BAB II

LANDASAN TEORI

2.1. Tinjauan Pustaka

Dalam pengerjaan tugas akhir ini terdapat beberapa penelitian yang terkait yang digunakan sebagai referensi, berikut merupakan informasi singkat tentang penelitian tersebut. Tinjauan pertama yaitu penelitian dari Dheni Indra Rachmawan yang membuat skripsi berjudul Pembuatan Dokumen SOP (Standar Operasional Prosedur) Keamanan Aset Informasi Yang Mengacu Pada Kontrol Kerangka Kerja ISO 27002:2013 (Studi Kasus : CV Cempaka Tulungagung) pada tahun 2017 (Rachmawan, 2017). Hasil penelitian dari Dheni Indra Rachmawan menghasilkan penelitian berupa identifikasi dan penilaian risiko aset informasi yang dapat mengancam proses bisnis yang berkaitan dan mengetahui tindakan yang harus dilakukan untuk mengatasi risiko pada CV Cempaka Tulungagung. Untuk hubungan dari penelitian ini dengan tugas akhir penulis yaitu berkaitan dengan penelitian yang terletak pada penggunaan metode FMEA yang dibuat untuk penilian risiko pada aset yang akan diteliti.

Selanjutnya penelitian kedua menggunakan referensi dari I Putu Adi Wiranata yang membuat skripis berjudul Pembuatan Panduan Audit Keamanan Fisik Dan Lingkungan Teknologi Informasi Berbasis Risiko Berdasarkan ISO/IEC 27002:2013 Pada Ruang Server STIE Perbanas Surabaya pada tahun 2017 (Wiranata, 2017). Hasil penelitian yang dilakukakan oleh I Putu Adi Wiranata berupa penelitian berdasarkan hasil identifikasi risiko yang telah dilakukan didapatkan 30 risiko yang dikembangkan dari identifikasi ancaman dan kerentanan terhadap setiap aset di ruang server. Semua risiko yang berhasil diidentifikasi termasuk ke dalam kontrol keamanan fisik dan lingkungan. Untuk hubungan dengan tugas akhir yang peneliti buat yaitu berkaitan pada penggunaan metode FMEA.

Pada penelitian ketiga, penulis menggunakan referensi dari Nimas Nawangsih yang membuat skripsi berjudul Pembuatan Standar Operasional Prosedur Kontrol Akses *Physical* dan *Logical* pada Aplikasi Sistem Informasi

Rumah Sakit (SIMRS) Menggunakan Kerangka Kerja OCTAVE, FMEA dan Kontrol ISO 27002:2013 (Studi Kasus: Instalasi Pengelola Data Elekronik Rumah Sakit Dokter Moewardi). Pada tahun 2017 (Nawangsih, 2017) Hasil penelitian yang dilakukan yaitu mengenai hasil identifikasi risiko akses *physical* dan *logical* pada aset informasi yang terkait dengan Aplikasi SIMRS di Rumah Sakit Dokter Moewardi berdasarkan metode analisis risiko OCTAVE dengan mengidentifikasi aset informasi terkait dengan Aplikasi SIMRS. Pada hubungannya dengan skripsi penulis yaitu terletak pada penggunaan metode OCTAVE dan FMEA dalam mengidentifikasi risiko aset nya.

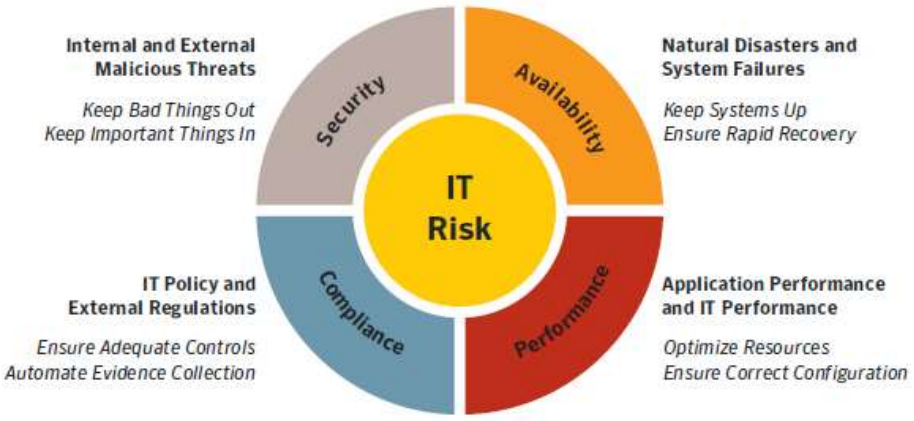
Pada penelitian keempat, penulis menggunakan referensi dari Wenni Syafitri yang membuat jurnal berjudul Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus: Sistem Informasi Akademik Universitas XYZ). Penelitian ini selain metode yang ada diatas yaitu OCTAVE dan FMEA juga ada metode lain yaitu NIST 800-30. Hasil yang didapat dari jurnal ini yaitu NIST 800-30 yang memberikan rekomendasi kontrol Berdasarkan hasil penilaian risiko berbasis keamanan informasi, universitas xyz memiliki 1 tingkat risiko tinggi, 5 tingkat risiko sedang dan 52 tingkat risiko rendah. (Syafitri, 2016).

Pada penelitian kelima, penulis menggunakan referensi jurnal dari Bambang Supradono yang berjudul Manajemen Risiko Keamanan Informasi Dengan Menggunakan Metode OCTAVE (*Operationally Critical Threat, Asset, And Vulnerability Evaluation*). Hasil penelitian yang dilakukan adalah untuk memberikan panduan secara sistemik dan komprehensif dalam manajemen risiko keamanan informasi. Metode ini lebih menekankan pengelolaan risiko berbasis ancaman (*threat*) dan kelemahan (*vulnerability*) terhadap aset-aset informasi organisasi meliputi perangkat keras, lunak, sistem, informasi dan manusia. Pada hubungannya dengan skripsi penulis yaitu terletak pada penggunaan metode OCTAVE (Supradono, 2009).

2.2. Information Technology Risk Management

Information technology risk management adalah peluang atau kemungkinan dari suatu bahaya, kehilangan atau konsekuensi buruk lainnya. Risk management juga bisa disebut sebagai ketidakpastian dari peristiwa di masa yang akan datang.

(Obrand, Augustsson, Holmstrom, & Mathiassen, 2012). Risiko merupakan potensi dari kerusakan pada *organization value,* sering kali dari proses manajemen dan kejadian yang tidak memadai dan dapat dianggap sebagai komponen dari sistem menejemen risiko. Manajemen risiko meliputi tiga proses yaitu: risiko penilaian, mitigasi risiko dan evaluasi dan penilaian. (Gary Stonebumer, Alice Goguen, 2002). Kerangka kerja klasifikasi *information technology management* bisa dilihat pada Gambar 2.1.



Gambar 2. 1 *Framework* Klasifikasi *IT Risk Management* (Symantec, 2008)

Berdasarkan kerangka kerja risiko teknologi informasi ini tidak hanya mencakup dampak negatif seperti risiko yang mungkin dihadapi di organisasi yang berhubungan dengan keuangan atau transaksi. Risiko bisnis dari komponen operasional merupakan hasil daripada transaksi termasuk risiko dari internal seperti kualitas produk, organisasi, dan kinerja pabrik, sedangkan dari eksternal terkait dengan bencana alam atau ada perubahan dalam peraturan pemerintahan. (Symantec, 2008).

Kerangka kerja pada Gambar 2.1 mengklasifikasikan *Information Technology Risk* sebagai berikut :

1. ***Security Risk –*** Informasi itu akan diubah, diakses atau digunakan oleh pihak yang tidak berwenang.

2. ***Availability Risk –*** Informasi atau aplikasi tidak dapat diakses karena kegagalan sistem atau bencana alam, ancaman ini termasuk sebagai periode yang memakan waktu lama untuk pemulihannya.

3. ***Performance Risk –*** Yaitu kinerja yang kurang baik dari sistem, aplikasi, personal atau teknologi informasi dengan keseluruhan akan mengurangi produktivitas atau nilai bisnis.

4. ***Compliance Risk –*** Yaitu penanganan atau pemrosesan informasi yang gagal memenuhi persyaratan peraturan dari suatu kebijakan teknologi informasi dan bisnis.

Dari keempat kategori ini sudah dapat mengklasifikasikan semua elemen *Information technology risk management.*

Manfaat manajemen risiko juga dapat diidentifikasi dalam kaitannya dengan tiga kali skala kegiatan dalam organisasi. (Paul Hopkin, 2010). Output dari kegiatan manajemen risiko dapat menguntungkan organisasi dalam tiga skala waktu dan memastikan bahwa organisasi mencapai:

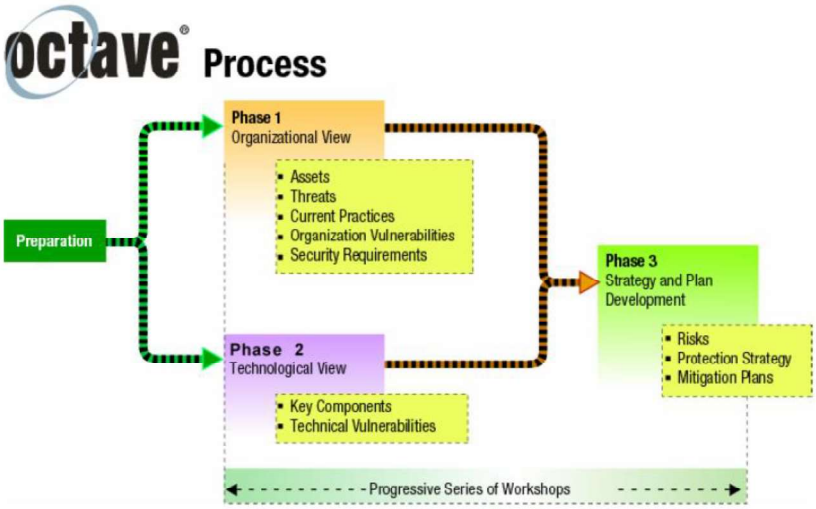
1. Strategi yang efektif
2. Proses dan proyek yang efektif
3. Operasi yang efisien

Untuk mencapai kontribusi manajemen risiko yang berhasil, manfaat yang diharapkan dari setiap inisiatif manajemen risiko harus diidentifikasi. Risk Management akan sangat membantu manajemen organisasi untuk menyeimbangkan antara dampak dari risk yang dibutuhkan untuk meminimalisir resiko tersebut Jika hasil itu belum teridentifikasi, maka tidak akan ada sarana untuk mengevaluasi apakah manajemen risiko telah berhasil. Oleh karena itu, manajemen risiko yang baik harus memiliki serangkaian hasil / manfaat yang jelas. Perhatian yang tepat harus diberikan kepada setiap tahap proses manajemen risiko, serta rincian desain, implementasi dan pemantauan kerangka kerja yang mendukung kegiatan manajemen risiko ini.

2.3. Metode OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*)

OCTAVE (*Operationally Critical Threat, Asset and Vulnerability Evaluation*) merupakan kerangka kerja untuk mengidentifikasi dan mengelola risiko keamanan informasi.(Alberts C. J., Behrens, S. G., Pethia, R. D. & Wilson, 1999). Kerangka kerja ini berfokus pada permasalahan strategi dan praktik keamanan yang terkait, dengan begitu organisasi dapat merancang dan menerapkan strategi perlindungan untuk mengurangi risiko keseluruhan aset informasinya.

OCTAVE lebih pada penerapan praktik keamanan ditujukan pada internal organisasi dan strategi untuk mengantisipasi keamanan di masa yang akan datang dan diselaraskan dengan kepentingan organisasi. Fase OCTAVE pada Gambar 2.2.



Gambar 2. 2 Fase OCTAVE (Hayes & Stevens, 2004)

Berdasarkan pada Gambar 2.2 kerangka kerja OCTAVE memiliki empat proses yang diantaranya yaitu:

1. Fase 0: Persiapan *(Preparation)*

Hal penting yang harus dipersiapkan sebelum melaksanakan kerangka kerja OCTAVE ada tiga cara yaitu :

1. Menyusun jadwal.

2. Membentuk Tim analis.
3. Mempersiapkan logistik/peralatan.

2. Fase 1: Membangun Aset Berbasis Profil Ancaman

Tim analisis menentukan apa yang penting bagi organisasi dan apa yang saat ini sedang diterapkan dalam melindungi aset. Setelah itu dipilih mana yang paling penting bagi organisasi yaitu aset kritis dan dideskripsikan kebutuhan keamanan ancaman dan profil ancaman pada masing – masing aset kritis.

3. Fase 2: Mengidentifikasi Kerentanan Infrastruktur

Pada proses OCTAVE yang kedua, mengidentifikasi kerentanan infrastruktur menjelaskan tentang aktifiktas untuk mendapatkan pengetahuan berupa aset, ancaman dan strategi pengamanan dari orang yang berada pada bidang terkait. Tujuan lain sebagai tindakan evaluasi atas informasi infrastruktur. (Alberts C. J., Behrens, S. G., Pethia, R. D. & Wilson, 1999)

4. Fase 3: Mengembangkan rencana dan strategi keamanan

Risiko atas aset kritis organisasi diidentifikasi dan ditentukan langkah yang harus diambil dalam menyikapinya. Strategi perlindungan diciptakan untuk organisasi dan rencana mitigasi ditambahkan untuk membantu pengelolaan risiko terhadap aset kritis berdasarkan analisis informasi yang telah dikumpulkan.

2.4. Metode FMEA (*Failure Mode and Effect Analysis*)

FMEA (*Failure Mode and Effect Analysis*) adalah cara yang terstruktur untuk mengidentifkasi dan mengatasi masalah potensial, atau kegagalan dan efek yang dihasilkan pada sistem atau proses sebelum suatu peristiwa buruk terjadi, FMEA akan mengidentifikasi dan akan menghilangkan proses kegagalan untuk mencegah suatu peristiwa yang tidak diinginkan (QAPI, 2006). Menilai suatu risiko dengan proses kegagalan yang teridentifikasi efek, penyebabnya dan memperioritaskan masalah yang ada agar dapat dilakukan tindakan korektif.

FMEA harus menjadi panduan *development* untuk menyelesaikan tindakan yang akan mengurangi risiko yang terkait dengan sistem, subsistem, dan komponen atau proses manufaktur / perakitan ke tingkat yang dapat diterima. Tujuan dari FMEA adalah membantu untuk merancang kegagalan yang terindikasi dari sistem dengan biaya terendah dalam hal waktu dan uang. Berikut adalah proses dari FMEA (P L M Software, 2016)

2.4.1. Langkah-langkah Proses FMEA

a) Langkah 1 : Identifikasi potensial kegagalan dan efeknya

Langkah pertama adalah menganalisis kebutuhan fungsional dan pengaruhnya untuk mengidentifikasi semua kegagalan. Setelah itu membuat daftar semua kegagalan dari fungsi dengan istilah teknis dengan mempertimbangkan efek di akhir dari setiap kegagalan dan mencatat efek kegagalan.

b) Langkah 2 : Menentukan Dampak

Severity merupakan dampak yang dihasilkan dari kegagalan dan menimbulkan efek pada sistem. Dalam praktiknya *severity* dibuat dalam nilai 1 sampai 10, dimana nilai 1 merupakan nilai terendah yang mengindikasikan tidak terjadi efek/bahaya dan 10 sebagai nilai tertinggi yang mengindikasikan sangat berbahaya. Tabel 2.1 berikut akan menunjukan *severity rating* (P L M Software, 2016)

Tabel 2. 1 *Severity* Rating

Rating	Meaning
1	Tanpa efek, tanpa bahaya
2	Sangat kecil – Biasanya hanya diperhatikan oleh pengguna yang jeli
3	Kecil – Hanya sebagian kecil dari sistem yang terpengaruh
4-6	Sedang – Sebagian besar pengguna tidak nyaman dan terganggu
7-8	Tinggi – Kehilangan fungsi utama, pengguna tidak puas
9-10	Sangat tinggi – Berbahaya. Produk menjadi tidak beroperasi.

c) Langkah 3 : Frekuensi Terjadinya kegagalan

Occurrence merupakan seberapa sering kegagalan terjadi. Pada proses kegagalan yang sama dan kegagalan yang di dokumentasikan. Semua potensi kegagalan dapat diberikan peringkat *occurrence* dengan nilai 1 sampai 10 , dimana nilai 1 mengindikasikan tidak adanya kegagalan, nilai 10 mengindikasikan tingkat bahaya yang sangat tinggi. Dengan contoh pada tabel 2.2 berikut.

Tabel 2. 2 *Occurrence* Rating

Rating	Meaning
1	Tidak ada kegagalan yang didokumentasikan pada proses yang sama
2-3	Rendah - Kegagalannya sedikit
4-6	Sedang – Kegagalan yang jarang terjadi
7-8	Tinggi – Kegagalan yang berulang
9-10	Sangat tinggi – Kegagalan hampir pasti terjadi
9-10	Sangat tinggi – Berbahaya. Kegagalan merupakan bahaya keamanan

d) Langkah 4 : Pendeteksi Kegagalan

Detection menunjukan seberapa besar kemungkinan kegagalan itu akan terdeteksi. Semakin tinggi nilai pada *detection* maka semakin besar kemungkinan kegagalan tidak akan terdeteksi. dimana nilai 1 mengindikasikan tidak adanya kesalahan, nilai 10 mengindikasikan tingkat kesalahan sangat sulit di deteksi. (Scangas, n.d.) Berikut contoh *detection rating* pada Tabel 2.3

Tabel 2. 3 *Detection* Rating

Rating	Meaning
1	Kesalahan pasti ditemukan oleh penguji
2	Kesalahan hampir pasti ditemukan oleh penguji
3	Tinggi kemungkinan bahwa penguji akan menemukan kesalahan
4-6	Sedang kemungkinan bahwa penguji akan menemukan kesalahan
7-8	Rendah kemungkinan bahwa penguji akan menemukan kesalahan
9-10	Kesalahan tidak akan diketahui oleh pengguna

2.4.2. Risk Priority Number (RPN)

Merupakan metode yang memberi peringkat dari setiap risiko kegagalan yang berada pada sistem atau organisasi berdasarkan penghitungan dari tiga elemen yaitu, severity (dampak), occurrence (frekuensi), detection (deteksi). RPN akan mempengaruhi pilihan yang diambil untuk mengatasi kegagalan sebuah sistem. Hasil RPN akan menunjukan area yang paling bermasalah, dan RPN dengan peringkat tertinggi harus mendapatkan prioritas tertinggi dalam pengambilan tindakan untuk menyelesaikan permasalahan.

Tujuan dari pengambilan tindakan yaitu, menghilangkan potensi kegagalan, mengurangi dampak dari kegagalan, mengurangi frekuensi kegagalan, dan memudahkan deteksi kegagalan. (Software, 2016) Cara perhitungan rumus dari RPN yaitu dengan melakukan perkalian berdasarkan tiga elemen yaitu, severity (dampak), occurrence (frekuensi) dan detection (deteksi) selanjutnya hasil perkalian tersebut lah yang menjadi nilai akhir RPN di setiap asetnya. RPN akan mempengaruhi pilihan yang diambil untuk mengatasi kegagalan sebuah sistem (Lipol & Haq, 2011). Perhitungan ditentukan melalui persamaan (1).

$$\boldsymbol{RPN = S * O * D \ (or \ RPN = S \ x \ O \ x \ D)} \quad \textbf{(1)}$$

1. RPN = (Risk Priority Number) yaitu metode pemberian peringkat dari setiap risiko kegagalan yang ada
2. S = Severity (Dampak) yaitu dampak yang ditimbulkan dari setiap aset risiko yang ada
3. O = Occurrence (Frekuensi Kegagalan) yaitu seberapa sering kegagalan itu terjadi
4. D = Detection (Deteksi Kegagalan) yaitu seberapa besar kemungkinan kemungkinan kegagalan itu akan terjadi