BAB III

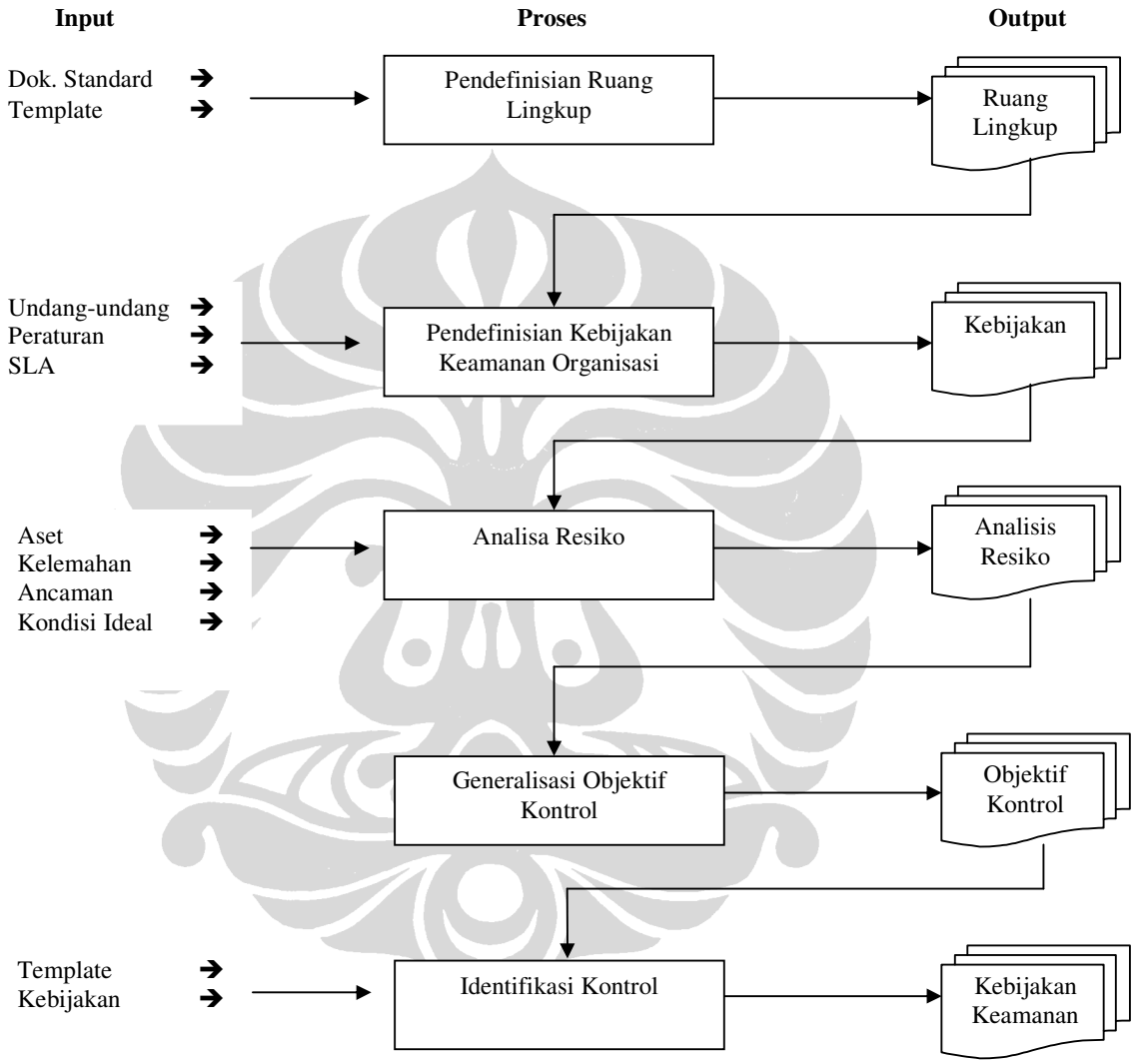
METODOLOGI PENELITIAN

3.1. RUANG LINGKUP PENELITIAN

Berhubung penelitian ini merupakan pengembangan kebijakan keamanan sistem informasi pada suatu organisasi atau perusahaan yang berbasiskan standard ISO/IEC seri 27000 maka cakupan metodologi penelitian yang digunakan adalah sebagai berikut:

- Pada tahap awal, suatu perusahaan / organisasi berusaha untuk mendefinisikan ruang lingkup dari kebijakan keamanan informasi yang akan dibuat. Tahapan ini menghasilkan dokumen ruang lingkup keamanan informasi yang ditawarkan. Dokumen tersebut menentukan unit bisnis, departemen, dan / atau sistem apa saja yang akan dicakup melalui penerapan kebijakan keamanan informasi.
- Tahapan berikutnya adalah pendefinisian kebijakan keamanan informasi yang sesuai dengan kondisi perusahaan. Adapun hasil dari proses pada tahapan ini adalah suatu dokumen kebijakan keamanan informasi.
- Tahapan berikutnya adalah menjalankan proses analisa resiko. Tahapan ini memerlukan sejumlah input yang berupa hasil identifikasi aset, ancaman-ancaman utama, resiko, dampak, dan kerentanan yang terdapat pada

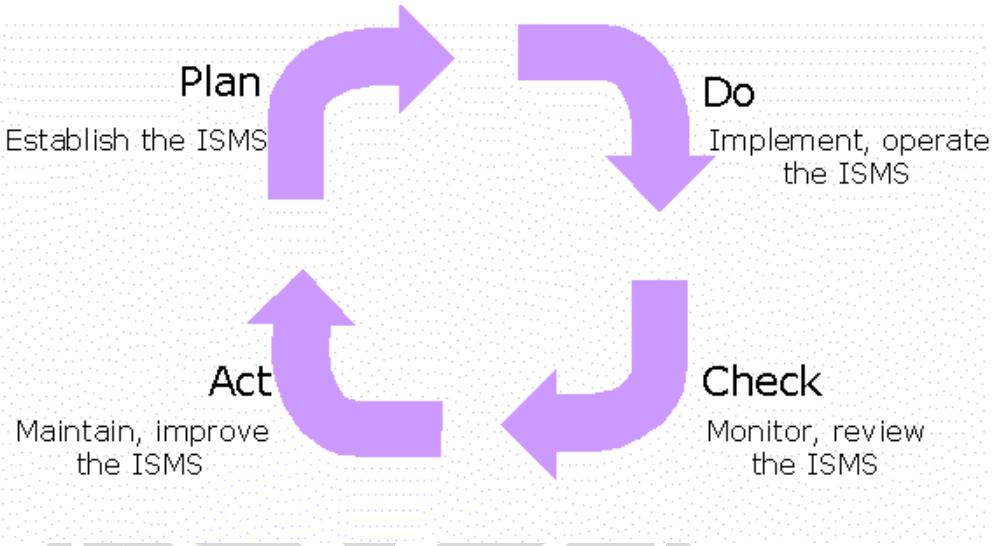
perusahaan. Sedangkan output yang dihasilkan melalui tahapan ini adalah dokumen atau rumusan tentang *risk assessment*.



Gambar 2 Metode Pengembangan Kebijakan Keamanan (www.27000.org)

- Setelah tahapan tersebut, tahapan selanjutnya adalah penentuan metode penanganan resiko yang berhasil teridentifikasi sebelumnya. Adapun hasil dari tahapan ini adalah pemilihan objektif dan kontrol yang akan diterapkan pada organisasi / perusahaan. Kontrol dan pedoman yang digunakan dapat berasal dari stadar ISO 17799 atau ISO 27002 maupun diluar standar tersebut.
- Tahapan berikutnya adalah proses identifikasi dan pemilihan objektif dan kontrol yang akan diterapkan pada organisasi / perusahaan. Kontrol dan pedoman yang digunakan dapat berasal dari stadar ISO 17799 atau ISO 27002 maupun diluar standar tersebut. Adapun hasil dari tahapan ini adalah keluarnya dokumen kebijakan keamanan yang dapat disetujui dan diterapkan pada organisasi / perusahaan.

Melalui model pengembangan kebijakan keamanan (sebagaimana tertuang pada Gambar 2), dapat dijelaskan bahwa fokus dari penelitian ini terbatas pada bingkai kerja sistem manajemen keamanan informasi (berupa area dalam garis putus-putus). Dengan kata lain, cakupan penelitian ini hanya sebatas fase *'Plan'* berdasarkan model PDCA (*Plan-Do-Check-Act*). Model ini dikembangkan oleh W. Edward Deming merupakan suatu model atau metodologi yang digunakan untuk menyempurnakan proses. Nama model ini merupakan akronim yang menjelaskan komponen dasar dari perbaikan proses. Gambar berikut merupakan visualisasi dari model PDCA.



Gambar 3 Model PDCA (www.Dartmouth.edu)

Adapun proses yang terdapat dalam metodologi ini adalah sebagai berikut.

- *Plan* (Perencanaan) merupakan tahapan dalam membangun proses dan objektif yang diperlukan sesuai dengan spesifikasi. Dalam konteks penelitian ini, tahapan perencanaan meliputi pembangunan bingkai kerja ISMS (*Information Security Management Systems*). Secara umum, sejumlah proses yang dijalankan pada tahapan ini meliputi (Osborne, 2006):
    - Pendefinisian ruang lingkup awal dari ISMS – dimana hal ini merupakan keputusan berbasisi bisnis dari suatu organisasi.
    - Pendefinisian kebijakan ISMS – dimana dalam proses ini kebijakan keamanan dan ISMS didokumentasikan.
    - Identifikasi Aset
    - Identifikasi Ancaman

- Melakukan *Risk Assessment* – atau umumnya dikenal dengan *business impact analysis* (berdasarkan standar BS 7799) merupakan proses yang meliputi pendaftaran aset serta memperkirakan akibat yang ditimbulkan terhadap bisnis suatu organisasi atau perusahaan (jika terjadi kerusakan atau kehilangan terhadap setiap aset tersebut). Dalam konteks standard ini, fokusnya lebih ditekankan pada konsep CIA.
- Pemilihan kontrol – dimana proses yang umumnya disebut dengan *risk treatment plan* ini berisi penyusunan daftar sejumlah kontrol yang digunakan dalam menangani atau mengantisipasi ancaman. Pada umumnya, kontrol-kontrol ini direferensikan standar yang relevan disamping kontrol-kontrol lainnya yang dapat ditambahkan untuk diterapkan dalam suatu organisasi.
- Menyusun *Statement of Applicability* (SoA)

- *Do* (Implementasi) merupakan tahapan implementasi. Proses pada tahapan ini umumnya meliputi:
  - Finalisasi dan *fine-tune* terhadap risk treatment plan yang telah dilakukan pada tahapan sebelumnya.
  - Penerapan risk treatmenr plan berrikut sejumlah kontrol yang relevan.

- *Check* (Pemeriksaan) merupakan tahapan pemantauan, review dan audit proses dan hasil objektif dan spesifikasi yang didefinisikan pada tahap awal. Sejumlah tugas yang dikerjakan pada tahapan ini meliputi:
    - Melakukan monitoring.
    - Menjalankan review secara berkala terhadap efektitas dan efisiensi dari ISMS yang telah diterapkan.
    - Memantau resiko yang dapat diterima
    - Mengadakan proses audit secara regular terhadap penerapan ISMS.
- *Act* (Aksi) merupakan tahapan aplikasi sejumlah aksi terhadap hasil untuk proses penyempurnaan yang diperlukan. Hal ini berarti review terhadap semua tahapan dan modifikasi proses untuk proses perbaikannya sebelum memulai implementasi selanjutnya. Beberapa hal yang dilakukan pada tahapan ini meliputi:
    - Implementasi perbaikan yang berhasil teridentifikasi berdasarkan temuan audit yang terdapat pada tahapan sebelumnya.
    - Mengambil langkah perbaikan yang sesuai.
    - Mengkomunikasikan hasil yang diperoleh kepada pihak yang berkepentingan.
    - Memastikan bahwa perbaikan yang telah dilakukan telah sesuai dengan objektif yang diharapkan.

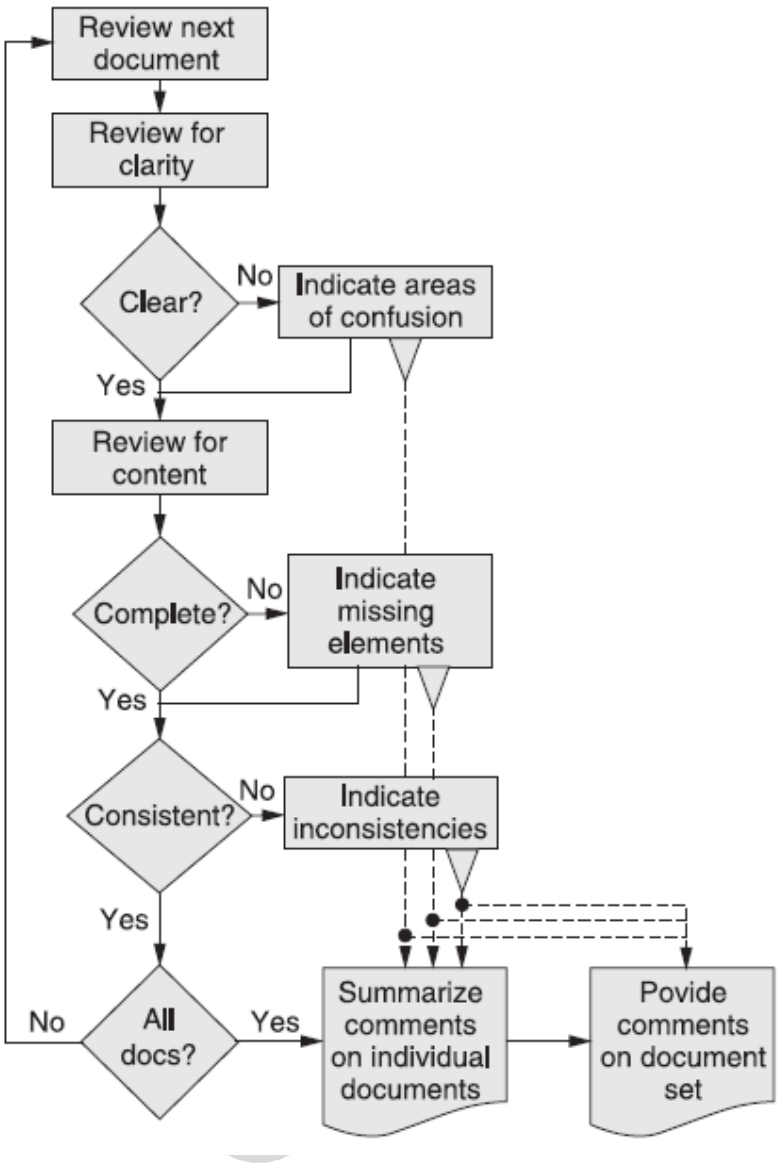
3.2. METODE PENGUMPULAN DATA

Dalam melakukan proses pengumpulan data dalam penelitian ini, penulis menggunakan metode RIIOT (Landoll, 2006). Metode ini bekerja dengan melakukan pemecahan terhadap proses pengumpulan data kedalam 5 pendekatan yang berbeda. Pendekatan yang dimaksud dalam metode ini adalah sebagai berikut.

- *Review* dokumen

  Proses *review* dokumen dalam pengumpulan data meliputi pengenalan terhadap dokumen mana saja yang perlu di-*request* serta bagaimana mereview dokumen tersebut dengan baik. Dokumen yang dimaksud dapat berupa dokumen konfigurasi, *rules*, arsitektur, *layout* serta elemen lainnya dari kontrol keamanan yang telah ada sebelumnya pada infrastruktur (IT khususnya) suatu organisasi.

  Dokumen relevan lainnya yang juga dapat direview meliputi dokumen kebijakan, prosedur, peta jaringan, penjadwalan backup, dan lain sebagainya. Adapun alur proses dalam review dokumen adalah sebagai berikut:



Gambar 4 Alur Proses dalam Review Dokumen (Landoll, 2006)

- Melakukan wawancara dengan *Key Porsonel*

  Proses ini ditujukan untuk menentukan kapabilitas personel dilapangan dalam menjalankan kewenangan yang diberikan (berdasarkan dokumen kebijakan atau dokumen relevan lainnya), implementasi terhadap kewenangan tersebut, dan obervasi terhadap tingkat

kepedulian yang mereka miliki terhadap kontrol keamanan yang ada saat ini.

- Memeriksa kontrol keamaan

  Proses ini bertujuan untuk memeriksa kontrol keamanan tertentu yang telah diimplementasi sebelumnya (seperti kontrol pengunjung melalui daftar pengunjung, file konfigurasi, detektor asap, respon penanganan terhadap suatu insiden). Kontrol-kontrol tersebut selanjutnya dapat dibandingkan dengan standar industri, daftar pengecekan terhadap tingkat kerentanan suatu sistem, dan lain sebagainya.

- Observasi terhadap perilaku para personel dilapangan

  Proses ini bertujuan untuk memberikan gambaran terhadap tingkat efektifitas dari kontrol keamanan yang sejauh ini telah diterapkan pada suatu organisasi / perusahaan.

- Pengujian terhadap kontrol keamanan

  Proses ini bertujuan untuk menguji kontrol keamanan tertentu seperti firewall, server, alarm, sensor gerak, dan lain sebagainya. Proses ini juga meliputi penggunaan pemindai tingkat kerapuhan terhadap kontrol keamanan logik, disamping pengujian terhadap kontrol keamanan fisik.