BAB 3
METODE PENELITIAN

Metode penelitian merupakan suatu cara untuk menjawab permasalahan-permasalahan penelitian yang dilakukan secara ilmiah.

3.1 Metode Pengumpulan Data

Pendekatan yang digunakan dalam penelitian ini adalah pendekatan survei yaitu suatu cara penelitian *deskriptif* yang digunakan untuk menggambarkan atau memotret masalah yang terkait dengan risiko yang ada pada organisasi.

Kualitas data bukan hanya di tentukan oleh faktor reliabilitas dan validitas dari alat ukurnya saja, tetapi juga ditentukan oleh bagaimana cara pengumpulannya, ada beberapa aspek dalam pengumpulan data meliputi :

1. Data apa yang akan dikumpulkan (*what*)
2. Dengan apa data itu dikumpulkan (*with*)
3. Kapan data tersebut akan dikumpulkan (*when*)
4. Dari mana data akan dikumpulkan (*where*)
5. Bagaimana cara mengumpulkan (*how*)

Sedangkan dalam pengumpulan data pada penelitian ini dengan menggunakan wawancara dan beberapa studi pustaka.

3.2 Jenis Data

Penelitian ini menggunakan jenis data kualitatif yaitu data yang cenderung bersifat *deskriptif* serta cenderung pada analisis. Data kualitatif diperoleh melalui berbagai macam teknik pengumpulan data seperti analisa dokumen, wawancara, diskusi, atau observasi. Dan dalam penelitian ini data kualitatif mengacu pada penggunaan metode octave. Karena metode octave baik digunakan untuk menganalisa asset-aset IT pada organisasi.

3.3 Sumber Data

Sumber data yang digunakan dalam penelitian tugas akhir ini adalah :

1. Data Primer

   Data primer adalah data yang diperoleh langsung dari responden. Data primer penelitian ini diperoleh langsung dari karyawan / pegawai Universitas Dian Nuswantoro tepatnya pada bagian yang menangani komponen-komponen TI yaitu pada Dinustek dan PSI dan faktor ancaman apa saja yang dihadapi oleh Universitas Dian Nuswantoro.

2. Data Sekunder

   Data sekunder adalah data yang diperoleh tidak langsung dari responden. Data sekunder dalam penelitian ini adalah data dari referensi buku dan jurnal yang barkaitan dengan keamanan asset dan komponen TI.

3.4 Metode Analisis Yang Digunakan

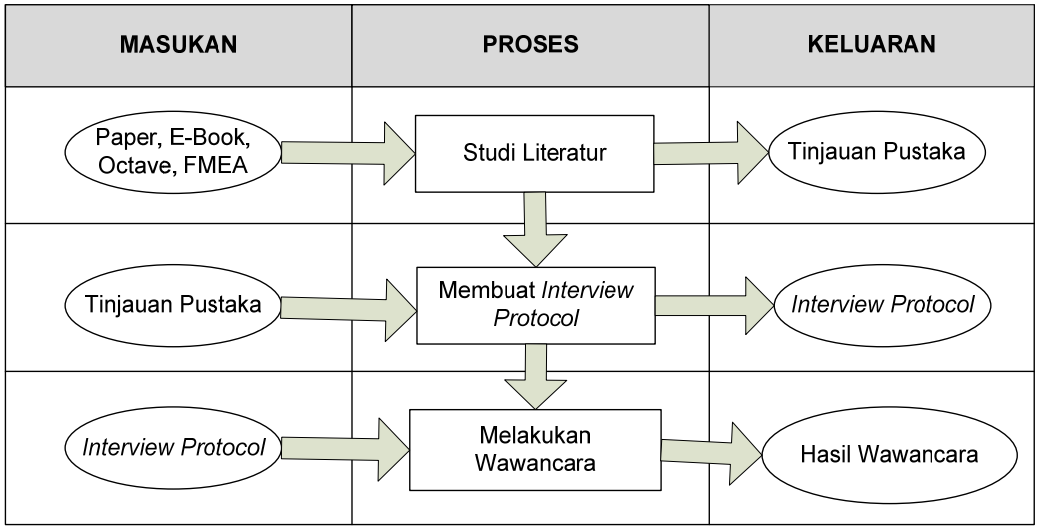
Metode analisis yang digunakan dalam penelitian ini menggunakan dua metode yaitu :

1. Metode OCTAVE yang digunakan untuk mengolah data hasil wawancara.
2. Metode FMEA yang digunakan untuk memberikan nilai pada setiap komponen – komponen teknologi informasi yang sudah didefinisikan pada metode octave.

Metodologi penelitian yang digambarkan dalam bentuk alur diagram. Alur diagram menggambarkan urutan proses secara mendetail dan hubungan antara satu proses dengan proses lainnya. Berikut merupakan alur diagram metodologi laporan ini :

3.4.1 FASE 0 *Preparation*

Tabel 3.1 Fase 0 kerangka kerja octave



1. Studi Literatur

   Studi literatur yang di lakukan menggunakan beberapa sumber baik buku fisik maupun *paper, e-book,* jurnal yang didapatkan secara online. Tujuan dari melakukan studi literatur adalah untuk mendapatkan pemahaman dan wawasan mengenai manajemen risiko TI dan kerangka kerja yang digunakan dalam melakukan penilaian risiko dan mitigasi terhadap risiko tersebut.

2. Membuat *interview protocol*

   Pemahaman dan wawasan yang dimiliki dari proses melakukan studi literatur sebelumnya , menjadi dasar untuk membuat *interview protocol* yang berisi mengenai daftar pertanyaan yang akan diajukan kepada pihak perusahaan.

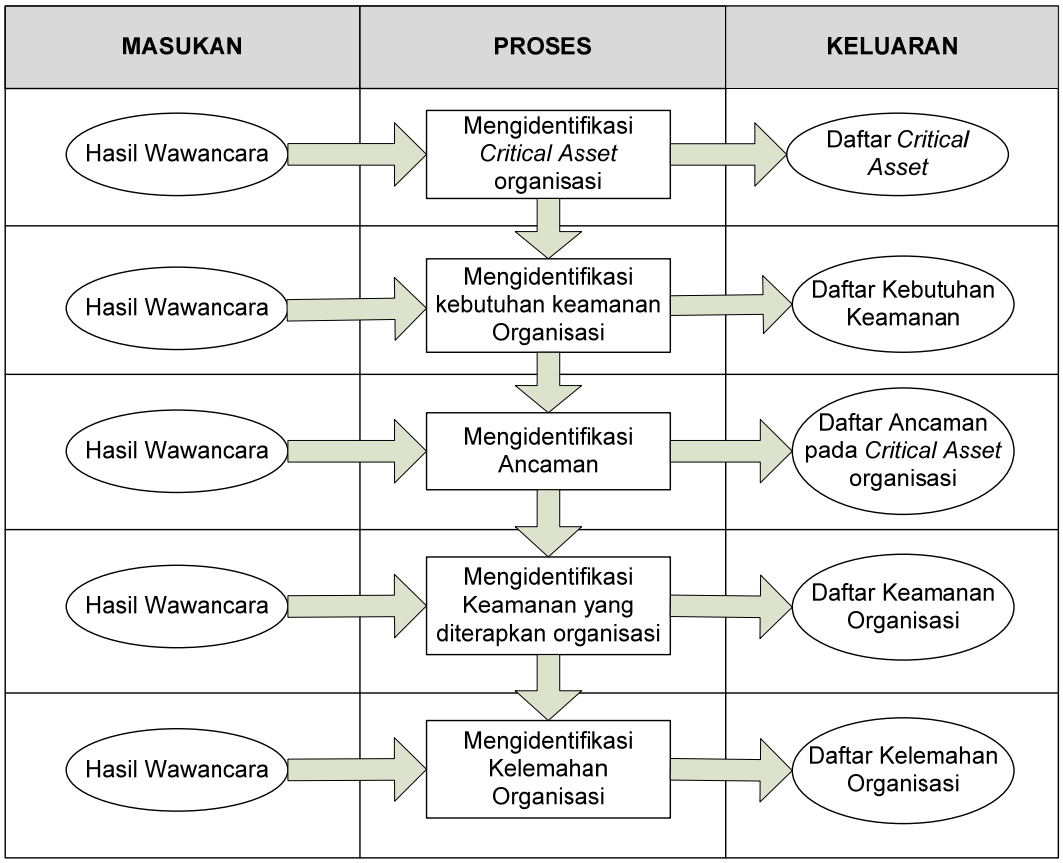
3. Melakukan wawancara

   Tujuan dari melakukan wawancara adalah untuk menggali informasi mengenai organisasi. Dan di penelitian kali ini mewawancarai *staff* sistem *administrator,* dan *network admin* Dinustek dan Kepala PSI, untuk mengetahui aset-aset atau fasilitas yang ada pada Universitas Dian

Nuswantoro, kebutuhan keamanan, ancaman, komponen utama, dan evaluasi komponen.

3.4.2 FASE I *Organizational View*

Tabel 3.2 Fase 1 kerangka kerja octave



Fase pertama dari *organizational view* meliputi lima proses yang harus dilakukan. Lima proses dibahas dalam penjelasan berikut :

1. Mengidentifikasi *Critical Asset* Perusahaan

   Dari hasil wawancara yang sudah dilakukan dengan pihak terkait, maka akan didapatkan informasi mengenai *critical asset* yang dimiliki oleh perusahaan.

2. Mengidentifikasi Kebutuhan Keamanan Perusahaan

   Dari hasil wawancara yang sudah dilakukan, maka akan didapatkan informasi mengenai kebutuhan keamanan pada perusahaan.

3. Mengidentifikasi Ancaman

   Dengan menganalisis hasil wawancara dan daftar kebutuhan keamanan yang ada pada perusahaan, maka dapat dilakukan identifikasi terkait ancaman pada setiap *critical asset*.

4. Mengidentifikasi Keamanan yang Sudah Diterapkan Perusahaan

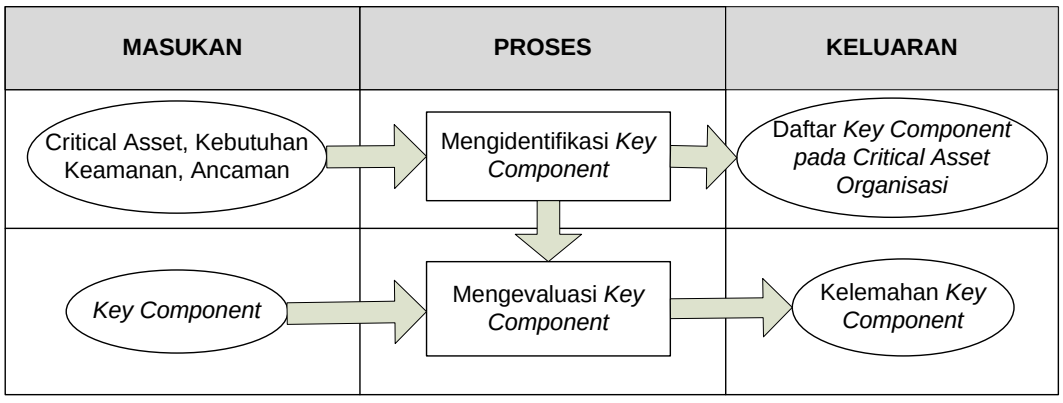
   Melakukan wawancara untuk mengidentifikasi keamanan yang diterapkan oleh perusahaan. Hasil dari proses ini adalah daftar keamanan yang sedang diterapkan perusahaan.

5. Mengidentifikasi Kelemahan Perusahaan

   Melakukan wawancara untuk mengidentifikasi kelemahan yang dimiliki oleh perusahaan.

3.4.3 FASE II *Technologycal View*

Tabel 3.3 Fase 2 kerangka kerja octave



Pada fase kedua akan dilakukan identifikasi *key components* perusahaan terkait dengan *critical assets* yang dimiliki , selain itu juga akan dilakukan identifikasi terhadap kerentanan teknologi yang dimiliki perusahaan. Proses yang terdapat pada fase kedua adalah sebagai berikut

1. Mengidentifikasi *Key Components*

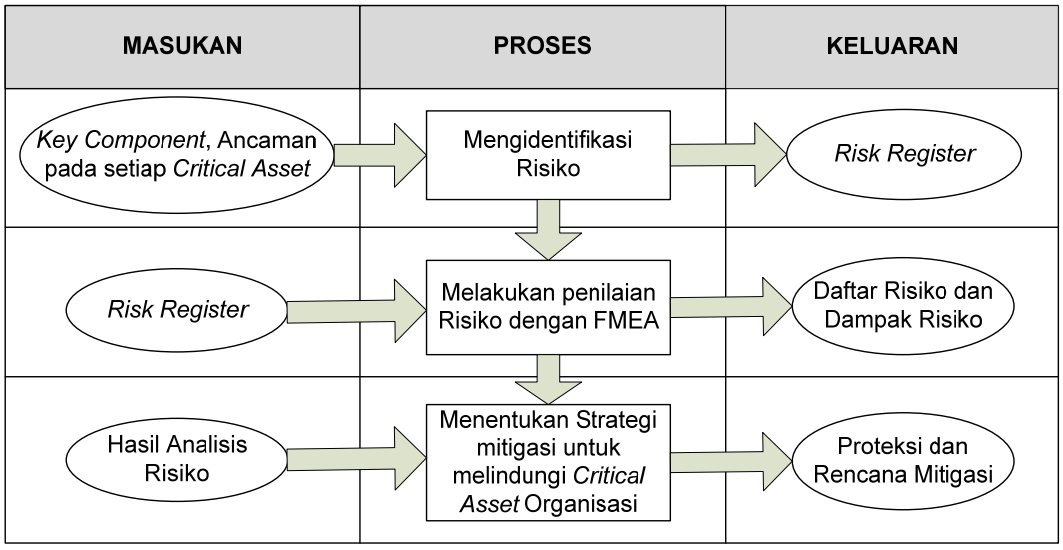
   Dari daftar *critical asset*, kebutuhan keamanan perusahaan dan ancaman yang didapat dari proses wawancara, selanjutnya akan dilakukan analisis dan idenfitikasi mengenai *key components* dari setiap *critical assets*.

2. Mengevaluasi *Key Components*

   Setelah mendapatkan daftar *key components* setiap *critical assets* maka selanjutnya akan dilakukan evaluasi untuk menemukan kerentanan atau kelemahan dari setiap *key components*.

3.4.4 FASE III *Strategy and Plan Development*

Tabel 3.4 Fase 3 kerangka kerja octave



Pada fase ketiga akan dilakukan pengidentifikasian risiko dan dampak yang akan ditimbulkan dan selanjutnya akan dirancang strategi untuk mitigasi risiko . Proses pada fase ketiga ini adalah sebagai berikut :

1. Mengidentifikasi risiko

   Pada tahap ini akan mengidentifikasi risiko-risiko yang mungkin terjadi terkait dengan *critical asset*. Risiko yang akan diidentifikasi berupa risiko yag pernah terjadi maupun perkiraan terhadap risiko yang mungkin terjadi di masa yang akan datang

2. Melakukan Penilaian Risiko dengan Metode FMEA

   Dalam melakukan penilaian terhadap risiko dibutuhkan sebuah kerangka kerja agar penilaian yang dilakukan obyektif dan terpercaya. Pada tugas akhir ini digunakan kerangka kerja FMEA untuk melakukan penilaian risiko. Penilaian risiko menggunakan FMEA didasarkan pada tiga faktor, yaitu :

   a. *Risk Severity*, digunakan untuk menganalisa risiko dengan menghitung seberapa besar dampak kejadian mempengaruhi output proses.
   b. *Risk Occurance*, menunjukan seberapa sering / intensitas risiko terjadi, serta menjabarkan skala pengukuran risiko berdasarkan peluang terjadinya.
   c. *Risk Detection*, adalah 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*.

   RPN = *Severity* x *Occurance* x *Detection* .....[1]

   Dari nilai RPN selanjutnya dikategorikan berdasarkan tingkat risiko yang ada.

3. Menentukan strategi mitigasi untuk melindungi asset kritis perusahaan Pada tahap ini akan diidentifikasi langkah mitigasi risiko berdasarkan ISO 27001 dan 27002, yaitu sesuai dengan panduan *Guide to Risk Assessment & Respons,* Agustus : 2012 yaitu *Avoidance* Menghindari risiko untuk terjadi bagaimanapun caranya. *Transfer* Membiarkan orang lain mengambil risiko (misalnya. oleh asuransi atau untuk kontraktor lewat tanggung jawab untuk risiko). *Limitation / Mitigation* Menerima risiko tetapi berupaya untuk mengurangi atau membatasi dampak dari risiko. *Acceptance* Menerima Risiko.