
Jurnal Politeknik Caltex Riau
Terbit Online pada laman https://jurnal.pcr.ac.id/index.php/jkt/
| e- ISSN : 2460-5255 (Online) | p- ISSN : 2443-4159 (Print) |

Analisis Risiko Sistem Informasi Pada RSIA Eria Bunda menggunakan Metode FMEA

Puja Hanifah[1], dan Jarot S.Suroso[2]

[1]Universitas Bina Nusantara, Magister Manajemen Sistem Informasi, email: pujahanifah@gmail.com
[2]Universitas Bina Nusantara, Magister Manajemen Sistem Informasi, email: jsembodo@binus.edu

Abstrak

Teknologi yang berkembang pesat pada bidang IT menjadi komponen penting dan saling melengkapi dalam pengolahan data dan informasi dalam sebuah organisasi. Banyak risiko-risiko yang mungkin terjadi yang akan mengancam organisasi. Oleh sebab itu, perlu dilakukan pengelolaan risiko terhadap ancaman – ancaman terhadap keamanan sistem informasi dan penilaian risiko. Terdapat banyak metode yang dapat digunakan dalam melakukan pengelolaan dan penilaian risiko. Salah satunya adalah metode FMEA (Failure Mode and Effect Analysis). Pada penelitian ini menggambil studi kasus di RSIA Eria Bunda. Sebagai industri yang bergerak dibidang kesehatan, RSIA Eria Bunda perlu menjaga kerahasian informasi mengenai data pasien, dokter, obat-obatan, dan staf lainya dari ancaman yang mungkin menimbulkan risiko yang dapat merugikan industri. Dimana tujuan penelitian untuk mengetahui bagaimana tingkatan risiko yang terjadi pada sistem informasi dan memberikan solusi mitigasi kepada RSIA Eria Bunda. Terdapat sepuluh tahapan dalam identifikasi dan penilaian risiko menggunakan metode FMEA. Sehingga dari hasil penelitian ini adalah terdapat satu aktivitas dengan kategori tinggi, enam aktivitas kategori sedang dan Sembilan belas aktivitas dengan kategori rendah.

Kata kunci: *Analisis Risiko, FMEA, RSIA Eria Bunda.*

Abstract

Technology that is rapidly developing in the IT field is an important and complementary component in processing data and information in an organization. There are many risks that may occur that will threaten the organization. Therefore, it is necessary to carry out risk management against threats to information system security and risk assessment. There are many methods that can be used in managing and assessing risk. One of them is the FMEA (Failure Mode and Effect Analysis) method. In this study, taking a case study at RSIA Eria Bunda. As an industry engaged in the health sector, RSIA Eria Bunda needs to maintain the confidentiality of information regarding patient data, doctors, medicines, and other staff from threats that may pose risks that can harm the industry. Where the research objective is to find out how the level of risk that occurs in the information system and provide mitigation solutions to RSIA Eria Bunda. There are ten stages in risk identification and assessment using the FMEA method. So from the results of this study there is one activity with a high category, 6 activities in the medium category and nineteen activities with a low category

Dokumen diterima pada September, 2020
Dipublikasikan pada November, 2020

Keywords: *Risk analysis, FMEA, RSIA Eria Bunda*.

1. Pendahuluan

Teknologi semakin berkembang khususnya pada bidang IT yang menjadi komponen penting dan pendukung dalam melakukan pengolahan data dan informasi yang sifatnya penting dalam operasional dari sebuah organisasi. Kehadiran IT sebaiknya didukung dengan sistem informasi yang matang, dimana sistem tersebut tidak rentan terhadap ancaman – ancaman yang mengganggu keamanaan data dan informasi yang dimiliki.

Terdapat banyak metode yang dapat digunakan dalam melakukan pengelolaan dan penilaian risiko. Salah satunya adalah metode FMEA (*Failure Mode and Effect Analysis*). Metode FMEA merupakan sebuah metodologi yang digunakan untuk mengevaluasi kegagalan terjadi dalam sebuah sistem, desain, proses, atau pelayanan (service). FMEA secara sistematis membantu untuk mengidentifikasi dan menilai (mode), penyebab (cause), dan dampak (effect) dari kegagalan suatu sistem sebelum itu terjadi. Hasil analisis dan penilaian tersebut akan membentuk peringkat dari setiap kegagalan sesuai dengan tingkat efek risiko dan probabilitas terjadinya [1].

FMEA biasanya sudah populer dibidang teknik industri, metode *failure* mode and effect analysis FMEA masih jarang yang dilaporkan dalam penelitiannya terhadap objek penelitian sistem informasi. Raden Budiarto (2017) melakukan penelitian yang mencakup perlindungan terhadap aset informasidilingkungan organisasi XYZ dengan melakukan penilaian risiko keamanan informasi. Dalam penilaian tersebut dilakukan penilaian menggunakan metode FMEA dan kerangka kerja ISO 27001 untuk melengkapi daftar rekomendasi penanggulangan mode kegagalan. Hasil dari penelitian ini berupa laporan hasil sebab dan permasalahan dan pengendalian risiko sesuai dengan standar ISO27001[2].

RSIA (Rumah Sakit Ibu dan Anak) Eria Bunda Pekanbaru merupakan rumah sakit ibu dan anak yang sebagian besar proses bisnis perusahaan yang berjalan telah menggunakan sistem informasi. kunjungan pasien di RSIA Eria bunda rata-rata meningkat. Maka diperlukan sebuah sistem yang handal yang dapat membantu proses bisnis yang berjalan disana. Sistem yang ada di RSIA Eria Bunda telah terintegrasi dan sekarang lagi mengalami transisi Selama transisi ada terjadi beberapa masalah yang muncul, masalah yang muncul datangnya manager, resignnya programmer yang membangun sistem, dan kesalahan yang dilakukan oleh *user* karena tidak semua dari mereka mengerti menggunakan sebuah sistem. Selain itu sistem mengalami *error* dan data pasien ada beberapa yang hilang setelah terjadi kesalahan sistem. [3].

Sebagai industri yang bergerak dibidang kesehatan, RSIA Eria Bunda perlu menjaga kerahasian informasi mengenai data pasien, dokter, obat-obatan, dan staf lainya dari ancaman yang mungkin menimbulkan risiko yang dapat merugikan industri. Dalam proses kegiatan di RSIA Eria Bunda, kegiatan dilakukan pada sistem pelayanan, dimana sistem pelayanan ini membantu berjalannya proses bisnis di ERIA Bunda. Dari proses pendaftaran, biaya adminstrasi, data riwayat pasien, dan lain-lain, sehingga banyak sekali informasi yang penting tersimpan di sistem ini. Sehingga ancaman dari luar dapat mempengaruhi proses bisnis yang ada. Untuk mengatasi itu, diperlukan manajemen keamanan sistem informasi untuk menjaga dan menjamin aset-aset perusahaan dari ancaman yang mungkin terjadi, serta menjaga kualitas pelayanan RSIA Eria Bunda.

Oleh Karena itu, dengan adanya pengelolaan dan penilaian risiko sistem informasi dengan menggunakan metode FMEA diharapkan dapat membantu sistem informasi pelayanan di RSIA Eria Bunda lebih baik lagi dalam mengidentifikasi ancaman, menganalisis risiko, penilaian dan penanganan risiko tersebut.

2. Tinjuan Pustaka

2.1 Manajemen Risiko

Manajemen risiko merupakan proses dengan tujuan untuk mendapatkan keseimbangan antara efisiensi dan merealisasikan peluang untuk mendapatkan keuntungan dan meminimalkan kerentanan dan kerugian. Manajemen risiko harus menjadi proses tanpa henti dan berulang yang terdiri dari beberapa fase, ketika diterapkan dengan benar, memungkinkan terjadinya perbaikan terus-menerus dalam pengambilan keputusan dan peningkatan kinerja [4].

2.2 Metode FMEA

Langkah-langkah dasar pengerjaan failure mode and effect analysis (FMEA) [5] yaitu:

1. Mengidentifikasi proses atau produk. Tim yang akan mengidentifikasi proses yang akan dianalisa, dapat mempertimbangkan diagram proses (flowchart) untuk memudahkan identifikasi proses FMEA.
2. Menganalisis kemungkinan setiap potensi mode kegagalan (potential failure mode) yang berpotensi dapat terjadi.
3. Menganalisis efek yang ditimbulkan dari terjadinya setiap potensi kegagalan (potential failure mode).
4. Menentukan peringkat atau ranking dari severity, occurrence, dan detection dengan skala penilaian dari 1 sampai 10.
5. Menghitung nilai Risk Priority Number atau RPN pada setiap potensi mode kegagalan (potential failure mode) dengan cara sebagai berikut:
   Risk Priority Number = Severity x Occurrence x Detection
6. Membuat daftar prioritas perbaikan untuk memperbaiki atau mencegah terjadinya potensi mode kegagalan (potential failure model)
7. Membuat analisis usulan perbaikan (recommended action).

3. Metode Penelitian

Metode penilaian Risiko menggunakan Metode FMEA. *Failure Mode and Effects Analysis* (FMEA) adalah cara terstruktur untuk mengidentifikasi dan mengatasi masalah potensial atau kegagalan pada sistem sebelum terjadi efek yang buruk terjadi. Tujuan FMEA adalah untuk mencegah terjadinya masalah pada produk dan proses. Dengan menggunakan desain dan proses manufaktur, maka hal tersebut akan mengurangi biaya dengan cara mengidentifikasi terutama pada peningkatan produk dan proses yang tidak membutuhkan banyak biaya dan mudah untuk dilakukan [5].

FMEA memiliki beberapa tahapan, yaitu:

- *Steps 1 - Review the Process*
- *Steps 2- Brainstorm potential failure modes*
- *Steps 3 – List potential effect of each failure*
- *Steps 4- Assign Severity rankings*
- *Steps 5 – Assign Occurence rankings*
- *Steps 6 – Assign Detection rankings*
- *Steps 7 – Calculate RPN*
- *Steps 8 – Develop the action plan*
- *Steps 9 – Take action to eliminate or reduce the high-risk failure modes*
- *Steps 10 – Calculate the resulting RPN*

4. Hasil Penelitian

Untuk meningkatkan kinerja sistem informasi yang merupakan bagian proses bisnis sistem RSIA Eria bunda, maka diperlukan analisis terhadap potensi - potensi kegagalan dan dampak dari kegagalan tersebut yang ada pada RSIA Eria Bunda.

3.1. *Review the process or product*

Pada tahapan ini dilakukan wawancara kepada IT staff yang berada di Eria Bunda untuk mengetahui bagaimana sistem pelayanan yang berjalan di Eria Bunda dan apa saja kendala yang didapatkan. Dari hasil wawancara didapatkan bahwa sistem yang sedang berjalan baru bermigrasi kurang lebih satu tahun ini. Selama proses migrasi dan sekarang, ada beberapa kesalahan yang terjadi.

4.1.1 Daftar Aset Kritis

Adapun daftar aset yang ada di RSIA Eria Bunda berdasarkan wawancara yang dilakukan adalah:

Tabel 1 Daftar Aset

Tabel Aset	
Aset Kritis	**Alasan / Sebab**
Data	Data-data yang terkait dengan proses bisnis RSIA Eria Bunda, seperti data pasien. Dokter, poli, ugd, apotik, dll
Jaringan	Jaringan digunakan untuk mengakses informasi.
Sistem RSIA Eria Bunda (Graphasoft)	Sistem yang mendukung berjalannya proses bisnis Eria Bunda, dalam satu sistem ini sudah terintegrasi dari satu unit ke unit yang lainnya.
SDM	Suatu aset yang penting, karena jika SDM handal maka semua proses bisnis dapat berjalan dengan lancer
Server	Komputer yang digunakan sebagai tempat penyimpanan data dan diakses oleh seluruh user yang membutuhkan data
Laptop / PC	Digunakan oleh setiap user setiap unitnya dalam kelangsungan bisnis proses

4.1.2 Hasil identifikasi risiko

Risiko yang didapatkan dilakukan dengan *Risk Breakdown Structure*, dimana pengelompokkan risiko berdasarkan kategori.

Tabel 2 Identifikasi Risiko RSIA Eria Bunda

Level 0	Level 1	Level 2	Level 3	RBS Code
Sistem RSIA Eria Bunda	Risiko Eksternal	Bencana Alam	Kebakaran	RBS-01
		Gangguan Fasilitas Umum	*Cybercrime*	RBS-02
			Power Failure	RBS-03
	Risiko Internal	Operasional	Sistem *error*	RBS-04
			Hardware rusak	RBS-05
			Network gagal	RBS-06
			Modifikasi dan Pencurian data	RBS-07

			Backup data gagal	RBS-08
			Human Error	RBS-09
			Ruangan yang tidak memadai	RBS-10
			Memory full	RBS-11
			Peyalahgunaan hak akses	RBS-12
			Pelanggaran terhadap peraturan yang berlaku	RBS-13

3.2. Brainstorm Potential Failure Modes

Kegagalan yang terjadi di sistem informasi yang menyebabkan proses bisnis yang ada dalam sebah perusahaan terganggu, maka diperlukan identifikasi kerentanan sistem informasi yang ada pada perusahaan. Berikut ini *failure mode* yang terdapat di perusahaan sesuai dengan hasil wawancara yang dilakukan kepada *user*, sebagai berikut:

Tabel 3 Potensi Failure Mode

RBS Code	Potensial Failure Mode
RBS-01	Hubungan arus pendek
RBS-02	Kuranganya keamanan rumah sakit
	Antivirus yang tidak *update*
RBS-03	Hubungan arus pendek
	Generator listrik yang tidak berfungsi
RBS-04	Kesalahan fungsi pada sistem
	Hardware yang tidak mendukung
RBS-05	Pemakaian tidak sesuai prosedur
	Maintenance yang tidak teratur
	Virus
	Human Error
RBS-06	Kabel LAN yang rusak/longgar
	Human Error
	Jaringan *Down*
RBS-07	*User* yang tidak berkepentingan berhasil *login* ke database dan melakukan perubahan data
RBS-08	Server Down
	Koneksi LAN terputus
RBS-09	Kesalahan penginputan data
	Data yang tersedia tidak update
	Kurangnya pengetahuan mengenai sistem
RBS-10	Server yang diletakin berbarengan dengan ruangan IT
RBS-11	Kapasitas yang sudah penuh
	Beban kerja server yang terlalu tinggi
RBS-12	Staf yang memberikan hak aksesnya kepada orang lain
	Password masing-masing staf jarang diganti
RBS-13	Kurangnya sosialisasi peraturan terhadap karyawan

3.3. List Potential Failure Mode

Kegagalan yang terjadi pada RSIA Eria Bunda menyebabkan menghambatnya proses bisnis yang sedang berjalanan. Adapun kegagalan yang terjadi di RSIA Eria Bunda adalah

Tabel 4 List Potential Failure di RSIA Eria Bunda

	RBS Code	Potensial Failure Mode
Sistem RSIA Eria Bunda (Graphasoft)	RBS-01	Hubungan arus pendek
	RBS-02	Antivirus yang tidak *update*
	RBS-03	Hubungan arus pendek
	RBS-04	Kesalahan fungsi pada sistem
		Hardware yang tidak mendukung
	RBS-05	Pemakaian tidak sesuai prosedur
		Maintenance yang tidak teratur
		Virus
		Human Error
	RBS-06	Kabel LAN yang rusak/longgar
		Human Error
		Jaringan *Down*
	RBS-08	Server Down
		Koneksi LAN terputus
	RBS-09	Kesalahan penginputan data
		Data yang tersedia tidak update
		Kurangnya pengetahuan mengenai sistem
	RBS-10	Server yang diletakin berbarengan dengan ruangan IT
	RBS-11	Kapasitas yang sudah penuh
		Beban kerja server yang terlalu tinggi
	RBS-12	Staf yang memberikan hak aksesnya kepada orang lain
		Password masing-masing staf jarang diganti
	RBS-13	Kurangnya sosialisasi peraturan terhadap karyawan

3.4. Assign a severity ranking for each effect

Berdasarkan hasil kuisioner yang dilakukan terhadap tiga belas staf, maka berikut ini merupakan hasil dari menentukan rating keparahan atau *severity* dari setiap potensi kegagalan yang ada pada sistem informasi tersebut.

Tabel 5 Tabel Severity di RSIA Eria Bunda

RBS Code	Potensi Kegagalan	Severity atau rating keparahan	Keterangan
RBS-01	Kebakaran	6	Sistem mengalami penurunan performa sehingga mempengaruhi output
RBS-02	Cybercrime	5	Mengalami penurunan kinerja secara bertahap
RBS-03	Power Failure	4	Efek yang kecil pada performa sistem
RBS-04	Sistem error	5	Mengalami penurunan kinerja secara bertahap
RBS-05	Hardware rusak	5	Mengalami penurunan kinerja secara bertahap
RBS-06	Network gagal	5	Mengalami penurunan kinerja secara bertahap
RBS-07	Modifikasi dan Pencurian data	5	Mengalami penurunan kinerja secara bertahap
RBS-08	Backup data gagal	5	Mengalami penurunan kinerja secara bertahap
RBS-09	Human Error	4	Efek yang kecil pada performa sistem
RBS-10	Ruangan yang tidak memadai	3	Sedikit berpengaruh pada kinerja sistem
RBS-11	Memory full	4	Efek yang kecil pada performa sistem

RBS-12	Peyalahgunaan hak akses	6	Sistem beroperasi dan aman tetapi mengalami penurunan performa sehingga mempengaruhi output
RBS-13	Pelanggaran terhadap peraturan yang berlaku	5	Mengalami penurunan kinerja secara bertahap

3.5. Assign an occurent ranking for each effect

Berdasarkan dari nilai yang telah dikumpulkan dan diberikan oleh responden, maka didapatkan nilai *occurent* untuk setiap kegagalan seperti Tabel 6.

Tabel 6 Tabel Occurent RSIA Eria Bunda

Potensi Kegagalan	Penyebab Kegagalan	Occurent
Kebakaran	Hubungan arus pendek	3
Cybercrime	Kuranganya keamanan rumah sakit	2
	Antivirus yang tidak *update*	4
Power Failure	Hubungan arus pendek	3
	Generator listrik yang tidak berfungsi	2
Sistem *error*	Kesalahan fungsi pada sistem	4
	Hardware yang tidak mendukung	4
Hardware rusak	Pemakaian tidak sesuai prosedur	3
	Maintenance yang tidak teratur	6
	Virus	5
	Human Error	5
Network gagal	Kabel LAN yang rusak/longgar	5
	Human Error	4
	Jaringan *Down*	4
Modifikasi dan Pencurian data	*User* yang tidak berkepentingan berhasil *login* ke database dan melakukan perubahan data	2
Backup data gagal	Server Down	3
	Koneksi LAN terputus	3
Human Error	Kesalahan penginputan data	5
	Data yang tersedia tidak update	5
	Kurangnya pengetahuan mengenai sistem	4
Ruangan yang tidak memadai	Server yang diletakin berbarengan dengan ruangan IT	4
Memory full	Kapasitas yang sudah penuh	4
	Beban kerja server yang terlalu tinggi	3
Penyalahgunaan hak akses	Staf yang memberikan hak aksesnya kepada orang lain	3
	Password masing-masing staf jarang diganti	4
Pelanggaran terhadap peraturan yang berlaku	Kurangnya sosialisasi peraturan terhadap karyawan	4

3.6. Assign a detection ranking for each effect

Berdasarkan dari nilai yang telah dikumpulkan dan diberikan oleh responden, maka didapatkan nilai *detection* untuk setiap kegagalan seperti Tabel 7.

Tabel 7 Tabel Deteksi RSIA Eria Bunda

Potensi Kegagalan	Penyebab Kegagalan	Identifikasi Pencegahan Saat ini	Detection
Kebakaran	Hubungan arus pendek	menyiapkan APAR	2
Cybercrime	Kuranganya keamanan rumah sakit	menggunakan *firewall* dan *security* keamanan	3
	Antivirus yang tidak *update*	*Update antivirus secara berkala dan menggunakan deepprize*	3
Power Failure	Hubungan arus pendek	Menyiapkan APAR	3
	Generator listrik yang tidak berfungsi	Melakukan pengecekan berkala	4
Sistem *error*	Kesalahan fungsi pada sistem	melakukan *maintanance*	3
	Hardware yang tidak mendukung	*update* hardware sesuai kebutuhan	3
Hardware rusak	Pemakaian tidak sesuai prosedur	memberikan penjadwalan penggunaan	3
	Maintenance yang tidak teratur	membuat jadwal *maintanance* yang berkala	3
	Virus	scan secara berkala dan *update* antivirus	4
	Human Error	memberikan SOP dan pelatihan	5
Network gagal	Kabel LAN yang rusak/longgar	melakukan *maintanance* secara berkala	4
	Human Error	perbaikan dilakukan oleh tenaga ahli	4
	Jaringan *Down*	melakukan pengecekan terhadap jaringan	4
Modifikasi dan Pencurian data	*User* yang tidak berkepentingan berhasil *login* ke database dan melakukan perubahan data	diberi sanksi kepada yang ketahuan memberikan hak aksesnya	5
Backup data gagal	Server Down	menggunakan backup server	3
	Koneksi LAN terputus	melakukan perbaikan kepada koneksi LAN	4
Backup data gagal	Kesalahan penginputan data	dalam sistem dikurangi penginputan secara manual, sehingga mengurangi kesalahan inputan	4
	Data yang tersedia tidak update	melakukan update data secara berkala	2
	Kurangnya pengetahuan mengenai sistem	memberikan penjelasan kepada mengenai sistem yang akan digunakan	4
Ruangan yang tidak memadai	Server yang diletakkan berbarengan dengan ruangan IT	menyediakan backup server	3
Memory full	Kapasitas yang sudah penuh	melakukan upgrade kapasitas	4
	Beban kerja server yang terlalu tinggi	membagi kerja server	4
Peyalahgunaan hak akses	Staf yang memberikan hak aksesnya kepada orang lain	diberi sanksi sesuai kebijakan RSIA	4
	Password masing-masing staf jarang diganti	mengingatkan *user* untuk melakukan *update password* secara berkala	5
Pelanggaran terhadap peraturan yang berlaku	Kurangnya sosialisasi peraturan terhadap karyawan	jika ada perubahan dari peraturan, maka laukan sosialisasi	5

3.7. Calculate RPN Value

Setelah kita menganalisa nilai *severity, occurrence dan detection*, maka tahapan selanjutnya adalah menentukan nilai RPN (*Risk Priority Number*). Untuk nilai maksimal dari RPN adalah 1000, karena setiap nilai maksimal dari *severity, occurent,* dan *detection* adalah 10. Sedangkan hasil RPN dari RSIA Eria Bunda dapat dilihat pada Tabel 8.

Tabel 8 Tabel RPN Eria Bunda

Potensi Kegagalan	Penyebab Kegagalan	RPN
Kebakaran	Hubungan arus pendek	36
Cybercrime	Kuranganya keamanan rumah sakit	30
	Antivirus yang tidak *update*	60
Power Failure	Hubungan arus pendek	36
	Generator listrik yang tidak berfungsi	32
Sistem *error*	Kesalahan fungsi pada sistem	60
	Hardware yang tidak mendukung	60

Hardware rusak	Pemakaian tidak sesuai prosedur	45
	Maintenance yang tidak teratur	90
	Virus	100
	Human Error	125
Network gagal	Kabel LAN yang rusak/longgar	100
	Human Error	80
	Jaringan *Down*	80
Modifikasi dan Pencurian data	*User* yang tidak berkepentingan berhasil *login* ke database dan melakukan perubahan data	50
Backup data gagal	Server Down	45
	Koneksi LAN terputus	60
Human Error	Kesalahan penginputan data	80
	Data yang tersedia tidak update	40
	Kurangnya pengetahuan mengenai sistem	64
Ruangan yang tidak memadai	Server yang diletakkan berbarengan dengan ruangan IT	36
Memory full	Kapasitas yang sudah penuh	64
	Beban kerja server yang terlalu tinggi	48
Penyalahgunaan hak akses	Staf yang memberikan hak aksesnya kepada orang lain	72
	Password masing-masing staf jarang diganti	100
Pelanggaran terhadap peraturan yang berlaku	Kurangnya sosialisasi peraturan terhadap karyawan	100

3.8. Prioritize the Failure Mode for Action

Setelah dilakukan perhitungan RPN, maka tahap selanjutnya dilakukan memprioritaskan risiko berdasarkan RPN yang didapatkan. Berikut ini daftar RPN yang diurutkan dari besar dan kecil.

Tabel 9 Nilai RPN RSIA Eria Bunda dari besar ke kecil

Potensi Kegagalan	Penyebab Kegagalan	RPN	Kategori
Hardware rusak	*Human Error*	125	High(tingggi)
Hardware rusak	Virus	100	Moderate (Sedang)
Network gagal	Kabel LAN yang rusak/longgar	100	Moderate (Sedang)
Penyalahgunaan hak akses	Password masing-masing staf jarang diganti	100	Moderate (Sedang)

Pelanggaran terhadap peraturan yang berlaku	Kurangnya sosialisasi peraturan terhadap karyawan	100	Moderate (Sedang)
Hardware rusak	*Maintenance* yang tidak teratur	90	Moderate (Sedang)
Network gagal	*Human Error*	80	Low(Rendah)
Network gagal	Jaringan *Down*	80	Low(Rendah)
Human Error	Kesalahan penginputan data	80	Low(Rendah)
Peyalahgunaan hak akses	Staf yang memberikan hak aksesnya kepada orang lain	72	Low(Rendah)
Human Error	Kurangnya pengetahuan mengenai sistem	64	Low(Rendah)
Cybercrime	Antivirus yang tidak *update*	60	Low(Rendah)
Sistem *error*	Kesalahan fungsi pada sistem	60	Low(Rendah)
Sistem *error*	Hardware yang tidak mendukung	60	Low(Rendah)
Sistem error	Hardware yang tidak mendukung	60	Low(Rendah)
Backup data gagal	Koneksi LAN terputus	60	Low(Rendah)
Modifikasi dan Pencurian data	User yang tidak berkepentingan berhasil login ke database dan melakukan perubahan data	50	Low(Rendah)
Memory full	Beban kerja server yang terlalu tinggi	48	Low(Rendah)
Hardware rusak	Pemakaian tidak sesuai prosedur	45	Low(Rendah)
Backup data gagal	Server Down	45	Low(Rendah)
Human Error	Data yang tersedia tidak update	40	Low(Rendah)
Power Failure	Hubungan arus pendek	36	Low(Rendah)
Ruangan yang tidak memadai	Server yang diletakkan berbarengan dengan ruangan IT	36	Low(Rendah)
Kebakaran	Hubungan arus pendek	36	Low(Rendah)
Power Failure	Generator listrik yang tidak berfungsi	32	Low(Rendah)
Cybercrime	Kuranganya keamanan rumah sakit	30	Low(Rendah)

3.9 Take Action to Elimination or Reduce High Risk Failure

Rencana Mitigasi risiko dari enam risiko yang yang menjadi perhatian dari RSIA Eria Bunda adalah:

a. *User Responsibilities*, ini sangat penting untuk mengurangi potensi kegagalan yang terjadi. pihak rumah sakit RSIA Eria Bunda harus dapat membuat para staff memiliki kesadaran untuk peduli terhadap apa saja yang dilakukan.

b. *User Access Management, Application Access control.* Aspek ini sangat berkaitan dengan keamanan dan penyalahangunaan hak akses yang dimiliki oleh staf. Sebaiknya dibuat dokumentasi terhadap pihak siapa saja yang memiliki kewenangan dan hak dalam mengakses dan mengelola suatu informasi atau sistem informasi yang ada diRSIA Eria Bunda. Tidak hanya itu,

peraturan dan prosedur dalam menambahkan dan mengurangi hak akses juga diberikan pada pihak yang memiliki wewenang tertinggi.

c. *Back up,* Aspek ini sangat penting dalam menjaga data yang akan digunakan aman dan tersedia. sebaiknya RSIA Eria bunda memiliki backup yang berada di tempat lain, dan melakukan penjadwalan *backup* secara berkala. Sehingga dapat membantu pihak RSIA Bunda dalam mencegah terjadinya ancaman yang dapat menggangu proses bisnis.

d. Perencanaan System dan penerimaan. Pada Aspek ini, RSIA Eria bunda sebaiknya memiliki bijakan dan peraturan terhadap penggunaan jasa vendor dalam melakukan pengembangan dan upaya keamanan informasi. Perencanaan dan peran vendor harus didokumentasikan dengan lengkap dan jelas sesuai dengan kebijakan yang dimiliki oleh RSIA Eria Bunda.

3.10. Calculate the resulting RPN

Ketika tindakan yang direkomendasikan merupakan cara untuk mengurangi kerentanan yang akan terjadi, maka nilai RPN pun akan mengalami penurunan. Setelah mendapatkan nilai RPN dari hasil perkalian severity, occurrence, dan detection, maka dilakukan evaluasi sehingga dapat diambil tindakan lebih lanjut untuk mengatasi masalah kegagalan dengan merujuk pada identifikasi pencegahan terkini.

5. Simpulan

Berdasarkan analisa penelitian yang telah dilakukan di RSIA Eria Bunda dapat disimpulkan bahwa:

1. Berdasarkan analisis FMEA yang telah dilakukan di RSIA Eria bunda didapatkan bahwa kegagalan dengan kategori tinggi ada 1 aktivitas, dengan kategori *moderate* (sedang) dengan 6 aktivitas, dan kategori *low* (rendah) sebanyak 19 aktivitas.
2. Adapun kegagalan yang perlu mendapatkan perhatian yang terjadi pada RSIA Eria Bunda setelah dilakukan penilaian dan pengukuran adalah
   a. *Hardware rusak* yang disebabkan oleh *human error* yang mendapatkan nilai RPN 125 dan dikategorikan tinggi.
   b. *Hardware rusak* yang disebabkan oleh virus yang mendapatkan nilai RPN 100 dan dikategorikan menengah.
   c. *Network gagal* yang disebabkan oleh kabel LAN yang rusak dengan nilai RPN 100 dan kategori menengah
   d. Penyalahgunaan hak akses yang disebabkan karena password yang jarang diganti dengan nilai RPN 100 dan kategori menengah
   e. Pelanggaran terhadap peraturan yang berlaku karena kurangnya sosialisai peraturan terhadap karyawan dengan nilai RPN 100 dan kategori menengah
   f. *Hardware rusak* yang disebabkan oleh waktu *maintenance* yang tidak teratur dengan nilai RPN 90 dan kategori menengah.
3. Mitigasi risiko yang dilakukan terhadap sistem informasi di RSIA Eria Bunda adalah
   a. Menumbuhkan rasa tanggung jawab terhadap aset yang dimiliki
   b. *Access Management, Application Access control.* Aspek ini sangat berkaitan dengan keamanan dan penyalahangunaan hak akses yang dimiliki oleh staf. Sebaiknya dibuat dokumentasi terhadap pihak siapa saja yang memiliki kewenangan dan hak dalam mengakses dan mengelola suatu informasi atau sistem informasi yang ada diRSIA Eria Bunda

c. RSIA Eria bunda memiliki backup yang berada di tempat lain, dan melakukan penjadwalan *backup* secara berkala. Sehingga dapat membantu pihak RSIA Bunda dalam mencegah terjadinya ancaman yang dapat menggangu proses bisnis.
d. RSIA Eria bunda sebaiknya memilili kebijakan dan peraturan terhadap penggunaan jasa vendor dalam melakukan pengembangan dan upaya keamanan informasi

Daftar Pustaka

[1] G. Setyadi and Y. Kusumawati, "Mitigasi Risiko Aset Dan Komponen Teknologi Informasi Berdasarkan Kerangka Kerja OCTAVE Dan FMEA Pada," *J. Inf. Syst.*, 2016.

[2] R. Budiarto, "Manajemen Risiko Keamanan Sistem Informasi," vol. 2, no. 2, pp. 105–115, 2017.

[3] R. S. I. dan A. E. Bunda, "Our Profile : Sejarah Berdirinya RSIA EriaBunda," 2018. .

[4] Task, J., & Transformation, F. (2011). Managing Information Security Risk, (March).

[5] McDermott, R. E., Mikulak, R. J., & Beauregard, M. R. B. (2009). *The Basics Of FMEA*.