BAB 2
TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Beberapa penelitian yang sebelumnya pernah digunakan/dilakukan diantaranya sebagai berikut:

1. Penelitian mengenai penilaian risiko kemanan informasi menggunakan metode FMEA oleh Innike Desy, Bekti Cahyo Hidayanto dan Hanim Maria Astuti. Penelitian tersebut dilakukan karena belum adanya upaya pencegahan terhadap aset TI yang dipunyai bank XYZ dan tentunya berperan penting dalam proses bisnis [1].
2. Penelitian mengenai evaluasi mitigasi risiko aset dan komponen TI yang menggunakan metode OCTAV dan FMEA oleh Gunawan Setyadi, Yupie Kusumawati. Penelitian tersebut dilakukan karena belum adanya pencegahan dan evaluasi pada jaringan komputer terutama bagian server sering mengalami down pada saat KRS yang digunakan oleh UDINUS yang tersimpan data-data penting menyangkut mahasiswa sehingga dapat menyebabkan rentan kerusakan ataupun hilangnya data [2].
3. Penelitian mengenai analisis risiko keamanan informasi dengan menggunakan metode OCTAVE oleh Balqis Lembah Mahersmi, Feby Artowini Muqtadiroh dan Bekti Cahyo Hidayanto. Penelitian tersebut dilakukan karena belum adanya upaya pencegahan terhadap asset TI yang dipunyai Dinas Perhubungan Komunkasi dan Informasi yang tentunya sangat berpengaruh dalam proses bisnis yang dapat sesuai dengan harapan organisasi [3].
4. Penelitian mengenai penilaian risiko atas keamanan jaringan komputer di rumah Sakit Mohammad Hosein Palembang oleh Muhammad Iqbal, M. Akbar dan Rusmala Santi. Penelitian tersebut dilakukan karena tidak adanya bentuk pencegahan dan evaluasi atas jaringan komputer yang digunakan pada

rumah sakit yang yang tersimpan data-data penting menyangkut pasien sehingga dapat menyebabkan rentan kerusakan ataupun data hilang [4].

5. Penelitian mengenai mitigasi risiko untuk perbaikan kualitas produk dengan menggunakan metode FMEA oleh Richma Yulinda Hanif, Hendang Setyo Rukmi dan Susy Susanti. Penelitian tersebut dilakukan karena belum adanya pencegahan untuk meminimalisir kecacatan terhadap produk keraton *luxury* yang tentunya berperan penting dalam layanan yang begitu berkualitas maupun dalam optimalisasi proses bisnisnya [5].
6. Penelitian mengenai evaluasi mitigasi risiko untuk mengatasi kecacatan proses produksi dengan menggunakan metode FMEA oleh Andi Nugroho. Penelitian tersebut dilakukan karena belum adanya pencegahan untuk mengurangi masalah kegagalan pada proses produksi yang dimiliki oleh PT.Intigarmindo Persada yang tentunya berperan penting dalam proses pembuatan celana jins [6].

Tabel 2.1 Penelitian terikat

No	Nama Peneliti dan Tahun	Masalah	Metode	Hasil
1.	Innike Desy, Bekti Cahyo Hidayanto dan Hanim Maria Astuti, 2014	Belum adanya bentuk pencegahan pada aset TI sehingga masih sering terjadi ketidaksesuaian input data dan kelengkapan data menjadi tidak	Dengan menerapkan metode FMEA untuk mengevaluasi dan mengidentifikasi kegagalan/ kesalahan yang potensial, dapat	Memberikan nilai pada setiap aset. Aset dengan nilai paling tinggi harus mendapatkan kepedulian khusus. Sehingga dari proses mengidentifikasi risiko tersebut dapat diketahui penyebab

No	Nama Peneliti dan Tahun	Masalah	Metode	Hasil
		lengkap, karena semua data yang penting belum tentu terkait dengan nasabah yang terdapat di dalam dokumen bagian IT serta beberapa kemungkinan lainnya.	memberikan nilai risiko kegagalan/ kesalahan dan langkah-langkah yang harus diperlukan.	terjadinya suatu risiko dan tingkatan risiko (nilai assesment risiko). Dan hasil RPN atas penilaian risiko menggunakan metode FMEA yang diberikan saran untuk menanganinya ataupun tindakan pengendalian dan kontrol atas risiko. Saran pengendalian mengacu pada ISO 27002 dimana standar tersebut berfokus pada ISMS.
2.	Gunawan Setyadi, Yupie Kusumawati , 2012	Belum adanya pencegahan dan evaluasi atas jaringan komputer terutama bagian server sering mengalami down pada saat KRS	Menggunakan metode OCTAV dan FMEA untuk mengolah hasil informasi dan untuk menghitung seberapa tinggi	Mengidentifikasi risiko-risiko yang mungkin terjadi terkait dengan critical aset. Risiko yang akan diidentifikasi berupa risiko yang pernah

No	Nama Peneliti dan Tahun	Masalah	Metode	Hasil
		yang digunakan oleh UDINUS yang menyimpan begitu banyak data penting tentang mahasiswa sehingga menyebabkan rentannya rusak maupun hilang data	dampak dari risiko perusahaan jika terjadi dan membuat rating prioritas untuk masing-masing risko	dan perkiraan terjadi terhadap risiko yang mungkin pada masa yang akan datang dapat terjadi. Menggunakan metode FMEA untuk memberikan penilaian pada setiap komponen TI yang telah diidentifikasi pada metode OCTAVE. Kontrol ISO yang digunakan yaitu dengan menggunakan 27001 dan 27002
3.	Balqis Lembah Mahersmi, Feby Artowini Muqtadiroh dan Bekti Cahyo	Belum adanya upaya pencegahan terhadap aset TI untuk mengarahkan dan mengendalian organisasi dalam mengelola risiko yang mungkin	Menggunakan metode OCTAVE untuk menganalisis risiko keamanan informasi dapat memberikan penilaian terhadap	Metode OCTAVE cocok digunakan untuk melakukan identifikasi risiko yang dapat terjadi kepada Dinas Perhubungan Komunikasi dan Informatika

No	Nama Peneliti dan Tahun	Masalah	Metode	Hasil
	Hidayanto, 2016	terjadi yang dimiliki oleh Dinas Perhubungan Komunkasi dan Informasi yang tentunya berperan penting dalam proses bisnis yang dapat sesuai dengan harapan organisasi.	terjadinya risiko dari berbagai perspektif organisasi.	Kab.Tulungagung terkait implementasi teknologi informasi dan memberikan masukan atau rekomendasi mitigasi IS0 27001 pada pihak Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung bagaimana langkah mitigasi risiko yang tepat sesuai dengan hasil identifikasi risiko yang akan muncul terkait implementasi TI
4.	Muhammad Iqbal, M. Akbar dan Rusmala Santi, 2011	Belum adanya bentuk pencegahan atau evaluasi atas jaringan komputer yang digunakan,	Menggunakan metode *OCTAVE* sebagai alat ukur pada tingkat resiko	Mengidentifikasi, menganalisis dan mengukur tingkat keamanan atas risiko. Sehingga dapat diketahui

No	Nama Peneliti dan Tahun	Masalah	Metode	Hasil
		sehingga sistem jaringan komputer yang digunakan rumah sakit yang yang tersimpan data-data penting menyangkut pasien sehingga dapat menyebabkan rentan kerusakan ataupun data hilang, dll	keamanan jaringan pada rumah sakit Moh. Hosein.	bahwa keamanan jaringan rumah sakit Mohammad Hosein sangat bergantung pada staff dan karyawan, risiko-risiko yang serius terhadap data dan jaringan pada komputer dapat diketahui, dan hasil penelitian ini memberikan bantuan saran atas perbaikkan resiko keamanan pada jaringan komputer rumah sakit Mohammad Hosein untuk dapat memperkecil risiko yang terdapat pada jaringan.
5.	Richma Yulinda Hanif,	Belum adanya pencegahan untuk meminimalisir	Menggunakan metode FMEA untuk	Mengidentifikasi, menentukan komponen dari

No	Nama Peneliti dan Tahun	Masalah	Metode	Hasil
	Hendang Setyo Rukmi dan Susy Susanti, 2015	kecacatan terhadap produk keraton *luxury* yang tentunya berperan penting dalam layanan yang berkelas maupun dalam optimalisasi proses bisnisnya.	mengidentifikasi, menetapkan, dan untuk menghilangkan kegagalan dari proses produksi yang diketahui	sistem. Produk dan jenis-jenis kegagalan tersebut akan dianalisa untuk diketahui penyebab dari kecacatan yang ditimbulkan, agar kualitas menjadi semakin baik.
6.	Andi Nugroho, 2015	Belum adanya pencegahan untuk mengurangi masalah kegagalan pada proses produksi yang dimiliki oleh PT.Intigarmindo Persada yang tentunya berperan penting dalam proses pembuatan celana jins.	Menggunakan metode FMEA yaitu untuk mengatasi atau mengidentifikasi risiko kegagalan pada proses produksi dari sebuah produk jins.	Mengidentifikasi dan mengevaluasi potensi penyebab dari kegagalan dalam suatu proses produksi serta melakukan perbaikan pada suatu proses produksi sehingga didapatkan nilai efisiensi yang telah meningkat.

2.2 Definisi Risiko

Akibat yang dapat terjadi, yang kurang menggembirakan (membahayakan, merugikan) dari suatu tindakan ataupun perbuatan dan akan memiliki dampak terhadap tujuan tersebut.

Menurut [7] sifatnya, maka risiko dapat dibedakan sebagai berikut :

1. *Particular Risks* (Risiko Khusus), merupakan risiko khusus yang menimbulkan dampak kecil dan risiko tersebut merupakan kesalahan yang dihasilkan oleh individu sendiri.
2. *Fundamental Risks* (Risiko Fundamental), merupakan risiko yang ditimbulkan oleh masyarakat dan mempunyai dampak besar bagi banyak orang.
3. *Dinamic Risks* (Risiko Dinamis) merupakan risiko yang mengalami perubahan sesuai dengan perkembangan zaman.
4. *Static Risks* (Risiko Statis) merupakan suatu risiko yang tidak ada pengaruhnya dari zaman apapun.

2.3 Manajemen Risiko

Manajemen risiko adalah suatu proses yang berkelanjutan untuk mengidentifikasi risiko dan melaksanakan rencana untuk mengelola, memonitor, mengendalikan, dan mengatasinya.

2.4 Manajemen Risiko Teknologi Informasi

Manajemen Risiko merupakan suatu bentuk proses penilaian atau pengukuran juga pengembangan/evaluasi strategi pengelolaan risiko. Manajemen Risiko TI itu sendiri adalah suatu cara untuk mengurangi risiko teknologi informasi yang ditimbulkan, karena telah menghambat hasil pada organisasi terkait [8].

2.5 Metode OCTAVE

Metode OCTAVE *(Operationally Critical Threat, Aset, And Vulnerability Evoluation)* yaitu sebuah pendekatan evaluasi aset, membingkai risiko organisasi dalam konteks asetnya. Pendekatannya disusun dalam satu set kriteria yang

mengidentifikasi aset informasi terkait (misalnya informasi, sistem) yang penting bagi organisasi dan kegiatan analisis risiko fokus pada aset-aset dinilai paling penting bagi organisasi.

Kriteria Octave menginginkan katalog informasi untuk dapat mengukur praktek suatu organisasi, menganalisa hubungan antara aset kritis, ancaman terhadap aset tersebut, dan kerentanan (baik organisasi dan teknologi) yang dapat mengekspos aset untuk ancaman. Hanya metode tersebut yang dapat mengevaluasi risiko dalam konteks operasional. Dengan kata lain, OCTAVE berfokus pada bagaimana sistem operasional yang digunakan untuk melakukan bisnis organisasi dan bagaimana sistem-sistem berisiko karena ancaman keamanan [9].

Organisasi, teknologi, dan aspek analisis yang berpengaruh pada evaluasi informasi keamanan risiko yang digunakan pada tiga (3) fase pendekatan. Tiga fase metode Octave dibangun untuk memungkinkan personil organisasi untuk merakit gambaran yang komprehensif tentang kebutuhan keamanan informasi organisasi. Fase-fase itu sendiri yaitu sebagai berikut [9]:

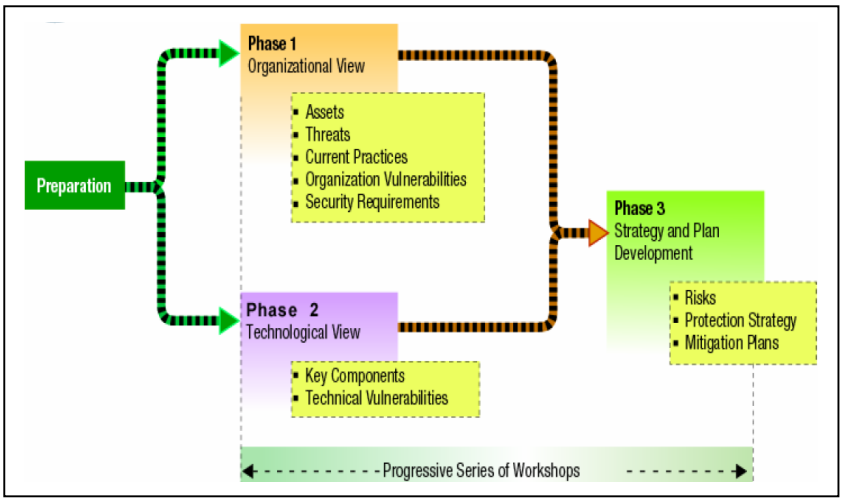
1. **Fase Pertama: Membangun profil ancaman dan berdasarkan aset pada organisasi.**

   Merupakan aspek evaluasi atas organisasi. Tim analisis dari organisasi berkontribusi tentang apa yang penting bagi organisasi dan apa yang saat ini sedang dilakukan untuk melindungi aset-aset tersebut. Tim analisis memilih aset-aset mana yang paling penting bagi organisasi (aset kritis) dan mendeskripsikan kebutuhan keamanan pada masing-masing aset kritis tersebut. Kemudian, mengidentifikasi ancaman pada tiap aset kritis dan dibuatkan profil ancaman.

2. **Fase kedua: Identifikasi kerentanan infrastruktur.**

   Merupakan aspek pengembangan atas infrastruktur komputasi. Tim analisis mengidentifikasi sistem teknologi informasi kunci dan komponen yang terkait pada setiap aset kritis. Kemudian memeriksa komponen kunci untuk mengetahui luasan tiap-tiap komponen dalam bertahan dari serangan jaringan.

3. **Fase ketiga: Membangun strategi keamanan dan rencana organisasi.**
   Bagian dari proses evaluasi, tim analisis mengidentifikasi proses untuk dianalisa risiko yang membahayakan dalam organisasi dan mengambiil langkah yang tepat untuk penyelesaian kemudian menyusun rencana untuk mengatasi risiko tersebut berdasarkan hasil analisa-analisa yang telah terkumpulkan.



Gambar 2.1 Fase Metode OCTAVE [9]

Tahapan-tahapan menggunakan metode OCTAVE

Fase pertama: Membangun Profil Ancaman Berdasarkan Asset Pada fase ini dapat dimulai dengan mengumpulkan informasi atau membangun pandangan organisasi OCTAVE dengan berfokus pada orang-orang dalam organisasi serta mengumpulkan profil ancaman atas aset kritis.

Proses 1: Identifikasi Aset Kritis

Tim analisis mengumpulkan informasi-informasi terkait aset kritis yang ada di perusahaan yang dianalisa terlebih dahulu dan diproses oleh bagian IT yang menjadi perwakilannya

Proses 2: Identifikasi Keperluan Keamanan Aset Kritis

Tim analisis mengumpulkan informasi-informasi terkait aset, keperluan keamanan yang dibutuhkan untuk dianalisa terlebih dahulu dan diproses oleh bagian IT yang menjadi perwakilannya.

Proses 3: Analisis Ancaman Aset Kritis.

Tim analisis mengumpulkan informasi-informasi terkait aset, keperluan keamanan, ancaman aset kritis pada perusahaan yang dianalisa terlebih dahulu dan diproses oleh bagian IT yang menjadi perwakilannya.

Empat kegiatan yang dilakukan untuk memperoleh pengetahuan dari peserta workshop selama proses 1 sampai 3 (kegiatan dasar yang sama untuk masing-masing proses):

1. Identifikasi aset dan prioritas relatif.
2. Identifikasi bidang yang menjadi perhatian.
3. Identifikasi persyaratan keamanan untuk aset yang paling penting.
4. Menangkap pengetahuan tentang praktik keamanan saat ini dan kerentanan organisasi.

Proses 4: Melakukan Penerapan Keamanan

Tim analisis mengumpulkan informasi dengan mengidentifikasi aset yang paling penting atau yang sudah diterapkan pada perusahaan sebagai bentuk untuk mengamankan atas aset kritis dari ancaman dan risiko yang mungkin nanti akan terjadi.

Proses 5: Mengidentifikasi Kelemahan Perusahaan

Tim analisis mengumpulkan informasi dengan mengidentifikasi kelemahan yang ada pada perusahaan dengan menjelaskan kekurangan-kekurangan dalam menjaga aset kritis masing-masing.

Fase kedua: Identifikasi kerentanan infrastruktur/prasarana.

Pada fase ini dimana sistem organisasi insfrastruktur dapat mendorong risiko atas aset kritis pada kerentanan teknologi untuk dinilai.

Proses 1: Identifikasi Komponen Utama

Mengidentifikasi komponen utama yang dapat mempengaruhi ataupun mendukung dalam pencarian data-data aset kritis pada infrastruktur yang akan dikembangkan dan dinilai.

Proses 2: Evaluasi Komponen Terpilih

Mengevaluasi kerentanan pada komponen infrastruktur yang dipilih untuk menganalisa dan kemudian mengetahui hasil profil ancaman masing-masing aset tersebut.

Fase ketiga: Menganalisa Keamanan dan Pengembangan Strategi

Pada fase ini dirancang untuk memahami informasi yang telah dikumpulkan untuk di evaluasi. Tujuan dalam hal ini untuk mengembangkan strategi keamanan dan rencana yang dirancang untuk mengatasi risiko terhadap aset kritis.

Proses 1: Analisis Risiko atas Aset Kritis

Tim analisis melakukan proses untuk mengidentifikasi dan menganalisis komponen penting yang mempengaruhi proses bisnis utamanya. Kegiatan tersebut untuk menentukan dampak ancaman terhadap aset kritis. Semua risikonya dianalisa kemudian melakukan evaluasi dampak

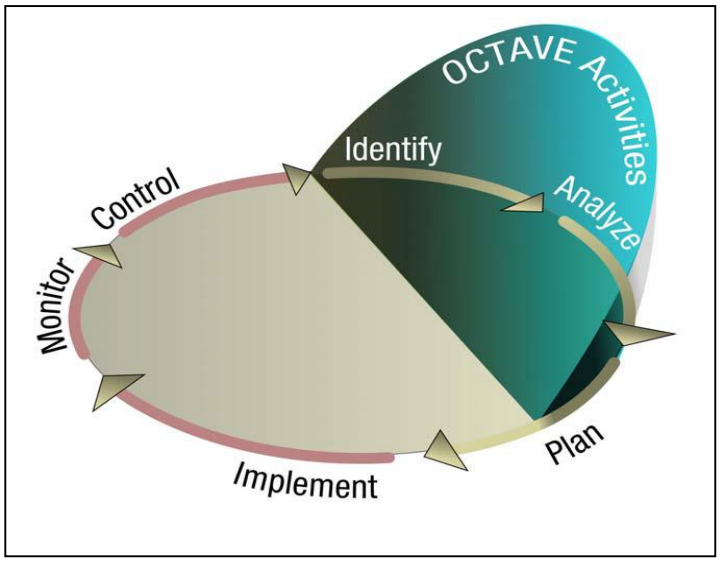
Proses 2: Penilaian atas Risiko Aset

Tim analisis melakukan proses untuk memberikan penilaian risiko terhadap aset kritis dengan menggunakan metode FMEA yang didasari dengan 3 faktor Saverity, Occurance, Detection yang nantinya menghasilkan Risk Priority Number (RPN).

Proses 3: Pengembangan Strategi Perlindungan.

Tim analisis melakukan proses untuk mengembangkan strategi perlindungan bagi organisasi, rencana mitigasi untuk risiko terhadap aset kritis dan daftar tindakan-tindakan jangka pendek. Untuk menentukan hasil evaluasi manajer memeriksa dan merevisi strategi dan rencana yang diperlukan dan kemudian memutuskan bagaimana organisasi akan dibangun.

PA, Carnegi Mellon



Gambar 2.2 Kegiatan OCTAVE dan Manajemen Risiko [9]

2.6 Metode FMEA

Metode FMEA *(Failure Mode and Effect Analysis)* merupakan strategi sistematis yang menerapkan suatu metode untuk mencegah produk dan proses masalah sebelum terjadi, dan dapat mengidentifikasi mode kegagalan potensial dan efeknya. FMEA difokuskan pada mencegah cacat, meningkatkan keselamatan, dan meningkatkan kepuasan pelanggan. Idealnya, meningkatkan FMEA dilakukan dalam desain produk atau proses pembangunan tahap, meskipun melaksanakan FMEA pada produk dan proses yang ada juga dapat menghasilkan manfaat besar [10].

Secara umum ada 2 jenis penggolongan FMEA, yaitu [11]:

1. Proses FMEA, merupakan sebagai alat untuk mengungkap masalah terjadinya kegagalan/perubahan yang telah disebabkan pada perubahan-perubahan yang ada di variabel proses. Misalnya terjadinya serangan hacker, kesalahan petugas dalam menginput, dll.
2. Desain FMEA, merupakan sebagai alat untuk mengungkap masalah terjadinya kegagalan/perubahan yang terkait dengan karakteristik desain. Misalkan aplikasi yang digunakan yang tidak tepat, kegagalan sistem yang tidak dapat berjalan dengan lancar, dan lain-lain.

Tujuan dari penerapan FMEA (*Failure Mode And Effect Analysis*), sebagai berikut:

1. Mengetahui atau memprediksi mode kesalahan-kesalahan dari produk dan sebesar apa efek sampingnya.
2. Menganalisa atau mengevalusi aset kritis dan aset yang digunakan dengan relevan.
3. Mendokumentasikan atau menyusun proses secara keseluruhan.

Keuntungan dari penerapan FMEA, yaitu:

1. Menumbuhkan ketahanan terkait dalam proses untuk memberikan hasil yang lebih baik pada suatu output.
2. Menganalisa atau mengevaluasi tahapan setiap proses untuk mengetahui seberapa parah tingkat terjadinya suatu kegagalan/kesalahan dan cara mengatasinya.
3. Menganalisa pada sistem produksinya.
4. Memberikan sarana untuk mendiskusikan sebab dan akibat terjadinya kegagalan yang ditimbulkan.
5. Menyediakan dan memberikan suatu kerangka kemajuan pada organisasi untuk dapat dianalisis secara berkelanjutan.
6. Hemat waktu dan biaya

Langkah-langkah dalam penerapan FMEA, yaitu [12]:

1. Langkah ke-1: Tinjau Proses

   Memilih aset untuk dianalisa, perlu dilakukan karena untuk mendapatkan kesalahan yang sering terjadi terhadap proses. Jika sudah dilakukan maka perlu ditinjau untuk meningkatkan pemahaman terhadap proses yang telah dianalisa.
2. Langkah ke-2: Brainstorm Potensi Kegagalan Proses

   Setelah melakukan peninjauan terhadap proses yang di analisis maka tiap anggota tim melakukan brainstorm terhadap terjadinya kesalahan atau kegagalan pada proses yang telah dianalisis. Proses brainstorm ini dilakukan untuk mengetahui dampak dari satu kesalahan atau kegagalan tiap komponen yang mungkin dapat menimbulkan kesalahan yang lainnya.
3. Langkah ke-3: Daftar Potensi Efek untuk Setiap Mode Kegagalan

Setelah diketahui daftar kesalahan yang mungkin akan terjadi, maka kemudian melakukan penyusunan terhadap dampak pada mode kegagalan yang terjadi. Untuk tiap kesalahan, mungkin hanya ada satu dampak kegagalan sedangkan untuk mode lain mungkin ada beberapa dampak.

4. Langkah ke-4-6: Menetapkan *Severity*, *Occurence*, *Detection*.

   Menentukan masalah dengan risiko paling serius yang dilakukan dengan cara mencari tahu bagaimana kegagalan/kesalahan akan terjadi dan bagaimana kegagalan akan memberikan dampak pada organisasi. Untuk meningkatkan FMEA desain dan dengan meningkatkan FMEA proses untuk masing-masing tiga peringkat keparahan, kejadian, dan deteksi. Sistem ini harus disesuaikan dengan organisasi untuk digunakan dengan semua FMEA. Setiap kesalahan dapat diidentifikasi dengan menerapkan:

   a. *Severity* (S): Tingkat keparahan, merupakan penilaian seberapa serius efek atas kesalahan/kegagalan yang berpotensial terjadi.
   b. *Occurence* (O): Tingkat kejadian, merupakan seberapa sering terjadi kesalahan/kegagalan terhadap suatu aset.
   c. *Detection* (D): Penilaian seberapa jauh mendeteksi kemungkinan terjadinya suatu kesalahan/kegagalan ataupun yang menimbulkan dampak kegagalan pada suatu aset.

   Nilai *Severity*

   Severity merupakan langkah pertama untuk menganalisa risiko yaitu dengan menghitung seberapa besar/serius dampak jika kegagalan dapat berpengaruh pada hasil akhir dari suatu proses. Dampaknya tersebut kemudian diberi rating mulai dari skala 1 – 10, dimana 1 merupakan dampak terkecil dan 10 mewakili dampak terburuk. Penentuan rating dapat ditentukan pada tabel sebagai berikut:

Tabel 2.2 Nilai *Severity*

Rating	Severity of Effect	Criteria
1.	*Negible* (Sangat Rendah)	Suatu dampak buruk/kegagalan pada suatu produk yang dapat merugikan bagi penggunanya namun tidak terlalu difikirkan (dapat diabaikan)
2. 3.	*Mild* (Rendah)	Suatu akibat yang akan ditimbulkan namun bagi pengguna akhir tidak akan merasakan dampaknya, karena hanya bersifat ringan dan dapat di evalusikan lagi dimasa pemeliharaan.
4. 5. 6	*Moderate* (Sedang)	Suatu pengaruh buruk yang dapat diselesaikan dalam waktu singkat, dalam hal ini pengguna akan mengalami penurunan namun dapat ditoleransi.
7. 8.	*High* (Tinggi)	Dampak pengaruh ini akan sangat dirasakan oleh pengguna tanpa ada toleransi karena membutuhkan biaya mahal dalam perbaikan.
9. 10.	*Very High* (Sangat Tinggi)	Dampak yang berbahaya untuk keselamatan pengguna.

Nilai *Occurence*

Langkah selanjutnya setelah menentukan rating pada proses *severity* yaitu menentukan *rating* atas nilai *occurance*. Metode terbaik untuk menentukan peringkat terjadinya yaitu dengan menggunakan data aktual dari proses. *Occurence* merupakan penilaian atas tingkatan penyebab yang akan dan sudah terjadi kegagalan terhadap suatu aset. Penentuan rating ditentukan dengan menggunakan tabel berikut:

Tabel 2.3 Nilai *Occurence*

Rating	Occurence of Effect	Frequency of Failure
1.	*Remote* (Sangat Rendah)	Kegagalan terjadi tiap satu kali dari lima tahun ke atas
2. 3.	Low (Rendah)	Kegagalan terjadi tiap satu sampai tiga tahun
4. 5. 6.	*Moderate* (Sedang)	Kegagalan terjadi tiap tahun
7. 8.	*High* (Tinggi)	Kegagalan terjadi tiap satu sampai empat bulan
9. 10.	*Very High* (Sangat Tinggi)	Kegagalan terjadi tiap sehari sampai seminggu

Nilai *Detection*

Setelah menentukan nilai occurence langkah selanjutnya yaitu menentukan nilai detection. *Detection* merupakan penilaian untuk mendeteksi kemungkinan terjadinya suatu kesalahan/kegagalan atau menimbulkan dampak kegagalan pada suatu asset. Menentukan nilai *detection* dapat ditentukan dengan menggunakan tabel sebagai berikut:

Tabel 2.4 Nilai *Detection*

Rating	Detection of Effect	Frequency of Failure
1.	*Very High* (Sangat Tinggi)	Suatu penyebab kegagalan yang tidak terjadi atau terasa untuk penggunanya.
2. 3.	*High* (Tinggi)	Penyebab kegagalan yang masih bisa dicegah karena dapat terdeteksi.
4. 5. 6.	*Moderate* (Sedang)	Kegagalan yang lebih sulit untuk dideteksi tetapi masih bisa untuk dihindari/dicegah.
7. 8.	*Low* (Rendah)	Kegagalan yang lebih sulit untuk dideteksi dan juga sulit untuk dihindari/dicegah.
9. 10.	*Very Low* (Sangat Rendah)	Kegagalan yang tidak bisa untuk dideteksi dan tidak dapat dihindari/dicegah.

7. Langkah ke-7: Hitung *Risk Priority Number* (RPN) untuk Setiap Mode Kegagalan.

   Jumlah prioritas risiko (RPN) hanya dihitung dengan mengalikan peringkat kali terjadinya Peringkat kali deteksi peringkat untuk setiap item keparahan.

   Risk Priority Number = Severity × Terjadinya × Detection

   Jumlah total prioritas risiko harus dihitung dengan menambahkan semua nomor prioritas risiko. Jumlah ini sendiri tidak berarti karena setiap FMEA memiliki nomor yang berbeda dari mode kegagalan dan dampak. Namun, dapat berfungsi sebagai alat ukur untuk membandingkan jumlah RPN revisi sekali tindakan yang direkomendasikan telah dilembagakan.

Nilai RPN digunakan untuk mengidentifikasikan tingkatan atas resiko yang serius, dan sebagai petunjuk ke arah tindakan perbaikan.

Tabel 2.5 Nilai RPN

Tingkatan/Level	**Nilai RPN**
Very Low (Sangat Rendah)	0 sampai 20
Low (Rendah)	21 sampai 70
Moderate (Sedang)	71 sampai 110
High (Tinggi)	111 sampai 199
Very High (Sangat Tinggi)	Lebih dari 200

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

8. Langkah ke-8: Mengurutkan Prioritas Mode Kegagalan yang Memerlukan Penanganan Lanjut

   Mode kegagalan sekarang dapat diprioritaskan dengan peringkat, dari jumlah prioritas risiko tertinggi sampai dengan yang terendah.

9. Langkah ke-9: Me*lakukan tindak mitigasi risiko terhadap kegagalan tersebut*

   Menggunakan proses pemecahan masalah terorganisir, mengidentifikasi dan menerapkan tindakan untuk menghilangkan atau mengurangi mode kegagalan berisiko tinggi. Idealnya, mode kegagalan harus dihilangkan sepenuhnya.

10. Langkah ke-10: Hitung Hasil RPN (*Risk Priority Number*) untuk Mengurangi Mode Kegagalan

Setelah tindakan telah diambil untuk meningkatkan produk atau proses, peringkat baru untuk keparahan, kejadian, dan deteksi harus ditentukan, dan RPN dihasilkan dihitung ulang. Untuk mode kegagalan di mana tindakan yang diambil, harus ada penurunan yang signifikan dalam RPN. Jika tidak, itu berarti tindakan tidak mengurangi keparahan, kemungkinan terjadinya, atau pendeteksian. RPN yang dihasilkan dapat diatur pada diagram Pareto dan dibandingkan dengan RPN asli.

2.7 Keamanan Informasi

Keamanan informasi menentukan cara-cara yang dilakukan agar suatu informasi dapat terjaga kerahasiaan dan keamanannya dari suatu risiko adanya kecurangan-kecurangan dalam mengelola informasi yang ada agar tidak disalahgunakan informasi tersebut.

Tujuan yang ingin dicapai dalam penerapan keamanan informasi, yaitu [13]:

1. Kerahasiaan (*Confientiality*) merupakan salah satu aspek penting alam menjaga keamanan informasi. Segala upaya atau cara agar tersimpannya tidak tersebarnya suatu informasi dari bahaya/risiko penyalahgunaan.
2. Ketersediaan (*Availability*) merupakan informasi data-data yang ada juga harus ditunjukan ke pihak-pihak yang berkepentingan dalam mengolah atau memperoleh informasi oleh karenanya diperlukan ketersediaan informasi untuk mengaksesnya tanpa ada gangguan apapun.
3. Integritas (*Integrity*) merupakan semua informasi yang tersedia yang ditujukan pada pihak-pihak yang memerlukan data yang akurat tanpa ada perubahan ataupun kebohongan data.

Bentuk dari ancaman keamanan informasi bisa datang dari pihak internal maupun eksternal yang dapat membahayakan data perusahaan ataupun organisasi yang ada. Beberapa bentuk dari ancaman keamanan informasi diantaranya sebagai berikut:

1. Ancaman *Internal*

   Merupakan ancaman–ancaman yang datang dari pihak dalam organisasi atau perusahaan yang dapat membahayakan karena, telah mengetahui lebih detail data-data yang ada.

2. Ancaman *Eksternal*

   Merupakan ancaman-ancaman yang datang dari pihak-pihak luar misalnya, perusahaan lain yang bersaing dalam produk yang sama.

3. *Malicious Software/Malware*

   Merupakan program-program lengkap ataupun unit code yang dapat menyerang sistem serta melakukan fungsi-fungsi yang sebenarnya tidak diharapkan terjadi oleh pemilik sistem. Beberapa contohnya dari *malicious software/malware* yaitu worm, virus, trojan horse, *spyware, adware*.

2.8 Aset Kritis

Aset informasi merupakan suatu pengetahuan yang dapat diatur dan dikelola sebagai unit informasi sehingga bisa dipahami, dilindungi, dibagi, ataupun dimanfaatkan dengan ekfektif dan merupakan sesuatu yang berguna bagi organisasi atau perusahaan. Sedangkan aset kritis merupakan fasilitas-fasilitas atau peralatan yang dapat membahayakan atau memberikan risiko besar jika terjadi kehilangan/kerusakan pada organisasi atau perusahaan.

2.9 ISO 27002:2013

Merupakan pedoman untuk standar keamanan informasi organisasi dan praktek manajemen keamanan informasi termasuk pemilihan, pelaksanaan dan pengelolaan kontrol dengan mempertimbangkan lingkungan risiko keamanan informasi pada suatu organisasi. Penggunaan ISO 27002:2013 menerapkan kontrol keamanan dimana pengontrolannya terbentuk 5 chapter pengenalan, dengan 14 chapter utama yang berisikan 144 kontrol objektif. Pemberian kontrol objektif dilakukan dengan menentukan klausa terlebih dulu. Untuk setiap satu risiko, bisa didapat lebih dari 1 kontrol objektif. [14].