenti untuk cedera, kehilangan, kebakaran dan lain –lain[2]. Jadi dapat disimpulkan bahwa risiko adalah suatu potensi dari suatu kejadian yang menyebabkan kerugian negatif dan menyebabkan tujuan yang telah ditargetkan tidak tercapai karena adanya ketidakpastian tersebut.

Sebuah organisasi atau individu dapat mengecilkan tingkat terjadinya risiko dengan melakukan pengendalian terhadap kemungkinan terjadinya risiko tersebut, tapi tidak akan bisa untuk sepenuhnya menghilangkan adanya *exposure*. Hal ini dikarenakan pada risiko tidak ada metode apapun yang dapat menjamin 100% bahwa akibat negatif yang ditimbulkan dari suatu peristiwa tersebut dapat terhindarkan.

3.2 Manajemen Risiko

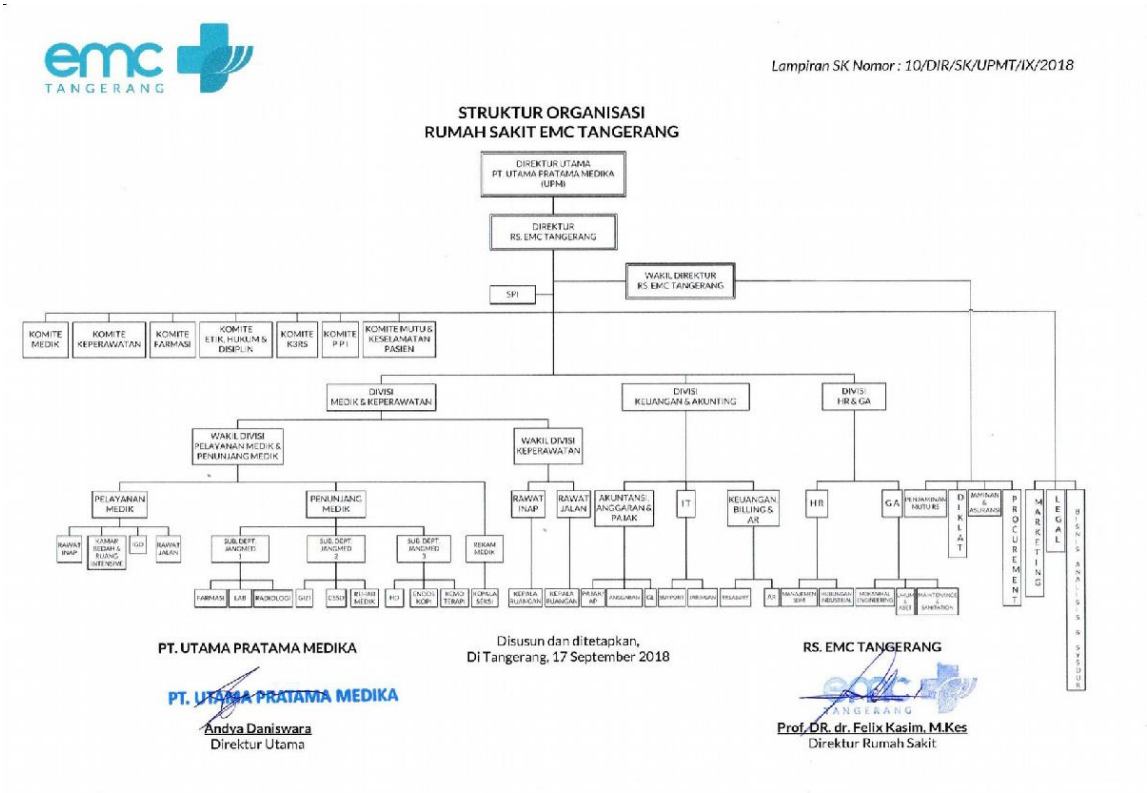
Manajemen risiko adalah suatu praktik mengidentifikasi, menilai, mengendalikan, dan memitigasi risiko [3]. Selain itu manajemen risiko juga dapat diartikan sebagai sebuah aktivitas perencanaan, pengorganisasian, memimpin dan pengendalian sumber daya organisasi yang lakukan untuk mengurangi dampak dari kerugian akibat bencana[4]. Sedangkan pengertian manajemen risiko TI adalah upaya dalam meminimalisir dampak negatif dari suatu peristiwa seperti, berhentinya aktivitas bisnis, memperburuk keadaan keuangan organisasi dan lain – lain [5].

Aktivitas manajemen risiko harus dilakukan oleh sebuah organisasi secara terus-menerus dan berulang, ketika manajemen risiko itu dilaksanakan dengan baik maka organisasi tersebut berkemungkinan untuk terjadi perbaikan secara terus-menerus dan peningkatan kinerja. Namun dalam melakukan manajemen risiko di sebuah organisasi maka harus diseimbangkan antara pengendalian risiko dan pembiayaan pengendalian risiko dengan visi, misi dan tujuan organisasi. Dalam melakukan sebuah penilaian risiko teknologi informasi diperlukan beberapa tahapan, diantaranya sebagai berikut :

1. Identifikasi dan Prioritaskan Aset
2. Identifikasi Ancaman

3. Identifikasi Kerentanan
4. Analisis Kontrol
5. Tentukan Kemungkinan Insiden
6. Menilai Dampak yang Mungkin Terjadi pada Ancaman
7. Prioritaskan Risiko Keamanan Informasi
8. Rekomendasi Kontrol
9. Dokumentasi Hasil

3.3 Rumah Sakit EMC Tangerang



Gambar 1. Struktur Organisasi Rumah Sakit EMC Tangerang 2018

Rumah sakit EMC Tangerang adalah rumah sakit swasta pertama yang berdiri di kota Tangerang yang awalnya bernama rumah sakit Usada Insani. Pada awal pendiriannya rumah sakit ini berada di bawah PT Usada Insani Abadi. Rumah sakit ini telah mengalami beberapa pergantian penanggung jawab hingga pada Oktober 2017 rumah sakit Usada Insani ini berganti nama menjadi rumah sakit EMC Tangerang dan di bawah PT Utama Pratama Medika dan menjadi kepemilikan Group EMTEK.

Rumah sakit EMC Tangerang memiliki visi yakni "Menjadi penyedia layanan kesehatan yang unggul dan terpercaya bagi seluruh lapisan masyarakat, demi memajukan kualitas layanan kesehatan di Indonesia". Dengan misi rumah sakit EMC Tangerang sebagai berikut :

1. Memprioritaskan kebutuhan dan keselamatan pasien
2. Menggalakkan budaya pembelajaran, inovasi, dan perbaikan yang berkesinambungan
3. Membangun pusat-pusat unggulan layanan kesehatan spesialis bertaraf Internasional.

Rumah sakit EMC Tangerang juga memiliki motto yakni PRIMA, dengan filosofi motto sebagai berikut :

- P : Peduli memperhatikan / mengindahkan / simpati.
- R : Responsif menanggapi / tidak bersikap bodo amat / empati.
- I : Inovatif menemukan sesuatu yang baru.
- M : Mandiri dilandasi kompetensi / mampu berdiri sendiri.
- A : Aktual berbasis terhadap pengetahuan yang EBM.

4 Metodologi Penelitian

Penelitian ini menggunakan metode penelitian kualitatif dikarenakan lebih cenderung menggunakan kemampuan analisis penulis dengan pendekatan studi kasus. Penelitian ini dilakukan dengan cara melakukan studi literatur, observasi dan melakukan pendeskripsian terhadap hal-hal yang berkaitan dengan objek penelitian. Fokus utama dalam penelitian ini adalah melakukan penilaian terhadap risiko – risiko yang dapat terjadi pada sistem informasi rumah sakit EMC Tangerang melalui 9 tahapan. 9 tahapan dalam mengukur risiko sistem informasi rumah sakit EMC Tangerang yaitu :

1. Identifikasi dan Prioritas Aset
2. Identifikasi Ancaman
3. Identifikasi Kerentanan
4. Analisis Kontrol
5. Tentukan Kemungkinan Insiden
6. Menilai Dampak yang Mungkin Terjadi pada Ancaman
7. Prioritaskan Risiko Keamanan Informasi
8. Rekomendasi Kontrol
9. Dokumentasi Hasil

Setelah melakukan 9 langkah di atas untuk mengukur risiko sistem informasi rumah sakit EMC Tangerang maka langkah terakhir adalah memberikan kesimpulan yang diperoleh penulis selama melakukan penelitian.

5 Hasil dan Pembahasan

5.1 Identifikasi dan Prioritaskan Aset

Tahapan identifikasi dan mengurutkan prioritas aset pada website Rumah Sakit EMC Tangerang dilakukan melalui studi literatur dan observasi. Pada tahap ini identifikasi dan prioritas aset dapat dilihat pada tabel berikut.

Tabel 1. Identifikasi Aset Sistem Informasi Rumah Sakit EMC Tangerang

No	Jenis / Kategori	Aset
1	Perangkat Keras	a. Komputer Server b. Perangkat Jaringan
2	Perangkat Lunak	a. *Database Server* b. *Storage Server* c. Sistem Informasi RS
3	Data	a. Data Rumah Sakit b. Data Dokter c. Data Pasien d. Data Penyakit e. Data Alat f. Data Praktik Dokter

5.2 Identifikasi Ancaman

Identifikasi ancaman dapat dilihat dari sumber ancaman, yang mana sumber ancaman adalah sesuatu hal yang berpotensi untuk menyebabkan kerusakan terhadap sistem IT baik disengaja atau tidak disengaja.

Tabel 2. Ancaman terhadap Sistem Informasi Rumah Sakit EMC Tangerang

No	Sumber Ancaman	Jenis Ancaman
1	Sumber Daya Manusia	Kesalahan manusia meliputi miskomunikasi, kesalahan memasukan data, ketidaktelitian, kelalaian, dan lain-lain.
2	Faktor Sistem dan Infrastruktur	Kerusakan dan kegagalan sistem meliputi *server down*, hilangnya data, *data overload*, serangan virus, pembobolan data, dan lain-lain.
3	Faktor Alam dan	Bencana alam, listrik padam, kebakaran, dan lain-lain.

	Lingkungan

5.3 Identifikasi Kerentanan

Tabel 3. Ancaman terhadap Sistem Informasi Rumah Sakit EMC Tangerang

No	Sumber Kerentanan	Kerentanan
1	Sumber Daya Manusia	Miskomunikasi antar pegawai dalam transfer pengetahuan atau data sehingga menyebabkan kesalahan terhadap data yang dimasukkan.
		Ketidaktelitian pegawai dalam memasukan data sehingga *output* yang dihasilkan tidak valid.
		Pegawai yang tidak bertanggung jawab melakukan pembocoran data atau memberikan hak akses kepada orang yang tidak berwenang.
		Pegawai kurang mengerti atau *skill* yang tidak mendukung terhadap penggunaan sistem informasi yang ada.
2	Faktor Sistem dan Infrastruktur	*Server down* akibat ketidaksiapan sistem informasi apabila diakses oleh banyak pengguna.
		Hilangnya data akibat tidak adanya *back up database* dari pihak rumah sakit.
		Data yang *overload* karena redudansi data atau data yang sudah tidak dipakai, sehingga menumpuk pada penyimpanan *database* dan menyebabkan sistem yang lambat.
		Sistem diserang oleh virus karena tidak adanya *firewall* atau antivirus yang mendukung.
		Pembobolan data diakibatkan kurangnya keamanan sistem yang baik atau ruangan server yang tidak memiliki tingkat keamanan yang tinggi.
3	Faktor Alam dan Lingkungan	Bencana alam menyebabkan rusaknya aset baik dari perangkat lunak maupun perangkat keras sehingga data dapat hilang dan berhentinya proses bisnis yang sedang berlangsung.
		Listrik padam dapat menyebabkan tidak adanya ketersediaan data sehingga menghambat proses bisnis yang berlangsung.
		Kebakaran menyebabkan rusaknya aset baik dari perangkat lunak maupun perangkat keras sehingga data dapat hilang dan berhentinya proses bisnis yang sedang berlangsung.

5.4 Analisis Kontrol

Analisis kontrol merupakan tahapan untuk menganalisis kemungkinan risiko yang akan terjadi dengan melihat kerentanan sebuah sistem informasi, sehingga dapat melakukan tindakan preventif untuk mengantisipasi dan menghentikan kejadian yang tidak diinginkan.

Tabel 4. Hasil Analisis Kontrol Sistem Informasi Rumah Sakit EMC Tangerang

No	Sumber Kerentanan	Kerentanan	Kontrol
1	Sumber Daya Manusia	Miskomunikasi antar pegawai dalam transfer pengetahuan atau data sehingga menyebabkan kesalahan terhadap data yang dimasukkan.	a. Melakukan budaya *sharing knowledge* agar setiap pegawai mempunyai level pemahaman yang sama. b. Melakukan pelatihan teknis agar setiap pegawai memiliki kemampuan yang sama dalam mengoperasikan sistem. c. Melakukan validasi data terhadap data yang dimasukkan. d. Melakukan perubahan hak akses secara berkala .
		Ketidaktelitian pegawai dalam memasukan data sehingga *output* yang dihasilkan tidak valid.	
		Pegawai yang tidak bertanggung jawab melakukan pembocoran data	

		atau memberikan hak akses kepada orang yang tidak berwenang.	e. Melakukan seminar etika profesi. f. Membuat dan menjalankan SOP agar pegawai tahu lebih jelas peraturan dan sanksi di bidang kerjanya. g. Memperbaiki komunikasi antar pegawai agar tidak terjadi miskomunikasi lagi.
		Pegawai kurang mengerti atau *skill* yang tidak mendukung terhadap penggunaan sistem informasi yang ada.	
2	Faktor Sistem dan Infrastruktur	*Server down* akibat ketidaksiapan sistem informasi apabila diakses oleh banyak pengguna.	a. Mempunyai *back-up database* rumah sakit. b. Melakukan *maintenance* secara berkala. c. Memperhatikan suhu komputer server untuk menghindari *overhead*. d. Penggunaan *Database Management System* yang bertujuan untuk mengontrol redundansi, sehingga data yang dipakai dapat konsisten dan tidak terdapat duplikasi data e. Instalasi *firewall, antivirus, deep freeze.* f. Memiliki ruangan server sistem yang dilengkapi dengan sistem keamanan yang tinggi (misalnya menggunakan pintu yang dapat diakses dengan *fingerprint*) guna mencegah pihak yang tidak berwenang dapat masuk ke ruangan tersebut. g. Memantau sistem secara berkala untuk mencegah agar tidak terjadi aktivitas ilegal yang dilakukan oleh pihak yang tidak terotorisasi. h. Menerapkan *Security Operation Center.*
		Hilangnya data akibat tidak adanya *back up database* dari pihak rumah sakit.	
		Data yang *overload* karena redudansi data atau data yang sudah tidak dipakai, sehingga menumpuk pada penyimpanan *database* dan menyebabkan sistem yang lambat.	
		Sistem diserang oleh virus karena tidak adanya *firewall* atau antivirus yang mendukung.	
		Pembobolan data diakibatkan kurangnya keamanan sistem yang baik atau ruangan server yang tidak memiliki tingkat keamanan yang tinggi.	
3	Faktor Alam dan Lingkungan	Bencana alam menyebabkan rusaknya aset baik dari perangkat lunak maupun perangkat keras sehingga data dapat hilang dan berhentinya proses bisnis yang sedang berlangsung.	a. Mempunyai *back-up server* di tempat lain yang lebih aman. b. Melakukan penyediaan cadangan infrastruktur baik *hardware* maupun perangkat jaringan. c. Melakukan perbaikan dan penambahan kapasitas generator set listrik. d. Membeli dan menggunakan UPS (uninterrupted power supply). e. Menyediakan alat pemadam kebakaran yang dapat digunakan ketika hal tersebut terjadi.
		Listrik padam dapat menyebabkan tidak adanya ketersediaan data sehingga menghambat proses bisnis yang berlangsung.	
		Kebakaran menyebabkan rusaknya aset baik dari perangkat lunak maupun perangkat keras sehingga data dapat hilang dan berhentinya proses bisnis yang sedang berlangsung.	

5.5 Tentukan Kemungkinan Insiden

Dalam hal menentukan nilai kemungkinan sebuah insiden digunakan kategori rendah dengan skor 0.1, sedang dengan skor 0.5, dan tinggi dengan skor 1.0.

Tabel 5. Kemungkinan Terjadinya Risiko pada Sistem Informasi Rumah Sakit EMC Tangerang

No	Sumber Kerentanan	Kerentanan	Kemungkinan
1	Sumber Daya Manusia	Miskomunikasi antar pegawai dalam transfer pengetahuan atau data sehingga menyebabkan kesalahan terhadap data yang dimasukkan.	Rendah (0.1)
		Ketidaktelitian pegawai dalam memasukan data sehingga *output* yang dihasilkan tidak valid.	Sedang (0.5)
		Pegawai yang tidak bertanggung jawab melakukan pembocoran data atau memberikan hak akses kepada orang yang tidak berwenang.	Tinggi (1.0)
		Pegawai kurang mengerti atau *skill* yang tidak mendukung terhadap penggunaan sistem informasi yang ada.	Sedang (0.5)
2	Faktor Sistem dan Infrastruktur	*Server down* akibat ketidaksiapan sistem informasi apabila diakses oleh banyak pengguna.	Sedang (0.5)
		Hilangnya data akibat tidak adanya *back up database* dari pihak rumah sakit.	Tinggi (1.0)
		Data yang *overload* karena redudansi data atau data yang sudah tidak dipakai, sehingga menumpuk pada penyimpanan *database* dan menyebabkan sistem yang lambat.	Sedang (0.5)
		Sistem diserang oleh virus karena tidak adanya *firewall* atau antivirus yang mendukung.	Tinggi (1.0)
		Pembobolan data diakibatkan kurangnya keamanan sistem yang baik atau ruangan server yang tidak memiliki tingkat keamanan yang tinggi.	Tinggi (1.0)
3	Faktor Alam dan Lingkungan	Bencana alam menyebabkan rusaknya aset baik dari perangkat lunak maupun perangkat keras sehingga data dapat hilang dan berhentinya proses bisnis yang sedang berlangsung.	Tinggi (1.0)
		Listrik padam dapat menyebabkan tidak adanya ketersediaan data sehingga menghambat proses bisnis yang berlangsung.	Sedang (0.5)
		Kebakaran menyebabkan rusaknya aset baik dari perangkat lunak maupun perangkat keras sehingga data dapat hilang dan berhentinya proses bisnis yang sedang berlangsung.	Tinggi (1.0)

5.6 Menilai Dampak yang Mungkin Terjadi pada Ancaman

Tabel 6. Nilai Dampak Terhadap Risiko

No	Risiko	Keterangan	Dampak
1	Miskomunikasi antar pegawai dalam transfer pengetahuan atau data sehingga menyebabkan kesalahan terhadap data yang dimasukkan.	Miskomunikasi berdampak sedang karena akan berpengaruh terhadap informasi yang nantinya akan diakses oleh para pengguna mengenai jadwal praktik dokter, pembuatan *appointment* fasilitas rumah sakit.	Sedang (50)
2	Ketidaktelitian pegawai dalam memasukan data sehingga *output*	Ketidaktelitian pegawai berdampak tinggi karena mempengaruhi operasional	Tinggi (100)

e-ISBN 978-623-93343-3-8
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 20 April 2021

	yang dihasilkan tidak valid.	seperti misalnya salah meng-*input* jadwal dokter.	
3	Pegawai yang tidak bertanggung jawab melakukan pembocoran data atau memberikan hak akses kepada orang yang tidak berwenang.	Pembocoran data atau memberikan hak akses kepada yang tidak berwenang berdampak tinggi karena data yang ada dalam sistem informasi merupakan data krusial salah satunya menyangkut informasi pribadi dokter dan pasien.	Tinggi (100)
4	Pegawai kurang mengerti atau *skill* yang tidak mendukung terhadap penggunaan sistem informasi yang ada.	Pegawai yang kurang mengerti atau *skill* tidak mendukung berdampak sedang karena hanya memperlambat proses tetapi tidak mengganggu proses bisnis secara fatal dan berkelanjutan.	Sedang (50)
5	*Server down* akibat ketidaksiapan sistem informasi apabila diakses oleh banyak pengguna.	*Server down* berdampak sedang karena hanya mengganggu ketidaksediaan sistem sesaat dan tidak memberikan efek jangka panjang.	Sedang (50)
6	Hilangnya data akibat tidak adanya *back up database* dari pihak rumah sakit.	Hilangnya data berdampak tinggi karena data yang ada merupakan sumber data utama (data master) sehingga apabila hilang akan mengganggu proses bisnis yang sedang berjalan.	Tinggi (100)
7	Data yang *overload* karena redudansi data atau data yang sudah tidak dipakai, sehingga menumpuk pada penyimpanan *database* dan menyebabkan sistem yang lambat.	Data yang *overload* berdampak sedang karena mengganggu jalannya sebuah sistem informasi menjadi lambat.	Sedang (50)
8	Sistem diserang oleh virus karena tidak adanya *firewall* atau antivirus yang mendukung.	Sistem yang diserang berdampak tinggi karena dapat memengaruhi sistem serta data yang ada, dapat dihilangkan dan dirusak.	Tinggi (100)
9	Pembobolan data diakibatkan kurangnya keamanan sistem yang baik atau ruangan server yang tidak memiliki tingkat keamanan yang tinggi.	Pembobotan data berdampak tinggi karena memengaruhi data bersifat krusial terutama data pribadi dokter dan pasien yang dapat digunakan untuk hal yang tidak bertanggung jawab.	Tinggi (100)
10	Bencana alam menyebabkan rusaknya aset baik dari perangkat lunak maupun perangkat keras sehingga data dapat hilang dan berhentinya proses bisnis yang sedang berlangsung.	Bencana alam berdampak tinggi karena dapat menyebabkan rusaknya perangkat lunak maupun perangkat keras yang dapat menyebabkan berhentinya proses bisnis yangsedang berlangsung, terlebih jika tidak mempunyai dokumentasi BCP dan DRP.	Tinggi (100)
11	Listrik padam dapat menyebabkan tidak adanya ketersediaan data sehingga menghambat proses bisnis yang berlangsung.	Listrik padam dapat berdampak sedang karena ketidaktersediaan data dalam waktu tertentu, namun dapat diatasi dengan *back up server* yang berada di tempat lain.	Sedang (50)
12	Kebakaran menyebabkan rusaknya aset baik dari perangkat lunak maupun perangkat keras sehingga data dapat hilang dan berhentinya proses bisnis yang sedang berlangsung.	Kebakaran berdampak tinggi karena dapat menyebabkan rusaknya perangkat lunak maupun perangkat keras yang dapat menyebabkan berhentinya proses bisnis yangsedang berlangsung, terlebih jika tidak mempunyai dokumentasi BCP dan DRP.	Tinggi (100)

e-ISBN 978-623-93343-3-8
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 20 April 2021

5.7 Prioritaskan Risiko Keamanan Informasi

Tabel 7. Prioritaskan Risiko Keamanan Informasi

No	Risiko	Nilai Kemungkinan	Nilai Dampak	Nilai Kemungkinan * Nilai Dampak
1	Miskomunikasi antar pegawai dalam transfer pengetahuan atau data sehingga menyebabkan kesalahan terhadap data yang dimasukkan.	Rendah (0.1)	Sedang (50)	0.1 * 50 = 5 (Rendah)
2	Ketidaktelitian pegawai dalam memasukan data sehingga *output* yang dihasilkan tidak valid.	Sedang (0.5)	Tinggi (100)	0.5 * 100 = 50 (Sedang)
3	Pegawai yang tidak bertanggung jawab melakukan pembocoran data atau memberikan hak akses kepada orang yang tidak berwenang.	Tinggi (1.0)	Tinggi (100)	1.0 * 100 = 100 (Tinggi)
4	Pegawai kurang mengerti atau *skill* yang tidak mendukung terhadap penggunaan sistem informasi yang ada.	Sedang (0.5)	Sedang (50)	0.5 * 50 = 25 (Sedang)
5	*Server down* akibat ketidaksiapan sistem informasi apabila diakses oleh banyak pengguna.	Sedang (0.5)	Sedang (50)	0.5 * 50 = 25 (Sedang)
6	Hilangnya data akibat tidak adanya *back up database* dari pihak rumah sakit.	Tinggi (1.0)	Tinggi (100)	1.0 * 100 = 100 (Tinggi)
7	Data yang *overload* karena redudansi data atau data yang sudah tidak dipakai, sehingga menumpuk pada penyimpanan *database* dan menyebabkan sistem yang lambat.	Sedang (0.5)	Sedang (50)	0.5 * 50 = 25 (Sedang)
8	Sistem diserang oleh virus karena tidak adanya *firewall* atau antivirus yang mendukung.	Tinggi (1.0)	Tinggi (100)	1.0 * 100 = 100 (Tinggi)
9	Pembobolan data diakibatkan kurangnya keamanan sistem yang baik atau ruangan server yang tidak memiliki tingkat keamanan yang tinggi.	Tinggi (1.0)	Tinggi (100)	1.0 * 100 = 100 (Tinggi)
10	Bencana alam menyebabkan rusaknya aset baik dari perangkat lunak maupun perangkat keras sehingga data dapat hilang dan berhentinya proses bisnis yang sedang berlangsung.	Tinggi (1.0)	Tinggi (100)	1.0 * 100 = 100 (Tinggi)
11	Listrik padam dapat menyebabkan tidak adanya ketersediaan data sehingga menghambat proses bisnis yang berlangsung.	Sedang (0.5)	Sedang (50)	0.5 * 50 = 25 (Sedang)
12	Kebakaran menyebabkan rusaknya aset baik dari perangkat lunak maupun perangkat keras sehingga data dapat hilang dan berhentinya proses bisnis yang sedang berlangsung.	Tinggi (1.0)	Tinggi (100)	1.0 * 100 = 100 (Tinggi)

5.8 Rekomendasi Kontrol

Tabel 8. Rekomendasi Kontrol Terhadap Risiko yang Ada

No	Risiko	Tingkat Risiko	Rekomendasi Kontrol
1	Miskomunikasi antar pegawai dalam transfer pengetahuan atau data sehingga menyebabkan kesalahan terhadap data yang dimasukkan.	Rendah (5)	a. Melakukan *cross check* atau validasi data terhadap data yang dimasukkan. b. Memperbaiki komunikasi antar pegawai agar tidak terjadi miskomunikasi lagi.
	Ketidaktelitian pegawai dalam memasukan data sehingga *output* yang dihasilkan tidak valid.	Sedang (50)	a. Melakukan *cross check* atau validasi data terhadap data yang dimasukkan. b. Membuat dan menjalankan SOP agar pegawai tahu lebih jelas peraturan dan sanksi di bidang kerjanya
	Pegawai yang tidak bertanggung jawab melakukan pembocoran data atau memberikan hak akses kepada orang yang tidak berwenang.	Tinggi (100)	a. Membuat dan menjalankan SOP agar pegawai tahu lebih jelas peraturan dan sanksi di bidang kerjanya. b. Melakukan pengecekan hak akses secara berkala. c. Melakukan seminar etika profesi.
	Pegawai kurang mengerti atau *skill* yang tidak mendukung terhadap penggunaan sistem informasi yang ada.	Sedang (25)	a. Melakukan budaya *sharing knowledge* agar setiap pegawai mempunyai level pemahaman yang sama. b. Melakukan pelatihan teknis agar setiap pegawai memiliki kemampuan yang sama dalam mengoperasikan sistem.
2	*Server down* akibat ketidaksiapan sistem informasi apabila diakses oleh banyak pengguna.	Sedang (25)	a. Melakukan *maintenance server* secara berkala. b. Memperhatikan suhu komputer server untuk menghindari *overhead.*
	Hilangnya data akibat tidak adanya *back up database* dari pihak rumah sakit.	Tinggi (100)	a. Menyediakan *back up database* bagi rumah sakit.
	Data yang *overload* karena redudansi data atau data yang sudah tidak dipakai, sehingga menumpuk pada penyimpanan *database* dan menyebabkan sistem yang lambat.	Sedang (25)	a. Penggunaan *Database Management System* yang bertujuan untuk mengontrol redundansi, sehingga data yang dipakai dapat konsisten dan tidak terdapat duplikasi data.
	Sistem diserang oleh virus karena tidak adanya *firewall* atau antivirus yang mendukung.	Tinggi (100)	a. Instalasi *firewall, antivirus, deep freeze.*
	Pembobolan data diakibatkan kurangnya keamanan sistem yang baik atau ruangan server yang tidak memiliki tingkat keamanan yang tinggi.	Tinggi (100)	a. Memantau sistem secara berkala untuk mencegah agar tidak terjadi aktivitas ilegal yang dilakukan oleh pihak yang tidak terotorisasi. b. Memiliki ruangan server sistem yang dilengkapi dengan sistem keamanan

e-ISBN 978-623-93343-3-8
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 20 April 2021

			yang tinggi (menggunakan pintu yang dapat diakses dengan *fingerprint*) guna mencegah pihak yang tidak berwenang dapat masuk ke ruangan tersebut. c. Menerapkan *Security Operation Center*.
3	Bencana alam menyebabkan rusaknya aset baik dari perangkat lunak maupun perangkat keras sehingga data dapat hilang dan berhentinya proses bisnis yang sedang berlangsung.	Tinggi (100)	a. Mempunyai *back up server* yang berada di tempat lain. b. Melakukan penyediaan cadangan infrastruktur baik *hardware* maupun perangkat jaringan.
	Listrik padam dapat menyebabkan tidak adanya ketersediaan data sehingga menghambat proses bisnis yang berlangsung.	Sedang (25)	a. Perbaikan dan penambahan kapasitas generator set listrik. b. Membeli dan menggunakan UPS (*uninterrupted power supply).*
	Kebakaran menyebabkan rusaknya aset baik dari perangkat lunak maupun perangkat keras sehingga data dapat hilang dan berhentinya proses bisnis yang sedang berlangsung.	Tinggi (100)	a. Rumah Sakit harus menyediakan alat pemadam kebakaran yang dapat digunakan ketika hal tersebut terjadi. b. Melakukan penyediaan cadangan infrastruktur baik *hardware* maupun perangkat jaringan

5.9 Dokumentasi Hasil

Tabel 9. Dokumentasi Hasil Penilaian Risiko Sistem Infromasi Rumah Sakit EMC Tangerang

No	Sumber Risiko	Risiko	Tingkat Risiko	Mitigasi
1	Sumber Daya Manusia	Miskomunikasi antar pegawai dalam transfer pengetahuan atau data sehingga menyebabkan kesalahan terhadap data yang dimasukkan.	Rendah (5)	a. Melakukan *cross check* atau validasi data terhadap data yang dimasukkan. b. Memperbaiki komunikasi antar pegawai agar tidak terjadi miskomunikasi lagi.
		Ketidaktelitian pegawai dalam memasukan data sehingga *output* yang dihasilkan tidak valid.	Sedang (50)	a. Melakukan *cross check* atau validasi data terhadap data yang dimasukkan. b. Membuat dan menjalankan SOP agar pegawai tahu lebih jelas peraturan dan sanksi di bidang kerjanya.
		Pegawai yang tidak bertanggung jawab melakukan pembocoran data atau memberikan hak akses kepada orang	Tinggi (100)	a. Membuat dan menjalankan SOP agar pegawai tahu lebih jelas peraturan dan sanksi di bidang

e-ISBN 978-623-93343-3-8
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 20 April 2021

		yang tidak berwenang.		pekerjanya. b. Melakukan pengecekan hak akses secara berkala. c. Melakukan seminar etika profesi.
		Pegawai kurang mengerti atau *skill* yang tidak mendukung terhadap penggunaan sistem informasi yang ada.	Sedang (25)	a. Melakukan budaya *sharing knowledge* agar setiap pegawai mempunyai level pemahaman yang sama. b. Melakukan pelatihan teknis agar setiap pegawai memiliki kemampuan yang sama dalam mengoperasikan sistem.
2	Faktor Sistem dan Infrastruktur	*Server down* akibat ketidaksiapan sistem informasi apabila diakses oleh banyak pengguna.	Sedang (25)	a. Melakukan *maintenance* secara berkala. b. Memperhatikan suhu komputer server untuk menghindari *overhead*.
		Hilangnya data akibat tidak adanya *back up database* dari pihak rumah sakit.	Tinggi (100)	a. Menyediakan *back up database* bagi rumah sakit.
		Data yang *overload* karena redudansi data atau data yang sudah tidak dipakai, sehingga menumpuk pada penyimpanan *database* dan menyebabkan sistem yang lambat.	Sedang (25)	a. Penggunaan *Database Management System* yang bertujuan untuk mengontrol redundansi, sehingga data yang dipakai dapat konsisten dan tidak terdapat duplikasi data.
		Sistem diserang oleh virus karena tidak adanya *firewall* atau antivirus yang mendukung.	Tinggi (100)	a. Instalasi *firewall, antivirus, deep freeze.*
		Pembobolan data diakibatkan kurangnya keamanan sistem yang baik atau ruangan server yang tidak memiliki tigkat keamanan yang tinggi.	Tinggi (100)	a. Memantau sistem secara berkala untuk mencegah agar tidak terjadi aktivitas ilegal yang dilakukan oleh pihak yang tidak terotorisasi. b. Memiliki ruangan server sistem yang dilengkapi dengan sistem keamanan yang tinggi (menggunakan pintu yang dapat diakses dengan *fingerprint*) guna mencegah pihak yang tidak berwenang dapat masuk ke ruangan tersebut. c. Menerapkan *Security Operation Center*.

3	Faktor Alam dan Lingkungan	Bencana alam menyebabkan rusaknya aset baik dari perangkat lunak maupun perangkat keras sehingga data dapat hilang dan berhentinya proses bisnis yang sedang berlangsung.	Tinggi (100)	a. Mempunyai *back up* server yang berada di tempat lain. b. Melakukan penyediaan cadangan infrastruktur baik *hardware* maupun perangkat jaringan.
		Listrik padam dapat menyebabkan tidak adanya ketersediaan data sehingga menghambat proses bisnis yang berlangsung.	Sedang (25)	a. Perbaikan dan penambahan kapasitas generator set listrik. b. Membeli dan menggunakan UPS (*uninterrupted power supply).*
		Kebakaran menyebabkan rusaknya aset baik dari perangkat lunak maupun perangkat keras sehingga data dapat hilang dan berhentinya proses bisnis yang sedang berlangsung.	Tinggi (100)	a. Rumah Sakit harus menyediakan alat pemadam kebakaran yang dapat digunakan ketika hal tersebut terjadi. b. Melakukan penyediaan cadangan infrastruktur baik *hardware* maupun perangkat jaringan

6 Kesimpulan

Berdasarkan penelitian yang dilakukan dengan cara melakukan penilaian risiko terhadap keberlangsungan sistem informasi Rumah Sakit EMC Tangerang dapat disimpulkan:

1. Pada langkah identifikasi dan prioritas aset penelitian ini mendeskripsikan berbagai prioritas aset sehingga Rumah Sakit EMC Tangerang tau aset-aset apa saja yang perlu diprioritaskan. Berdasarkan penelitian, prioritas aset dibagi menjadi tiga jenis atau kategori aset, yaitu perangkat keras, perangkat lunak dan data.
2. Pada penilaian risiko yang dilakukan terhadap sistem informasi Rumah Sakit EMC Tangerang, penelitian ini mendeskripsikan berbagai macam ancaman serta melakukan penentuan risiko, sehingga nantinya Rumah Sakit EMC Tangerang mengetahui risiko apa saja yang harus diprioritaskan untuk dilakukan mitigasi risiko. Berdasarkan penelitian risiko pada sistem informasi Rumah Sakit EMC Tangerang, terdapat beberapa risiko yang harus diprioritaskan atau memiliki nilai risiko yang tinggi diantaranya adalah kebocoran data yang disebablan oleh pemberian hak akses kepada orang yang tidak berwenang yang dilakukan oleh oknum pegawai yang tidak bertanggung jawab, hilangnya data akibat tidak adanya *back up database* yang dilakukan pihak RS EMC Tangerang, kerusakan pada sistem yang disebabkan oleh serangan virus karena pihak RS tidak melakukan pemasangan *firewall* yang mendukung, pembobolan data karena kurangnya keamanan pada sistem ataupun ruangan server dan risiko yang ditimbulkan dari bencana alam ataupun kebakaran yang menyebabkan rusaknya sistem secara keseluruhan.

Berdasarkan penelitian, mitigasi risiko yang harus dilakukan Rumah Sakit EMC Tangerang adalah dengan melakukan *back up database* dan *server* ditempat yang berbeda, memperkuat keamanan sistem informasi serta ruangan penyimpanan server, membuat dan menjalankan SOP bagi setiap aktivitas di RS EMC Tangerang, menyediakan *back up database* rumah sakit, melakukan pemantauan sistem secara berkala, serta melakukan penyediaan cadangan infrastruktur baik hardware maupun perangkat jaringan untuk menghindari risiko-risiko tinggi yang teridentifikasi.

Referensi

[1] Hopkin, P. (2010). Fundamentals Of Risks Management : Understanding, Evaluating and Implementing Effective Risk Management. London : Kogan Page.
[2] Darmawi, H. (2006). Manajemen Risiko. Jakarta : BumiAksara.
[3] Gibson, D. (2011). Managing Risk in Information Systems. Sudbury : Jones & Barlett Learning.
[4] Blokdijk, G, dkk. (2008). IT Risk Management Guide : RiskManagement Implementation Guide, Presentations, Blueprints, Templates. AU : Emereo Pty Limited
[5] Maulana, M. M., & Supangkat, S. H. (2006). Pemodelan Framework Manajemen Risiko Teknologi Informasi untuk Perusahaan di Negara Berkembang. *Prosiding Konferensi Nasional Teknologi Informasi & Komunikasi untuk Indonesia*, 121-126.