BAB 2
TINJAUAN PUSTAKA

2.1 Penelitian Terkait

Dari topik yang akan penulis ambil untuk penelitian ini, penulis mencari beberapa penelitian sebelumnya yang pernah dilakukan untuk dijadikan referensi. Diharapkan dengan adanya referensi tersebut dapat membantu penulis dalam pengerjaan tugas akhir ini dengan lebih efisien. Berikut merupakan beberapa penelitian sebelumnya yang dijadikan referensi :

Tabel 2. 1 Penelitian Terkait Mitigasi Risiko

No	Nama Peneliti dan Tahun	Masalah	Metode	Hasil
1.	Roy Kurniawan, 2014	Penanganan terhadap aset kritis TI perusahaan kurang maksimal.	Menggunakan metode FMEA untuk melakukan perhitungan risiko pada masing-masing aset kritis TI perusahaan.	• RPN tertinggi 540 • RPN terendah 10
2.	Dea Anjani, 2015	Kurangnya kesadaran pihak perusahaan terhadap proteksi keamanan data yang dimiliki .	Menggunakan metode octave untuk mengidentifikasi aset kritis TI dan metode FMEA untuk melakukan penilaian risiko.	• RPN tertinggi 336 • RPN terendah 18

No	Nama Peneliti dan Tahun	Masalah	Metode	Hasil
3.	Mukhammad Iqbal, 2014	Kurang adanya kontroling pada aplikasi dan jaringan komputer oleh pihak perusahaan.	Menggunakan metode octave untuk melakukan evaluasi risiko pada keamanan jaringan komputer.	Memberikan saran perbaikan pada risiko keamanan jaringan komputer guna mengurangi ancaman yang terdapat pada jaringan.

Berdasarkan beberapa penelitian terkait yang relevan dengan penelitian ini, dapat disimpulkan bahwa metode octave dan FMEA cukup efektif digunakan untuk melakukan identifikasi, pembobotan atau penilaian, serta perencanaan untuk mitigasi risiko terhadap aset kritis TI yang dimiliki oleh perusahaan.

2.2 Risiko

Risiko merupakan suatu kondisi ketidakpastian dengan segala konsekuensi yang dapat merugikan [2].

Macam-macam risiko dapat dibedakan berdasarkan bagaimana cara risiko itu terjadi, antara lain [3] :

1. Risiko murni merupakan suatu risiko yang terjadi tanpa adanya kesengajaan dan dapat menimbulkan kerugian, misalnya saja risiko terjadinya kebakaran dan pencurian yang bisa terjadi kapan saja tanpa bisa diprediksi.
2. Risiko spekulatif merupakan suatu risiko yang terjadi karena adanya kesengajaan dari pihak bersangkutan agar ketidakpastian tersebut dapat menghasilkan keuntungan, misalnya saja pada risiko utang piutang.

3. Risiko fundamental merupakan suatu risiko yang terjadi bukan karna ulah seseorang namun efeknya berdampak pada banyak orang, misalnya saja terjadinya bencana alam seperti banjir dan longsor.
4. Risiko khusus merupakan suatu risiko yang bersumber pada peristiwa mandiri dan penyebabnya dapat mudah diketahui, misalnya saja kecelakaan yang terjadi pada transportasi sehari-hari.
5. Risiko dinamis merupakan suatu risiko yang terjadi karena berkembangnya suatu teknologi dan kemajuan ilmu pengetahuan.

2.2.1 Manajemen Risiko

Manajemen risiko adalah suatu proses terstruktur mulai dari mengidentifikasi risiko yang mungkin terjadi hingga menangani risiko yang ada disertai dengan *monitoring* [4].

Tindakan manajemen risiko sendiri terdiri dari 2 macam yaitu tindakan mencegah yang digunakan untuk menghindari terjadinya sutau risiko dan tindakan memperbaiki yang digunakan untuk mengurangi dampak dari efek-efek ketika sutau risiko harus diambil [5].

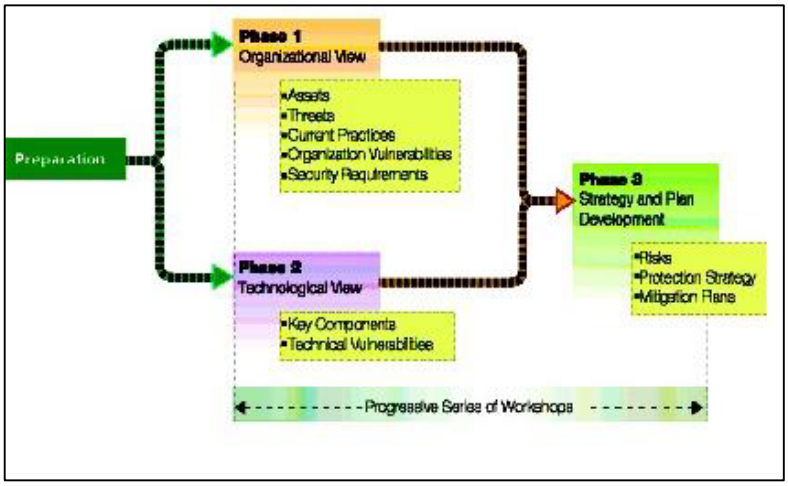
2.2.2 Manajemen Risiko TI

Manajemen risiko TI adalah kemampuan organisasi dalam mengelola dan meminimalisir risiko-risiko TI yang mungkin akan menjadi pengahalang bagi suatu organisasi dalam mencapai tujuannya terkait dengan pemanfaatan TI itu sendiri [6].

2.3 Metode Octave

Octave *(Operationally Critical Threat, Asset, and Vulnerability Evaluation)* merupakan suatu kerangka kerja untuk mengidentifikasi dan mengelola risiko keamanan informasi. Metode ini mendefinisikan sebuah metode evaluasi menyeluruh yang memungkinkan organisasi untuk mengidentifikasi aset informasi yang penting bagi organisasi [7].

Metode ini menggunakan pendekatan tiga fase untuk menganalisa masalah, yaitu :



Gambar 2. 1 Fase Octave [8]

FASE PERSIAPAN

Pada fase ini dilakukan pembentukan tim analisis, menentukan studi kasus yang akan diambil serta menyiapkan kebutuhan lainnya yang terkait dengan fase ini.

FASE 1 : Menentukan Aset berdasarkan Profil Ancaman

Fase ini merupakan tahap pengumpulan data dengan melakukan identifikasi aset kritis dan ancaman yang terjadi pada tiap-tiap aset TI yang ada di perusahaan. Pada fase ini hasil keluaran yang di dapat adalah daftar aset kritis TI bagi perusahaan dan ancaman yang terjadi pada masing-masing aset. Proses yang berjalan pada fase ini antara lain :

1. **Proses 1 : pendataan aset kritis**

   Proses pendataan aset kritis TI yang dimiliki oleh perusahaan dan nantinya akan menghasilkan keluaran berupa daftar aset-aset TI yang sangat penting bagi perusahaan.

2. **Proses 2 : identifikasi kebutuhan keamanan aset kritis**

   Proses identifikasi kebutuhan keamanan apa saja yang diperlukan dari masing-masing aset kritis TI berdasarkan ancamannya. Pada keamanan informasi terdapat tiga aspek yang biasa dikenal dengan CIA Triad Model, yang terdiri dari *Confidentiality, Integrity,* dan *Availability.*

3. **Proses 3 : identifikasi ancaman pada aset kritis**

   Proses identifikasi darimana sumber ancaman dari masing-masing aset kritis TI berasal dan apa saja dampak yang mungkin terjadi pada aset tersebut.

4. **Proses 4 : keamanan yang sudah diterapkan**

   Proses pendataan keamanan apa saja yang sudah diterapkan dan diupayakan oleh pihak perusahaan untuk melindungi aset kritis TI yang dimiliki.

5. **Proses 5 : identifikasi kerentanan organisasi**

   Proses ini merupakan proses mengidentifikasi kerentanan dalam perusahaan dilakukan.

FASE 2 : identifikasi kerentanan infrastruktur

Fase ini merupakan tahapan dimana proses identifikasi kerentanan teknologi dan infrastruktur yang ada di dalam perusahaan dilakukan untuk melihat risiko yang mungkin akan terjadi pada komponen kunci yang mendukung proses bisnis perusahaan. Selanjutnya akan dilakukan evaluasi dan pencegahan untuk meminimalisir terjadinya risiko. Proses yang berjalan pada fase ini antara lain :

1. **Proses 1 : identifikasi komponen kunci**

   Proses ini merupakan proses untuk mengidentifikasi komponen kunci dari infrastruktur teknologi informasi yang dimiliki oleh perusahaan. Hasil keluaran dari proses ini adalah daftar komponen kunci pada perusahaan,

2. **Proses 2 : evaluasi kerentanan teknologi saat ini**

   Proses ini merupakan proses untuk mengevaluasi kerentanan dari teknologi yang sudah diterapkan di dalam organisasi dan selanjutnya hasilnya akan dianalisis untuk dilakukan perbaikan.

FASE 3 : mengembangkan rencana dan strategi keamanan

Fase ini merupakan tahapan dimana proses evaluasi risiko terhadap aset kritis TI dilakukan dan mengembangkan perlindungan keamanan informasi dalam perusahaan, serta pembuatan rencana mitigasi risiko. Proses yang berjalan di dalam fase ini antara lain :

1. **Proses 1 : identifikasi risiko terhadap aset kritis**

   Pada proses ini akan dilakukan identifikasi risiko berdasarkan aset kritis yang ada di perusahaan.

2. **Proses 2 : pengukuran risiko**

   Pada proses ini akan dilakukan proses pengukuran risiko yaitu dengan memberikan penilaian dan pembobotan pada masing-masing risiko yang terjadi di setiap aset kritis TI.

3. **Proses 3 : strategi perlindungan**

   Pada proses ini akan dilakukan perencanaan untuk perlindungan keamanan pada setiap aset kritis yang dimiliki oleh perusahaan.

4. **Proses 4 : rencana mitigasi risiko**

   Pada proses ini akan dilakukan perencanaan untuk mitigasi dari masing-masing risiko yang dimiliki oleh tiap aset kritis TI di dalam perusahaan.

2.4 Metode FMEA

FMEA (*Failure Mode and Effect Analysis*) merupakan salah satu metode yang digunakan untuk mengidentifikasi, mengevaluasi dan mencegah mode kegagalan dari sebuah sistem untuk memperkirakan efek dari kegagalan sebuah sistem tersebut [9].

2.4.1 Tujuan FMEA

Terdapat beberapa tujuan yang perlu dicapai di dalam FMEA (*Failure Mode and Effect Analysis*), diantaranya adalah [9] :

1. Mengidentifikasi dan memprediksi kegagalan yang mungkin dapat terjadi.
2. Mengevaluasi dampak dari kegagalan yang terjadi pada sistem.
3. Memberikan tingkat prioritas dari risiko yang terjadi guna mempermudah proses perbaikan pada berdasarkan ranking prioritasnya.
4. Merencanakan dan melakukan tindakan perbaikan untuk mencegah dan mengurangi potensi terjadinya kegagalan sistem.
5. Mendokumentasikan keseluruhan proses yang dilakukan.

2.4.2 Manfaat FMEA

Terdapat beberapa manfaat yang diperoleh bila menerapkan metode FMEA dalam memanajemen risiko di organisasi, diantaranya adalah [9] :

1. Mengurangi terjadinya masalah pada sistem.
2. Memperkirakan tindakan yang dapat mengurangi terjadinya risiko.
3. Menghemat biaya untuk pengembangan sistem.

2.4.3 Menentukan *Severity, Occurrence,* dan *Detection*

Penilaian risiko perlu di lakukan terlebih dahulu dengan didasarkan pada 3 faktor yaitu *Severity, Occurrence,* dan *Detection*, agar kemudian dapat dilakukan perankingan prioritas terjadinya suatu risiko. Lalu nantinya akan dapat menghasilkan *Risk Priority Number.*

2.4.3.1 Severity

Severity merupakan tahap awal dalam menganalisa suatu risiko dengan memberikan ranking berdasarkan seberapa besar dampak dari kejadian tersebut dapat mempengaruhi proses *output*. Skala yang diberikan mulai dari 1 sampai 10, dimana 10 merupakan yang terburuk.

Tabel 2. 2 Skala *Severity* [10]

Rank	Effect	*Severity*
10	Berbahaya tanpa peringatan	Kegagalan sistem akan menghasilkan efek yang berbahaya tanpa peringatan.
9	Berbahaya dengan peringatan	Kegagalan sistem akan menghasilkan efek yang berbahaya dengan adanya peringatan sebelumnya.
8	Sangat tinggi	Semua sistem pendukung tidak akan berfungsi.
7	Tinggi	Sistem dapat beroperasi tetapi tidak maksimal.

Rank	Effect	*Severity*
6	Sedang	Sistem dapat beroperasi dan aman tetapi mengalami penurunan performa.
5	Rendah	Sistem mengalami penurunan kinerja secara bertahap.
4	Sangat rendah	Efek yang kecil pada performa sistem.
3	Kecil	Sedikit berpengaruh pada kinerja sistem.
2	Sangat kecil	Efek yang diabaikan pada kinerja sistem.
1	Tidak ada efek	Efek kegagalan tidak akan terjadi pada sistem.

2.4.3.2 Occurrence

Occurrence merupakan suatu keadaan dimana penyebab dari risiko tersebut akan terjadi dan menyebabkan kegagalan selama aset tersebut digunakan. Skala yang diberikan mulai dari 1 sampai 10.

Tabel 2. 3 Skala *Occurence* [10]

Rank	Effect	*Occurrence*
10	**Sangat tinggi :** Kegagalan hampir tidak bisa dihindari	Kemungkinan kegagalan terjadi 1 kali dalam 1 hari.
9		Kemungkinan kegagalan terjadi 5 kali dalam 1 minggu.
8	**Tinggi :** Kegagalan kadang terjadi	Kemungkinan kegagalan terjadi 3 kali dalam 1 minggu.
7		Kemungkinan kegagalan terjadi 2 kali dalam 1 minggu.

Rank	Effect	*Occurrence*
6	**Sedang :** Kegagalan kadang terjadi namun tidak dalam jumlah yang besar	Kemungkinan kegagalan terjadi 5 kali dalam 1 bulan.
5		Kemungkinan kegagalan terjadi 3 kali dalam 1 bulan.
4		Kemungkinan kegagalan terjadi 2 kali dalam 1 bulan.
3	**Rendah :** Kegagalan yang terjadi relatif kecil	Kemungkinan kegagalan terjadi 1 kali dalam 1 bulan.
2	**Sangat jarang** : Kegagalan yang terjadi relatif kecil dan jarang.	Kemungkinan kegagalan terjadi 1 kali dalam 3 bulan.
1	**Remote :** Kegagalan tidak pernah terjadi	Kemungkinan kegagalan terjadi 1 kali dalam 6 bulan.

2.4.3.3 Detection

Detection merupakan pengukuran terhadap kemampuan dalam mengontrol suatu kegagalan yang nantinya dapat terjadi. Dimana nilai dari *detection* disesuaikan dengan pengendalian yang saat ini dilakukan oleh perusahaan. Indeks skala dari *detection* adalah 1-10.

Tabel 2. 4 Indeks Skala *Detection* [10]

Rank	Effect	*Detection*
10	Hampir tidak mungkin	Kemampuan kontrol saat ini tidak ada yang dapat mendeteksi kegagalan.

Rank	Effect	*Detection*
9	Sangat jarang	Kemampuan kontrol saat ini sangat sulit mendeteksi penyebab kegagalan.
8	Jarang	Kemampuan kontrol saat ini sulit mendeteksi penyebab kegagalan.
7	Sangat rendah	Kemampuan kontrol saat ini untuk mendeteksi penyebab kegagalan sangat rendah.
6	Rendah	Kemampuan kontrol saat ini untuk mendeteksi penyebab kegagalan rendah.
5	Sedang	Kemampuan kontrol saat ini untuk mendeteksi penyebab kegagalan sedang.
4	Agak tinggi	Kemampuan kontrol saat ini untuk mendeteksi penyebab kegagalan sedang sampai tinggi.
3	Tinggi	Kemampuan kontrol saat ini untuk mendeteksi penyebab kegagalan tinggi.
2	Sangat tinggi	Kemampuan kontrol saat ini untuk mendeteksi penyebab kegagalan sangat tinggi.
1	Hampir pasti	Kemampuan kontrol saat ini hampir pasti dapat mendeteksi penyebab dan mencegah kegagalan.

2.4.4 Risk Priority Number (RPN)

Dalam FMEA nilai RPN merupakan proses perhitungan yang digunakan untuk menentukan level dari masing-masing risiko. Diperoleh berdasarkan 3 faktor yang telah dijabarkan sebelumnya yaitu *Severity, Occurrence,* dan *Detection.* Nilai RPN dapat ditunjukkan dengan menggunakan rumus sebagai berikut [9] :

$$\mathbf{RPN = S * O * D} \qquad \mathbf{(2.1)}$$

Setelah melakukan proses perhitungan selanjutnya adalah menentukan level risiko berdasarkan nilai RPN. Skala tersebut nantinya akan digunakan untuk menilai risiko mana yang paling tinggi. Dengan begitu pihak perusahaan akan dapat menentukan tindakan pencegahan terhadap risiko yang bernilai paling tinggi. Skala RPN akan digambarkan pada tabel berikut.

Tabel 2. 5 Skala RPN

RPN	Level Risiko
>= 200	Very High
120 – 199	High
80 – 119	Medium
20 – 79	Low
0 – 19	Very Low

2.5 Keamanan Informasi

Perlindungan terhadap keamanan informasi terdiri atas beberapa aspek yang terdiri dari *Confidentiality* (Kerahasiaan), *Integrity* (Integritas), *Availability* (Ketersediaan) yang biasa dikenal sebagai CIA triad. CIA triad sendiri merupakan salah satu model yang dirancang sebagai panduan kebijakan kemanan informasi pada sebuah perusahaan. Berikut merupakan penjabaran dari ketiga aspek keamanan informasi tersebut [11] :

1. *Confidentiality* (Kerahasiaan)

   Kerahasiaan adalah aspek keamanan yang memberlakukan pembatasan hak akses pada informasi yang bersifat sensitif dan penting di dalam perusahaan dan hanya orang-orang tertentu lah yang memiliki wewenang untuk melihat dan mengolah data tersebut untuk mencegah bocornya informasi perusahaan ke pihak yang tidak bertanggung jawab.

2. *Integrity* (Integritas)

   Integritas adalah aspek keamanan yang memastikan informasi dan data perusahaan tidak bisa diubah dan dimodifikasi verifikasi oleh pihak yang berhak dan memiliki hak akses.

3. *Availability* (Ketersediaan)

   Ketersediaan adalah aspek keamanan yang memberikan jaminan bahwa setiap informasi yang diperuntukan bagi para pengguna yang memiliki hak akses pada informasi tersebut dapat digunakan, diakses dimanapun dan akan selalu tersedia setiap saat.

2.6 Aset

Aset merupakan sebuah barang yang memiliki nilai ekonomi dan nilai tukar yang dimiliki oleh sebuah perusahaan, organisasi, instansi atau bahkan individu. Aset sendiri terdiri dari benda yang bergerak dan benda tidak bergerak, berwujud dan tidak berwujud yang termasuk menjadi harta kekayaan dari sebuah perusahaan, organisasi, instansi atau individu [12].

2.7 Aset Kritis

Aset kritis merupakan sesuatu yang dianggap penting dan berharga dalam suatu perusahaan, dimana jika aset tersebut tidak dapat berfungsi dengan baik maka akan berpengaruh terhadap proses bisnis di dalam perusahaan tersebut.

2.8 Mitigasi Risiko

Mitigasi risiko adalah suatu tindakan terencana yang dilakukan oleh pemilik risiko agar bisa mngurangi dampak dari suatu kejadian yang berpotensi merugikan atau bahkan membahayakan pemilik risiko dan mengganggu proses bisnis di dalam

perusahaan tersebut. Ada beberapa strategi mitigasi risiko yang biasanya digunakan, yaitu [13] :

1. *Risk Assumption*

   Strategi dimana risiko tersebut diterima dan sistem teknologi informasi tetap dioperasikan untuk menerapkan kontrol yang ada agar risiko dapat diturunkan ke tingkat yang lebih rendah yang dapat diterima.

2. *Risk Avoidance*

   Strategi dimana risiko tersebut dihindari dan dihilangkan penyebabnya agar tidak menimbulkan kerugian di dalam perusahaan tersebut dan biasanya memerlukan biaya yang cukup tinggi.

3. *Risk Limitation*

   Strategi untuk membatasi risiko dengan melakukan kontroling agar dampak dari risiko tersebut dapat diminimalisir dan tidak menimbulkan kerugian yang besar bagi perusahaan.

4. *Risk Planning*

   Strategi untuk mengelola risiko dengan membuat perencanaan mitigasi sebelum risiko tersebut terjadi.

5. *Research and Acknowledgment*

   Strategi yang dilakukan dengan melakukan kontroling dan perbaikan dari kerentanan yang ada pada sistem sehingga meminimalisir kerugian perusahaan.

6. *Risk Transference*

   Strategi dimana risiko tersebut diserahkan kepada pihak ketiga untuk dilakukan perbaikan karena pihak perusahaan tidak kompeten terhadap penanganan risiko tersebut atau mengganti kerugian yang dialami oleh perusahaan seperti program asuransi.

2.9 ISO 27001

ISO 27001 merupakan dokumen standar yang telah disiapkan untuk memberikan persyaratan guna mendirikan, melaksanakan, menjaga dan meningkatkan sistem manajemen keamanan informasi pada suatu perusahaan dengan mempertahankan

kerahasiaan, integritas serta ketersediaan informasi. Standar ini berisi tentang detail tugas manajerial seperti penilaian risiko dan meninjau kemanan pada aset informasi yang dimiliki oleh perusahaan [14].

2.10 ISO 27002

ISO 27002 merupakan standar yang dirancang untuk organisasi yang nantinya akan digunakan sebagai referensi untuk memilih kontrol dalam proses menerapkan Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan ISO/IEC 27001 dan sebagai panduan organisasi dalam menerapkan kontrol keamanan informasi yang dapat diterima secara umum. Standar ini juga dimaksudkan untuk digunakan dalam mengembangkan industri dan pedoman manajemen keamanan informasi organisasi spesifik, dengan mempertimbangkan risiko keamanan informasi yang lebih spesifik di lingkungan mereka [15].

Detail kontrol yang terdapat di dalam ISO 27002:2013 akan dijabarkan secara lebih rinci pada lampiran [16].