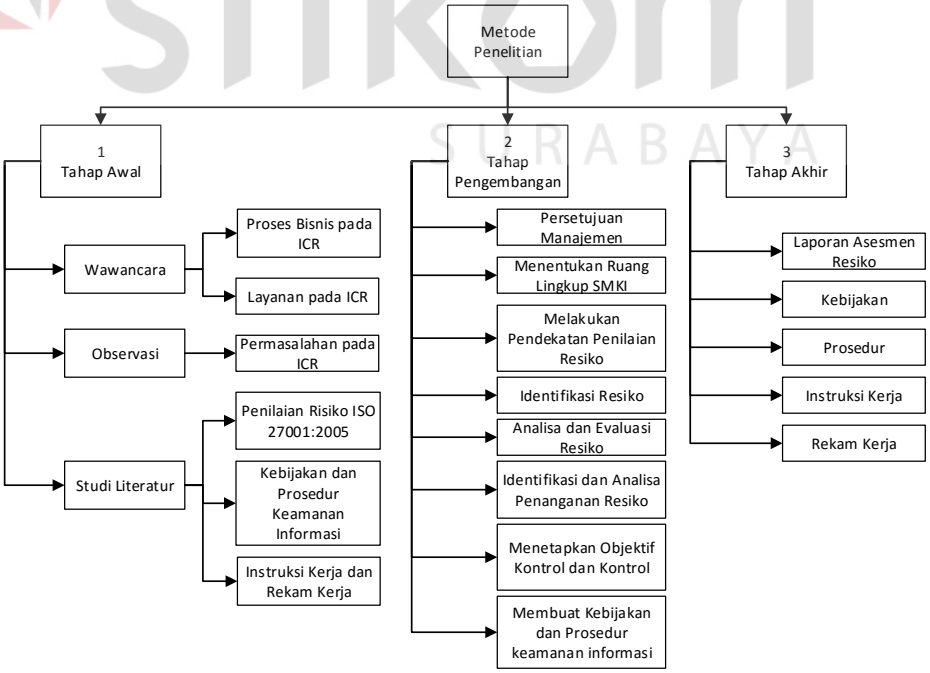
BAB III

METODE PENELITIAN

3.1 Model Usulan

Pada model usulan yang digunakan yaitu model usulan yang digunakan pada tahap Perencanaan berdasarkan pada standar ISO/IEC 27001:2005. Metode penelitian yang akan dilakukan melalui 8 tahap sesuai dengan model perencanaan pada ISO/IEC 27001:2005. Tahapan penelitian yang akan dilakukan dalam penelitian ini sampai pada fase Perencanaan (*Plan*) karena pada fase *Do, Check,* dan *Act* hanya dapat dilakukan oleh pihak perusahaan dan organisasi terkait karena membutuhkan sangat panjang dalam melakukan implementasi dan monitoring terhadap hasil perencanaan yang telah dibuat sebelumnya. Gambar 3.1 dibawah adalah tahapan dalam melakukan penelitian perencanaan sistem manajemen keamanan informasi.



Gambar 3.1. Tahapan dalam Metode Penelitian

3.2 Tahap Awal

Tahap awal dilakukan untuk pengumpulan data dan penggalian informasi agar memperoleh data yang dibutuhkan dalam menyelesaikan penelitian ini. Pengumpulan data dan penggalian informasi dilakukan dengan wawancara, studi literatur, dan observasi.

1. Wawancara

Wawancara dilakukan dengan supervisor teknologi dan informasi pada PT PJB UP Gresik mengenai kebutuhan yang akan dilakukan dalam pelaksanaan tugas akhir. Wawancara bertujuan untuk mengetahui informasi, dan kelemahan apa yang di dapat serta nantinya dapat memberikan solusi bagi permasalahan yang ada. Berikut adalah data-data yang didapat dari hasil wawancara yaitu :

a. Proses bisnis dalam ICR

b. Layanan yang terdapat pada ICR

2. Observasi

Observasi dilakukan pada proses bisnis dari ICR yang bertujuan untuk mendapatkan data tentang suatu masalah, sehingga diperoleh pemahaman yang telah diperoleh sebelummnya. Observasi yang dilakukan menghasilkan permasalahan yang terdapat pada ICR

3. Studi Literatur

Studi literatur yang dilakukan yaitu dengan cara mencari studi literatur pada buku di perpustakaan, atau menggunakan internet. Dalam hal ini meliputi beberapa jenis studi literatur yang digunakan antara lain :

a. Penilaian Risiko ISO 27001:2005

b. Kebijakan dan Prosedur Keamanan Informasi

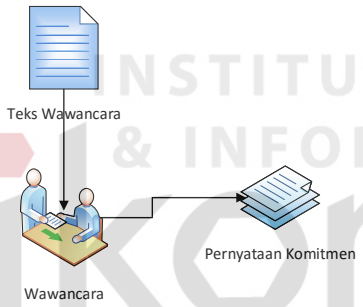
c. Instruksi Kerja dan Rekam Kerja

3.3 Tahap Pengembangan

Tahap pengembangan dilakukan sesuai dengan langkah-langkah pada sistem manajemen keamanan informasi yang ada pada standar ISO/IEC 27001:2005 dan ISO/IEC 27002:2005 mengenai tahap perencanaan sistem manajemen keamanan informasi yang akan dijelaskan sebagai berikut:

1. Persetujuan Manajemen

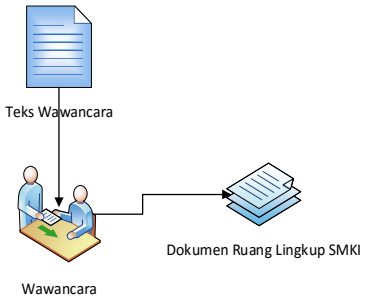
Dalam tahapan menentukan komitmen manajemen dibutuhkan persetujuan komitmen perusahaan sebelum melaksanakan sistem manajemen keamanan informasi. Alur persetujuan komitmen manajemen digambarkan pada Gambar 3.2.



Gambar 3.2. Tahapan Persetujuan Manajermen

2. Menentukan Ruang Lingkup SMKI

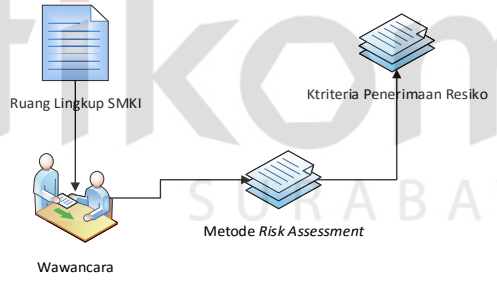
Menentukan ruang lingkup sangat diperlukan untuk pemenuhan dalam tahapan penelitian agar tujuan dokumen yang akan dihasilkan dapat dibuat dengan tepat sesuai dengan kebutuhan permasalahan keamanan informasi perusahaan. Ruang lingkup yang ditentukan berdasarkan kebutuhan organisasi dan aset yang dimiliki oleh perusahaan. Penetapan ruang lingkup ini harus didiskusikan dengan organisasi perusahaan terkait**.** Alur untuk menentukan ruang lingkup dapat dilihat pada Gambar 3.3.



Gambar 3.3. Alur Tahapan Ruang Lingkup SMKI

3. Melakukan Pendekatan Penilaian Resiko

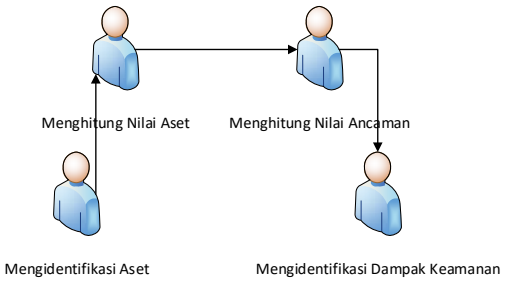
Langkah berikutnya yaitu bagaimana cara melakukan penilaian resiko terhadap informasi yang dimiliki oleh PT PJB. Cara Penilaian resiko ini bergantung pada ruang lingkup yang telah dibentuk sebelumnya. Dalam tahap penilaian resiko terdapat dua hal yang harus dilakukan yaitu menentukan metode *risk assessment* dan menentukan kriteria penerimaan resiko yang telah disetujui oleh perusahaan. Adapun alur dalam tahapan ini dijelasakan pada Gambar 3.4.



Gambar 3.4. Tahapan Penentuan Cara Penilaian Resiko

4. Identifikasi Resiko

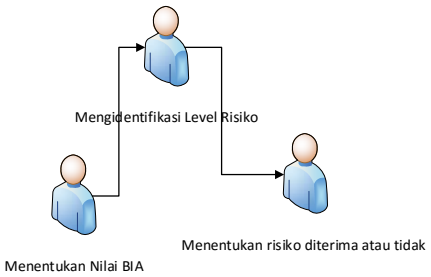
Identifikasi dilakukan untuk mengetahui seberapa besar dan identifikasi resiko apa yang akan diterima oleh PT PJB jika informasi unit mendapat ancaman atau gangguan pada pengamanan informasi. Identifikasi risiko terdiri dari identfikasi aset, nilai aset, nilai ancaman, dan dampak keamanan pada masing-masing aset. Tahapan identifkasi resiko ini akan dijabarkan pada Gambar 3.5.



Gambar 3.5. Tahapan Identifikasi Resiko

5. Analisa dan Evaluasi Resiko

Setelah melakukan identifikasi resiko, maka tahapan selanjutnya yaitu analisa dan evaluasi resiko ysng bertujuan untuk menganalisa hasil dari identifikasi resiko yang telah dibuat sebelumnya dan mengevaluasi apakah resiko dapat diterima sepenuhnya atau masih diperlukan pengolahan agar resiko dapat diterima dengan dampak yang bisa ditoleransi. Analisa dan evaluasi risiko terdiri dari tiga tahapan yaitu tahap pertama menghitung nilai BIA pada aset, tahap kedua mengidentifikasi level risiko yang telah dilakukan sebelumnya dengan melakukan wawancara serta menghasilkan pengukuran nilai pada dampak (*impact)* dan kemungkinan (*probability*) sesuai dengan pedoman umum manajemen risiko PT PJB nomor 128.K/D10/DIR/2014 (Bali, 2014), tahapan ketiga yaitu menentukan apakah risiko diterima atau tidak sesuai dengan kriteria penerimaan risiko yang ditetapkan. Alur dalam analisa dan evaluasi resiko dijelaskan pada Gambar 3.6.



Gambar 3.6. Tahapan Analisa dan Evaluasi Resiko

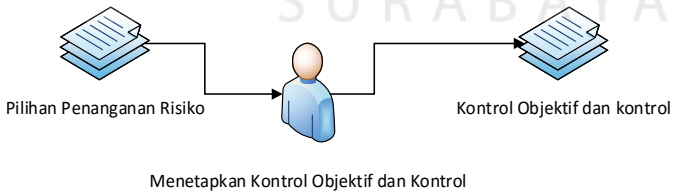
6. Identifikasi dan Evaluasi Penanganan Resiko

Pada tahap ini PT PJB harus melakukan identifikasi dan evaluasi penanganan resiko apakah resiko yang timbul tidak langsung diterima tetapi perlu dikelola lebih lanjut dengan menggunakan kriteria penerimaan risiko yang sudah ditentukan pada saat tahap pendekatan penilaian resiko sesuai dengan keputusan perusahaan. Gambar 3.7 menjelaskan alur tahapan evaluasi resiko.

Gambar 3.7. Tahapan Evaluasi Penanganan Resiko

7. Menetapkan Kontrol Objektif dan Kontrol

Tahapan ini dilakukan dengan tujuan menetapkan kontrol objektif dan kontrol yang sesuai dengan kebututuhan dan kondisi pada ICR berdasarkan ISO/IEC 27002. Kontrol ini dibutuhkan untuk mengelola set perusahaan yang memiliki nilai tinggi dalam permasalahan resiko yang ada pada ICR. Alur dari penetapan kontrol objektif dan kontrol dijelaskan pada Gambar 3.8.

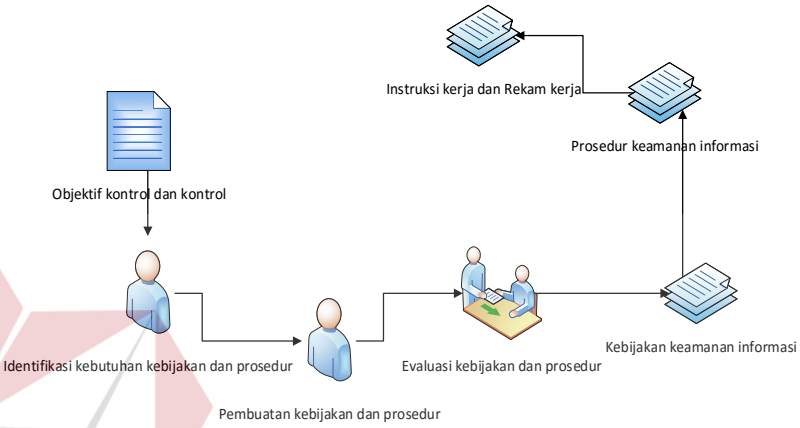


Gambar 3.8 . Tahapan Penetapan Kontrol Objektif dan Kontrol

8. Membuat Kebijakan dan Prosedur Keamanan Informasi dan Instruksi Kerja

Penyusunan kebijakan dan prosedur disusun dengan memperhatikan sasaran kontrol yang telah dipilih sesuai dengan kontrol objektif dan kontrol yang

telah ditetapkan pada aset dengan nilai level risiko paling tinggi (*Medium/High*) dalam ICR. Kebijakan dan prosedur disini berfungsi sebagai panduan bagi PT PJB agar unit PT PJB Gresik dapat memenuhi kriteria ICR. Sedangkan instruksi kerja bertujuan untuk merincikan satu aktivitas tertentu yang ada dalam prosedur. Tahapan dalam penyusunan SOP dan Instruksi kerja dijelaskan pada Gambar 3.9.



Gambar 3.9. Tahapan pembuatan kebijakan dan prosedur

3.4 Tahap Akhir

Tahap terakhir yang di lakukan adalah menentukan hasil dari proses – proses yang telah dilaksanakan pada tahap pengembangan yang telah dilakukan sebelumnya dan akan menghasilkan keluaran sebagai berikut.

1. **Laporan Assesmen Resiko**

Laporan asessmen resiko adalah laporan yang memuat langkah pada tahap perencanaan SMKI dari langkah 3 sampai 5 yang memuat pendekatan penilaian resiko, identifikasi resiko, analisis dan evaluasi resiko, analisis dan evaluasi penanaganan risiko, menetapkan kontrol objektif dan kontrol.

2. Kebijakan

Kebijakan adalah pernyataan resmi dari PT PJB UP Gresik yang merefleksikan komitmen yang dijasikan sebagai landasan utama dan aktivitas utama dalam bagian dan fungsi PT PJB UP Gresik.

3. Prosedur

Standar Operasional Prosedur (SOP) adalah dokumen prosedur keamanan informasi yang dihasilkan pada perencanaan sistem manajemen keamanan informasi dan bertujuan sebagai pedoman untuk mengarahkan langkah kerja yang harus dilakukan oleh PT PJB UP Gresik.

4. Instruksi Kerja

Instruksi kerja memuat hasil rinci dari prosedur yang telah dibuat sehingga intruksi kerja merupakan dokumen kompleks yang lebih detail dari prosedur.

5. Rekam Kerja

Rekam kerja adalah dokumen terdokumentasi yang dilakukan untuk melaksanakan dan memudahkan jejak telusur dalam kegiatan sistem manajamen keamanan informasi.