Techno.COM, Vol. 16, No. 4, November 2017 : 367-377

Strategi Mitigasi Risiko Aset Kritis Teknologi Informasi Menggunakan Metode Octave Dan FMEA

Risk Mitigation Strategy Of Critical Asset Information Technology Using Octave And FMEA Method

Alvina Hendika Putri[1], Yupie Kusumawati[2]
[1,2]Jurusan Sistem Informasi, Universitas Dian Nuswantoro, Semarang
Jl. Nakula I, No. 5-11, Semarang, Kode Pos 50131, Telp (024) 3520165, Fax: 3569684
e-mail: [1*]112201304871@mhs.dinus.ac.id, [2]yupie@dsn.dinus.ac.id

Abstrak

Pengelolaan risiko dengan baik sangat berpengaruh terhadap proses bisnis perusahaan. SMC RS Telogorejo merupakan salah satu rumah sakit yang memiliki banyak aset TI di dalamnya untuk menunjang proses bisnis utamanya. Permasalahan yang sering dialami adalah kerusakan yang terjadi pada aset TI akibat proses kontrol dan maintenance yang belum dilakukan secara rutin dan adanya serangan dari hacker. Kejadian tersebut mengakibatkan semua kegiatan operasional terganggu dan kadang terhenti. Tujuan dari penelitian ini adalah untuk mengetahui apa saja aset TI yang ada di perusahaan, menganalisa risiko yang terjadi pada setiap aset TI dan mengetahui mitigasi apa saja yang perlu dilakukan apabila risiko tersebut terjadi pada aset TI. Metode penelitian yang digunakan adalah Octave untuk mengelola risiko aset TI dan FMEA untuk melakukan penilaian terhadap masing-masing risiko, yang kemudian diranking berdasarkan prioritasnya. Hasil yang diperoleh dalam peneltian ini adalah 0 risiko very high, 0 risiko high, 0 risiko medium, 9 risiko low, 36 risiko very low. Walaupun hanya diperoleh risiko dengan level low dan very low, namun tetap dilakukan mitigasi guna perbaikan Sistem Manajemen Keamanan Informasi perusahaan.

Kata kunci— Aset Kritis, Octave, FMEA, Mitigasi Risiko, Teknologi Informasi

Abstract

Good risk management greatly affect the company's business processes. SMC Telogorejo Hospital is one of hospital that has a lot of IT assets in it to support the main business processes. The problem that is often occured is the damage to the IT assets as a result of process control and maintenance that have not been done regularly and attacks from hackers. The incident caused all operations disrupted and sometimes stalled. The purpose of this research is to find out what IT assets in the company, analyzing the risks that occur on any IT assets and determine what measures are needed if these risks occur on IT assets. This research use Octave method to manage IT assets and FMEA risk to assess the individual risk, which are then ranked based on their priority. The results obtained in this research are at very high risk 0, 0 high risk, medium risk 0, 9 low risk, very low risk 36. Although the risk was only obtained with low and very low level, but still do the mitigation to improve Information Security Management System.

Keywords— Critical Assets, Octave, FMEA, Risk Mitigation, Information Tecnology

1. PENDAHULUAN

Saat ini teknologi informasi menjadi salah satu hal yang tidak terpisahkan dari suatu perusahaan atau organisasi dalam mendukung dan meningkatkan proses bisnisnya. Teknlogi informasi juga dapat memberikan kemudahan bagi para penggunanya dalam berbagai bidang kehidupan, karena segala hal yang terlibat di dalamnya sebagian besar tidak terlepas dari sentuhan teknologi yang ada. Namun perkembangan teknologi informasi yang kian hari kian pesat dapat memberikan dampak positif serta negatif di dalamnya, agar penggunaannya dapat berjalan dengan maksimal diperlukan adanya pengelolaan TI yang baik dan benar supaya keberadannya mampu membantu perusahaan atau organisasi dalam mencapai tujuannya.

Beberapa sektor yang telah menerapkan teknologi informasi ke dalam proses bisnisnya antara lain sektor pemerintahan, finansial, telekomunikasi, pendidikan, dan bahkan sektor kesehatan pun tak luput dari pemanfaatan TI untuk menunjang proses bisnisnya. Pada sektor kesehatan salah satu rumah sakit yang memanfaatkan teknologi informasi sebagai pendukung proses bisnisnya agar dapat melayani pasien dengan maksimal adalah Semarang Medical Center (SMC) Rumah Sakit Telogorejo.

Setiap aset TI yang menjadi aset penting SMC RS Telogorejo, pasti memiliki risiko apabila tidak dilakukan perawatan dan penanganan yang tepat. Langkah pencegahan pun perlu diambil untuk meminimalisir terjadinya risiko, agar proses bisnis di dalam SMC RS Telogorejo tidak terganggu dan bisa berjalan dengan baik.

Risiko sendiri merupakan suatu keadaan yang tidak pasti, dimana jika terjadi suatu keadaan yang tidak dikehendaki bisa menimbulkan sebuah kerugian yang mungkin akan terjadi pada masa mendatang. Risiko tersebut diidentifikasi, dinilai, dan selanjutnya disusun langkah strategis yang dapat digunakan dalam mengatasi risiko tersebut [1].

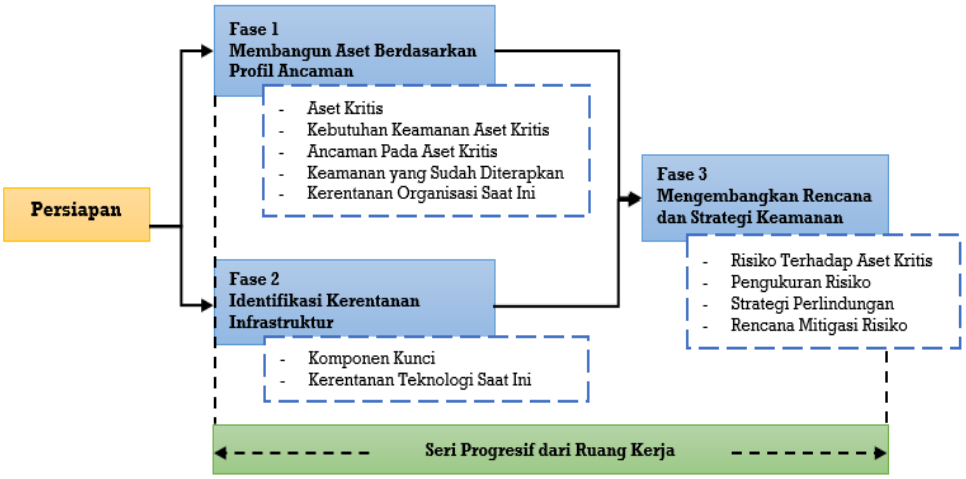
SMC RS Telogorejo sudah memperoleh sertifikasi ISO 9001 versi 2008 pada bulan April tahun 2009, sehingga sudah dipastikan SMC RS Telogorejo sudah memiliki kualitas yang bagus dalam mutu dan pelayanannya [2]. Salah satu bagian di SMC RS Telogorejo yang memiliki tanggung jawab untuk mengelola seluruh aset teknologi informasi milik perusahaan adalah Departemen IT, mulai dari melakukan kontrol dan *maintenance*, *instalasi* dan pengembangan perangkat lunak hingga proses pengumpulan dan pengamanan data dilakukan oleh Departemen IT, namun belum diterapkan manajemen risiko guna penanganan dan mitigasi risiko pada tiap aset teknologi informasi milik perusahaan. Terbukti dengan adanya aset teknologi informasi yang sering mengalami kerusakan karena kurangnya proses kontrol dan *maintenance*, serta adanya serangan dari *hacker* yang mengacaukan sistem kerja jaringan. Beberapa metode yang sering digunakan untuk mengelola dan memitigasi risiko aset kritis teknologi informasi adalah OCTAVE dan FMEA. Terdapat tiga jurnal penelitian terkait yang relevan dengan penelitian ini, dimana jurnal pertama hanya menggunakan metode FMEA [3], jurnal kedua menggabungkan kedua metode yaitu OCTAVE dan FMEA [4], dan jurnal ketiga hanya menggunakan metode OCTAVE [5]. Ketiga jurnal tersebut menggunakan metode OCTAVE dan FMEA untuk mengidentifikasi dan melakukan penilaian risiko, salah satu dari dua penelitian sebelumnya pun menggunakan kombinasi metode yang sama, sehingga dapat disimpulkan bahwa metode OCTAVE dan FMEA cukup efektif digunakan untuk melakukan identifikasi, pembobotan atau penilaian, serta perencanaan untuk mitigasi risiko terhadap aset kritis teknologi informasi yang dimiliki perusahaan. Kedua metode tersebut akan diterapkan pada Semarang Medical Center (SMC) Rumah Sakit Telogorejo, sehingga diharapkan dapat membantu pihak rumah sakit dalam mengidentifikasi risiko ancaman yang terjadi pada aset kritis TI yang mungkin akan terjadi, sehingga dapat dilakukan kontrol yang sesuai dengan standar ISO 27002.

2. METODE PENELITIAN

Pada penelitian kali ini metode pengambilan data yang digunakan adalah dengan studi literatur dan wawancara sehingga menghasilkan data kualitatif.

2.1 Dasar Teori

Dalam manajemen risiko terdapat beberapa kerangka kerja yang biasa digunakan oleh perusahaan, salah satunya adalah OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) yang digunakan untuk mengidentifikasi dan mengelola risiko keamanan informasi [6]. Berikut merupakan tahapan dan proses dari metode Octave :



Gambar 1 Fase Octave [7]

Selanjutnya untuk melakukan proses penilaian risiko digunakan metode FMEA (*Failure Mode and Effect Analysis*) agar menghasilkan RPN (*Risk Priority Number*). RPN diperoleh berdasarkan perkalian 3 variabel faktor penilaian risiko, diantaranya *Severity* (besarnya dampak kegagalan), *Occurence* (intensitas kegagalan), dan *Detection* (kemampuan kontrol) [8]. Berikut adalah rumus yang digunakan untuk menghitung nilai RPN :

$$RPN = Severity * Occurence * Detection \quad \text{.....(1)}$$

Hasil dari penilaian risiko tersebut kemudian dirangking untuk menentukan prioritas dan level risiko.

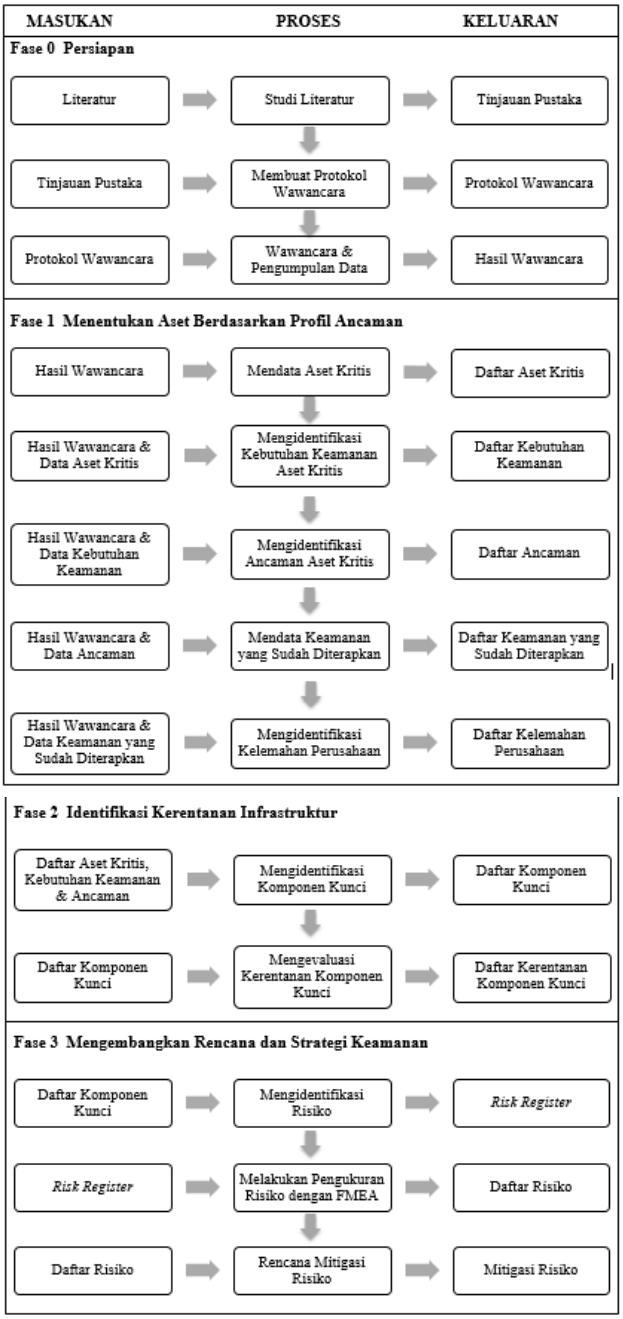
2.2 Metode Analisis

Pada penelitian ini penulis menggunakan dua metode analisis, diantaranya adalah :

1. Metode OCTAVE digunakan untuk mengidentifikasi risiko berdasarkan data yang sudah diperoleh.
2. Metode FMEA digunakan untuk memberikan penilaian dan pembobotan risiko terhadap aset kritis teknologi informasi yang sudah di identifikasikan dengan metode Octave [9].

2.3 Langkah – Langkah Penelitian

Metode analisis pada penelitian ini akan digambarkan melalui diagram alur sebagai berikut :



Gambar 2 Diagram Alur Metode Analisis

Fase Persiapan

1. Studi literatur

   Studi literatur dilakukan untuk mendapatkan informasi dari beberapa sumber seperti jurnal, buku, *e-book*, atau situs *online* mengenai manajemen risiko teknologi informasi dan metode yang digunakan dalam penelitian serta mitigasi risiko.

2. Membuat Interview Protocol

   Interview protokol dibuat untuk mengajukan daftar pertanyaan terkait penelitian terhadap pihak perusahaan berdasarkan studi literatur yang telah dilakukan sebelumnya.

3. Wawancara dan Pengumpulan Data
   Wawancara dilakukan untuk mengumpulkan data dan menggali informasi lebih mendalam lagi seputar perusahan terkait dengan penelitian yang sedang dilakukan.

Fase 1 Menentukan Aset Berdasarkan Profil Ancaman

1. Mendata aset kritis
   Aset kritis diperoleh dari wawancara yang sudah dilakukan dengan pihak terkait di perusahaan.
2. Mengidentifikasi kebutuhan keamanan aset kritis
   Berdasarkan hasil wawancara yang sudah dilakukan sebelumnya, maka akan dilakukan identifikasi mengenai kebutuhan keamanan pada masing-masing aset kritis teknologi informasi di perusahaan tersebut.
3. Mengidentifikasi ancaman aset kritis
   Identifikasi ancaman terhadap aset kritis dilakukan dengan mengacu pada hasil analisis kebutuhan kemanan aset kritis di perusahaan.
4. Mendata keamanan yang sudah diterapkan
   Pendataan dilakukan berdasarkan hasil wawancara yang sudah dilakukan sebelumnya kepada pihak terkait.
5. Mengidentifikasi kelemahan perusahaan
   Proses identifikasi kelemahan perusahaan dilakukan berdasarkan hasil wawancara yang sudah dilakukan sebelumnya kepada pihak terkait.

Fase 2 Identifikasi Kelemahan Infrastruktur

1. Mengidentifikasi komponen kunci
   Berdasarkan data aset penting, kebutuhan keamanan dan daftar ancaman yang sudah di peroleh tahap berikutnya adalah melakukan identifikasi komponen penting dari masing-masing aset kritis.
2. Mengevaluasi kerentanan komponen kunci
   Evaluasi kerentanan dari masing-masing komponen kunci dilakukan setelah memperoleh daftar komponen kunci pada proses sebelumnya.

Fase 3 Mengembangkan Rencana dan Strategi

1. Mengidentifikasi risiko
   Proses identifikasi risiko dilakukan pada komponen penting yang berkaitan dengan aset kritis perusahaan yang dapat mempengaruhi proses bisnis perusahaan. Identifikasi risiko ini dilakukan berdasarkan hasil identifikasi dan evaluasi yang sebelumnya telah dilakukan.
2. Melakukan pengukuran risiko
   Pengukuran risiko dilakukan dengan menggunakan metode FMEA berdasarkan daftar kemungkinan risiko yang telah dibuat sebelumnya. Dari hasil penilaian risiko ini nantinya dapat diketahui seberapa besar tingkat risiko yang dihadapi perusahaan. Pengukuran risiko dengan metode FMEA didasari oleh 3 faktor yaitu *Severity, Occurrence, Detection*. Nilai dari masing-masing faktor kemudian dikalian, nantinya akan diperoleh Risk Priority Number. Kemudian risiko dikategorikan berdasarkan levelnya.
3. Rencana mitigasi risiko
   Rencana mitigasi risiko dibuat berdasarkan ISO 27001 dan ISO 27002, untuk melakukan pengamanan terhadap masing-masing komponen aset kritis perusahaan dari risiko yang mungkin dapat terjadi.

3. HASIL DAN PEMBAHASAN

Berikut merupakan uraian hasil penelitian yang diperoleh berdasarkan studi literatur dan wawancara yang sudah dilakukan pada SMC RS Telogorejo :

3.1 Mendata Aset Kritis

Dari proses wawancara yang sudah dilakukan guna penggalian data dan informasi, diperoleh data aset kritis teknologi informasi yang dimiliki oleh SMC RS Telogorejo.

Tabel 1 Daftar Aset Kritis TI

Kategori Aset	**Aset Kritis**
Hardware	*Server*
	Server IVR (*Interactive Voice Response*)
	Server PABX (*Private Automatic Branch Exhange*)
	Switch
	Manage switch
	Accesspoint
	Manage accesspoint
	Kabel LAN
	UPS
	PC
	Printer
	Printer label
	Printer karcis
	Core Switch
	PACS (*Picture Archiving and Communication System*) *Server*
	LIS (*Location Information Server*) *Server*
Software	OS *microsoft*
	OS *server*
	Antivirus ESET
	LIS (*Location Information Server*)
	PACS (*Picture Archiving and Communication System*)
	HIS (*Hospital Information System*)
People	Admin IT dan Jaringan
	Admin *Database*
	Admin Sistem
	IT *Support*
	Software Develompment
	Analyst Programmer
Data	Data pasien
	Data karyawan
	Data dokter
	Data keuangan
	Data Obat
Network	Jaringan internet
	Jaringan intranet
Procedure	SOP (*Standart Operational Procedure*)

3.2 Mengidentifikasi Kebutuhan Keamanan

Identifikasi kebutuhan keamanan dilakukan pada tiap aset kritis TI perusahaan dengan menyertakan CIA Triad, yaitu *Confidentiality* (kerahasiaan), *Integrity* (Integritas), dan *Availability* (Ketersediaan) [10]. Berikut merupakan daftar kebutuhan keamanan pada masing-masing aset kritis.

Tabel 2 Daftar Kebutuhan Keamanan Aset Kritis

Aset Kritis	Kebutuhan Keamanan	CIA Triad
Server, Server IVR, *Server* PABX, PACS *Server,* LIS *Server*	Pemasangan CCTV di ruang *server*	*Confidentiality*
	Adanya kontrol secara rutin	*Availability*
	Adanya proses *backup* data secara berkala	*Availability*
	Pemasangan mesin *fingerprint* atau mesin gesek kartu pada pintu ruangan server	*Confidentiality*
	Pemasangan pendingin ruangan di ruang *server*	*Availability*
	Perlindungan *server* dari serangan *hacker*	*Confidentiality*
	Pembatasan hak akses dan penggantian *password* secara berkala	*Confidentiality*
Switch¸Manage Switch, Core Switch	Adanya kontrol secara rutin	*Availability*
Accesspoint, Manage Accesspoint	Adanya kontrol secara rutin	*Availability*
Kabel LAN	Adanya pelindung kabel	*Availability*
UPS	Adanya kontrol secara rutin	*Availability*
PC	Adanya kontrol secara rutin	*Availability*
	Memberikan *password* pada semua PC	*Confidentiality*
	Memberikan antivirus pada semua PC	*Integrity*
	Memberikan batasan hak akses USB	*Integrity*
Printer, Printer Label, Printer Karcis	Adanya kontrol secara rutin	*Availability*
OS *Microsoft,* OS *Server*	Sistem operasi meggunakan lisensi yang resmi	*Integrity*
	Melakukan *update* sistem operasi secara berkala	*Availability*
Antivirus ESET	Melakukan *update* antivirus secara berkala	*Availability*
LIS, PACS, HIS	Adanya pembatasan hak akses	*Integrity*
Admin IT dan Jaringan, Admin *Database,* Admin Sistem, IT *Support, Software Development, Analyst Programmer*	Adanya pelatihan	*Availability*
	Adanya aturan kerja	*Availability*
Data Pasien, Data Karyawan, Data Dokter, Data Keuangan, Data Obat	Menerapkan batasan hak akses dan pemberian *password* pada lokasi penyimpanan data	*Confidentiality*
	Adanya *backup* data secara berkala	*Availability*
Jaringan Internet, Jaringan Intranet	Adanya pengecekan jaringan secara berkala	*Availability*

Aset Kritis	Kebutuhan Keamanan	CIA Triad
	Pemasangan *firewall*	*Confidentiality*
SOP	Didokumentasikan dengan baik	*Availability*

3.3 Mengidentifikasi Ancaman Aset Kritis

Proses identifikasi ancaman dilakukan pada masing-masing aset kritis TI milik perusahaan disertai dengan penyebab dari terjadinya ancaman tersebut.

3.4 Mendata Keamanan Yang Sudah Diterapkan

Berdasarkan wawancara yang sudah dilakukan kepada pihak SMC RS. Telogorejo tindakan keamanan yang sudah diterapkan yaitu pemasangan CCTV, pembatasan penggunaan USB, *backup* data, pelatihan karyawan, penggunaan antivirus dan OS berlisensi, pemasangan mesin *fingerprint* di ruang *server*, pemberian hak akses pada *server*, dan pemasagan alat pendeteksi suhu ruangan dan tegangan listrik.

3.5 Mengidentifikasi Kelemahan Perusahaan

Ditemukan beberapa kelemahan dalam mengamankan aset kritis TI yang dimiliki, diantaranya adalah belum terelisasinya DRC (*Disaster Recovery Center*) dan belum terlaksananya *maintenance* secara rutin.

3.6 Mengidentifikasi Komponen Kunci

Komponen kunci di identifikasikan berdasarkan data aset kritis TI yang sekiranya menjadi komponen pendukung proses bisnis utama.

Tabel 3 Daftar Komponen Kunci

Kategori Aset	Komponen Kunci
Hardware	*Server*, *Server* IVR (*Interactive Voice Response*), *Server* PABX (*Private Automatic Branch Exhange*), *Manage switch, Manage accesspoint,* PC, *Core Switch,* PACS (*Picture Archiving and Communication System*) *Server,* LIS (*Location Information Server*) *Server*
Software	OS *microsoft,* OS *server,* LIS (*Location Information Server*), PACS (*Picture Archiving and Communication System*), HIS (*Hospital Information System*)
People	IT *Support, Software Develompment, Analyst Programmer*
Data	*Database*
Network	Jaringan internet, Jaringan intranet

3.7 Mengevaluasi Kerentanan Komponen Kunci

Evaluasi kerentanan yang mungkin terjadi dilakukan hanya pada masing-masing komponen kunci TI yang dimiliki oleh SMC RS. Telogorejo. Masing-masing aset memiliki evaluasi kerentanan yang berbeda seperti pada tabel berikut :

Tabel 4 Evaluasi Kerentanan Komponen Kunci

Komponen Utama	Kerentanan
Server, Server IVR, *Server* PABX, PACS *Server,* LIS *Server*	Serangan DOS
Manage switch, Manage accesspoint, Core Switch	Serangan *hacker*
PC	Virus
OS *microsoft*, OS *server*	Penggunaan OS yang tidak berlisensi
LIS, PACS, HIS	Serangan *hacker*
IT *Support, Software Development, Analyst Programmer*	*Social Engineering*
Database	*SQL Injection*
Jaringan internet, Jaringan intranet	Terputusnya koneksi jaringan

3.8 Mengidentifikasi Risiko

Proses identifikasi risiko dilakukan untuk mengetahui dampak dan penyebab dari risiko yang nantinya dapat terjadi terhadap aset kritis TI.

3.9 Melakukan Pengukuran Risiko Dengan FMEA

Pengukuran risiko dilakukan dengan menggunakan metode FMEA (*Failure Modes and Effect Analysis*) sehingga menghasilkan nilai RPN (*Risk Priority Number*). RPN diperoleh dari hasil perkalian antara S, O, dan D, dimana Severity merupakan seberapa besar dampak yang dihasilkan, Occurence merupakan seberapa sering intensitas terjadinya kegagalan, dan Detection merupakan kemampuan kontrol dari perusahaan dalam mengatasi suatu kegagalan, yang kemudian digunakan untuk melakukan perangkingan risiko. Jumlah dari nilai RPN juga menentukan level dari masing-masing risiko. Setelah dilakukan perangkingan risiko maka diperoleh jumlah hasil penilaian level risiko sebagai berikut :

Tabel 5 Jumlah Hasil Penilaian Risiko

Level Risiko	Jumlah
Very High	0 risiko
High	0 risiko
Medium	0 risiko
Low	9 risiko
Very Low	36 risiko

3.10 Rencana Mitigasi Risiko

Mitigasi risiko pada aset kritis TI dilakukan setelah diperoleh hasil dari perangkingan risiko yang sudah dilakukan pada tahapan sebelumnya, sehinga dilakukan kontrol objektif berdasarkan ISO 27002 yang memiliki 14 klausul dan 34 sub klausul di dalamnya [11], untuk dilakukan rencana mitigasi risiko. Tindakan mitigasi yang biasa digunakan terdiri dari *Risk Assumption* (menerima risiko), *Risk Avoidance* (menghindari risiko), *Risk Limitation* (mencegah risiko), *Risk Planning* (perencanaan mitigasi risiko), *Research and Acknowledgment* (perbaikan

risiko), *dan Risk Transference* (pengalihan risiko) [12]. Berikut merupakan jumlah dari hasil mitigasi risiko :

Tabel 6 Jumlah Hasil Tindakan Mitigasi

Mitigasi	Jumlah
Risk Assumption	3 risiko
Risk Avoidance	2 risiko
Risk Limitation	38 risiko
Risk Planning	39 risiko
Research and Acknowledgment	4 risiko
Risk Transference	1 risiko

4. KESIMPULAN

Berdasarkan penelitian yang sudah dilakukan terkait dengan analisa dan mitigasi risiko terhadap aset kritis teknologi informasi di RS Telogorejo, maka bisa diambil kesimpulan :

1. Terdapat beberapa penyebab terjadinya risiko di RS Telogorejo yang dapat mengganggu dan menghambat proses bisnis. Namun penyebab yang paling sering terjadi adalah kontrol dan *maintenance* terhadap aset kritis teknologi informasi yang dimiliki perusahaan belum dilakukan secara teratur sesuai dengan jadwal yang sudah dibuat karena keterbatasan SDM yang ada, gangguan pada aliran listrik karena tegangan listrik yang tidak stabil serta pemadaman listrik dari pihak PLN yang bisa terjadi sewaktu waktu, dan adanya serangan dari *hacker* yang dapat mengacaukan jaringan.
2. Pada penelitian ini level risiko yang diperoleh hanyalah level *low* dan *very low*, walaupun risiko hanya berlevel *low* dan *very low* akan tetap dilakukan tindakan mitigasi risiko untuk perbaikan Sistem Manajemen Keamanan Informasi pada perusahaan.

5. SARAN

Adapun saran yang bisa peneliti sampaikan untuk penelitian selanjutnya, diantaranya adalah :

1. Menggunakan *framework* atau ISO yang berbeda pada penelitian selanjutnya, namun tetap berfokus pada standarisasi Sistem Manajemen Keamanan Informasi (SMKI).
2. Pada penelitian selanjutnya diharapkan mampu menurunkan jumlah tindakan mitigasi *risk limitation* dan *risk planning* pada perusahaan. Semakin rendah jumlah saran mitigasi yang diberikan, semakin baik proses kontrol dan perencanaan yang dilakukan perusahaan.

DAFTAR PUSTAKA

[1] Harahap, 2010. *Pengukuran Risiko Manajemen Proyek Teknologi Informasi.*

[2] Pertiwi, R.A., 2013. *Strategi Public Relation Dalam Membangun Branding Rumah Sakit Telogorejo Menjadi Semarang Medical Center, 7.*

[3] Kurniawan, R., 2014. Analisis Dan Pengukuran Tingkat Eksposur Resiko Teknologi Informasi Dengan Metode FMEA Pada PT. Bank Central Asia, Tbk. ComTech, 5.

[4] Dea Anjani, 2015. Identifikasi, Penilaian, Dan Mitigasi Risiko Keamanan Informasi Pada Sistem Elctronic Medical Record (Studi Kasus : Aplikasi Healthy Plus Modul Rekam Medis Di RSU Haji Surabaya. [Online] Available at : http://www.academia.edu/20027129/IDENTIFIKASI_PENILAIAN_DAN_MITIGAS

I_RISIKO_KEAMANAN_INFORMASI_PADA_SISTEM_ELECTRONIC_MEDICAL_RECORD_STUDI_KASUS_APLIKASI_HEALTHY_PLUS_MODUL_REKAM_MEDIS_DI_RSU_HAJI_SURABAYA_. [Accessed September 2016].

[5] Mukhammad Iqbal, 2014. Evaluasi Resiko Keamanan Jaringan Komputer Pada Rumah Sakit Mohammad Hosein Palembang Dengan Menggunakan Metode Octave. [Online] Available at : https://www.binadarma.ac.id/download.php?id=853. [Accessed September 2016].

[6] Alberts, C.J., 1999. OCTAVE Framework. *Networked Systems Survivability Program*, 1.

[7] Alberts, C.J., 2003. Introduction To The OCTAVE. *Networked System Survivability Program, 1*.

[8] Academia, 2015. *FMEA Sebagai Tindakan Pencegahan Pada Kegagalan Pengujian.* [Online] (Updated 2015) Available at: http://www.academia.edu/20155877/FAILURE_MODE_AND_EFFECT_ANALYSIS_FMEA_SEBAGAI_TINDAKAN_PENCEGAHAN_PADA_KEGAGALAN_PENGUJIAN. [Accessed Oktober 2016].

[9] Ibnu Idham. *Failure Modes and Effect Analysis*. [Online] (Updated April 2014) Available at: http://www.academia.edu/7652952/FAILURE_MODES_AND_EFFECT_ANALYSIS. [Accessed Oktober 2016].

[10] Margaret Rouse, 2014. *WhatIs*. [Online] (Updated November 2014) Available at: http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA. [Accessed November 2016].

[11] ISO/IEC, 2013. *International Standard ISO/IEC 27002*, 2, 1.

[12] Binus University, 2010. *Analisis Resiko Sistem Informasi Dengan OCTVAE-S Pada PT. Lyto Datarindo Fortuna*. [Online] (Updated 2010) Available at: https://library.binus.ac.id/Thesis/RelatedSubject/TSA-2010-0039. [Accessed 2016].