BAB 2
TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Penelitian yang pernah dilakukan yaitu Identifikasi, penilaian, dan mitigasi risiko keamanan informasi menggunakan metode octave di Institut Teknologi Sepuluh Nopember (M.Bachtyar Rosyadi, 2013). Didalam penelitian oleh M.Bactyar terdapat beberapa kekurangan dalam penelitiannya seperti untuk mengetahui atau mengevaluasi keamanan mana yang tingkat risikonya paling tinggi sehingga mendapatkan penanganan kemanan yang lebih dibandingkan dengan penanganan kemanan yang tingkat risikonya lebih rendah.

Penilaian, mitigasi, dan pengendalian risiko keamanan informasi menggunakan metode FMEA (*Failure Mode & Effect Analysis*) di divisi TI PT Bank XYZ Surabaya (Innike Desy K.D.K.S, 2014). Metode FMEA merupakan metode yang digunakan untuk mengetahui potensial kegagalan didalam sistem, subsistem, dan komponen serta memprioritaskan kegagalan yang potensial dalam sistem yang nantinya digunakan untuk menentukan tindakan untuk mencegah kemungkinan terjadinya kegagalan tersebut. Akan tetapi didalam penelitian Innike terdapat kelemahan yaitu tidak ada ketentuan yang jelas mengenai identifikasi asset secara spesifik dan modus kegagalan setiap komponen kurang dipahami sehingga dalam rangka untuk menilai solusi terbaik setiap komponen kurang maksimal.

Tabel 2.1 Penelitian Terkait Mitigasi Risiko

No	Nama Peneliti dan Tahun	Masalah	Metode	Hasil
1.	M. Bactiar Rosadi , 2013	Kurang memahami	Metode yang digunakan	Mengkategorikan beberapa asset

		pentingnya asset TI didalam organisasi dan tidak ada dokumentasi tentang asset TI	dengan menggunakan metode octave untuk mengidentifikasi asset TI	menjadi asset critical, key component.
2.	Innike Desy K.D.K.S, 2014	Kurang optimalnya prosedur yang menangani tentang asset TI	Menggunakan metode fmea dan juga analisa kinerja menggunakan metode kualitatif dimana data yang diperoleh dari responden.	Memberikan nomor prioritas pada setiap asset dimana asset yang memiliki prioritas dengan angka yang besar merupakan asset yang perlu diperhatikan khusus.

Sehingga perbedaan dengan penelitian ini adalah pada penelitian ini menggabungkan metode penelitian yang sebelumnya yaitu metode octave dan metode fmea. Metode octave digunakan untuk mengolah data yang sudah didapat dan data yang sudah diolah dengan metode octave selanjutnya diberikan nilai untuk masing-masing komponen yang risikonya lebih tinggi diberi nilai yang besar sehingga penanganan yang dilakukan bisa tepat dan akurat. Sehingga bisa menutupi kekurangan yang ada pada penelitian sebelumnya.

2.2 Definisi Risiko

Menurut Australian / NZ Standard 4360 : 1999 Risiko adalah suatu kesempatan atas sesuatu untuk terjadi, yang akan memiliki dampak terhadap tujuan (*goal*). Sedangkan berdasarkan ISO 31000 : 2009, risiko adalah *effect of uncertainty on objectives,* atau dapat dikatakan bahwa risiko adalah efek yang muncul akibat adanya ketidakpastian dalam tujuan. Tujuan – tujuan bisa juga ditujukan untuk tujuan – tujuan perusahaan maupun organisasi.

PMBoK (*Project Management Body of Knowledge*), buku yang berisi mengenai pedoman untuk manajemen proyek yang diterbitkan oleh *Project Management Institute* (PMI) juga mendeskripsikan mengenai definisi dari risiko. Risiko menurut PMBoK adalah sebuah kejadian yang tidak pasti atau sebuah kondisi yang apabila terjadi, akan menimbulkan efek setidaknya pada satu tujuan proyek.

Efek dari sebuah kejadian yang tidak pasti atau ketidakpastian ini adalah suatu hal yang tidak diperkirakan sebelumnya. Efek dari risiko ini juga tidak selamanya negative, dapat juga bernilai positif. Tujuan yang akan berimbas dari risiko ini sendiri tentunya ada berbagai macam jenis.

Menurut [4], ada dua macam jenis risiko :

1. Risiko spekulatif, yakni risiko yang memiliki dua kemungkinan, baik yang bersifat menguntungkan maupun yang bersifat merugikan. Contohnya: perjudian, pembelian saham atau valuta asing.
2. Risiko murni (*Pure Risks*), yakni risiko dimana satu kemungkinan yakni kemungkinan rugi saja. Contoh: banjir, gempa, gunung meletus, kecelakaan, kebakaran, kebanjiran dll.

Selain itu terdapat perbedaan antara risiko (*risk)* dan ketidakpastian (*uncertainty).* Perbedaan antara keduanya adalah semua risiko pasti adalah ketidakpastian, namun tidak semua ketidakpastian merupakan risiko.

2.2.1 Manajemen Risiko

Berdasarkan standard ISO/IEC 31000:2009, identifikasi risiko memegang peranan penting pada penilaian risiko. Baik identifikasi maupun penilaian risiko merupakan rangkaian tahap dari manajemen risiko. Identifikasi risiko penting karena merupakan tahap pertama yang harus dilakukan karena dalam tahap ini dilakukan penentuan risiko – risiko beserta karakteristiknya yang mungkin akan mempengaruhi proyek. Kegagalan dalam tahapan ini akan berpengaruh besar terhadap tahapan manajemen risiko selanjutnya dan tentu akan mempengaruhi reliabilitas bagi proyek karena banyaknya kerentanan/celah yang mungkin bisa terjadi di masa yang akan datang.

Tujuan utama dalam identifikasi risiko adalah untuk mengetahui daftar – daftar risiko yang potensial dan berpengaruh terhadap tujuan/proses bisnis utama suatu organisasi [5]. Sesuai dengan ISO/IEC 31000:2009, identifikasi risiko tersebut dapat dilakukan dengan memperhatikan hal – hal berikut:

1. Masukan Identifikasi Risiko
2. Teknik Identifikasi Risiko

Panduan manajemen risiko ISO/IEC 31000:2009 menjelaskan masukan dan teknik dari identifikasi risiko, namun belum dapat menjelaskan proses identifikasi risiko itu sendiri. Oleh karena itu, dibutuhkan standar lain yang dapat menjelaskan bagaimana proses identifikasi risiko yang komprehensif, yaitu ISO/IE 27001.

1. Identifikasi aset – aset teknologi informasi yang dimiliki oleh organisasi.
2. Identifikasi ancaman pada setiap aset – aset teknologi informasi tersebut.
3. Identifikasi kerentanan yang diakibatkan oleh ancaman.
4. Identifikasi dampak kerugian dalam aspek *confidentiality, integrity* dan *availability*.

2.2.2 Manajemen Risiko TI

IT dalam suatu organisasi telah bertransformasi seiring dengan perkembangan jaman dan sekarang memiliki nilai lebih dari sekedar mendukung bisnis. IT juga dapat meningkatkan *competitive advantage* dari suatu perusahaan. Hal ini menyebabkan IT menjadi sesuatu yang *cost center* atau menjadi pengeluaran terbanyak dari beberapa perusahaan. Risiko dari IT sendiri memiliki cakupan yang luas terhadap suatu organisasi, sehingga tidak mungkin apabila tiap divisi dari suatu perusahaan mengidentifikasi risiko IT mereka sendiri sendiri tanpa memiliki kordinasi ataupun pandangan terhadap peran lainnya.

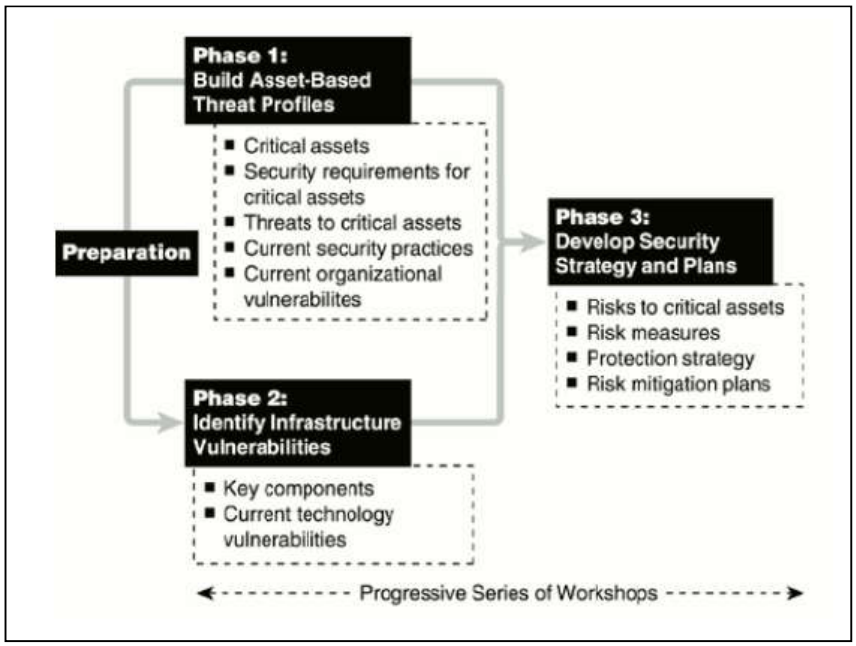
Oleh karena itu dibutuhkan manajemen risiko, manajemen risiko itu sendiri adalah pengelolaan risiko teknologi informasi atau sistem informasi di suatu perusahaan atau organisasi yang memiliki tujuan untuk meminimalisasi risiko yang berkaitan dengan teknologi informasi atau sistem informasi untuk muncul.

2.3 Metode Octave

Octave (*Operationally Critical Threat, Asset, And Vulnerability Evaluation*) adalah sebuah metode yang dikembangkan oleh *Software Engineering Institute* (SEI) pada tahun 2001. Metode Octave merupakan sebuah tools, teknik, dan metode dalam menilai dan merencanakan strategi keamanan informasi berdasasarkan pengidentifikasian risiko. Metode Octave menitikberatkan pada aset TI yang dimiliki organisasi dalam melakukan pengidentifikasian, prioritas dan manajemen risiko keamanan informasinya. Pendekatannya disusun dalam satu set kriteria yang mendefinisikan elemen esensial dari evaluasi risiko keamanan informasi. Proteksi aset TI yang dilakukan akan berdasarkan pada risiko dari tiga area keamanan informasi yaitu *confidentiality, integrity* dan *availability* dari setiap kritikal aset yang dimiliki organisasi.

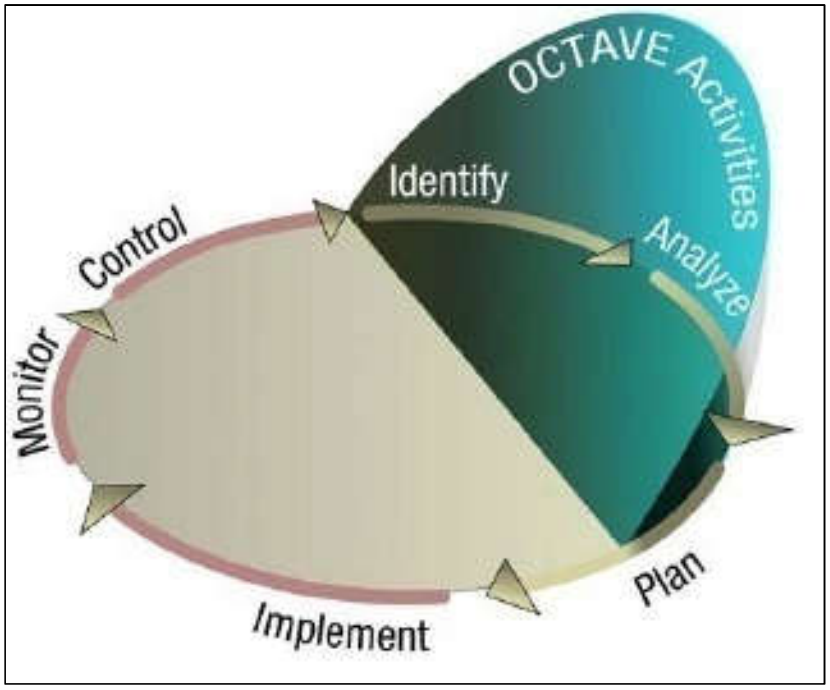
Secara umum metode octave menggunakan pendekatan tiga tahap yaitu Membangun Profil Ancaman berdasarkan Aset *(Build Asset-Based Threat Profile),* Mengidentifikasi Kerentanan Infrastruktur *(Identify Infrastructure Vulnerabilities)*, dan Mengembangan Rencana dan Strategi Keamanan *(Develop*

Security Strategy and Plan). Langkah langkah dalam menerapkan metode Octave dilakukan dengan pendekatan terhadap tiga tahap diatas. Dalam setiap fase dalam metode Octave memiliki beberapa proses yang mampu menguji isu teknologi dalam sebuah organisasi atau perusahaan dan memberikan sebuah gambaran komperhensif keamanan informasi yang dibutuhkan organisasi. Berikut ini merupakan metode Octave tiga tahap dan masing masing proses didalamnya :



Gambar 2.1 Fase Octave [3]

Setelah mengetahui tahapan dari metode octave selanjutnya mengetahui proses yang ada didalam octave *plan-do-check-act cycle* seperti (gambar 2.2) :



Gambar 2.2 Proses dalam Octave [3]

Fase 1 :Membangun Profil Ancaman berdasarkan Aset

Fase ini merupakan tahap mengidentifikasi aset yang kritikal dan ancaman pada masing masing aset TI. Dengan cara mengklasifikasikan aset yang penting bagi organisasi dan pengamanan yang dibutuhkan. Penentuan klasifikasi aset dilakukan dengan mengumpulkan informasi tentang aset, kebutuhan keamanan, ancaman dan kekuatan serta kelemahan organisasi dari beberapa tingkatan manjamen mulai dari *top level* hingga operasional. Proses dalam metode octave antara adalah identifikasi aset kritis, identifikasi kebutuhan keamanan aset kritis, identfikasi ancaman aset kritis, identifikasi keamanan yang sudah diterapkan, identifikasi kelemahan organisasi. Dalam fase ini luaran yang akan dihasilkan yaitu daftar aset-aset kritis bagi organisasi beserta ancaman dari masing masing aset.

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

   Proses ini merupakan proses dalam mengidentifikasikan aset kritis yang dimiliki oleh organisasi dan akan menghasilkan luaran berupa aset aset penting/kritis bagi organisasi.

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

   Proses ini merupakan proses dalam mengidentifikasikan kebutuhan keamanan dari masing-masing aset kritis bagi organisasi. Luaran yang dihasilkan adalah daftar kebutuhan keamanan aset-aset kritis bagi organisasi berdasarkan aspek *confidentiality, integrity, availability*.

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

   Proses ini merupakan proses dalam mengidentifikasi sumber ancaman dari masing-masing aset kritis dan pengaruhnya terhadap masing masing aset. Luaran dari proses ini adalah daftar sumber ancaman dan pengaruhnya terhadap aset.

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

   Proses ini merupakan proses dalam mengidentifikasikan praktik praktik kemananan terkini yang diimplementasikan dalam organisasi maupun upaya yang telah dilakukan organisasi dalam melindungi aset informasi. Luaran dalam proses ini adalah berupa daftar praktik keamanan yang dimiliki organisasi.

5. **Proses 5: identifikasi kelemahan organisasi**

   Proses ini merupakan proses dalam mengidentifikasi kelemahan kebijakan organisasi yang sedang diterapkan. Luaran dalam proses ini adalah berupa daftar kelemahan kebijakan organisasi.

Fase 2 :Mengidentifikasi Kerentanan Infrastruktur

Fase ini merupakan tahap mengidentifikasi kelemahan pada teknologi atau infrastruktur organisasi. Fase dua akan melakukan identifikasi komponen penting dalam sistem yang kemudian dilakukan evaluasi terhadap komponen utamanya. Hasilnya akan dianalisis untuk lebih memperjelas kembali profil ancaman pada aset TI yang sudah diidentifikasi diawal. Proses dalam fase dua adalah identifikasi komponen utama dan kelemahan teknologi yang sudah ada. Dalam fase ini luaran yang akan dihasilkan yaitu daftar ancaman dari masing masing aset yang kritis.

1. **Proses 1: identifikasi komponen utama**

   Proses ini adalah proses dalam mengidentifikasikan komponen utama dari infrastruktur teknologi informasi seperti server, PC, laptop, dan perangkat jaringan lainnya. Luaran dari proses ini adalah daftar komponen utama dalam organisasi.

2. **Proses 2: identifikasi kelemahan teknologi yang sudah ada**

   Proses ini adalah proses dalam mengevaluasi kelemahan informasi infrastruktur baik dalam segi teknologi yang sudah diterapkan organisasi maupun dalam konfigurasinya yang dapat menimbulkan akses keamanan yang tidak terautorisasi. Luaran dalam proses ini adalah daftar kelemahan dalam penerapan infrastruktur teknologi perusahaan.

Fase 3 : Mengembangan Rencana dan Strategi Keamanan

Fase ini merupakan tahap mengevaluasi risiko dan mengembangkan strategi keamanan informasi berdasarkan *best practice* serta membuat rencana mitigasi risiko. Pada tahap ini hasil dari proses analisa risiko akan dikembangkan kedalam strategi yang tepat untuk melindungi aset yang berfokus pada perbaikan praktik keamanan organisasi. Selain itu juga akan dibuat perencanaan mitigasi bila terjadi *accident*. Proses dalam tahapan tiga adalah identifikasi risiko aset kritis, penilian risiko, strategi perlingungan, rencana mitigasi risiko.

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

   Proses ini adalah proses dalam mengidentifikasi risiko berdasarkan aset kritis dalam organisasi. Luaran dalam proses ini daftar risiko dari masing masing aset kritis yang dimiliki organisasi.

2. **Proses 2: penilaian risiko**

   Proses ini adalah proses dalam melakukan penilaian risiko dari hasil identifikasi risiko aset kritis organisasi. Penilaian yang dilakukan akan berdasarkan pada standard metode FMEA. Luaran dalam proses ini adalah RPN *(Risk Priority Number)* dari masing masing aset kritis.

3. **Proses 3: strategi perlindungan**

   Proses ini adalah proses dalam mengidentifikasikan dan membangun startegi perlindungan bagi masing masing aset kritis. Luaran dalam proses ini adalah daftar strategi perlindungan aset kritis.

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

   Proses ini adalah proses dalam mengidentifikasikan dan membangun rencana mitigasi dari masing masing risiko yang dimiliki oleh aset kritis. Luaran dalam proses ini adalah dokumen rencana mitigasi risiko. Sehingga berdasarkan uraian metode Ocatve tiga tahap beserta prosesnya maka dapat disimpulkan luaran dari masing masing proses adalah sebagai berikut.

Sehingga berdasarkan uraian metode Octave tiga tahap beserta prosesnya maka dapat disimpulkan luaran dari masing masing proses adalah sebagai berikut.

Tabel 2.2 Metode Octave dan luaran

Tahap	Output
Fase I	• Aset Kritis • Kebutuhan keamanan untuk

	aset kritis • Ancaman pada aset kritis • Praktik keamanan saat ini • Kerentanan organisasi saat ini
Fase II	• Komponen utama • Kerentanan teknologi saat ini
Fase III	• Risiko aset kritis • Pengukutan risiko • Strategi perlindungan • Perencanaan mitigasi risiko

Berdasarkan penerapan langkah langkah dalam metode octave dalam mengidentifikasi aset kritis dan masing masing ancaman beserta identifikasi risiko dan strategi mitigasinya, maka akan didapatkan hasil luaran metode octave secara umum sebagai berikut.

1. Perencanaan mitigasi risiko yang berfokus pada perlindungan pada aset-aset kritis organisasi sehingga risiko-risiko tersebut dapat dikurangi.
2. Perencanaan mitigasi risiko yang berfokus pada perlindungan pada aset-aset kritis organisasi sehingga risiko-risiko tersebut dapat dikurangi.
3. Perencanaan aksi langkah-langkah mitigasi risiko. Perencanaan ini termasuk dalam pembuatan rencana jangka pendek untuk mengatasi beberapa kelemahan tertentu

2.4 Metode FMEA

Keberadaan TI dalam perkembangan zaman saat ini menjadi objek utama yang sangat dibutuhkan *Failure Mode and Effect Analysis* (FMEA) merupakan suatu pendekatan yang sistematik menerapkan suatu metode pentabelan untuk membantu proses pemikiran yang digunakan oleh *engineers* untuk mengidentifikasi mode kegagalan potensial dan efeknya. FMEA merupakan

teknik evaluasi tingkat keandalan dari sebuah sistem untuk menentukan efek dari kegagalan dari sistem tersebut. Kegagalan digolongkan berdasarkan dampak yang diberikan terhadap kesuksesan suatu misi dari sebuah sistem.

FMEA *(Failure Mode and Effect Analysis)* adalah metode yang akan digunakan dalam melakukan analisis risiko secara kuantitatif.

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.

Tujuan dari pembuatan metode FMEA bagi perusahaan anatara lain :

1. Mengidentifikasi *mode* operasional dan aset-aset internal perusahaan.
2. Mengidentifikasi potensi kegagalan dan penyebabnya.
3. Mengevaluasi efek dari setiap potensi kegagalan.
4. Meminimalakan risiko kegagalan dengan langkah-langkah penanganan risiko.
5. Menginfomasian kepada *stakeholder* terkait agar memiliki pemahaman yang jelas mengenai keterbatasan sistem.
6. Mendokumentasikan keseluruhan proses tersebut.

Secara umum, FMEA (*Failure Mode and Effect Analysis*) didefinisikan sebagai sebuah teknik yang mengidentifikasi tiga hal, yaitu :

1. Penyebab kegagalan yang potensial dari sistem, desain produk, dan proses selama siklus hidupnya,

2. Efek dari kegagalan tersebut,

3. Tingkat kekritisan efek kegagalan terhadap fungsi sistem, desain produk, dan proses.

2.4.1 Tujuan FMEA

Terdapat banyak variasi didalam rincian *Failure Mode and Effect Analysis* (FMEA), tetapi semua itu memiliki tujuan untuk mencapai :

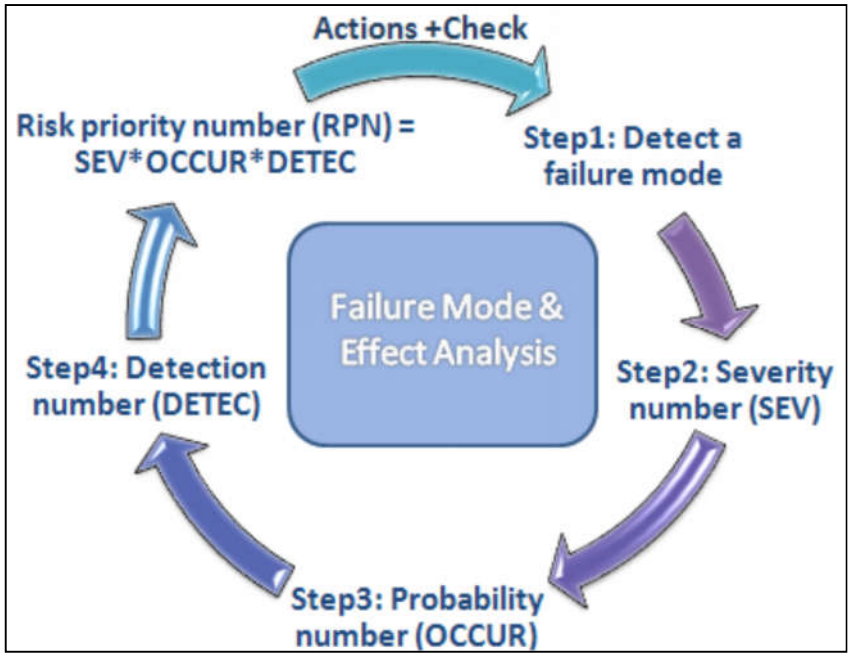
1. Mengenal dan memprediksi potensial kegagalan dari produk atau proses yang dapat terjadi.
2. Memprediksi dan mengevaluasi pengaruh dari kegagalan pada fungsi dalam sistem yang ada.
3. Menunjukan prioritas terhadap perbaikan suatu proses atau sub sistem melalui daftar peningkatan proses atau sub sistem yang harus diperbaiki.
4. Mengidentifikasi dan membangun tindakan perbaikan yang bisa diambil untuk mencegah atau mengurangi kesempatan terjadinya potensi kegagalan atau pengaruh pada sistem.
5. Mendokumentasikan proses secara keseluruhan.

2.4.2 Manfaat FMEA

Selain memiliki beberapa tujuan diatas, dalam penerapannya kerangka kerja FMEA juga memiliki manfaat, yaitu:

1. Membantu *engineer* untuk memprioritaskan dan mengurangi masalah-masalah serta mencegah terjadinya masalah
2. Membantu dalam pembuatan *control plan*
3. Mengidentifikasi dan mengeliminasi potensi kegagalan produk/proses dari awal
4. Mengurangi waktu dan biaya pengembangan ulang produk
5. Memberikan mitigasi/pencegahan dari penyebab potensi kegagalan
6. Memperbaiki kepuasan customer

Langkah langkah dalam menerapkan metode FMEA dilakukan dengan 5 tahapan. Tahapan pertama *detect a failure mode, Severity number* (SEV), *Probability number* (OCCUR), *Detection number* (DETEC), *Risk Priority Number* (RPN). Seperti pada (gambar 2.3) :



Gambar 2.3 Sirklus tahapan metode FMEA [6]

2.4.3 Tahap Metode FMEA

Metode FMEA secara keseluruhan prosesnya, Langkah-langkah dalam pembuatan digambarkan dalam bentuk sirklus seperti gambar di bawah ini [7] :

Berikut ini adalah penjelassan mengenai setiap langkah yang dilakukan dalam membuat FMEA *(Failure Modes and Effects Analysis)* sesuai dengan gambar siklus diatas :

1. **Langkah 0 (FMEA *Pre Work*)**
   a. Mengidentifikasi setiap *stakeholder* yang terlibat
   b. Mendefinisikan ruang lingkup dari konsep FMEA yang akan dibuat
   c. Mengumpulkan infomasi-informasi yang relevan dan yang dibutuhkan

2. Langkah 1 (*Development : Detect a Failure Mode*)

a. Mengidentifikasi dan mendata *failure mode* yang berpotensial

b. Mengidentifikasi dan mendata efek risiko bisnis yang berjalan

c. Mengidentifikasi dan mendata penyebab masing-masing *failure mode*

3. Langkah 2 (*Development : Severity Number*)

Dari setiap efek yang ditimbulkan akan diprioritaskan dari level 1 sebagai efek yang tidak parah hingga level 10 yang bisa mengakibatkan efek yang sangat parah, berikut adalah penjelasan akan *level severity* :

Setiap aset TI yang digunakan dalam organisasi atau perusahaan tentulah memiliki risiko yang ada didalamnya. Menurut Risk IT kerangka kerja [ISACA, 2009], Risiko Teknologi Informasi dapat dikategorikan sebagai :

1. Risiko nilai/keuntungan penggunaan Teknologi Informasi (*IT benefit / value enablement risk*)
2. Risiko pelaksanaan program dan proyek (*IT programme and project delivery risk*)
3. Risiko penghantaran operasional dan layanan Teknologi Informasi (*IT operations and service delivery risk*).

Tabel 2.3 *Severity number* [7]

Rank	***Effect***	***Severity of Effect***
10	***Dangerous High***	Kegagalan akan terjadi tanpa peringatan.
9	***Extreamly High***	Kegagalan akan terjadi dengan peringatan.
8	***Very High***	Semua proses bisnis utama dan pendukung terganggu. Penundaan

		yang signifikan dalam memulihkan fungsi.
7	***High***	Beberapa bagian dari proses bisnis utama dan pendukung hilang. Penundaan yang signifikan dalam memulihkan fungsi.
6	***Moderate***	Beberapa bagian dari proses bisnis utama dan pendukung hilang. terlambat dalam memulihkan fungsi.
5	***Low***	100% dari proses bisnis utama dan pendukung mungkin perlu di kerjakan ulang atau proses tertunda.
4	***Very Low***	Beberapa bagian dari proses bisnis utama dan pendukung mungkin perlu dikerjakan ulang atau proses tertunda.
3	***Minor***	Perbaikan juga teratasi selama terdapat peringatan namun tidak menunda proses bisnis

		utama dan pendukung.
2	***Very Minor***	Perbaikan kegagalan dalam teratasi selama terdapat peringatan masalah
1	***None***	Tidak perlu untuk memperkirakan kegagalan yang berpengaruh terhadap keselamatan, kesehatan, lingkungan atau proses bisnis utama dan pendukung.

4. Langkah 3 (Development : Occureness Number)

Dari setiap kegagalan yang telah diidentifikasi akan diprioritaskan dari level 1 hingga level 10 dengan penjelaskan berikut :

Tabel 2.4 *Occureness number* [7]

Rank	***Effect***	***Description***
10	***Dangerous High*** Kegagalan hampir/ tidak bisa dihindari	Kegagalan terjadi setiap saat
9	***Extreamly High***	Kegagalan terjadi

	Kegagalan selalu terjadi	setiap tiga atau empat hari
8	***Very High*** Kegagalan terjadi berulang kali	Kegagalan terjadi setiap seminggu
7	***High*** Kegagalan sering terjadi	Kegagalan terjadi setiap sebulan
6	***Moderate High*** Kegagalan terjadi saat watu tertentu	Kegagalan terjadi setiap tiga bulan
5	***Moderate*** Kegagalan terjadi sesekali waktu	Kegagalan terjadi setiap enam bulan
4	***Moderate Low*** Kegagalan jarang terjadi	Kegagalan terjadi setiap tahun
3	***Low*** Kegagalan terjadi relatif kecil	Kegagalan terjadi setiap tiga tahun
2	***Very Low*** Kegagalan terjadi relatif kecil dan sangat jarang	Kegagalan terjadi setiap lima tahun
1	***Remote*** Kegagalan tidak	Kegagalan terjadi setiap lebih dari lima

	pernah terjadi	tahun

5. Langkah 4 (Development : Detection Number)

Dari setiap kegagalan yang telah diidentifikasi akan diprioritaskan dari level 1 hingga level 10 dengan penjelaskan berikut :

Tabel 2.5 *Detection number* [7]

Rank	***Effect***	***Description***
10	***Absolutely Uncertainty***	Potensi penyebab tidak terdeteksi/ kontrol tidak mampu mencegah penyebab tersebut
9	***Very Remote***	Penyebab terdeteksi dan sangat kecil kemungkinan kontrol dapat mencegah kegagalan
8	***Remote***	Penyebab terdeteksi dan kecil kemungkinan kontrol dapat mencegah kegagalan
7	***Very Low***	Penyebab terdeteksi dan kemampuan kontrol dapat mencegah kegagalan adalah sangat rendah

6	***Low***	Penyebab terdeteksi dan kemampuan kontrol dapat mencegah kegagalan adalah rendah
5	***Moderate***	Penyebab terdeteksi dan kemampuan kontrol dapat mencegah kegagalan adalah cukup
4	***Moderate High***	Penyebab terdeteksi dan kemampuan kontrol dapat mencegah kegagalan adalah cukup tinggi
3	***High***	Penyebab terdeteksi dan kemampuan kontrol dapat mencegah kegagalan adalah tinggi
2	***Very High***	Penyebab terdeteksi dan kemampuan kontrol dapat mencegah kegagalan adalah sangat tinggi
1	***Almost Certain***	Penyebab terdeteksi dan kontrol yang ada pasti dapat mencegah kegagalan

6. Langkah 5 (*Risk Priority Number* (RPN))

Pada metode perhitungan FMEA, nilai RPN (*Risk Priority Number*) digunakan sebagai penentu level dari setiap risiko. Berikut ini adalah penentuan level risiko berdasarkan nilai RPN.

Tabel 2.6 *Risk Priority Number* [7]

Level Risiko	Skala Nilai RPN
Very High	**>= 200**
High	**120 sampai 199**
Medium	**80 sampai 119**
Low	**20 sampai 79**
Very Low	**0 sampai 19**

Skala RPN dari setiap risiko yang ada akan digunakan sebagai penentu level, di mana perusahaan dapat menilai risiko manakah yang bernilai paling tinggi. Perusahaan perlu melakukan antisipasi, mitigasi dan strategi terhadap risiko yang memiliki tingkatan paling tinggi, sehingga operasional bisnis perusahaan dapat tetap berjalan dengan optimal meskipun terjadi gangguan atau bencana.

2.5 Keamanan Informasi

Informasi adalah salah satu aset penting yang sangat berharga bagi proses bisnis utama organisasi/perusahaan. Keamanan informasi terdiri dari perlindungan terhadap 3 aspek CIA (*Confidentiality, Integrity, Avaiability*). *Confidentiality* (kerahasiaan) adalah aspek dalam menjamin kerahasiaan data atau informasi,

Integrity (integritas) yaitu aspek yang menjamin bahwa data tidak dirubah atau dimanipulasi tanpa ijin (*unauthorized access*) dan *Availabiity* (ketersediaan) merupakan aspek yang menjamin bahwa data akan tersedia saat dibutuhkan.

ISO 27002 merupakan standar khusus yang berisikan struktur dan pedoman yang diakui secara internasional untuk keamanan informasi. Standard ISO 27002 memberikan rekomendasi praktik terbaik untuk manajemen keamanan informasi dan penerapan sistem manajemen keamanan informasi (ISMS).

2.5.1 Komponen Keamanan Informasi

Keamanan informasi dapat dicapai dengan kontrol secara simultan dan prosedur manajemen aset informasi yang terstruktur dan sesuai standar. Komponen keamanan informasi secara umum dibedakan kedalam 6 komponen utama yaitu *Physical security, Personal security, Operation security, Communication security, Network security*, dan *Information security*.

Physical security adalah keamanan informasi yang memfokuskan pada strategi untuk mengamankan individu dalam organisasi, aset fisik tempat kerja dari berbagai ancaman. *Personal security* adalah keamanan informasi yang berhubungan dengan keamanan personil. *Operation security* adalah kemanan informasi yang berkaitan dengan strategi suatu organisasi dalam beroperasi. *Communication security* adalah keamanan informasi yang bertujuan dalam mengamankan seluruh media komunikasi dan teknologi komunikasi. *Network security* adalah keamanan informasi yang berfokus pada pengamanan jaringan dan data informasi organisasi.

2.5.2 Aspek Keamanan Informasi

Keamanan informasi menurut Mattord, Dr. Michael E. Whitman mencakup lima aspek utama yaitu *privacy* (kerahasiaan), *identification* (identifikasi), *authentication* (autentifikasi), *authorization* (autorisasi), *accountability* (akuntabilitas) [8].

Privacy akan menjamin kerahasiaan data informasi dari pemilik informasi agar tidak jatuh pada orang lain. *Identification* adalah langkah pertama dalam memperoeh hak akses kedalam sistem informasi yang diamankan. *Authentication* adalah proses yang dilakukan sistem untuk melakukan pembuktian bahwa pengguna memang benar orang yang memiliki identifikasi yang benar. *Authorization* adalah proses kelanjutan dari *authentication* yang berarti memberikan jaminan bahwa pengguna telah mendapat validasi secara spesifik dan jelas untuk mengakses, mengubah ataupun menghapus isi dari aset informasi. *Accountability* adalah proses yang dilakukan sistem untuk menyajikan data semua aktifitas aset informasi yang telah dilakukan.

Dari kelima elemen tersebut secara umum aspek informasi dapat diklasifikasikan kedalam 3 aspek utama yaitu *Confidentiality, Integrity* dan *Availability*. (ISO/IEC 27000, 2014).

1. *Confidentiality* merupakan aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang memiliki hak akses dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
2. *Integrity* merupakan aspek yang menjamin tidak adanya pengubahan data tanpa adanya *authentication* oleh orang yang mengakses, mejaga keakuratan dan keutuhan informasi.
3. *Availability* merupakan aspek yang menjamin bahwa data akan tersedia saat dibutuhkan kapanpun dan dimanapun, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait.

2.5.3 Ancaman Keamanan Informasi

Ancaman terhadap kemanan informasi dapat dikategorikan kedalam ancaman yang berasal dari internal seperti kesalahan teknis, dan kesalahan manusia (*human errors*) maupun kesalahan yang berasal dari luar sistem seperti adanya gangguan untuk masuk kedalam sistem secara illegal oleh beberapa *hacker/cracker*. Berikut ini merupakan beberapa ancaman umum pada keamanan sistem informasi.

1. *Data Tampering/Data Diddling*

Data Tampering adalah perubahan data yang berlangsug sebelum dan selama proses dan sesudah proses dari sistem informasi. Data diubah sebelum dipros yaitu pada saat dokumen dasar di-*verifikasi* sebelum dimasukan ke sistem informasi. Data diubah saat proses adalah perubahan data saat dilakukannya proses *input*. Data diubah setelah proses yaitu dengan mengganti nilai keluarannya. Pada umumnya ancaman ini dilakukan oleh orang dalam internal perusahaan.

2. *Programming Fraud*

Programming fraud merupakan penyelewengan program yang berarti memodifikasi program komputer untuk maksut kejahatan tertentu. Berikut ini merupakan contoh dari programming fraud.

a. *Virus* merupakan penggalan kode yang dapat secara pasif mengaktifkan dirinya sendiri. Virus bersifat karena hanya akan aktif jika terdapat *trigger* untuk memulai proses penyalinan kode dan penempelan berkas program yang akan dieksekusi.
b. *Worm* adalah program yang dapat menggandakan dirinya sendiri dengan cepat dan masuk kedalam sistem komputer melalui jaringan.
c. *Trojan Horse* adalah program komputer yang dirancang agar dapat digunakan untuk menyusup kedalam sistem. Contohnya adalah program yang dapat menciptakan pemakai dengan *authorized* sebagai *supervisor* atau *superuser*.

d. *Round Down Technique* adalah bagian program yang akan membulatkan nilai pecahan kedalam nilai bulat dan mengumpulkan nilai pecahan yang dibulatkan tersebut. Hal ini bila diterapkan pada sistem perbankan maka akam membuat program melakukan pembulatan ke bawah untuk semua biaya Bunga yang dibayarkan nasabah dan memasukan pecahan yang dibulatkan tersebut ke rekeningnya.
e. *Salami Slicing* merupakan bagian program yang mendorong sebagian kecil dari nilai transaksi yang besar dan mengumpulkan potongan potongan ini dalam suatu periode tertentu.

3. Penetrasi Sistem Informasi

Berikut ini merupakan beberapa teknik dalam penetrasi sistem informasi yang dapat mengancam keamanan aset informasi.

a. *Piggybacking* adalah menyadap jalur telekomunikasi dan ikut masuk ke dalam sistem komputer bersama-sama dengan pemakai sistem komputer yang resmi.
b. *Masquerading /impersonation* yaitu penetrasi ke sistem komputer dengan memakai identitas dan *password* dari orang lain yang sah. Identitas dan *password* ini biasanya diperoleh dari orang dalam.
c. *Sniffer* merupakan teknik yang diimplementasikan dengan membuat program yang dapat melacak paket data seseorang ketika paket tersebut melintasi internet, menangkap *password* atau menangkap isinya.
d. *Spoofing* merupakan melakukan pemalsuan alamat *e-mail* atau *web* dengan tujuan untuk menjebak pemakai agar memasukkan informasi yang penting seperti *password* atau nomor kartu kredit.

2.6 Definisi Aset

Pengertian aset menurut Siregar tahun 2004 adalah barang atau sesuatu yang mempunyai nilai ekonomi, nilai komersil, atau nilai tukar yang dimiliki oleh suatu

badan usaha, instansi atau individu. Aset terbagi menjadi 2 jenis yaitu *tangible* (asset berwujud) dan *intangible* (aset tidak berwujud).

Sedangkan menurut Robert T. Kiyosaki, aset adalah setiap benda yang dapat menjadi sumber pendapatan organisasi dan dapat dijual/dimiliki nilai. Dari kedua pendapat para ahli diatas, dapat disimpulkan bahwa aset adalah sesuatu yang mempunyai nilai bagi individu atau organisasi.

2.7 Definisi Aset Kritis

Pengertian Aset menurut ISO 55000 adalah sesuatu yang bersifat potensial dan memiliki nilai yang terukur (*tangible)* maupun tidak terukur (*intangible)* bagi organisasi. Sedangkan Aset kritis berdasarkan ISO 55000:2014 adalah sesuatu yang memiliki potensi dampak signifikan dalam ketercapaian tujuan organisasi. Aset kritis dapat pula berupa sebuah asset yang diperlukan untuk menyediakan layanan yang bersifat kritis.

2.8 Komponen SI/TI dan Ancaman

Sistem Informasi merupakan suatu kombinasi dari beberapa komponen *people* (orang), *hardware* (perangkat keras), *software* (perangkat lunak), *computer networks* dan *data communcations* (jariangan komunikasi) serta *database* (basis data) yang mengumpulkan, mengubah dan menyebarkan informasi di dalam suatu bentuk organisasi [O'Brien JA, 2010]. Model sistem informasi menurut O'Brienmerujuk pada kerangka konsep dasar untuk berbagai komponen dan aktivitas sistem informasi. Berdasarkan pengertian tersebut, maka terdapat lima komponen utama dalam sistem Informasi. Kelima komponen tersebut adalahsebagai berikut :

1. *People* (orang) merupakan semua pihak yang bertanggung jawab dalam pengembangan sistem informasi, pemrosesan, dan penggunaan keluaran sistem informasi.

2. *Hardware* (perangkat keras) mencakup tidak hanya mesin seperti komputer dan perlengkapan lainnya, tetapi juga semua media data, yaitu objek

berwujud tempat data dicatat (*disk magnetis*). Hardware sebagai sumber daya pemrosesan informasi dibagi kedalam sistem komputer yang terdiri dari unit pemrosesan pusat berisi pemrosesan mikro dan berbagai peripheral yang saling berhubungan.

3. *Software* merupakan sember daya yang meliputi semua rangkaian perintah pemrosesan informasi. Konsep umum software ini meliputi rangkaian perintah operasi dengan hardware komputer yang disebut program, rangkaian perintah pemrosesan informasi yang disebut prosedur.
4. *Database* merupakan sekumpulan tabel, hubungan dan lain lainnya yang saling berhubungan dan disimpan, diatur serta dapat diakses oleh berbagai teknologi pengelolaan.
5. *Network and data communications* (jaringan dan komunikasi data) merupakan sistem penghubung yang memungkinkan sumber (*resources*) dipakai secara bersama atau diakses oleh sejumlah pemakai.

Threat atau ancaman merupakan suatu potensi yang disebabkan oleh insiden yang tidak diinginkan dan membahayakan jalannya proses bisnis utama organisasi [9]. Berdasarkan kelima komponen sistem informasi tersebut, identifikasi terhadap ancaman sistem informasi dibagi kedalam dua tipe yaitu pasif dan aktif.

Tabel 2.7 Ancaman Komponen SI/TI [10]

Tipe	Ancaman	Contoh
Aktif	Bencana alam dan politik	Gempa bumi, banjir, kebakaran, perang, krisis ekonomi
	Kesalahan manusia *(Human error)*	Kesalahan pemasukan data, Kesalahan penghapusan data
Pasif	Kegagalan perangkat lunak dan perangkat keras	Ganggguan listrik, Kegagalan fungsi perangkat lunak Kegagalan peralatan
	Kecurangan dan kejahatan komputer (*Hacker*)	Penyelewengan aktivitas, Penyalahgunaan kartu kerdit Sabotase Pengaksesan oleh orang yang tidak berhak
	Program komputer	*Virus, worm, Spy*

2.9 Mitigasi Risiko

Mitigasi Risiko didefinisikan sebagai mengambil langkah – langkah untuk mengurangi kerugian yang ditimbulkan dari dampak atas risiko tersebut. Ada 4 tipe stragtegi mitigasi yang dibutuhkan untuk kelangsungan bisnis (*Business Continuity*) dan pemulihan bencana (*Disaster Recovery*). Dari panduan *Guide to Risk Assessment & Respons,* Agustus:2012:

1. **Penerimaan Risiko (*Risk Acceptance*)**

   Strategi ini biasanya digunakan apabila efek dari risiko ini dinilai cukup besar dan tidak dapat dihindari. Seperti risiko alamiah berupa becana alam dan lain sebagainya. Strategi ini juga bisanya dilakukan karena biaya untuk mengatasi maupun menghindari risiko ini sendiri lebih besar daripada jika perusahaan memilih untuk menerimanya. Strategi ini juga biasanya digunakan apabila risiko memiliki kemungkinan terjadi yang kecil.

2. **Penghindaran Risiko (*Risk Avoidance*)**

   Berbeda dengan penerimaan risiko, strategi penghindaran risiko atau *risk avoidance* ini adalah menghindari risiko itu untuk terjadi bagaimanapun caranya. Strategi ini biasanya memerlukan biaya yang tinggi dan dilakukan apabila dampak dari risiko yang akan terjadi cukup merugikan organisasi atau perusahaan.

3. **Pembatasan Risiko (*Risk Limitation/Mitigation*)**

   Pembatasan risiko ini adalah strategi dimana organisasi atau perusahaan melakukan beberapa kegiatan untuk mengurangi atau membatasi dampak dari risiko ini. Pembatasan risiko ini adalah gabungan dari penerimaan risiko (*risk acceptance*) dan penghindaran risiko (*risk avoidance*).

4. **Pentransferan Risiko (*Risk Tranference*)**

   Pentransferan risiko adalah bagaimana melibatkan pihak lain untuk menyerah risiko tersebut kepada mereka. Hal ini biasanya dilakukan apabila risiko yang ditransferkan bukan meruapakan kompetensi utama dari perusahaan, sehingga perusahaan akan lebih berfokus kepada kompetensi utama mereka.

Dalam penentuan penanganan dan strategi risiko, tindakan yang diambil untuk penanganan tiap masing risiko akan mengacu pada standar ISO/IEC 27001 dan ISO/IEC 27002 yang mana merupakan standar dalam Sistem Manajemen Keamanan Informasi atau *Information Security Management System* (ISMS).

2.9.1 ISO 27001

ISO/IEC 27001 adalah suatu standar yang dikeluarkan oleh *International Organization for Standardization* (ISO) dan *International Electrotechnical Comission* (IEC) pada bulan Oktober, 2005. ISO/IEC 27001 adalah standar mengenai *Information Security Management* yang dapat membantu organisasi melakukan standarisasi untuk menjaga keamanan dari asset informasi. ISO/IEC menyediakan kebutuhan kebutuhan yang harus dipenuhi perusahaan terkait dalam Sistem Manajemen Keamanan Informasi atau *Information Security Management System* (ISMS).

2.9.2 ISO 27002

ISO/IEC 27002 merupakan standar mengenai keamanan informasi yang dikeluarkan oleh *International Organization for Standardization* (ISO) dan *International Electrotechnical Commission* (IEC). ISO/IEC 27002 masih memiliki keterkaitan dengan dokumen ISO/IEC 27001, dokumen di dalamnya berisi mengenai teknik keamanan – *Code of Practice* untuk manajemen keamanan informasi.

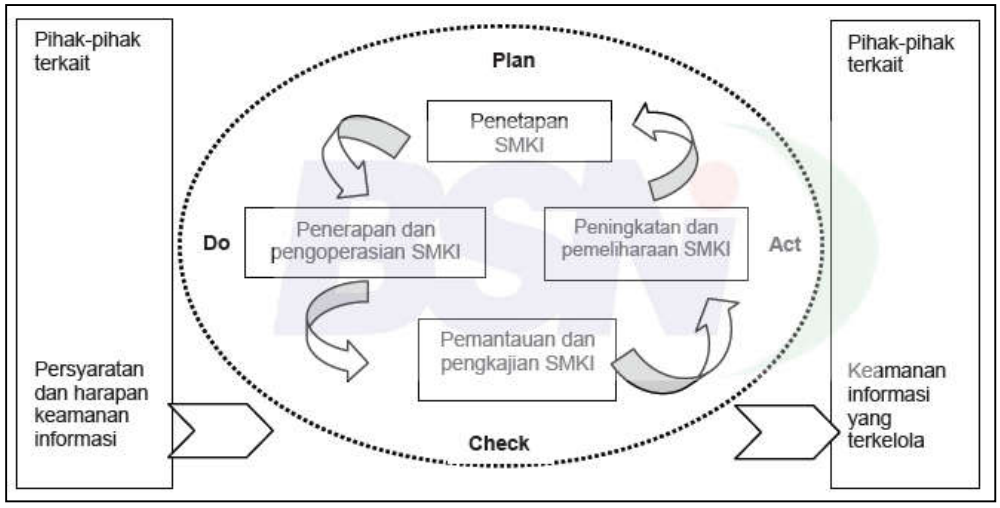
2.10 ISO 27001

ISO (*International Organization for Standarzitation*) adalah pengembang terbesar di dunia standar internasional. Tujuan dari ISO 27001 adalah untuk menyediakan model guna penetapan, penerapan, pengoperasian, pemantauan, pengkajian, memelihara, dan meningkatkan SMKI [11].

Menurut [12] standar ISO 27001 ini berlandaskan sistem manajemen berbasis risiko dan dirancang untuk menjamin agar kontrol-kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko. Standar ISO 27001 berisi 5 elemen utama yang harus dipenuhi menyangkut:

1. Sistem manajemen keamanan informasi
2. Tanggung jawab manajemen
3. Audit internal Sistem Manajemen Keamanan Informasi (SMKI)
4. *Management review*
5. *Continous improvement*

Standar ISO 27001 mengadopsi model *Plan – Do – Check - Act* yang diterapkan untuk membentuk seluruh proses SMKI. Berikut merupakan penjelasan fase *Plan-Do-Check-Act* pada ISO 27001: [11]



Gambar 2.4 Fase pada ISO 27001 [11]

Menurut [11] manfaat dari penerapan ISO 27001 pada manajemen risiko adalah Menyimpan keamanan informasi yang rahasia sebagai berikut:

1. Mengemukakan bagaimana perusahaan mengelola risiko dengan percaya diri pada pelanggan dan pihak yang berkepentingan.
2. Memungkinkan untuk pertukaran informasi yang aman.
3. Memberikan keunggulan kompetitif.
4. Meningkatkan kepuasan pelanggan yang meningkatkan retensi klien.
5. Konsisten dalam penyampaian pelayanan ataupun produk.