BAB II
LANDASAN TEORI

2.1 Manajemen Risiko

Jones & Rama (2008) mengungkapkan bahwa manajemen risiko adalah kegiatan pemimpinan puncak mengidentifikasi, mengevaluasi, menangani dan memonitor risiko bisnis yang dihadapi perusahaan mereka di masa yang akan datang.

Blokdijk, Engle, & Brewster (2008) mengungkapkan bahwa tugas manajemen risiko adalah mengelola risiko suatu proyek untuk risiko. Tujuannya adalah untuk mengelola risiko bahwa dengan melakukan tindakan untuk menjaga hubungan ke tingkat yang dapat diterima dengan cara yang hemat biaya.

Manajemen risiko meliputi :

a. Akses yang bisa dipercaya, tentang risiko yang terbaru
b. Proses pengambilan keputusan didukung oleh kerangka analisis risiko dan proses evaluasi
c. Memantau risiko
d. Pengendalian yang tepat untuk menghadapi risiko

Sentosa (2009) mengungkapkan bahwa manajemen risiko merupakan aplikasi dari manajemen umum yang secara khusus membahas strategi untuk mengatasi aktivitas-aktivitas yang menimbulkan risiko terjadi.

Jadi dapat disimpulkan manajemen risiko adalah proses menyeluruh yang secara khusus digunakan untuk membahas strategi, mengenali, mengukur, dan mengelola risiko.

2.2 Risiko

2.2.1 Pengertian Risiko

Hanafi (2006) mengungkapkan bahwa risiko adalah bahaya, akibat atau konsekuensi yang dapat terjadi akibat sebuah proses yang sedang berlangsung atau kejadian yang akan datang.

2.2.2 Jenis-jenis Risiko

Hanafi (2006) mengungkapkan bahwa terdapat dua jenis risiko secara umum, yaitu:

a. Risiko Murni (*pure risk*)

Risiko murni adalah ketidakpastian terjadinya suatu kerugian atau dengan kata lain hanya ada suatu peluang merugi dan bukan suatu peluang keuntungan. Risiko murni adalah suatu risiko yang bilamana terjadi akan memberikan kerugian dan apabila tidak terjadi maka tidak menimbulkan kerugian namun juga tidak menimbulkan keuntungan. Risiko ini akibatnya hanya ada dua macam: rugi atau *break event*, contohnya adalah pencurian, kecelakaan atau kebakaran.

b. Risiko Spekulasi (*speculative risk*)

Risiko spekulasi adalah risiko yang berkaitan dengan terjadinya dua kemungkinan, yaitu peluang mengalami kerugian finansial atau memperoleh keuntungan. Risiko ini akibatnya ada tiga macam: rugi, untung atau break event, contohnya adalah investasi saham di bursa efek, membeli undian dan sebagainya.

2.2.3 Sumber-sumber Risiko

Godfrey (1996) mengungkapkan bahwa terdapat sumber-sumber risiko yang perlu diketahui dan diidentifikasi sebagai langkah awal penanganan risiko, yaitu sebagai berikut:

1. **Politik (*Political*)**.

   Contohnya: Kebijaksanaan pemerintah, pendapat publik, perubahan ideologi, peraturan, kekacauan (perang, terorisme, kerusuhan).

2. **Lingkungan (*Environmental*)**.

   Contohnya: Pencemaran, kebisingan, perizinan, opini publik, kebijakan internal/perusahaan, perundangan yang berkaitan dengan lingkungan, dampak lingkungan.

3. **Perencanaan (*Planning*)**.

   Contohnya: Persyaratan perizinan, kebijakan dan praktik, tata guna lahan, dampak sosial dan ekonomi, opini publik.

4. **Pemasaran (*Market*)**.

   Contohnya: Permintaan (perkiraan), persaingan, keusangan, kepuasan pelanggan, mode.

5. **Ekonomi (*Economic*)**.

   Contohnya: Kebijakan keuangan, perpajakan, inflasi, suku bunga, nilai tukar.

6. **Keuangan (*Financial*)**.

   Contohnya: Kebangkrutan, keuntungan, asuransi, risk share.

7. **Alami (*Natural*)**.

   Contohnya: Kondisi tanah di luar dugaan, cuaca, gempa, kebakaran dan ledakan, temuan situs arkeologi.

8. **Proyek (*Project*)**.

   Contohnya: Definisi, strategi pengadaan, persyaratan unjuk kerja, standar, kepemimpinan, organisasi (kedewasaan, komitmen, kompetensi dan

pengalaman), perencanaan dan pengendalian kualitas, rencana kerja, tenaga kerja dan sumber daya, komunikasi dan budaya.

9. **Teknis (*Technic*)**.

   Contohnya: Kelengkapan desain, efisiensi operasional, keandalan.

10. **Manusia (*Human*)**.

    Contohnya: Kesalahan, tidak kompeten, kelalaian, kelelahan, kemampuan berkomunikasi, budaya, bekerja dalam kondisi gelap atau malam hari.

11. **Kriminal (*Criminal*)**.

    Contohnya: Kurang aman, perusakan, pencurian, penipuan, korupsi.

12. **Keselamatan (*Safety*)**.

    Contohnya: Peraturan (kesehatan dan keselamatan kerja), zat berbahaya, bertabrakan, keruntuhan, kebanjiran, kebakaran dan ledakan.

2.3 Ancaman Keamanan Informasi

Sarno & Iffano (2009) mengungkapkan bahwa threat atau ancaman adalah suatu potensi yang disebabkan oleh insiden yang tidak diinginkan yang mungkin membahayakan jalannya proses bisnis organisasi. Alberts (2002) mengungkapkan bahwa ancaman-ancaman SI atau TI tersebut diantaranya:

1. *Compromises to intellectual property* (seperti pembajakan, pelanggaran hak cipta)
2. *Espionage* atau pelanggaran (akses yang tidak sah dan/atau pengumpulan data)
3. *Forces of nature* (seperti kebakaran, banjir, gempa bumi, petir)
4. *Human error or failure* (seperti kecelakaan, kesalahan karyawan, kegagalan mengikuti kebijakan)
5. *Information extortion* (seperti memaksa pengungkapan informasi)

6. *Missing, inadequate, or incomplete controls* (kontrol perangkat lunak, keamanan fisik)

   Missing, inadequate, or incomplete organizational policy or planning (masalah pelatihan, privasi, kurangnya kebijakan yang efektif) dan lain-lain.

2.4 Aspek Keamanan Informasi

Whitman & Mattord (2011) mengungkapkan bahwa organisasi keamanan informasi memiliki tiga aspek yang harus dipahami untuk bisa menerapkannya, aspek tersebut biasa disebut dengan CIA Triad Model, antara lain adalah:

1. *Confidentiality* (kerahasiaan) merupakan aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
2. *Integrity* (integritas) merupakan aspek yang menjamin tidak adanya pengubahan data tanpa seizin pihak yang berwenang, menjaga keakuratan dan keutuhan informasi.
3. *Availability* (ketersediaan) 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 Metode OCTAVE

A. Definisi Singkatan Dari OCTAVE

1. *Operationally*

Alberts, C., Dorofee, A., Stevens, J., Woody. C. (2005) mengungkapkan bahwa merupakan praktik keamanan yang berfokus pada hal-hal yang berkaitan dengan

teknologi, seperti bagaimana cara penggunaannya, interaksinya, dan perlindungan terhadap teknologi pada kegiatan sehari-hari.

2. *Critical*

Kritis adalah suatu keadaan krisis, gawat, genting atau dalam keadaan yang paling menentukan berhasil atau gagalnya suatu usaha (Kamus Besar Bahasa Indonesia, 2008).

3. *Threat*

Alberts, C., Dorofee, A., Stevens, J., Woody. C. (2005) mengungkapkan bahwa *threat* merupakan suatu indikasi atas potensi kejadian yang tidak diinginkan. Ancaman mengarah pada situasi dimana seseorang dapat melakukan sesuatu yang tidak diinginkan atau kejadian alam yang dapat menyebabkan sesuatu yang tidak diinginkan.

4. *Asset*

Aset merupakan sesuatu yang memiliki nilai bagi perusahaan. Aset TI merupakan kombinasi dari aset fisik dan non fisik serta dikelompokan kedalam kelas yang spesifik seperti informasi, sistem, sumber daya manusia, layanan dan aplikasi (Alberts, C., Dorofee, A., Stevens, J., Woody. C., 2005).

5. *Vulnerability*

Kerentanan merupakan suatu kelemahan pada praktek atau kebijakan yang ada pada perusahaan yang dapat menyebabkan aksi-aksi yang tidak sah (Alberts, C., Dorofee, A., Stevens, J., Woody. C., 2005).

6. *Evaluation*

Evaluasi adalah kegiatan untuk mengumpulkan informasi tentang bekerjanya sesuatu, yang selanjutnya informasi tersebut digunakan untuk menentukan

alternatif yang tepat dalam mengambil keputusan. Fungsi utama evaluasi dalam hal ini adalah menyediakan informasi-informasi yang berguna bagi pihak *decision maker* untuk menentukan kebijakan yang akan diambil berdasarkan evaluasi yang telah dilakukan (Suharsimi, 2009).

7. *Critical Assets*

Aset yang paling penting bagi perusahaan. Perusahaan akan menderita kerugian yang besar apabila aset kritis diakses oleh pihak yang tidak berwenang, dimodifikasi tanpa diketahui perusahaan, mengalami kerusakan atau hilang, serta akses terhadap aset kritis terinterupsi (Alberts, C., Dorofee, A., Stevens, J., Woody. C., 2005).

B. Pengertian OCTAVE

OCTAVE adalah sebuah pendekatan terhadap evaluasi risiko keamanan informasi yang komprehensif, sistematik, terarah dan dilakukan sendiri. Pendekatannya disusun dalam satu set kriteria yang mendefinisikan elemen esensial dari evaluasi risiko keamanan informasi. Kriteria OCTAVE memerlukan evaluasi yang harus dilakukan oleh sebuah tim interdisipliner yang terdiri dari personil teknologi informasi dan bisnis organisasi (Supradono, 2009).

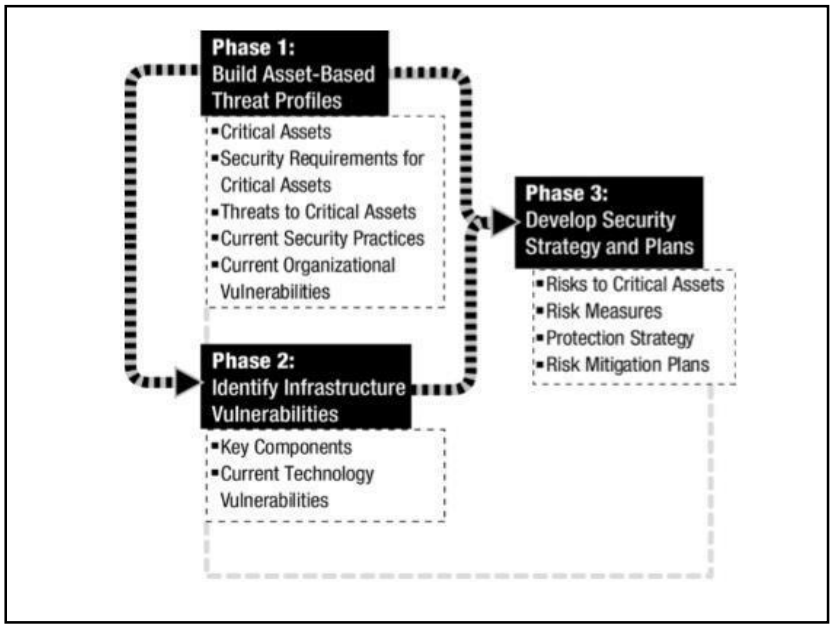
OCTAVE adalah metodologi untuk mengidentifikasi dan mengevaluasi risiko keamanan informasi. Hal ini dimaksudkan untuk membantu organisasi untuk mengembangkan kriteria evaluasi risiko kualitatif yang menggambarkan toleransi risiko operasional organisasi, mengidentifikasi aset yang penting bagi misi organisasi, mengidentifikasi kerentanan dan ancaman terhadap aset tersebut, menentukan dan mengevaluasi konsekuensi potensi untuk organisasi jika ancaman yang diwujudkan.

OCTAVE adalah informasi evaluasi risiko keamanan mandiri. Konsep inti dari OCTAVE didefinisikan sebagai situasi di mana orang-orang dari sebuah organisasi mengelola dan mengarahkan evaluasi risiko keamanan informasi untuk organisasi mereka. Orang organisasi mengarahkan kegiatan evaluasi risiko dan bertanggung jawab untuk membuat keputusan tentang upaya organisasi untuk meningkatkan keamanan informasi. Dalam OCTAVE, tim interdisipliner, yang disebut tim analisis, memimpin evaluasi.

OCTAVE memerlukan tim analisis untuk mempertimbangkan hubungan antara aset kritis, ancaman terhadap aset tersebut, dan kerentanan (baik organisasi dan teknologi) yang dapat mengekspos aset untuk ancaman. Hal ini membutuhkan tim analisis untuk 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.

C. Fase atau Tahapan Metode OCTAVE

Organisasi, teknologi, dan analisis aspek evaluasi risiko keamanan informasi meminjamkan kepada pendekatan tiga tahap. OCTAVE diselenggarakan pada aspek-aspek dasar (diilustrasikan pada Gambar 2.1), memungkinkan personel organisasi untuk merakit gambaran yang komprehensif tentang kebutuhan keamanan informasi organisasi.



Sumber : Octave Criteria Version 2.0, Software Engineering Institute, Carnegie Mellon University

Gambar 2.1 Fase atau Tahapan Metode Octave

Tahap 1: Membangun Aset Berdasarkan Profil Ancaman, dalam tahap ini dibagi jadi 5 proses yaitu:

1. Mendata aset kritis
2. Mengidentifikasi kebutuhan keamanan aset kritis
3. Mengidentifikasi ancaman aset kritis
4. Mendata keamanan yang sudah diterapkan
5. Mengidentifikasi kelemahan perusahaan

Tahap 2: Identifikasi Kerentanan Infrastruktur, ada 2 proses dalam tahap ini yaitu:

1. Mengidentifikasi komponen kunci
2. Mengevaluasi kerentanan komponen kunci

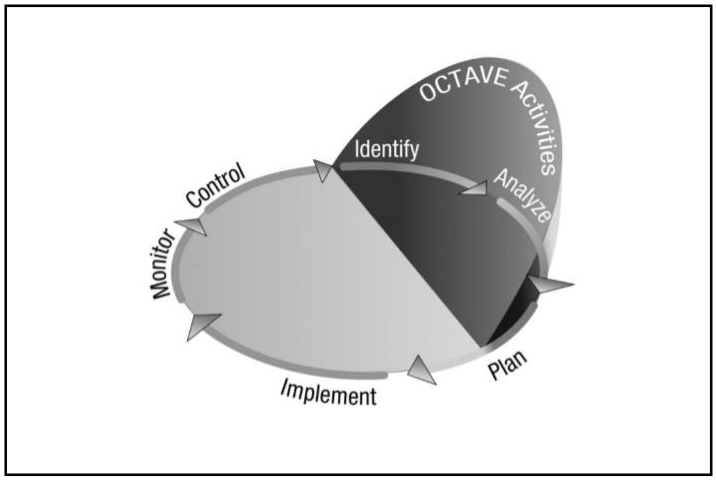
Tahap 3: Mengembangkan Strategi Keamanan dan Rencana, proses dalam tahap ini adalah:

1. Mengidentifikasi risiko
2. Melakukan pengukuran risiko

3. Rencana mitigasi risiko

OCTAVE memberikan pandangan organisasi seperti risiko keamanan informasi saat ini. Memberikan bidikan dalam waktu, atau dasar yang dapat digunakan untuk memfokuskan kegiatan mitigasi dan perbaikan. Setelah menggunakan metode OCTAVE, tim analisis melakukan kegiatan untuk mengenali risiko keamanan informasi organisasi, menganalisa risiko untuk menentukan prioritas, mengembangkan strategi perlindungan untuk perbaikan organisasi dan mitigasi risiko berencana untuk mengurangi risiko terhadap aset organisasi kritis.

Evaluasi risiko keamanan informasi merupakan bagian dari kegiatan manajemen risiko keamanan informasi organisasi. OCTAVE adalah kegiatan evaluasi, bukan proses yang berkesinambungan. Dengan demikian, ia memiliki awal pasti dan akhir. Gambar 2.2 menunjukkan hubungan antara kegiatan-kegiatan ini dan octave cocok. Selain itu, tercatat bahwa ada aspek berkelanjutan untuk kegiatan mengidentifikasi dan menganalisis.



Sumber : Introduction To The Octave Approach, Software Engineering Institute, Carnegie Mellon University

Gambar 2.2 Proses dalam Octave

Secara berkala, sebuah organisasi harus “reset” dasar dengan melakukan OCTAVE lain. Waktu antara evaluasi dapat ditentukan sebelumnya (misalnya, tahunan) atau dipicu oleh peristiwa besar (misalnya, reorganisasi perusahaan atau desain ulang dari infrastruktur komputasi organisasi). Di antara evaluasi, sebuah organisasi secara berkala dapat mengidentifikasi risiko baru, menganalisis risiko ini dalam kaitannya dengan risiko yang ada, dan mengembangkan rencana mitigasi untuk mereka.

2.6 Metode Analisis FMEA

FMEA (*Failure Mode Effect Analysis*) FMEA adalah sebuah metode evaluasi kemungkinan terjadinya sebuah kegagalan dari sebuah sistem, desain, proses atau servis untuk dibuat langkah penanganannya (Yumaida, 2011). Dalam FMEA, setiap kemungkinan kegagalan yang terjadi dikuantifikasi untuk dibuat prioritas penanganan. Dalam penelitian ini FMEA dilakukan untuk melihat risiko-risiko yang mungkin terjadi pada operasi perawatan dan kegiatan operasional perusahaan.

Dengan menggunakan metode FMEA dapat mengidentifikasi dan memahami potensi kesalahan yang akan terjadi serta penyebabnya dan efek pada organisasi, sistem atau pengguna. Dapat mengelola risiko berdasarkan dari kesalahan, dampak dan penyebab serta kasus prioritas dengan tindakan memperbaiki dan dapat mengidentifikasi serta mengarahkan tindakan perbaikan pada masalah yang paling serius.

Tujuan penerapan FMEA adalah:

1. Mengidentifikasi mode kegagalan beserta seberapa parah tingkat efeknya.

2. Mengidentifikasi aset kritis dan aset yang digunakan secara signifikan.

3. Mengurutkan proses.

FMEA (*Failure Mode and Effect Analysis*) adalah suatu prosedur terstruktur untuk mengidentifikasi dan mencegah sebanyak mungkin mode kegagalan (*failure modes*) (Robin dkk, 1996).

Langkah-langkah dalam pembuatan FMEA adalah sebagai berikut:

1. Mereview proses.
2. Brainstorm potensi risiko.
3. Membuat daftar risiko, penyebab, dan efek yang berpotensi.
4. Menentukan tingkat *severity*, digunakan untuk menganalisa risiko dengan menghitung seberapa besar dampak kejadian mempengaruhi output 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 2.1 Nilai *Severity*

Rate	Tingkatan Efek	Kriteria
1	*Very low* (Sangat Rendah)	Merupakan rate dimana kegagalan dapat diabaikan/tidak perlu diperkirakan
2	*Low* (Rendah)	Perbaikan kegagalan masih ringan, dapat diatasi dengan peringatan masalah (25%)
3		Perbaikan kegagalan masih ringan, dapat diatasi dengan peringatan masalah (50%)
4	*Medium* (Sedang)	Perbaikan kegagalan masih ringan, dapat diatasi dengan peringatan masalah (75%)

5		Kegagalan mulai memberikan efek pada beberapa proses bisnis utama maupun pendukung (degradasi fungsi utama)
6	*High* (Tinggi)	Kegagalan mulai memberikan efek pada beberapa proses bisnis utama maupun pendukung (hilangnya fungsi utama)
7		Kegagalan mempengaruhi semua proses bisnis utama maupun pendukung sehingga mengganggu proses bisnis (degradasi fungsi utama)
8	*Very High* (Sangat Tinggi)	Kegagalan mempengaruhi semua proses bisnis utama maupun pendukung sehingga mengganggu proses bisnis (hilangnya fungsi utama)
9		Kegagalan menimbulkan efek bagi perusahaan secara menyeluruh dan terhitung fatal (dengan peringatan)
10		Kegagalan menimbulkan efek bagi perusahaan secara menyeluruh dan terhitung fatal (tanpa peringatan)

Sumber : C.S. Carlson, "Understanding and Applying the Fundamentals of FMEAs," 2014 Annu. Reliab. Maintainab. Symp., 2014

5. Menentukan tingkat *occurrence,* menunjukan seberapa sering / intensitas risiko terjadi, serta menjabarkan skala pengukuran risiko berdasarkan peluang terjadinya. Setelah menentukan rating pada proses *severity* tentukan *rating* terhadap nilai *occurance*.

Penentuan *rate* dilakukan dengan menggunakan tabel berikut:

Tabel 2.2 Nilai *Occurance*

Rate	Tingkatan Efek	Kriteria
1	*Very low* (Sangat Rendah)	Kegagalan terjadi satu kali tiap lima tahun ke atas
2 3	*Low* (Rendah)	Kegagalan terjadi tiap tiga sampai lima tahun

4 5 6	*Medium* (Sedang)	Kegagalan terjadi tiap tahun
7 8	*High* (Tinggi)	Kegagalan terjadi tiap tiga sampai enam bulan
9 10	*Very High* (Sangat Tinggi)	Kegagalan terjadi sangat sering

Sumber : C.S. Carlson, "Understanding and Applying the Fundamentals of FMEAs," 2014 Annu. Reliab. Maintainab. Symp., 2014

6. Menentukan tingkat *detection*, pengukuran terhadap kemampuan mengendalikan atau mengontrol kegagalan yang dapat terjadi. Setelah mendapatkan nilai dari setiap faktor *severity, occurance* dan *detection*, kemudian nilai tersebut akan dikalikan sehinga menghasilkan sebuah nilai *Risk Priority Number*. Selanjutnya kita menghitung nilai *detection*.

Penentuan *rate* dilakukan menggunakan tabel berikut:

Tabel 2.3 Nilai *Detection*

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

Sumber : C.S. Carlson, "Understanding and Applying the Fundamentals of FMEAs," 2014 Annu. Reliab. Maintainab. Symp., 2014

7. Menghitung RPN (*Risk Priority Number*), yaitu hasil perkalian *severity* (S), *occurrence* (O), dan *detection* (D).

RPN untuk menentukan prioritas dari kegagalan. RPN tidak memiliki nilai atau arti. Nilai tersebut digunakan untuk meranking kegagalan proses yang potensial. Kriteria RPN ditunjukkan pada tabel di bawah ini:

Tabel 2.4 Kriteria RPN

RPN	***Calculation Level***
0-19	*Very Low*
20-79	*Low*
80-119	*Medium*
120-199	*High*
≥200	*Very High*

Sumber : C.S. Carlson, "Understanding and Applying the Fundamentals of FMEAs," 2014 Annu. Reliab. Maintainab. Symp., 2014

8. Membuat prioritas risiko untuk ditindaklanjuti.
9. Mengambil tindakan untuk mengurangi atau menghilangkan risiko tertinggi atau risiko kritis.

2.7 Penelitian Terdahulu

Penelitian terdahulu ini menjadi salah satu acuan penulis dalam melakukan penelitian sehingga penulis dapat memperkaya teori yang digunakan dalam mengkaji penelitian yang dilakukan.

Yang pertama dari Wenni Syafitri dengan judul Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus: Sistem Informasi Akademik Universitas XYZ) pada tahun 2016 yang isinya Sistem informasi akademik Universitas XYZ merupakan terobosan terbaru dibidang pelayanan akademik. Sistem ini menyediakan berbagai informasi yang dibutuhkan oleh civitas akademika. Sehingga kebutuhan akan keberlangsungan sistem ini semakin penting.

Permasalahan yang pernah ada di SI Akademik Universitas XYZ seperti berkaitan dengan celah kerawanan keamanan informasi. Jika permasalahan ini tidak dapat diperbaiki secara berkelanjutan, alhasil akan memberikan dampak ataupun risiko kepada keberlangsungan sistem ini, khusunya civitas akademika. Penelitian ini menggunakan NIST SP 800-30 sebagai metode yang digunakan untuk menyelesaikan permasalahan tersebut. Maka berdasarkan hasil penelitian yang telah dilakukan, Universitas xyz memiliki 1 tingkat risiko tinggi, 5 tingkat risiko sedang dan 52 tingkat risiko rendah.

Selanjutnya dari Balqis Lembah Mahersmi, Feby Artowini Muqtadiroh, Bekti Cahyo Hidayanto dengan judul Analisis Risiko Keamanan Informasi Dengan Menggunakan Metode Octave Dan Kontrol Iso 27001 Pada Dishubkominfo Kabupaten Tulungagung pada tahun 2016 Tujuan dari penelitian ini adalah untuk mengidentifikasi, menilai dan memitigasi risiko yang berkaitan dengan teknologi informasi yang dikelola oleh Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung berdasarkan metode OCTAVE. Hasil dari penelitian ini adalah melakukan identifikasi risko yang dapat terjadi pada Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung terkait implementasi teknologi informasi dan memberikan masukan atau rekomendasi mitigasi ISO 27001 kepada pihak Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung bagaimana langkah mitigasi risiko yang tepat sesuai dengan hasil identifikasi risiko yang akan muncul terkait implementasi teknologi informasi. Selanjutnya dari Fernando Reza Destrianto, Nelmiawati dan Maya Armys Roma Sitorus dengan judul Manajemen Risiko Ancaman pada Aplikasi Website Sistem Informasi Akademik Politeknik Negeri Batam Menggunakan Metode OCTAVE

pada tahun 2017 Penelitian ini bertujuan untuk melakukan pengujian keamanan dan manajemen risiko ancaman yang terjadi pada SIA dengan menggunakan metode OCTAVE. Berdasarkan Open Web Application Security Project (OWASP), OCTAVE merupakan sebuah metode dalam manajemen risiko secara sistematik dengan melakukan pengidentifikasian risiko. Metode ini bertujuan untuk menyediakan tahapan dalam mengelola risiko terhadap ancaman yang telah ditemukan. Hasil yang diperoleh menemukan bahwa terdapat 4 kategori ancaman terhadap SIA berupa otentikasi, enkripsi, manajemen sesi dan manajemen konfigurasi.

Selanjutnya dari Raden Budiarto dengan judul Penerapan Metode FMEA Untuk Keamanan Sistem Informasi (Studi Kasus: Website POLRI) pada tahun 2017 Penelitian ini menjabarkan pemecahan persoalan keamanan data dan jaringan serta manajemen risiko dengan menggunakan metode FMEA. Variabel yang diukur pada penelitian ini adalah occurence (frekuensi kejadian), severity (dampak) dan detection (deteksi atau pencegahan) dari masing-masing mode kegagalan. Hasil pengolahan data menunjukkan adanya tingkat kerawanan yang tinggi. Selama periode pengumpulan data setidaknya terdapat 4 celah keamanan yang berpotensi menimbulkan setidaknya 7 potensi kegagalan sistem informasi.

Selanjutnya dari Alvina Hendika Putri, Yupie Kusumawati dengan judul Strategi Mitigasi Risiko Aset Kritis Teknologi Informasi Menggunakan Metode Octave Dan FMEA pada tahun 2017 Tujuan dari penelitian ini adalah untuk mengetahui apa saja aset TI yang ada di perusahaan, menganalisa risiko yang terjadi pada setiap aset TI dan mengetahui mitigasi apa saja yang perlu dilakukan apabila risiko tersebut terjadi pada aset TI. Metode penelitian yang digunakan adalah

Octave untuk mengelola risiko aset TI dan FMEA untuk melakukan penilaian terhadap masing-masing risiko, yang kemudian diranking berdasarkan prioritasnya. Hasil yang diperoleh dalam peneltian ini adalah 0 risiko very high, 0 risiko high, 0 risiko medium, 9 risiko low, 36 risiko very low.

Selanjutnya dari Damar Nurcahyono dan Achmad Djunaedi dengan judul Evaluasi Pelaksanaan Manajemen Risiko Teknologi Informasi pada Kantor Arsip Daerah Kota Samarinda dengan Menggunakan The Risk IT Framework pada tahun 2013 Tujuan dari penelitian ini adalah untuk mengetahui apakah suatu insitusi tersebut sudah melakukan pencegahan terjadinya kesalahan dan meminimalkan kerugian maka perlu dilakukan evaluasi terhadap proses manajemen risiko teknologi informasi. Framework yang digunakan dalam melakukan evaluasi manajemen risiko teknologi informasi pada penelitian ini adalah Risk IT pada penelitian ini melakukan deskripsi tingkat kematangan kondisi saat ini serta merumuskan program untuk meningkatkan kondisi kematangan manajemen risiko TI dari tingkat kematangan saat ini menuju tingkat kematangan yang diharapkan pada Kantor Arsip Daerah Kota Samarinda. Hasil pada penelitian ini didapatkan proses pelaksanaan manajemen risiko teknologi informasi pada Kantor Arsip Daerah Kota Samarinda ada yang sesuai target dan ada yang belum sesuai target. Hal ini ditunjukan dengan atribut tingkat kematangan teknologi informasi yang sebagian besar berada pada tingkat kematangan repeatable but intuitive dan defined process. Pada penelitian ini juga telah dirumuskan beberapa program tiap domain untuk meningkatkan kondisi kematangan menuju yang diharapkan pada Kantor Arsip Daerah Kota Samarinda.

Selanjutnya dari Deni Ahmad Jakaria, R. Teduh Dirgahayu dan Hendrik dengan judul Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro pada tahun 2013 Penelitian ini bertujuan untuk melakukan analisis risiko pada sistem informasi akademik di perguruan tinggi. Hasil akhir dari penilaian risiko berupa rekomendasi mengenai langkah-langkah yang harus diambil untuk perlindungan sistem informasi beserta aset-asetnya.

Selanjutnya dari Saut Pintubipar Saragih dengan judul Implementasi Octave-S Dalam Evaluasi Manajemen Resiko Sistem Informasi Pada Balai Pelatihan Kesehatan Batam pada tahun 2018 Di pusat pelatihan kesehatan Batam (Bapelkes) yang juga telah menerapkan sistem informasi dalam proses bisnis dan organisasi juga menerima ancaman terhadap sistem informasi. Manajemen risiko sistem informasi dapat menggunakan beberapa metode untuk melakukan evaluasi atau penilaian salah satunya adalah dengan menggunakan metode OCTAVE-S. Octave-s memiliki tiga fase penilaian utama yang diikuti oleh setiap proses. Prosedur keamanan TI yang dilaksanakan oleh Bapelkes diotorisasi ke markas Bapelkes yang dikendalikan dari jarak jauh oleh sistem administrasi secara menyeluruh. Hasil penelitian menunjukkan bahwa institusi belum menerapkan semua manajemen risiko TI pada jalur yang tepat, ditemukan bahwa beberapa prosedur standar seperti kebijakan TI, sistem kolaborasi, audit sistem informasi, arsitektur, manajemen mitigasi tidak dikelola dengan baik. Selain itu, semua karyawan yang bekerja di bidang TI baik pengguna akhir atau administrator TI belum terlatih dengan baik.

Selanjutnya dari Henny Hendarti dan Maryani dengan judul Pengukuran Manajemen Risiko Teknologi Informasi Dengan Metode Octtave-S pada tahun

2014 Tujuan dari penelitian ini adalah melakukan pengukuran risiko untuk mengindetifikasi aset perusahaan dan menganalisis risiko-risiko, dan merencanakan strategi perlindungan keamanan, serta meminimalkan risiko. Metodologi yang digunakan adalah studi kasus berdasarkan literatur yang berhubungan dengan metode OCTAVE-S. Observasi dilakukan dengan pengamatan secara langsung ke perusahaan, wawancara dengan pihak yang berkaitan, serta mengunakan kuesioner berdasarkan metode OCTAVE-S. Hasil yang dicapai dari penelitian ini yaitu pengelolaan risiko teknologi informasi pada perusahaan agar dapat meminimalkan risiko. Dengan temuan yang diperoleh, maka diharapkan perusahaan dapat mengindentifikasi risiko yang mungkin terjadi dan menanggulanginya secara efisien dan efektif.

Dan yang terakhir dari Rosini, Meutia Rachmaniah dan Badollahi Mustafa dengan judul Penilaian Risiko Kerawanan Informasi Dengan Menggunakan Metode Octave Allegro Penelitian ini bertujuan untuk melakukan penilaian risiko pada kerentanan informasi, untuk mendapatkan tingkat kerentanan informasi, dan untuk menghasilkan rekomendasi strategis untuk mengatasi kerentanan informasi di Perpustakaan X menggunakan OCTAVE Allegro sebagai metode. Hasil penelitian menunjukkan bahwa dari 4 kategori, kerentanan informasi di X Library berada pada kategori 3 atau cukup rentan dengan 22 area yang menjadi perhatian atau setara dengan 42,31%. Penilaian risiko yang dilakukan di Perpustakaan X ternyata hasilnya adalah ada 10 informasi aset yang dimiliki oleh Kepala Perpustakaan Pusat, Unit Layanan Administrasi, Unit Kataloging dan Klasifikasi, Unit Layanan Sirkulasi, Unit Layanan Referensi. Hasil kedua berisi ancaman terhadap aset informasi oleh 52 bidang yang dilakukan oleh internal X Library

adalah 14 aktor, oleh internal X adalah 13 aktor, dan oleh eksternal adalah 2 aktor. Hasil ketiga adalah ada 62 konsekuensi dari 52 aset informasi dengan paling banyak konsekuensi ditemukan dalam koleksi dokumen elektronik X-ana yang dari 6 bidang yang menjadi perhatian menghasilkan 10 konsekuensi. Rekomendasi strategis untuk mengatasi kerentanan informasi di X Library disesuaikan sesuai dengan mitigasi risiko yang dilakukan di setiap bidang yang disebut kontrol atau pengendalian risiko. Dari hasil penilaian risiko yang dapat dilakukan adalah mengurangi atau menghilangkan risiko (memitigasi) sebanyak 21 bidang yang menjadi perhatian, untuk mentransfer atau memitigasi risiko sebanyak 16 bidang yang menjadi perhatian, untuk menunda risiko sebanyak 12 bidang menjadi perhatian, dan menerima risiko (menerima) atau menunda sebanyak 3 bidang yang menjadi perhatian.

Kelebihan penelitian saya dari jurnal-jurnal terdahulu yakni penelitian saya mencari risiko terhadap aset kritis, lalu menganalisis seberapa besar tingkat risiko tersebut sehingga dapat kita rekomendasikan SOP (*Standard Operating Procedure)* terhadap risiko-risiko yang akan timbul pada E-LKP UIN Raden Fatah Palembang.