BAB 2
TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Beberapa penelitian terkait mitigasi resiko yang sebelumnya telah dilakukan dengan menggunakan metode OCTAVE yaitu Evaluasi risiko atas keamanan jaringan komputer di rumah Sakit Mohammad Hoseim Palembang oleh Muhammad Iqbal, M. Akbar dan Rusmala Santi[2]. Penelitian itu dilakukan dikarenakan tidak adanya bentuk pencegahan dan penilaian atas jaringan komputer yang digunakan pada rumah sakit yang menyimpan begitu banyak data penting tentang pasien sehingga menyebabkan rentannya rusak maupun hilang data. Kemudian penggunaan metode OCTAVE juga dilakukan oleh Bambang Supradono.[3]

Penelitian mengenai evaluasi mitigasi resiko yang menggunakan metode FMEA sebelumnya pernah dilakukan oleh Innike Desy, Bekti Cahyo Hidayanto dan Hanim Maria Astuti[4]. Penelitian tersebut dilakukan karena belum adanya upaya pencegahan pada aset TI yang dimiliki oleh bank XYZ yang tentunya berperan penting dalam proses bisnis.

Penelitian dengan penggabungan dua metode ini pernah dilakukan oleh Dea Anjani, Dr. Apol Pribadi Subriadi, MT dan Aniszah hediyanti, S.Kom, M.Sc pada RSU Haji Surabaya[5]. Penelitian itu dilakukan karena belum adanua tindakan identifikasi, penilaian dan mitigasi risiko pada salah satu aplikasi yang digunakan dalam penjalanan proses bisnisnya.

Tabel 2.1 Penelitian Terkait

No	Nama Peneliti dan Tahun	Masalah	Metode	Hasil
1.	Muhammad Iqbal, M. Akbar dan Rusmala Santi, 2011	Belum adanya bentuk pencegahan maupun penilaian atas jaringan komputer yang digunakan, sehingga sistem jaringan komputer yang digunakan dalam proses bisnis masih berisiko besar dalam proses penjalanannya seperti misal penyalahgunaan wewenang, virus, *hacking,* dll.	Menggunakan metode OCTAVE sebagai alat pengukur tingkat resiko keamanan jaringan pada rumah sakit Moh. Hosein.	Mengelompokkan dan mengukur tingkat keamanan dan ancaman. Sehingga diketahui bahwa keamanan Jaringan rumah sakit Mohammad Hosein sangat bergantung pada staff dan karyawan, ancaman-ancaman yang serius terhadap data dan jaringan di komputer dapat diketahui, dan hasil penelitian ini memberikan kontribusi saran perbaikkan resiko keamanan pada jaringan komputer rumah sakit Mohammad Hosein untuk mengurangi acaman yang terdapat

No	Nama Peneliti dan Tahun	Masalah	Metode	Hasil
				di jaringan.
2.	Innike Desy, Bekti Cahyo Hidayanto dan Hanim Maria Astuti, 2014	Belum adanya bentuk pencegahan pada asset TI sehingga masih sering terjadinya ketidak-konsistenan input data dan data menjadi tidak lengkap, karena belum tentu semua data-data penting terkait pasien yang terdapat di dalam dokumen rekam medis juga ada pada rekam medis elektronik, dan beberapa kemungkinan lainnya.	Menggunakan metode FMEA untuk mengidentifikasi dan mengevaluasi kegagalan yang potensial, menentukan nilai risiko kegagalan dan tindakan yang harus diambil.	Memberikan nilai pada tiap asset. Asset dengan nilai paling besar harus mendapatkan perhatian khusus. Sehingga dari proses identifikasi risiko diketahui penyebab terjadinya suatu risiko dan tingkatan risiko (nilai assesment risiko). Dan hasil RPN atas penilaian risiko menggunakan metode FMEA diberikanlah saran penanganan maupun tindakan pengendalian dan kontrol atas risiko. Saran pengendalian mengacu pada ISO 27002 dimana standar tersebut berfokus kepada ISMS.

No	Nama Peneliti dan Tahun	Masalah	Metode	Hasil
3.	Bambang Supradono, 2009	Belum adanya pemahaman pihak organisasi mengenai hal yang harus dilindungi dan menentukan solusi secara tepat yang dapat menangani permasalahan atas kebutuhan keamanan informasi. Sehingga pengelolaan keamanan informasi yang sistemik dan komprehensif dibutuhkan.	Metode OCTAVE digunakan untuk menguji isu-isu pada organisasi dan teknologi terhadap penyusunan masalah-masalah yang komprehensif berdasarkan atas kebutuhan keamanan informasi sebuah organisasi.	Pemakaian metode OCTAVE memberikan panduan sistemik dan komprehensif dalam memanajemen risiko keamanan informasi pada organisasi. Metode ini lebih menekankan pada strategi pengelolaan risiko berbasis ancaman *(threat)* dan kelemahan *(vulnerability)* atas aset-aset informasi organisasi. Sehingga suatu rencana mitigasi risiko yang terkait dengan tingkat risiko yang dimiliki organisasi terbentuk.
4.	Dea Anjani, Dr. Apol Pribadi	Belum dilakukannya manajemen risiko sebagai	Penggunaan metode OCTAVE dan FMEA	Didapatkan bahwa penyalahgunaan hak akses sangat tinggi sehingga harus

No	Nama Peneliti dan Tahun	Masalah	Metode	Hasil
	Subriadi, MT, Aniszah hediyanti, S.Kom, M.Sc, 2014	panduan dalam mengarahkan dan mengendalikan organisasi untuk mengelola risiko yang mungkin terjadi pada Rumah Sakit Umum Haji Surabaya.	dilakukan untuk menghasilkan sebuah dokumen yang berisikan pedoman penanganan masalah pada EMR di RSU Haji Surabaya, sehingga kegunaan teknologi informasi lebih optimal.	diprioritaskan penyelesaiannya. Sehingga tindakan penanganan atas risiko tersebut yang mengacu pada ISO 27002 terbentuk.

Penelitian ini menggabungkan kedua metode tersebut untuk menyempurnakan bentuk penilaian yang sebelumnya hanya menggunakan salah satu metode. Dengan menggunakan metode OCTAVE dalam pengolahan data yang didapat, penulis akan mengelompokkan dan mengukur tingkat keamanan dan ancaman yang ada pada Politeknik Kesehatan Kemenkes Semarang. Kemudian pemberiaan nilai pada tiap komponen risiko aset TI pada Politeknik Kesehatan Kemenkes Semarang akan diberikan bobot sesuai dengan tingkatan risiko sehingga penilaian risiko menjadi semakin tepat dan akurat dengan menambahkan penggunaan metode FMEA.

2.2 Risiko

Merupakan akibat yang kurang menyenangkan (merugikan, membahayakan) dari suatu perbuatan atau tindakan sesuai dengan yang dituliskan di Kamus Besar Bahasa Indonesia.

Menurut [6] risiko dapat dibedakan dari sifatnya berikut:

1. *Particular risk* (Risiko Khusus), merupakan risiko yang disebabkan oleh individu dan memiliki dampak yang kecil.
2. *Fundamental risk* (Risiko Fundamental), merupakan risiko yang disesabkan oleh masyarakat umum dan efeknya mempengaruhi masyarakat luas.
3. *Static risk* (Risiko statis), merupakan risiko yang tidak berubah meskipun zaman telah berubah.
4. *Dinamic risk* (Risiko dinamis), merupakan risiko yang mengalami perubahan sesuai dengan perkembangan zaman.

2.2.1 Mitigasi Risiko

Berdasarkan UU Nomor 24 Tahun 2007, mitigasi risiko merupakan serangkaian upaya yang digunakan untuk mengurangi risiko bencana baik itu melalui penyadaran dan peningkatan kemampuan dalam menghadapi ancaman atas bencana maupun melalui pembangunan fisik.

2.2.2 Manajemen Risiko Teknologi Informasi

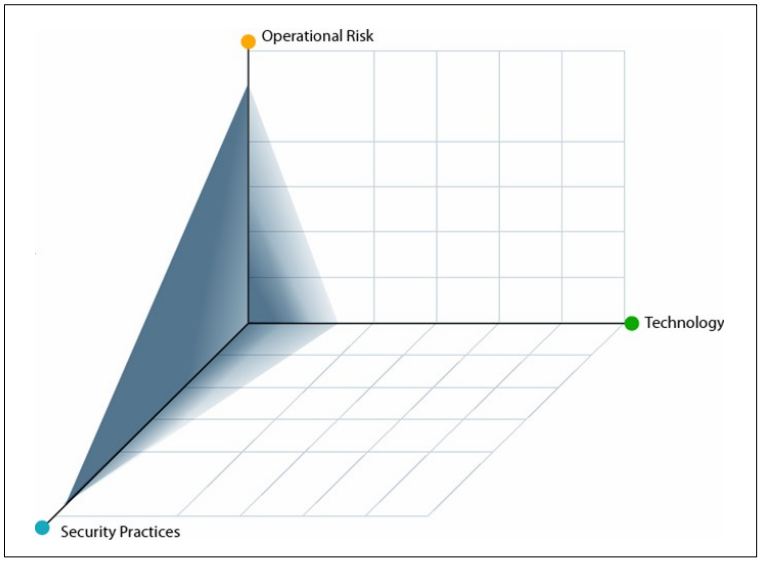
Manajemen risiko adalah bentuk dari proses pengukuran serta pengembangan strategi pengelolaan risiko. Strategi tersebut antara lain yaitu menghindari terjadinya risiko maupun mengurangi efek buruk yang dihasilkan oleh risiko. Penggunaan Teknologi Informasi (TI) dalam proses bisnis tentunya berdampak langsung pada kegiatan operasional organisasi dan memiliki risiko dalam penerapannya. Beberapa faktor penyebab munculnya risiko operasional yaitu proses internal yang tidak berfungsi dengan baik, kesalahan manusia dan sistem yang gagal dalam pemakaiannya. Dengan melakukan mitigasi risiko TI pada organisasi, akan didapatkan suatu perencanaan yang dapat digunakan untuk mendukung kelangsungan proses bisnis yang lebih baik. Sebuah rencana yang

terintegrasi yang mengidentifikasi kegiatan bisnis penting, risiko, rencana atas respon kegagalan maupun prosedur pemulihan[7].

2.3 Metode OCTAVE

Metode OCTAVE merupakan teknik strategi dan perencanaan untuk keamanan atas risiko. Perbedaan metode ini dengan metode penilaian lain yang berfokus pada teknologi yaitu bahwa OCTAVE ditargetkan kepada risiko organisasi dan terfokus pada strategi, penerapan keamanan, evaluasi organisasi, dan pengarahan organisasi kedepannya. Berbeda dengan metode pendekatan lain yang berfokus pada evaluasi sistem, metode OCTAVE berfokus kepada teknologi[8].

Dengan menggunakan pendekatan OCTAVE, organisasi menciptakan suatu keputusan proteksi informasi berdasarkan pada informasi sangat penting atas aset-aset yang ada. Seluruh aspek risiko termasuk didalamnya aset, ancaman, kelemahan dan dampaknya pada organisasi diolah untuk menentukan penentuan tindakan.



Gambar 2.1 Tiga aspek keseimbangan OCTAVE [8]

Tabel berikut merupakan gambaran singkat perbedaan antara OCTAVE dan metode lain:

Tabel. 2.2 Kunci perbedaan OCTAVE dengan metode lain

OCTAVE	Metode Lain
Evaluasi Organisasi	Evaluasi Sistem
Terfokus pada tindakan keamanan	Terfokus pada teknologi
Strategi	Taktis
Self direction	*Expert led*

Organisasi, teknologi, dan aspek analisis yang mempengaruhi evaluasi informasi keamanan risiko dilakukan dengan menggunakan tiga fase pendekatan. Fase-fase tersebut yaitu:

Fase 1 : Membangun profil ancaman berlandaskan aset yang ada di organisasi

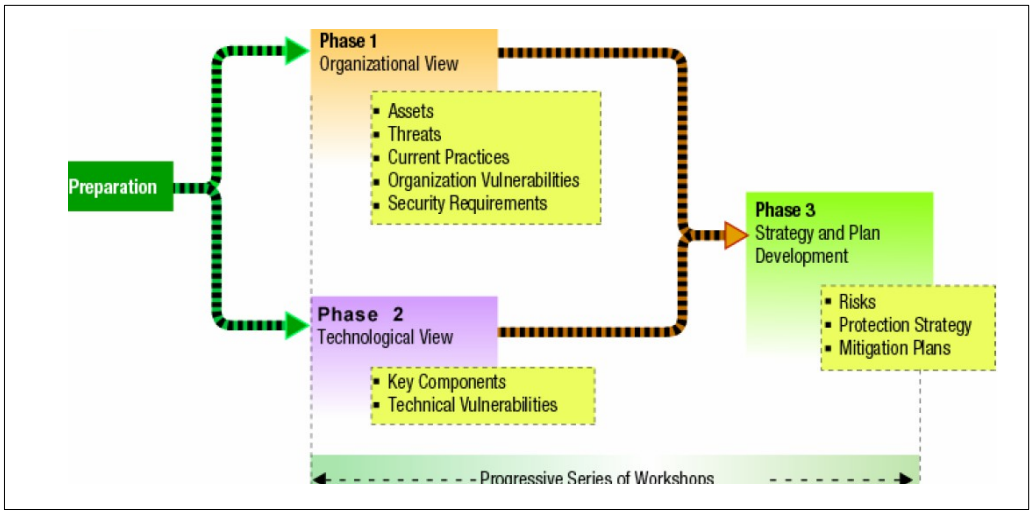
Merupakan langkah evaluasi atas organisasi. Tim analisis menentukan apa yang penting bagi organisasi dan apa yang saat ini sedang diterapkan dalam melindungi aset. Aset-aset tersebut kemudian dipilih mana yang paling penting bagi organisasi (aset kritis) dan mendeskripsikan kebutuhan keamanan pada masing-masing aset kritis. Kemudian, akan teridentifikasi ancaman pada tiap aset kritis dan dibuat profil ancaman.

Fase 2 : Mengidentifikasi Kerentanan Infrastuktur/Teknologi

Adalah evaluasi atas informasi infrastruktur baik itu berupa pemeriksaan jalur akses, mengidentifikasi kelas-kelas komponen teknologi informasi yang berkenaan dengan masing-masing aset kritis. Menentukan seberapa luas tiap komponen mampu bertahan atas serangan jaringan.

Fase 3 : Mengembangkan rencana dan strategi keamanan

Dalam proses evaluasi ini, risiko 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 analisa dari informasi yang telah dikumpulkan.



Gambar 2.2 Fase OCTAVE [8]

Tahapan penggunaan metode OCTAVE:

Fase 1: Membangun profil ancaman berdasarkan aset –dua fungsi utama pada fase ini yaitu mengumpulkan informasi dari seluruh bagian organisasi dan menentukan profil ancaman untuk aset kritis.

Proses 1: Mengidentifikasi pengetahuan manajemen senior

Tim analis mengumpulkan informasi mengenai aset penting, kebutuhan keamanan, ancaman, dan kekuatan organisasi saat ini dari tiap level manajemen oleh perwakilan dari senior manajer.

Proses 2: Mengidentifikasi aset kritis dan menentukan kebutuhannya atas keamanan

Tim analisis mengumpulkan informasi mengenai aset penting, kebutuhan keamanan, ancaman, dan kekuatan organisasi saat ini dari manajer dari area operasional tertentu.

Proses 3: Mengidentifikasi Pengetahuan Staf

Tim analisis mengumpulkan informasi mengenai aset penting, kebutuhan keamanan, ancaman, dan kekuatan organisasi saat ini dari staf dan star IT yang merupakan bagian dari divisi operasional bersangkutan.

Proses 4: Membuat profil ancaman

Tim analis memilih informasi kritis terkait aset dan menjabarkan profil ancaman untuk masing-masing aset.

Fase 2: Mengidentifikasi celah berupa kelemahan pada infrastruktur –pada fase ini komponen kunci sistem yang mendukung berjalannya aset kritis kerentanan teknologi di evaluasi.

Proses 1: Mengidentifikasi komponen kunci/*Key Component*

Mengidentifikasi serangkaian komponen kunci dari sistem yang mendukung kegiatan terkait informasi aset kritis dan dilakukan pendekatan untuk dilakukan evaluasi.

Proses 2: Mengevaluasi komponen yang telah dipilih –evaluasi atas komponen yang telah dipilih dilakukan dan hasilnya dianalisa untuk dibedakan atas profil ancaman seperti ancaman akses jaringan pada aset kritis juga ditentukan kelemahan dari komponen tersebut.

Fase 3: mengembangkan strategi dan rencana keamanan –tujuan utama dari fase ini yaitu untuk mengevaluasi risiko aset kritis dan mengembangkan strategi perlindungan organisasi dan rencana mitigasi.

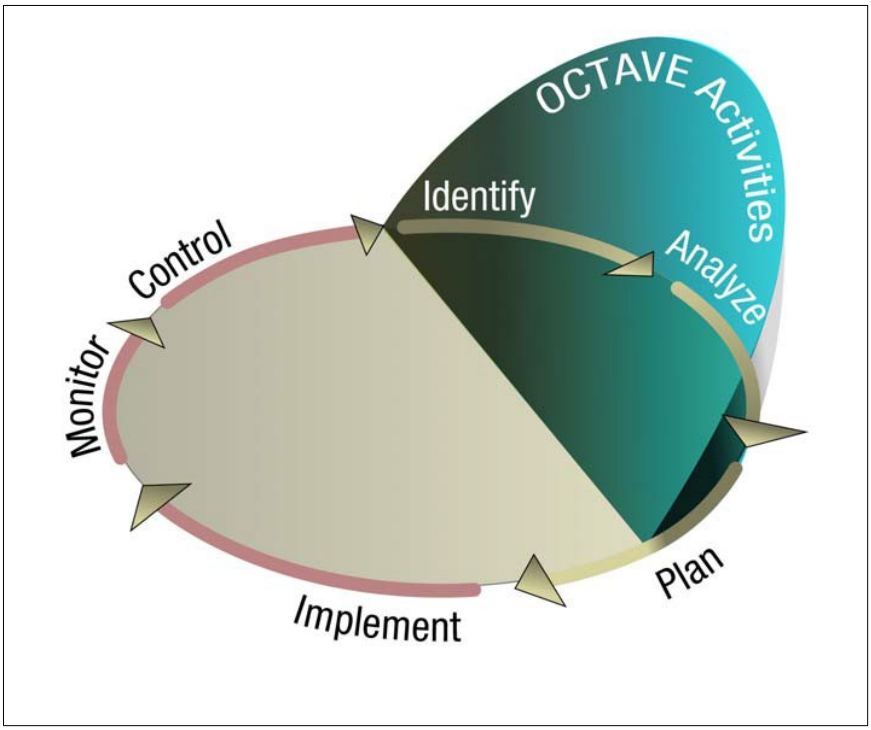
Proses 1: pengarahan analisis risiko

Menentukan dampak apakah termasuk tinggi, menengah, atau rendah yang tergantung pada ancaman tiap aset kritis. Semua risiko dievaluasi untuk mengetahui dampaknya.

Proses 2: Mengembangkan strategi perlindungan/keamanan

Strategi perlindungan menyeluruh atas organisasi yang terfokus pada pengembangan kegiatan keamanan organisasi termasuk didalamnya rencana mitigasi untuk mengurangi terjadinya risiko pada aset kritis yang notabene sangat penting bagi organisasi.

Sebuah evaluasi risiko keamanan informasi merupakan bagian dari organisasi untuk mengelola risiko keamaman informasi. OCVTAVE merupakan kegiatan evaluasi, bukan proses yang terus berulang. Gambar berikut menunjukan relasi antar aktivitas dalam OCTAVE. Kegiatan manajemen risiko merupakan siklus *plan-do-check-act.*



Gambar 2.3 kegiatan OCTAVE dan manajemen risiko [8]

2.4 Metode FMEA

Metode *Failure and Effects Analysis* (FMEA) merupakan pendekatan secara sistematis untuk mengidentifikasi peluang terjadinya kegagalan dalam sistem, proses, serta produk maupun servis. *Failure Mode* berfokus pada langkah ataupun penggunaan mode yang memungkinkan terjadinya kegagalan, sedangkan *Effects Analysis* berfokus pada evaluasi yang membahas konsekuensi yang akan diterima

dari kegagalan tersebut. Dalam penerapannya FMEA merupakan *living documents*, maka dokumen perlu di *up-to-date* secara teratur, agar terus dapat digunakan untuk mencegah serta mengantisipasi terjadinya kegagalan[9].

Dengan menggunakan metode FMEA, organisasi akan:

1. Mengidentifikasi dan memahami potensi kesalahan yang akan terjadi dan penyebabnya, efek pada organisasi, sistem atau pengguna.
2. Mengelola risiko berdasarkan dari kesalahan, dampak dan penyebab serta kasus prioritas dengan tindakan memperbaiki.
3. Mengidentifikasi dan mengarahkan tindakan perbaikan pada masalah yang paling serius.

Ada banyak hal yang dapat diselesaikan oleh FMEA, beberapa diantaranya yaitu:

1. Identifikasi dan mencegah kerusakan.
2. Meminimalisir kekurangan performa produk atau menurunnya performa.
3. Mengembangkan tes dan rencana verifikasi.
4. Mempertimbangkan perubahan pada desain produk atau proses.
5. Mengidentifikasi produk yang signifikan
6. Mengembangkan *maintenance* sebagai bentuk pencegahan.
7. Mengembangkan teknik diagnosa *online*

Penggolongan FMEA dibedakan menjadi dua jenis, yaitu[10]:

1. Desain FMEA, digunakan sebagai alat untuk memastikan jika peluang terjadinya kegagalan, sebab dan akibatnya telah diperhatikan terkait dengan karakteristik desain yang digunakan oleh tim yang bertanggung jawab atas desain. FMEA desain akan menguji fungsi dari komponen, sistem dan subsitem serta membantu menghilangkan kegagalan-kegagalan yang terkait dengan desain, misalkan kegagalan karena sistem tidak *user-friendly*, aplikasi yang digunakan tidak tepat, dan lain-lain.
2. Proses FMEA, merupakan alat yang digunakan untuk memastikan jika peluang terjadinya kegagalan, sebab dan akibatnya telah diperhatikan terkait dengan karakteristik prosesnya yang digunakan oleh tim pembuat. Proses FMEA akan meniadakan kegagalan yang disebabkan oleh perubahan dalam variabel proses, misalkan kesalahan input oleh petugas, terjadinya serangan oleh *hacker*, dan lain sebagainya.

Keuntungan dari penerapan metode FMEA

1. Meningkatkan ketahanan yang menyangkut proses untuk menghasilkan suatu *output*.
2. Mengidentifikasi tahapan tiap proses dimana kemungkinan resiko kegagalan tinggi terjadi dan mencegahnya.
3. Mengidentifikasi variabel-variabel proses yang perlu dikontrol.
4. Sarana untuk mendiskusikan sebab – sebab terjadinya kegagalan dan akibat apa saja yang mungkin ditimbulkan.
5. Menyediakan suatu kerangka untuk kemajuan organisasi pada proses yang dianalisis secara berkelanjutan.
6. Hemat biaya dan hemat waktu.

Tujuan penerapan *Failure Mode and Effects Analysis* (FMEA) yaitu:

1. Mengidentifikasi mode kegagalan beserta seberapa parah tingkat efeknya.
2. Mengidentifikasi aset kritis dan aset yang digunakan secara signifikan.
3. Mengurutkan proses.

Tahapan dalam FMEA[11]:

Tabel 2.3 Tahapan dalam FMEA

Tahapan	Penjelasan
1. Memilih aset yang ingin dianalisa	Pilih aset dimana kesalahan sering terjadi
2. Urutkan dan pilih aset serta tim yang bertanggung jawab	Analisis aset yang perlu dilakukan penerapan FMEA dan orang-orang terkait aset tersebut.
3. Jabarkan aset	Jabarkan secara lengkap mengenai aset yang akan dianalisa
4. Identifikasi kemungkinan terjadinya kesalahan pada masing-masing aset	Menjabarkan permasalahan yang mungkin terjadipada tiap aset yang telah lebih dulu di pilih
5. Pilih permasalahan dengan risiko paling serius	Fokus pengembangan perbaikan atas permasalahan yang sering terjadi atau memiliki efek yang cukup besar bagi

Tahapan	Penjelasan
	organisasi
6. Rancang dan implementasikan perubahan untuk mengurangi atau mencegah terjadinya masalah	Merencanakan rencana perbaikan atas risiko yang mungkin terjadi di kemudian hari untuk meminimalisisr atau bahkan menghilangkan risiko tersebut.
7. Ukur dan nilai keberhasilan perubahan aset	Mengevaluasi hasil dari penerapan perencanaan rencana perbaikan

Langkah 1: Memilih aset yang akan dianalisa

Wawancara atau penyebaran kuesioner pada kalangan staf menjadi salah satu cara untuk mengetahui performa penggunaan aset. Dari sini akan diketahui aset mana saja yang sering digunakan dan merupakan aset kritis bagi organisasi maupun seberapa sering terjadinya masalah ketika menggunakan aset tersebut.

Langkah 2: Urutkan dan pilih aset serta tim yang bertanggung jawab

Setelah aset yang akan dianalisis ditetapkan, urutkan tingkat kepentingan dan seberapa sering terjadinya kesalahan aset serta tentukan juga siapa saja orang-orang yang bertanggung jawab atas aset tersebut.

Langkah 3 - 4: Jabarkan aset dan Identifikasi kemungkinan terjadinya kesalahan pada masing-masing aset

Jabarkan aset-aset yang telah diidentifikasi dan datalah penyebab masing – masing penyebab kesalahan dan risiko apa saja yang mungkin terjadi, tanyakan kepada orang terkait aset tersebut.

Langkah 5: Pilih permasalahan dengan risiko paling serius

Menentukan masalah dengan risiko paling serius dilakukan dengan cara mencari tau bagaimana kesalahan akan terjadi dan bagaimana kesalahan akan memberikan dampak pada organisasi. Tiap kesalahan diidentifikasikan menggunakan:

1. *Severity* (S): Tingkat keparahan, merupakan penilaian seberapa serius efek atas kegagalan yang berpotensial terjadi.

2. *Occurence* (O): Keterjadian, seberapa sering terjadinya kegagalan pada suatu aset.
3. *Detection* (D): Merupakan penilaian atas kemungkinan terdeteksinya penyebab terjadinya suatu bentuk kegagalan pada aset.
4. *Risk Priority Number* (RPN): Merupakan hasil prioritas risiko yang didapat dari pengalian *Severity*, *Occurence* dan *Detection* dengan rumus RPN= S x O x D.

Nilai *Severity*

Langkah pertama untuk menganalisa risiko adalah *severity*, perhitungan atas seberapa besar dampak atau seberapa sering aset mempengaruhi hasil akhir dari proses. Dampak tersebut kemudian diberikan *rate* mulai 1 – 10, dimana 1 merupakan dampak paling kecil dan 10 mewakili dampak terburuk. Penentuan *rate* ditentukan berdasarkan tabel berikut:

Tabel 2.4 Nilai *Severity*

Rate	Tingkatan Efek	Kriteria
1	*Neglible* (Sangat Rendah)	Merupakan *rate* dimana kegagalan dapat diabaikan/tidak perlu diperkirakan
2 3	*Mild* (Rendah)	Perbaikan kegagalan masih ringan, dapat diatasi dengan peringatan masalah
4 5 6	*Moderate* (Sedang)	Kegagalan mulai memberikan efek pada beberapa proses bisnis utama maupun pendukung
7 8	*High* (Tinggi)	Kegagalan mempengaruhi semua proses bisnis utama maupun pendukung sehingga mengganggu proses bisnis

Rate	Tingkatan Efek	Kriteria
9 10	*Very High* (Sangat Tinggi)	Kegagalan menimbulkan efek bagi perusahaan secara menyeluruh dan terhitung fatal

Nilai *Occurance*

Setelah menentukan rating pada proses *severity* tentukan *rating* terhadap nilai *occurance*. *Occurance* adalah penilaian atas seberapa sering penyebab kegagalan muncul/terjadi. Penentuan *rate* dilakukan dengan menggunakan tabel berikut:

Tabel 2.5 Nilai *Occurance*

Rate	Tingkatan Efek	Frekuensi terjadinya kegagalan
1	*Remote* (Sangat Rendah)	Kegagalan terjadi satu kali tiap lima tahun ke atas
2	*Low* (Rendah)	Kegagalan terjadi tiap tiga sampai lima tahun
3		
4	*Moderate* (Sedang)	Kegagalan terjadi tiap tahun
5		
6		
7	*High* (Tinggi)	Kegagalan terjadi tiap tiga sampai enam bulan
8		
9	*Very High* (Sangat Tinggi)	Kegagalan terjadi sangat sering
10		

Nilai *Detection*

Langkah selanjutnya setelah menentukan nilai *occurance* yaitu menentukan nilai *detection*. Hal ini dilakukan sebagai bentuk usaha pencegahan terhadap kegagalan yang akan dialami oleh aset. Penentuan nilai *detection* dilakukan dengan menggunakan tabel berikut:

Tabel 2.6 Nilai *detection*

Rate	Tingkatan Efek	Tingkatan penyebab kegagalan
1	*Very high* (Sangat Tinggi)	Penyebab kegagalan tidak sampai muncul dan terjadi
2	*High* (Tinggi)	Penyebab kegagalan terdeteksi dan masih dapat dicegah
3		
4	*Moderate* (Sedang)	Penyebab kegagalan lebih susah terdeteksi namun masih dapat dicegah
5		
6		
7	*Low* (Rendah)	Penyebab kegagalan lebih susah terdeteksi dan mulai sulit dicegah
8		
9	*Very Low* (Sangat Rendah)	Penyebab kegagalan tidak terdeteksi dan tidak bisa dicegah
10		

Nlai RPN digunakan sebagai penentu tingkatan atas risiko yang telah diperkirakan. Berikut merupakan tabel penentu tingkatan berdasarkan perhitungan nilai RPN:

Tabel 2.7 Nilai RPN

Level	Nilai RPN
Very Low (Sangat Rendah)	0 sampai 20
Low (Rendah)	21 sampai 80
Moderate (Sedang)	81 sampai 120
High (Tinggi)	121 sampai 199
Very High (Sangat Tinggi)	Lebih dari 200

Dengan *very low* sebagai tingkatan terjadinya risiko kegagalan paling rendah dan *very high* sebagai tingkatan risiko paling tinggi, organisasi harus mengutamakan antisipasi dan mitigasi risiko pada level *very high* terlebih dahulu karena jika tidak dilakukan maka akan menyebabkan terganggunya proses bisnis.

2.5 Keamanan Informasi

Suatu cara bagaimana kita mencegah terjadinya kecurangan atau setidaknya mendeteksi adanya kecurangan pada sebuah sistem yang memiliki basis informasi dimana informasi tersebut tidak memiliki arti fisik merupakan bentuk dari keamanan informasi.

Aspek keamanan informasi termasuk didalamnya aspek CIA yang terdiri atas:

1. *Confidentiality* (Kerahasiaan)
   Merupakan aspek penjamin kerahasiaan data atau informasi dan memastikan bahwa informasi hanya bisa diakses oleh orang yang memiliki wewenang dan menjamin kerahasiaan informasi.
2. *Integrity* (Integritas)
   Merupakan aspek penjamin tidak adanya perubahan data tanpa ijin pihak berwenang (*authorized*), menjaga keakuratan dan keutuhan info.
3. *Availability* (Ketersediaan)
   Merupakan aspek penjamin data akan tersedia saat dibutuhkan oleh *user* yang memiliki wewenang (berhak) menggunakan informasi dan perangkat terkait.

Bentuk dari ancaman keamanan informasi diantaranya yaitu orang, organisasi, mekanisme maupun peristiwa yang berpotensi membahayakan sumber daya informasi milik perusahaan. Beberapa bentuk ancaman keamanan informasi diantaranya yaitu:

1. Ancaman *internal* dan *eksternal*
   Merupakan ancaman yang mencakup karyawan, konsultan, kontraktor maupun rekan bisnis. Ancaman *internal* akan menghasilkan kerusakan yang serius dikarenakan pengetahuannya yang mendalam atas sistem yang ada. Sedangkan contoh dari ancaman *eksternal* yaitu produk yang sama dari organisasi lain.

2. *Malicious software* yang merupakan program lengkap atau segmen kode yang bisa menyerang sistem dan mengeksekusi fungsi – fungsi yang sebenarnya tidak diharapkan untuk terjadi oleh pemilik sistem. Beberapa contoh *malicious software* yaitu virus, worm, trojan, *adware*, *spyware*.

2.6 Aset Kritis

Aset informasi merupakan suatu pengetahuan yang diatur dan dikelola sebagai unit informasi sehingga dapat dipahami, dibagi, dilindungi maupun dimanfaatkan secara efektif dan merupakan sesuatu yang berharga bagi organisasi. Sedangkan menurut OpenEI aset kritis adalah fasilitas, sistem, peralatan yang jika dihancurkan, rusak ataupun hilang akan memberikan efek yang sangat besar pada organisasi.

2.7 ISO 27002:2013

Merupakan pedoman pelaksanaan kontrol keamanan informasi, didalamnya termasuk proses implementasi, mengembangkan pedoman manajemen keamanan informasi yang sesuai dengan kebutuhan organisasi, maupun pemeliharaan Sistem Manajemen Keamanan Informasi (SMKI) pada suatu organisasi[12]. Standar ini berisikan 5 chapter pengenalan,dengan 14 chapter utama yang berisikan 144 kontrol objektif. Penggunaan ISO 27002:2013 pada tugas akhir kali ini sebagai pedoman tindakan mitigasi risiko untuk mengendalikan dan mengontrol keamanan informasi pada Politeknik Kesehatan Kemenkes Semarang. Pemberian kontrol objektif dilakukan dengan penentuan klausa terlebih dahulu. Untuk setiap satu risiko, bisa didapat lebih dari 1 kontrol objektif.