BAB II
TINJAUAN PUSTAKA

2.1 Studi Sebelumnya

Studi sebelumnya dikumpulkan dan digunakan sebagai pembanding dan referensi mengenai penggunaan metode OCTAVE untuk mengidentifikasi aset dan identifikasi ancamannya, penilaian risiko menggunakan metode FMEA, dan mitigasi risiko yang sesuai dengan standar ISO 27001.

Tabel 2.1 Tabel Hasil Studi Sebelumnya

No	Judul Penelitian	Penulis &Tahun	Hasil Penelitian	Perbedaan
1	Analisis Risiko dengan Menggunakan Metode OCTAVE dan Kontrol ISO 27001 pada Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung	Balqis Lembah Mahersmi, Surabaya, 2016	Penelitian aset dan analisis risiko terhadap Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungaagung menggunakan metode OCTAVE, disertai penilaian risiko menggunakan FMEA dan mitigasi risiko berdasarkan ISO 27001	Objek Penelitian

No	Judul Penelitian	Penulis &Tahun	Hasil Penelitian	Perbedaan
2	Manajemen Risiko Ancaman pada Aplikasi Website Sistem Informasi Akademik Politeknik Negeri Batam Menggunakan Metode OCTAVE	Fernando Reza Destrianto, Nelmiawati dan Maya Armys Roma Sitorus, Batam, 2017	Meneliti kelemahan keamanan dari aplikasi website sistem informasi di Politeknik Negeri Batam menggunakan metode OCTAVE	Objek Penelitian, tidak menggunakan FMEA dan mitigasi risiko yang berstandarkan ISO
3	Analisis dan Mitigasi Risiko Aset TI Menggunakan Framework OCTAVE dan FMEA [5]	Melita Dyah Purwitasari, Wellia Shinta Sari, Semarang, 2017	Penelitian yang dilakukan terhadap Politeknik Kesehatan Kemenkes Semarang menggunakan metode OCTAVE, penilaian risiko menggunakan FMEA, *risk registration*, dan mitigasi risiko sesuai	Objek penelitian dan standar mitigasi risiko menggunakan ISO 27002:2013

No	Judul Penelitian	Penulis &Tahun	Hasil Penelitian	Perbedaan
			dengan standar ISO 27002	
4	Pengukuran Risiko Keamanan Aset TI Menggunakan Metode FMEA dan Standar ISO/IEC27001:2013	Lailatul Munaroh,Yusuf Amrozi, Risky Agung Nurdian	Penelitian terhadap keamanan aset IT yang terdapat dalam Bidang Perdagangan Dalam Negri (PDN) Dinas Perdagangan dan Perindustrian Pemerintah Provinsi XYZ	Objek Penelitian
5	Penerapan Metode FMEA (Failure Mode and Effect Analysis) untuk Kuantifikasi dan Pencegahan Resiko Akibat Terjadinya *Lean Waste*	Surya Andiyanto, Agung Sutrisno, Charles Punuhsingon	Penelitian terhadap perusahaan cepat saji untuk menganalisis pemborosan (*waste*) di restoran X	Penelitian hanya menggunakan metode FMEA

2.2 Dasar Teori

2.1.1 Keamanan Sistem Informasi

Keamanan Sistem Informasi menurut G.J. Simons adalah bagaimana usaha untuk dapat mencegah penipuan (*cheating*) atau bisa mendeteksi adanya penipuan pada sistem yang berbasis informasi, di mana informasinya sendiri tidak memiliki arti fisik. Informasi menjadi aset yang sangat berharga bagi perseorangan, pemerintah maupun swasta. Informasi juga memiliki nilai yang harus dilindungi, sehingga menjadi penting bagi individu ataupun perusahaan untuk menerapkan perlindungan terhadap informasi yang dimiliki [6].

Gambar 2.1 CIA Keamanan Informasi [8]

Berdasarkan gambar 2.1 di atas, keamanan sistem informasi juga terbagi menjadi 3 aspek yaitu:

1. *Confidentiality*

   Aspek yang menjamin kerahasiaan informasi dan memastikan informasi yang bisa diakses hanya dari pihak yang memiliki hak akses dan dapat menjamin kerahasiaan informasi.

2. *Integrity*

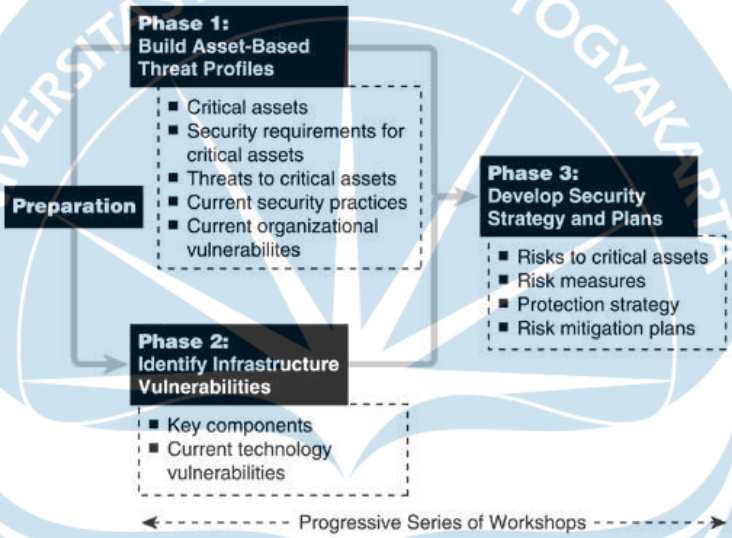
   Menjaga keakuratan dan keutuhan informasi, serta menjamin data yang tersedia tidak mengalami perubahan tanpa izin dari pihak tidak berwenang

3. *Availability*

   Menjamin ketersediaan data untuk dapat dipergunakan oleh pengguna yang memiliki hak akses informasi dan perangkat apabila diperlukan. [7]

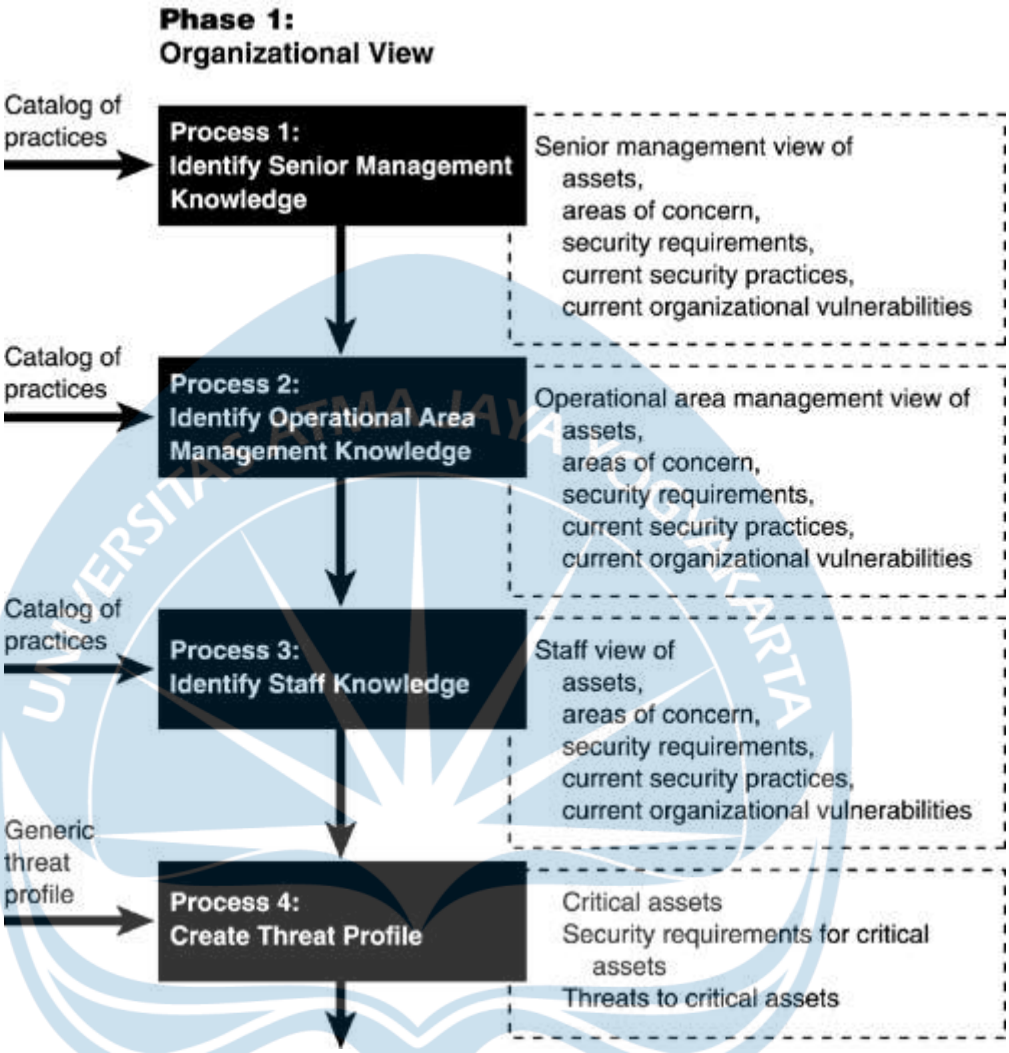
2.2.2 OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) adalah metode yang dikembangkan Software Engineering Institute, Carnegie Mellon University, 1999, yang digunakan sebagai kerangka kerja untuk mengidentifikasi, menganalisis dan mengawasi pengelolaan risiko keamanan informasi berdasarkan identifikasi risiko [1]. OCTAVE mendefinisikan komponen-komponen yang penting secara komprehensif, sistematis, terarah, dan dapat dilakukan sendiri berdasarkan konteks evaluasi risiko keamanan informasi. [9]



Gambar 2.2 Metode OCTAVE [7]

Gambar 2.2 di atas adalah keseluruhan langkah beserta rinciannya yang terdapat dalam metode OCTAVE, dan penjelasan dari tiap tahap yang sebagai berikut:



Gambar 2.3 Fase 1: *Organizational View* [10]

Berdasarkan gambar 2.3 di atas menjelaskan dari tahap pertama metode OCTAVE:

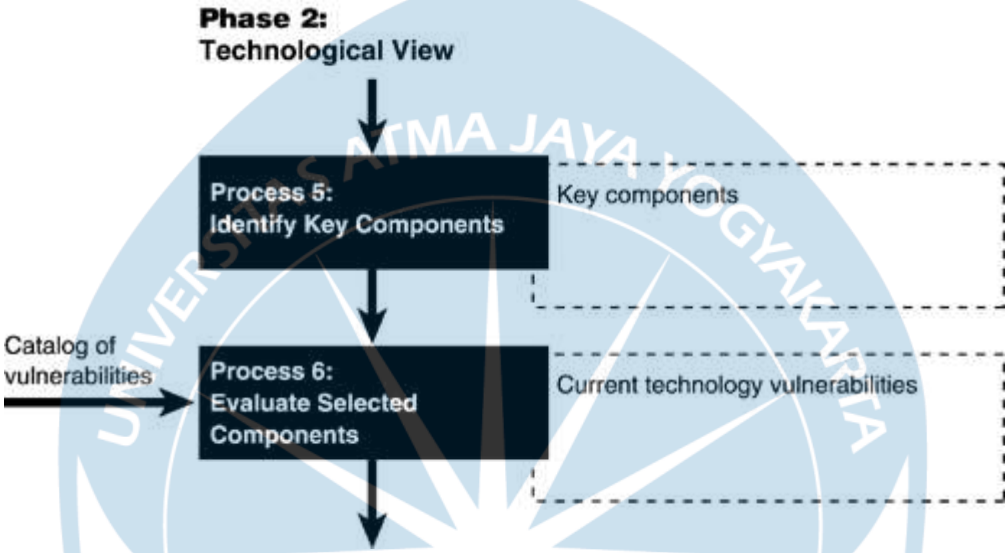
1. *Build Asset-Based Threat Profiles*: Tahap ini bisa disebut juga sebagai *Organizational view*, di mana identifikasi dilakukan terhadap aset yang memiliki potensi ancaman dan dianggap kritis.

   Proses 1: Identifikasi yang dilakukan terhadap *Senior Management* untuk mengetahui kondisi yang ada dalam perusahaan berdasarkan sudut pandang *Senior Management.*

   Proses 2: Identifikasi yang dilakukan terhadap *Operational Area Management* untuk mengetahui kondisi yang ada dalam perusahaan berdasarkan sudut pandang *Operational Area Management.*

Proses 3: Identifikasi yang dilakukan terhadap staff organisasi IT untuk mengetahui kondisi yang ada dalam perusahaan berdasarkan sudut pandang staff organiasasi IT.

Proses 4: Membuat *Threat Profiles* berdasarkan informasi yang didapat dari para narasumber [11].



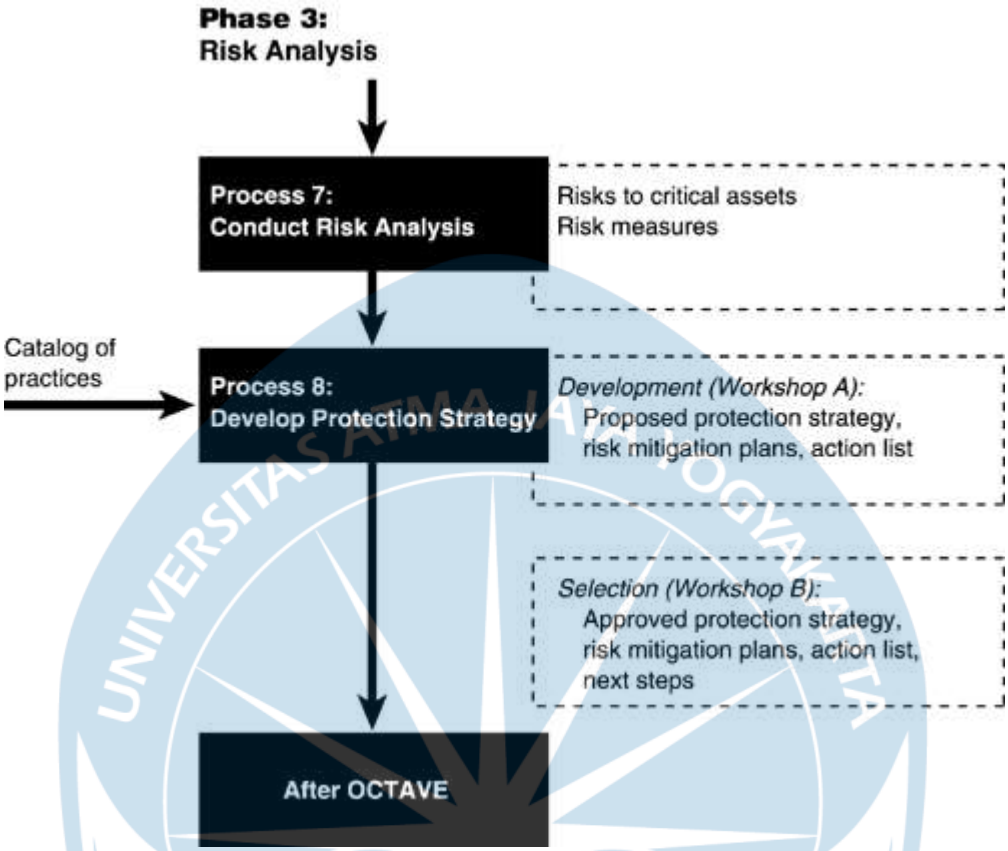
Gambar 2.4 Fase 2: *Technological View* [10]

Berdasarkan gambar 2.4 di atas menjelaskan dari tahap kedua metode OCTAVE:

2. *Identify Infrastructure Vulnerabilities*: tahap ini bisa disebut sebagai *Technological view*, karena pengidentifikasian yang dilakukan kelemahan pada teknologi dari aset penting yang digunakan dalam perusahaan.

   Proses 5: Identifikasi komponen inti perusahaan. Tujuan dari proses 5 adalah untuk menggali informasi mengenai infrastruktur teknologi yang digunakan perusahaan sebelum di evaluasi kerentanannya di proses 6.

   Proses 6: Evaluasi komponen yang dipilih. Tujuan dari proses ini adalah untuk mengidentifikasi kelemahan dari infrastruktur yang sudah diketahui dari proses 5. Kelemahan infrastruktur memberikan indikasi betapa rapuhnya infrastruktur dalam perusahaan [11].



Gambar 2.5 Fase 3: *Risk Analysis* [10]

Berdasarkan gambar 2.5 di atas menjelaskan tahap ketiga metode OCTAVE:

3. *Develop Security Strategy and Plans*: Tahap ini dilakukan untuk mengidentifikasi risiko terhadap aset dan membangun strategi untuk melindungi aset dan rencana mitigasi risiko.

   Proses 7: tujuan dari proses ini adalah untuk mengidentifikasi dan menganalisis risiko terhadap aset kritis perusahaan. Proses 7 meliputi 3 kegiatan, yaitu mengidentifikasi dampak dari ancaman kritis, membuat kriteria evaluasi risiko, dan mengevaluasi dampak dari ancaman terhadap aset kritis.

   Proses 8: tujuan dari proses 8 adalah untuk mengembangkan strategi perlindungan bagi perusahaan dan memberikan rencana mitigasi untuk risiko terhadap aset kritis [11].

2.2.3 Aset

Aset adalah sesuatu yang terdefinisi dan terkelola sebagai suatu unit informasi sehingga dapat dipahami, dibagi, dilindungi, dan dimanfaatkan secara efektif. Aset sendiri merupakan sesuatu yang berharga yang diakui oleh organisasi yang tidak mudah untuk diganti tanpa biaya, keahlian, waktu, sumber daya dan kombinasinya [12].

2.2.4 Manajemen Risiko

Manajemen risiko merupakan proses untuk mengidentifikasi, menganalisis, mengevaluasi, mengendalikan, dan berusahaa menghindari, meminimalkan, atau bahkan menghilangkan risiko yang tidak dapat diterima [13]. Dengan melakukan identifikasi risiko, perusahaan dapat menentukan strategi untuk meningkatkan keamanan dan meminimalisir kemungkinan terjadinya risiko.

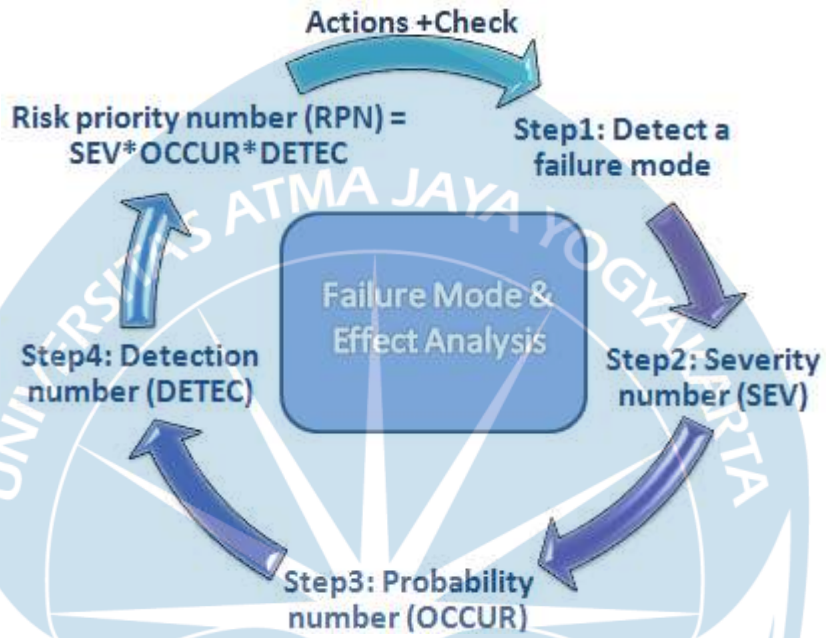
Menurut Stonebumer, Goguen dan Feringa, terdapat 6 perlakuan, yaitu:

1. *Risk assumption*: menerima kemungkinan risiko dan mengoperasikan sistem.
2. *Risk avoidance*: menghindari risiko dengan menghilangkan hal yang dapat menyebabkan risiko.
3. *Risk limitation*: menerapkan kontrol dengan melakukan pembatasan risiko untuk meminimalkan dampak kerugian.
4. *Risk planning*: mengembangkan rencana mitigasi risiko yang mengimplementasikan, memprioritaskan, dan mempertahankan kontrol.
5. *Research and Acknowledge*: mengurangi risiko kerugian dengan menerima risiko dan meneliti kontrol untuk memperbaiki risiko.
6. Pengalihan risiko: mentransferkan risiko dengan memakai pilihan keputusan lain untuk mengkompensasikan kerugian [2].

2.2.5 FMEA

Menurut Yumaida (2011), FMEA (*Failure Mode and Effect Analysis*) adalah metode evaluasi terhadap kemungkinan terjadinya sebuah kegagalan

dari sebuah sistem, proses, atau pelayanan untuk dibuat langkah penanganannya [14]. Dalam FMEA, setiap kemungkinan kegagalan yang terjadi dilakukan proses kuantifikasi dan dibuat prioritas penanganan berdasarkan tingkat kegagalannya.



Gambar 2.6 Metode FMEA [15]

Dalam gambar 2.6 dijelaskan bahwa langkah metode FMEA adalah sebagai berikut:

1. Membuat daftar potensi kegagalan.
2. Melakukan identifikasi potensi kegagalan yang dapat terjadi dalam setiap proses.
3. Melakukan identifikasi tingkat keseringan terhadap suatu masalah yang terjadi.
4. Melakukan identigikasi tingkat deteksi terhadap suatu masalah yang terjadi.
5. Melakukan perhitungan RPN dengan melakukan perkalian dari hasil identifikasi yang sudah dilakukan.
6. Membuat beberapa langkah perbaikan dan pemeriksaan ulang dengan melakukan prioritas terhadap masalah dengan nilai tingkat yang tinggi.

FMEA juga memiliki keuntungan menurut Gunjan & Himanshu Joshi, seperti:

1. Dapat mengurangi kegagalan yang serupa di masa depan.
2. Dapat meminimalkan biaya akibat dari kegagalan.
3. Meminimalkan perubahan yang drastis (*last minute of change*).
4. Meningkatkan baik proses maupun kualitas produk serta kehandalan dan keselamatan.
5. Meningkatkan kepuasan pengguna.
6. Berfokus kepada pencegahan. [16]

FMEA sendiri terdiri dari tiga hal yang berfungsi dalam menentukan tingkat kegagalannya:

- ***Severity Number* (SEV)**

  Severity Number dapat disebut sebagai tingkat kerusakan, yang berfungsi untuk menentukan seberapa serius kerusakan yang dihasilkan dari kegagalan yang dialami dari suatu proses [14]. Dalam tabel berikut adalah keterangan mengenai ranking dari *Severity Number*:

Tabel 2.2 Tingkat Kerusakan FMEA [17]

Dampak	Kriteria	Ranking
Berbahaya: Tanpa Peringatan	Kegagalan yang melukai pekerja/pihak ketiga/customer tanpa adanya peringatan	10
	Kegagalan yang terjadi dengan peringatan	9
Sangat Tinggi	Gangguan besar dan menyebabkan kerusakan yang besar dalam penggunaan yang ada	8
Tinggi	Gangguan kecil dan menyebabkan keluhan dari pihak ketiga/costumer	7

Sedang	Gangguan besar yang menyebabkan kerugian untuk perusahaan	6
Rendah	Gangguan kecil yang menyebabkan penurunan kinerja dari pekerja	5
Sangat Rendah	Gangguan yang menyebabkan sedikit kerugian	4
Minor	Menyebabkan gangguan kecil yang dapat diatasi tanpa kehilangan sesuatu	3
Sangat Minor	Tidak mengganggu dan hanya memberikan dampak kecil pada kinerja	2
Tidak Berdampak	Tidak ada efek dari gangguan	1

- ***Probablity Number* atau *Occurrence* (OCC)**

  Probability Number merupakan tingkat frekuensi untuk menentukan seberapa besar gangguan yang dapat menyebabkan kegagalan [14]. Dalam tabel berikut adalah keterangan mengenai ranking dari *Probability Number*:

Tabel 2.3 Tingkat Frekuensi FMEA [17]

Probabilitas Risiko	Periode Waktu	Ranking
Sangat Tinggi	Lebih dari satu kali tiap harinya	10
	Satu kali 4 hari	9
Tinggi	Satu kali setiap seminggu	8
	Satu kali setiap sebulan	7
Sedang	Satu kali setiap 3 bulan	6
	Satu kali setiap 6 bulan	5
	Satu kali setiap setahun	4
Rendah	Satu kali setiap 1-3 tahun	3
Sangat Rendah	Satu kali setiap 3-6 tahun	2
Remote	Lebih dari 7 tahun	1

- ***Detection Number* (DET)**

  Detection number menentukan tingkat deteksi untuk mengukur sejauh mana peluang potensi kegagalan dapat dideteksi [14]. Dalam tabel berikut adalah keterangan mengenai ranking dari *Detection Number*:

Tabel 2.4 Tingkat Deteksi FMEA [17]

Dampak	Kriteria	Ranking
Hampir tidak mungkin	Pengontrolan tidak dapat mendeteksi kegagalan	10
Sangat Kecil	Sangat jauh kemungkinan pengontrol akan menemukan potensi kegagalan	9
Kecil	Jarang kemungkinan pengontrol akan menemukan potensi kegagalan	8
Sangat Rendah	Kemungkinan pengontrol untuk mendeteksi kegagalan sangat rendah	7
Rendah	Kemungkinan pengontrol untuk mendeteksi kegagalan rendah	6
Sedang/Moderat	Kemungkinan pengontrol untuk mendeteksi kegagalan sedang	5
Cukup Tinggi	Kemungkinan pengontrol untuk mendeteksi kegagalan cukup tinggi	4
Tinggi	Kemungkinan pengontrol untuk mendeteksi kegagalan tinggi	3
Sangat Tinggi	Kemungkinan pengontrol untuk mendeteksi kegagalan sangat tinggi	2
Hampir Pasti	Kegagalan dalam proses tidak dapat terjadi karena telah dicegah melalui sistem solusi	1

2.2.6 ISO 27001

ISO 27001:2013 adalah suatu standar sistem manajemen keamanan informasi (*Information Security Management System*) yang diterbitkan oleh ISO/IEC pada Oktober 2005. Tujuan dari ISO 27001 adalah sebagai model guna penetapan, penerapan, pengoperasian, pemantauan, pengkajian, memelihara, dan peningkatan SMKI (Sistem Manajemen Keamanan Informasi). ISO 27001:2013 juga mencakup segala persyaratan dan penanganan risiko keamanan informasi yang disesuaikan dengan kebutuhan organisasi [18].

ISO 27001:2013 berisi 14 Annex yang mencakup 113 kontrol [19]:

A.5: *Information security policies*

A.6: *How information security is organized*

A.7: *Human resources security*

A.8: *Asset management*

A.9: *Access controls and managing user access*

A.10: *Cryptographic technology*

A.11: *Physical security of the organisation's sites and equipment*

A.12: *Operational security*

A.13: *Secure communications and data transfer*

A.14: *Secure acquisition, development, and support of information systems*

A.15: *Security for suppliers and third parties*

A.16: *Incident management*

A.17: *Business continuity/disaster recovery (to the extent that it affects information security)*

A.18: *Compliance*