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) |

Manajemen Risiko Teknologi Informasi Menggunakan Metode Fmea (Studi Kasus: Diskominfo Pemprov Riau)

Mutia Sari Zulvi[1]

[1]Politeknik Caltex Riau, Program Studi Sistem Informasi, email: mutia@pcr.ac.id[1]

Abstrak

Teknologi Informasi (TI) merupakan aspek penting bagi organisasi dalam mendukung setiap aktivitas bisnis. Penerapan TI mendukung terciptanya perubahan proses bisnis, pengurangan biaya operasional, meningkatkan kualitas layanan kepada konsumen, hingga pada akhirnya mendukung terhadap peningkatan kinerja organisasi. Saat ini TI dipandang tidak hanya sebatas sebagai alat bantu aktivitas bisnis saja, TI juga memiliki peranan terhadap pencapaian tujuan bisnis organisasi. Demi tercapainya tujuan tersebut perlu ditunjang dengan adanya pengelolaan TI yang memadai. Tentunya segala bentuk pemanfaatan dan pengolahan TI ini tidak bisa terlepas dari ancaman terhadap bentuk integritas data dan keamanan jaringan. Ancaman tersebut memerlukan manajemen risiko untuk kesuksesan / kelancaran pencapaiannya. Pemerintah Provinsi Riau sebagai bagian dari NKRI yang menyadari akan tuntutan perkembangan TIK sudah mempunyai banyak Sistem Informasi khususnya di Diskominfo. Berdasarkan hasil wawancara dengan staff IT Diskominfo, aset TI di Diskominfo belum memiliki manajemen risiko yang memadai dan optimal sehingga banyak problem yang dialami contohnya Hardware yang sering rusak karena tidak dirawat. Untuk mengatasi permasalahan tersebut, diperlukan manajemen risiko aset TI di Diskominfo. Tujuannya untuk meminimalisir terjadinya kerugian di Diskominfo. Terdapat berbagai metode untuk menganalisis manajemen risiko, salah satu yang banyak digunakan adalah FMEA (Failure Mode & Effect Analysis). Hasil Analisa yang didapatkan bahwa potensi kegagalan paling besar yaitu Hardware rusak karena Perawatan yang tidak berkala dan pemakaian tidak wajar sebesar RPN 144. Berdasarkan analisa yang dilakukan maka dapat diketahui potensi kegagalan apa saja yang memiliki nilai RPN tertinggi yang harus diprioritaskan terlebih dahulu.

Kata kunci: *Pemerintah Provinsi Riau, Sistem Informasi, Manajemen Risiko, FMEA*

Abstract

Information Technology (IT) is an important aspect for organizations in supporting every business activity. The application of IT supports the creation of business process changes, reduces operational costs, improves the quality of service to consumers, and ultimately supports the improvement of organizational performance. Currently IT is seen not only as a tool for business activities, IT also has a role in achieving organizational business goals. In order to achieve these goals, it is necessary to support adequate IT management. Of course, all forms of IT utilization and processing cannot be separated from threats to data integrity and network security. These

Dokumen diterima pada 24 Desember, 2021
Dipublikasikan pada 26 Desember, 2022

threats require risk management for success/smooth achievement. The Provincial Government of Riau as part of the Unitary State of the Republic of Indonesia, which is aware of the demands of ICT development, already has many Information Systems, especially in Diskominfo. Based on the results of interviews with Diskominfo IT staff, IT assets at Diskominfo do not yet have adequate and optimal risk management so that many problems are experienced, for example hardware which is often damaged because it is not maintained. To overcome these problems, IT asset risk management is required at Diskominfo. The goal is to minimize losses in Diskominfo. There are various methods for analyzing risk management, one of which is widely used is FMEA (Failure Mode & Effect Analysis). The results of the analysis found that the potential for failure is greatest, namely hardware damage due to irregular maintenance and improper use of RPN 144. Based on the analysis carried out, it can be seen which potential failure has the highest RPN value which must be prioritized first.

***Keywords**: Riau Provincial Government, Information Systems, Risk Management, FMEA*

---

1. Pendahuluan

Teknologi Informasi (TI) merupakan aspek penting bagi organisasi dalam mendukung setiap aktivitas bisnis. Penerapan TI mendukung terciptanya perubahan proses bisnis, pengurangan biaya operasional, meningkatkan kualitas layanan kepada konsumen, hingga pada akhirnya mendukung terhadap peningkatan kinerja organisasi. Saat ini TI dipandang tidak hanya sebatas sebagai alat bantu aktivitas bisnis saja, TI juga memiliki peranan terhadap pencapaian tujuan bisnis organisasi

Demi tercapainya tujuan tersebut perlu ditunjang dengan adanya pengelolaan TI yang memadai. Tentunya segala bentuk pemanfaatan dan pengolahan TI ini tidak bisa terlepas dari ancaman terhadap bentuk integritas data dan keamanan jaringan. Adapun bentuk-bentuk permasalahan tersebut dapat menimbulkan suatu ketidakpastian atau yang disebut risiko. Risiko tersebut dapat mempengaruhi tujuan organisasi. David Vose mengatakan bahwa risiko merupakan efek negatif berupa kerugian dari kejadian yang tidak terprediksi terhadap pencapaian suatu tujuan bisnis organisasi. Mulai data hilang, korup, virus serta dukungan TI perusahaan yang kurang diperbarui. Untuk meminimalisir efek dari risiko tersebut dapat diterapkan sebuah manajemen risiko atau pengukuran risiko. [10]

Menurut Emmett Vaughan dan Therese Vaughan, manajemen risiko adalah pendekatan secara ilmiah untuk mengatasi segala risiko dengan cara mencegah kerugian yang terjadi serta menerapkan metode atau prosedur yang mampu meminimalisir terjadinya kerugian. [9]

Pemerintah Provinsi Riau sebagai bagian dari Negara Kesatuan Republik Indonesia (NKRI) yang menyadari akan tuntutan perkembangan TIK sudah mempunyai banyak Sistem Informasi khususnya di Diskominfo. Untuk mengetahui risiko TI di sebuah perusahaan, tentu saja diskominfo mempunyai aset informasi mulai dari *hardware, software*, sistem informasi hingga manusia merupakan aset yang paling penting bagi suatu organisasi maupun perusahaan yang harus dilindungi dari risiko keamanannya mulai dari luar hingga dalam organisasi. Tapi dalam implementasinya, Diskominfo sangat jarang sekali melakukan manajemen risiko TI. Seperti kurangnya maintenance pada komputer, beberapa komputer yang mempunyai spesifikasi bagus jarang dugunakan karena beberapa pegawai ada yang menggunakan laptop pribadi selama bekerja.

Untuk mengatasi permasalahan tersebut, diperlukan manajamemen risiko dalam kelancaran dan kesuksesan mencapai tujuan bisnis. Terdapat berbagai metode untuk menganalisis manajemen risiko, salah satu yang banyak digunakan adalah FMEA (*Failure Mode & Effect Analysis*) [10].

Penelitian akan berfokus pada Manajemen Risiko IT di Diskominfo menggunakan Metode FMEA. Penelitian ini diharapkan menghasilkan rekomendasi kontrol atau penilaian risiko yang perlu diterapkan pada sistem informasi, kebijakan keamanan dan standar operasional prosedurnya.

2. Landasan Teori

2.1 *IT Risk Assessment*

Risk assessment adalah metode yang digunakan untuk menentukan dan meminimalisir risiko yang akan terjadi pada organisasi. Metode ini digunakan dalam perencanaan pemulihan sebuah bencana atau kerugian. Tahapan dalam melakukan manajemen risiko, mulai dari proses menganalisis dan menafsirkan kemungkinan-kemungkinan terburuk atau risiko yang akan terjadi. Risiko adalah efek negatif dari adanya suatu kegiatan yang menimbulkan kerugian. [1]

2.2 Tahapan Identifikasi *Risk Assessment*

Berikut merupakan tahapan Identifikasi *Risk Assessment* [1]:

1. Mengidentifikasi Sebuah Risiko

Diperlukan sebuah identifikasi pada setiap komponen-komponennya. Identifikasi yang dilakukan harus mencakup berbagai informasi risiko dari dalam dan luar kendali organisasi.

2. Menganalisis Sebuah Risiko

Tahapan selanjutnya adalah mengenali dan menganalisis karakteristik dari suatu risiko. Selain itu, juga dapat menentukan tingkatan dari sebuah risiko yang akan datang. Dalam menganalisis berbagai risiko yang akan terjadi, ada beberapa hal yang harus dilihat, mulai dari pertimbangan dari risiko, konsekuensi yang akan ditimbulkan dan tingkat keamanannya.

3. Memberikan Evaluasi Terhadap Risiko

Terakhir adalah evaluasi risiko. Dalam hal ini berguna untuk membantu berbagai pihak ketika akan mengambil suatu keputusan. Hal tersebut dilakukan berdasarkan apa yang ada di analisis risiko. Setelah risiko evaluasi, risiko akan diprioritaskan, mulai dari risiko dengan tingkatan yang menimbulkan kerugian paling besar.

2.3 Metode *Failure Mode and Effects Analysis* (FMEA)

Menurut Gaspersz (2002), *Failure Mode and Effects Analysis* (FMEA) merupakan metode analisa risiko yang digunakan untuk mengidentifikasi bagaimana komponen komponen di organisasi seperti peralatan ataupun sistem dapat gagal beroperasi serta akibat yang dapat ditimbulkan dari kegagalannya. Hasil FMEA berupa rekomendasi untuk perbaikan risiko yang akan terjadi guna meningkatkan tingkat keselamatan peralatan, fasilitas ataupun sistem. Berikut ini adalah langkah-Langkah FMEA.

Langkah	Deskripsi
1	Menentukan proses yang mempunyai resiko tinggi dan membentuk tim (*Select a high-risk process and assemble a team*) ... lihat HFMEA Decision Tree
2	Menyusun diagram proses (*Diagram the process*)
3	*Brainstorming potential failure modes* dan akibat-akibat yang ditimbulkan (*Brainstorm potential failure modes and determine their effects*)
4	Menentukan prioritas *failure modes* (*Prioritize failure modes*) ... lihat Langkah Penetapan Prioritas berdasarkan *Risk Priority Number* (RPN)
5	Identifikasi akar penyebab masalah dari *failure modes* (*Identify root causes of failure modes*)
6	Membuat rancangan ulang proses (*Redesign the process*)
7	Analisa dan pengujian proses baru (*Analyze and test the new process*)
8	Implementasi dan monitoring rancangan ulang proses (Implement and monitor the new process)

Gambar 1. langkah-Langkah *Failure Mode and Effect Analysis* [6]

3. Metode Penelitian

3.1 Pengumpulan dan Pengolahan Data

Metode penilaian Risiko menggunakan Metode *Failure Mode and Effects Analysis* (FMEA) adalah cara untuk mengidentifikasi dan mengatasi masalah kegagalan pada sistem sebelum terjadi kerugian pada organisasi. Tujuan FMEA adalah untuk mencegah terjadinya masalah pada komponen 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].

3.2 Review Proses

Pada tahapan ini dilakukan wawancara kepada IT staff yang berada di Diskominfo untuk mengetahui apa saja kendala yang didapatkan. Dari hasil wawancara didapatkan bahwa terdapat beberapa kesalahan ataupun permasalahan yang terjadi.

Adapun daftar aset yang ada di Diskominfo Pemprov Riau beserta alasan aspek tersebut dijadikan aspek kritis:

Tabel 1. Daftar Aset Kritis di Diskominfo Pemprov Riau

Aset Kritis	Alasan
Jaringan	Jaringan digunakan untuk mengakses berbagai informasi.
Sistem yang ada di Diskominfo Pemprov Riau	Sistem – sistem yang mendukung berjalannya proses bisnis Diskominfo.
Data	Data-data yang terkait dengan proses Diskominfo Pemprov Riau.
Sumber Daya Manusia (SDM)	Merupakan aset yang penting, karena dengan adanya SDM yang cakap dan handal maka kelangsungan proses bisnis dapat berjalan dengan lancar.
Server	Aset TI yang digunakan sebagai tempat untuk menyimpan data dan dapat diakses oleh seluruh user.
Laptop/ Komputer	Digunakan setiap user dalam kelangsungan proses bisnis.

Dari aset kritis pada tabel diatas, akan dirumuskan risiko yang akan terjadi dan dirumuskan menggunakan sebuah variabel dependen yakni RPN (*Risk Priority Number*) dan tiga variabel *Independent* yakni *occurrence, severity* dan *detection*. Nilai RPN merupakan hasil kali dari variabel *occurrence, severity* dan *detection*. Besaran variabel *occurrence, severity* dan *detection* adalah nilai skala ordinal dari 1 sampai 10.

3.3 Identifikasi Potensi Failure Mode

Kagagalan - 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. Identifikasi *failure mode* di dapatkan dengan cara wawancara yang dilakukan kepada user responden sejumlah 5 orang.

3.4 Penyebab Kegagalan Potensial

Berdasarkan hasil wawancara yang dilakukan dengan 1 orang staf, didapatkan penyebab kegagalan – kegagalan potensial yang terjadi di Diskomnfo, yaitu:
Berdasarkan hasil wawancara yang dilakukan dengan sembilan orang staf, didapatkan penyebab kegagalan – kegagalan potensial yang terjadi di Diskominfo, yaitu:

a. Listrik Padam,
b. Human Error, adalah kesalahan yang dilakukan oleh manuasia baik secara sengaja atau tidak sengaja yang dapat merugikan perusahaan.
c. Pemakaian yang tidak sesuai,

d. Perawatan yang tidak berkala
e. Virus

3.5 Identifikasi efek kegagalan potensial

Kegagalan – kegagalan yang terjadi pada Diskominfo menyebabkan terhambatnya proses bisnis yang sedang berjalan. Kegagalan dan hambatan tersebut antara lain:

1. Sistem yang error atau rusak kadang - kadang suka terjadi. Apabila sistem yang digunakan error atau rusak, maka tindakan yang dilakukan adalah me-*restart* PC, sehingga membutuhkan waktu yang cukup lama untuk menghidupkan kembali PC yang digunakan, dan pegawai pun berhenti bekerja sembari menunggu PC hidup.
2. Server yang tiba tiba mati karena listrik padam, efeknya pengguna sistem membutuhkan waktu yang sedikit banyak untuk menunggu sistem atau aplikasi dapat berjalan seperti semula.
3. Kerusakan yang lain terjadi pada hadware, yang biasanya sering menggalami kerusakan adalah mouse dan keyboard, ini suka diganti lebih kurang empat sampai enam bulan sekali.
4. Selain itu kerusakan juga terjadi pada saat listrik padam, banyak PC yang rusak termasuk PC Client. Kerusakan pada PC client yang menyebabkan petugas terganggu dalam menjalankan tugasnya.
5. Sering bermasalahnya kabel LAN (*Local Area Network*) bisa menghambat pekerjaan yang dilakukan karena membutuhkan waktu yang cukup lama dalam menjalankan proses.
6. Spesifikasi PC klien yang tidak memadai menyebabkan prosesnya lama karena PC lelet saat mengoperasikan PC tersebut.
7. Yang terakhir adalah ruang server yang tidak memadai tempatnya jika dilihat dari besar ruangan, suhu ruangan, kelembapan dan kebersihan ruangan. Ruang server saat ini kecil dan dapat dijangkau serta dilihat dari luar oleh staf lain. Standarnya ruang server jauh dari staf dan tidak bisa dilihat oleh staf lain kecuali Teknisi IT.

Kerusakan dan hambatan diatas sangat sulit diatasi Teknisi dengan cepat, jika dilihat dari Teknisi IT yang tidak semua ada di Kantor Organisasi Perangkat Daerah (OPD), hanya Teknisi IT pusat yang menangani banyak kerusakan atau hambatan yang berkaitan dengan IT di 40 an OPD. Hambatan lain tidak ada nya SOP atau tupoksi yang jelas jika terjadi kerusakan atau hambatan pada IT, sehingga Teknisi kebingungan saat terjadi kerusakan kecil hingga besar.

3.6 Menentukan Severity dan Rating Keparahan

Berdasarkan hasil wawancara yang dilakukan terhadap 1 orang staf, maka berikut ini merupakan hasil dari menentukan rating keparahan atau severity dari setiap potensi kegagalan yang ada pada Tabel 2.

Tabel 2. Hasil Severity

No	Potensi Kegagalan	Severity atau rating keparahan
1	Sistem Error	4
2	*Hardware* rusak	6
3	Komputer Client rusak	3
4	Kabel LAN rusak / longgar	3
5	Kapasitas jaringan lemot	3
6	Ruangan server yang tidak tersedia	7

Dilihat pada tabel 6, tingkat keparahan yang mungkin terjadi potensi kegagalan dan menimbulkan kerugian yang besar adalah ruangan server yang tidak tersedia dan *Hardware* rusak. Dari hasil wawancara yang didapatkan, jika ruangan server tidak memadai dan bisa dijangkau oleh banyak orang bahkan tidak aman dari bencana maka seluruh sistem ataupun database akan *down*. Akibatnya kelangsungan proses bisnis pun berhenti. Begitu juga dengan hardware rusak.

3.7 Menentukan *Occurent* atau Rating Kejadian

Kuisioner telah disebarkan kepada 5 orang staf untuk menghitung nilai *occurrent* terhadap masing-masing potensial.

Tabel 3. Hasil Occurent

No	Potensi Kegagalan	Penyebab Kegagalan	*Occurent*
1	Sistem Error	Listrik padam	6
		Human Eror	5
2	*Hardware* rusak	Pemakaian yang tidak wajar	6
		Perawatan yang tidak berkala	6
		Human Eror	5
3	Komputer klien rusak	Pemakaian yang tidak wajar	7
		Human Eror	7
		Virus	7
4	Kabel LAN rusak / longgar	Human Eror	7
		Kabel LAN rusak	7
5	Kapasitas jaringan lemot	Kapasitas yang disediakan kurang	5
		Banyak staf yang membuka aplikasi lain yang memakan *bandwith* banyak	5
6	Ruangan server yang belum memadai	Tidak adanya waktu untuk melakukan perpindahan server.	3
		Kurangnya perancanaan kedepan	4

Dilihat pada tabel 3, tingkat *occurent* yang paling besar adalah komputer klien rusak dan kabel LAN rusak / longgar. Dari hasil wawancara yang didapatkan, jika komputer klien rusak maka akibatnya kelangsungan proses bisnis pun terhambat. Begitu juga dengan kabel LAN yang sering rusak / longgar, internet pun akan bermasalah dan mengganggu jalannya kelangsungan proses bisnis.

3.8 Identifikasi pencegahan yang telah dilakukan

Berdasarkan hasil wawancara terhadap 5 orang staf, diperoleh informasi pencegahan yang telah dilakukan terhadap kegagalan, yaitu:

Tabel 4. Identifikasi Pencegahan

No	Potensi Kegagalan	Penyebab Kegagalan	Identifikasi pencegahan saat ini
1	Sistem Error	Listrik padam	UPS, server backup
		Human Eror	Pelatihan
2	*Hardware* rusak	Pemakaian yang tidak wajar	Jadwal pemakaian
		Perawatan yang tidak berkala	Jadwal *maintenance*
		Human Eror	Memberikan penjelasan penggunaan.
3	Komputer klien rusak	Pemakaian yang tidak wajar	Penjadwalan pemakaian
		Human Eror	Memberikan penjelasan penggunaan
		Virus	Menggunakan *deepprize* dan antivirus
4		Human Eror	Teguran dan sanksi

	Kabel LAN rusak / longgar	Kabel LAN rusak	Jadwal cek peralatan dan perbaikan
5	Kapasitas jaringan lemot	Kapasitas yang disediakan kurang	Menambah kapasitas
		Banyak staf yang membuka aplikasi lain yang memakan *bandwith* banyak	Membatasi aplikasi yang dibuka dan diberi teguran.
6	Ruangan server yang belum memadai	Tidak adanya waktu untuk melakukan perpindahan server.	Mem*backup* server secara berkala
		Kurangnya perancanaan kedepan	Membuat perancangan kedepan yang jelas.

Dilihat pada tabel 4, terdapat pencegahan yang sudah pernah dilakukan oleh staf Diskominfo tapi pencegahan tersebut belum maksimal.

3.9 Identifikasi Metode Deteksi

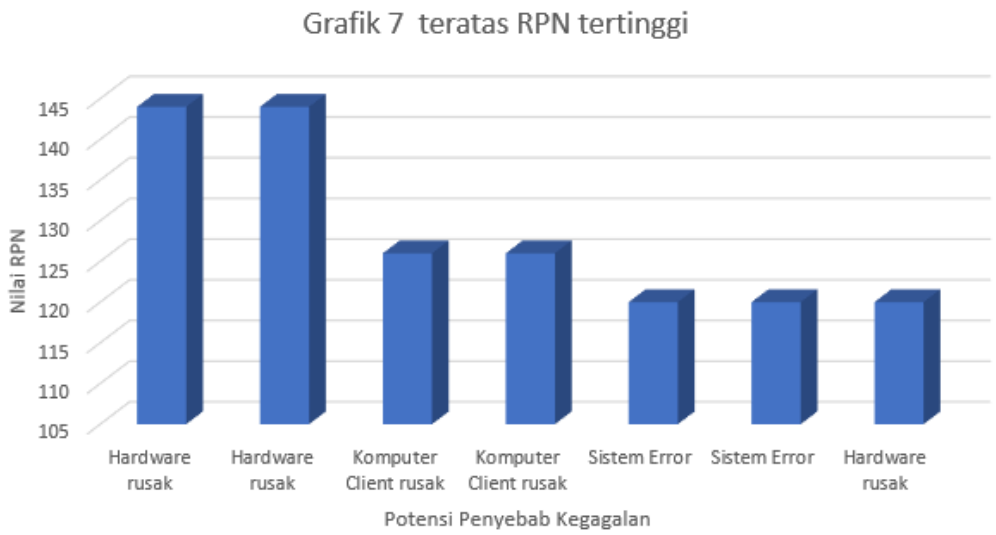
Kuisioner telah disebarkan kepada 5 orang staf untuk menghitung nilai *occurrent* terhadap masing-masing potensial. Detail perhitungan dapat dilihat pada lampiran. sedangkan untuk hasil *Occurent* dapat dilihat pada tabel dibawah ini.

Tabel 5. Hasil Deteksi

No	**Potensi Kegagalan**	**Penyebab Kegagalan**	**Identifikasi pencegahan saat ini**	**Deteksi**
1	Sistem Eror	Listrik padam	UPS, server backup	5
		Human Eror	Pelatihan	6
2	*Hardware* rusak	Pemakaian yang tidak wajar	Jadwal pemakaian	4
		Perawatan yang tidak berkala	Jadwal *maintenance*	4
		Human Eror	Memberikan penjelasan penggunaan.	4
3	Komputer klien rusak	Pemakaian yang tidak wajar	Penjadwalan pemakaiann	6
		Human Eror	Memberikan penjelasan penggunaan	6
		Virus	Menggunakan *deepprize* dan antivirus	5
4	Kabel LAN rusak / longgar	Human Eror	Teguran dan sanksi	4
		Kabel LAN rusak	Jadwal cek peralatan dan perbaikan	5
5	Kapasitas jaringan lemot	Kapasitas yang disediakan kurang	Menambah kapasitas	4
		Banyak staf yang membuka aplikasi lain yang memakan bandwith banyak	Membatasi aplikasi yang dibuka dan diberi teguran.	5
6	Ruangan server yang belum memadai	Tidak adanya waktu untuk melakukan perpindahan server.	Mem*backup* server secara berkala	4
		Kurangnya perancanaan kedepan	Membuat perancangan kedepan yang jelas.	4

3.10 Menghitung *Risk Priority Number* (RPN)

Setelah kita menganalisa nilai keparahan, kegagalan dan deteksi, maka tahapan selanjutnya adalah menentukan nilai RPN *(Risk Priority Number)*. Nilai RPN didapatkan dengan mengkalikan nilai keparahan, kegagalan dan deteksi, dimana nilai RPN yang didapatkan tinggi maka diperlukan prioritas tertinggi untuk dilakukan tindakan lebih lanjut. Berikut ini adalah hasil perhitungan RPN yang ditampilkan 7 RPN tertinggi.



Gambar 2. Grafik Tujuh teratas RPN tertinggi

3.11. Prioritas Risiko dari RPN

Setelah dilakukan perhitungan RPN, maka tahap selanjutnya dilakukan memprioritaskan risiko berdasarkan RPN yang didapatkan. Berikut ini daftar RPN yang diurutkan dari besar dan kecil. Dan RPN terbesar / high akan diprioritaskan terlebih dahulu karena akan menimbulkan kerugian yang besar.

Tabel 6. Prioritas Risiko dari RPN

No.	Potensi Kegagalan	Penyebab Kegagalan	RPN	
1	*Hardware* rusak	Perawatan yang tidak berkala	144	*High* (Tinggi)
2	*Hardware* rusak	Pemakaian yang tidak wajar	144	*High* (Tinggi)
3	Komputer klien rusak	Pemakaian yang tidak wajar	126	*Moderate* (Sedang)
4	Komputer klien rusa	Human Eror	126	*Moderate* (Sedang)
5	Sistem Eror	Listrik padam	120	*Low* (Rendah)
6	Sistem Eror	Human Eror	120	*Low* (Rendah)
7	*Hardware* rusak	Human Eror	120	*Low* (Rendah)

3.12 Analisis FMEA (*Action Plan*)

Dari hasil wawancara yang dilakukan di Diskominfo didapatkan beberapa potensi kegagalan yang muncul seperti sistem eror, *hardware* rusak, komputer klien rusak, kabel LAN rusak/longgar, kaspistas jaringan lemot dan ruang server yang belum memadai. Potensi kegagalan ini dapat menyebabkan bisnis proses dari Diskominfo tidak dapat berjalan dengan semestinya, sehingga dibutuhkan semua analisa risiko dengan menggunakan metode FMEA untuk membantu managerial disana untuk mengatasi potensi kegagalan. Berikut ini adalah penjelasan dari proses analisis:

1. Sistem Eror, dapat menyebabkan bisnis proses berjalan lambat. Ini disebabkan oleh beberapa penyebab yaitu:

a. Listrik Padam. Rekomendasi yang dapat digunakan adalah menggunakan generator set (genset) yang dapat hidup secara otomatis, meskipun sekarang sudah menggunakan genset jika listrik padam tapi hidup secara manual, karena genset dimiliki oleh Bagian Biro Umum (1 genset untuk 40 an OPD). Jika terdapat genset masing masing OPD atau 1 genset yang hidup otomatis. Maka semakin cepat hidup, genset akan mengurangi risiko yang terjadi.
b. Human Error, nilai RPN adalah 120. Sebenarnya tindakan memberikan memberikan pelatihan sudah sesuai karena menambah pengetahuan dari pihak – pihak yang terlibat, tetapi lebih baik jika ketika perekrutan pegawai juga mempertimbangan keahlian dalam menggunakan komputer dan berpengalaman.

2. *Hardware* rusak dapat mengganggu sebagian aktivitas proses bisnis yang berlangsung. Adapun penyebab yang ditimbulkan adalah sebagai berikut:

a. Pemakaian yang tidak wajar, ini disebabkan karena kurang pedulinya pengguna dengan barang yang digunakan. Dengan melakukan penjadwalan penggunaan seperti pencegahan yang dilakukan sudah dapat meminimalisir risiko, tetapi lebih baik jika barang yang digunakan disesuaikan kapasitas dan kemampuannya, seperti PC yang digunakan selama 24 jam menggunakan spesifikasi yang lebih bagus dari PC yang digunakan hanya untuk 8 jam pekerjaan.
b. Perawatan yang dilakukan tidak berkala. Rekomendasi yang dapat dilakukan adalah membuat kebijakan/SOP untuk peremajaan *hardware* yang sudah tidak layak digunakan.
c. Human Eror. Rekomendasi yang dapat dilakukan adalah membuat selalu melakukan soasialisasi jika ada *hardware* baru yang datang dan melakukan sosialiasi kepada pegawai baru.

3. Komputer klien rusak, kegagalan ini mempengaruhi aktivitas dari proses bisnis, contohnya jika yang rusak adalah komputer bagian yang menangani data covid, maka proses yang lainnya akan terganggu karena pencegahan tiap hari dilihat berdasarkan data covid. Adapun penyebab dari potensi kegagalan ini adalah:

a. Pemakaian yang tidak wajar. Rekomendasi yang dapat diberikan adalah terap melakukan penjadwalan sehingga penggunaan komputer sesuai waktu kerja.
b. Human Eror. Rekomendasi yang dapat diberikan adalah dengan sering melakukan sharing pengalaman dan penjelasaan penggunaan.
c. Virus. Rekomendasi yang dapat diberikan adalah selalu melakukan *update* antivirus secara berkala dan menggunakan antivirus yang asli atau berbayar.

4. Kabel LAN longgar atau rusak dapat mempengaruhi kinerja seperti server dan para client karena semuanya saling berhubungan dalam proses memberi dan menerima data. Adapun penyebab dari kegagalan tersebut adalah:

a. Human Eror. Rekomendasi yang didapat diberikan adalah memberikan pelatihan dan penggunaan mengenai jaringan dan sistem informasi.
b. Kabel LAN rusak. Rekomendasi yang didapat diberikan adalah memberikan pelatihan dan pengunaan mengenai jaringan.

5. Kapasitas jaringan lemot ini dapat mengganggu kinerja dalam bekerja yang menyebabkan pekerjaan menjadi melambat. Adapun penyebab yang menyebabkan potensi kegagalan ini terjadi adalah:

a. Kapasitas yang diberikan kurang. Dimana evalusi yang dilakukan sudah dapat mencegah risiko terjadi.

b. Banyaknya staf yang membuka aplikasi lain. Rekomendasi yang didapat diberikan adalah dengan memberikan teguran dan membangun kebijakan dan aturan (SOP) penggunaan aplikasi dan komputer.

6. Ruang server yang belum memadai dan backup server yang tidak ada dapat menyebabkan aktivitas dari bisnis proses berhenti. Adapun penyebab dari kegagalan tersebut adalah:

a. Tidak adanya waktu untuk melakukan perpindahan server. Rekomendasi yang dapat diberikan adalah pindahkan ruangan server ke ruangan standar server dan memiliki server backup diluar ruangan / ditempat lain.

5. Simpulan

Dari hasil penelitian didapatkan kesimpulan sebagai berikut:
Berdasarkan analisa yang telah dilakukan dapat disimpulkan bahwa:

1. FMEA diagram membantu pihak managemen dalam menganalisa risiko dengan nilai RPN yang didapatkan.
2. Berdasarkan analisis FMEA yang telah dilakukan, didapatkan bahwa potensi kegagalan paling besar adalah *Hardware* rusak karena Perawatan yang tidak berkala dan pemakaian tidak wajar sebesar 144.
3. Berdasarkan analisa yang dilakukan maka dapat diketahui potensi kegagalan apa saja yang memiliki nilai RPN tertinggi yang harus diprioritaskan terlebih dahulu.

Daftar Pustaka

[1] Cooper, D., S. Grey, G. Raymond and P. Walker. Project Risk Management Guidelines: Managing Risk in Large Projects and Complex Procurements, Chichester, West Sussex: John Wiley & Sons Ltd. (2004).

[2] Gaspersz, V. Pedoman implementasi program six sigma terintegrasi dengan ISO 9001:2000, MBNQA dan HACCP. Gramedia pustaka utama, Jakarta. (2002).

[3] Marimin, D. T. et al. Teknik dan Analisis Pengambilan Keputusan FUZZY Dalam Manajemen Rantai Pasok, IPB Press, Bogor. (2013).

[4] Martin, H and L. Priscila. "The World technological capacity to store, communicate and compute information," Science, vol. 332, no. 6025, pp. 60-65. (2011).

[5] Pratiwi, Vanny, Arie Desrianty dan Yuniar. Usulan Sistem Manajemen Keselamatan dan Kesehatan Kerja Berdasarkan Hasil Analisis. Jurusan Teknik Industri Itenas | No.03 | Vol.02: Jurnal Online Institut Teknologi Nasional Risk Assessment. (2014).

[6] Pyzdek, T. The six-sigma handbook. Selemba Empat, Jakarta. (2002).

[7] S. Lipol, L. "Risk Analysis Method: FMEA in the Organizations," International Journal of Basic & Applied Sciences IJBAS, vol. XI, no. 5, pp. 49-57. (2011).

[8] Siswanto, A. Risk Management. Surabaya: Balai Hiperkes dan Keselamatan Kerja Jawa Timur. (2009).

[9] Vaughan, E. and T. Vaughan. Fundamentals of Risk and Insurance, New Jersey: Wiley. (2013).

[10] Vose, D. Risk Analysis: A Quantitative Guide, 3rd ed., New Jersey: Wiley. (2008).