Bab I Pendahuluan

I.1 Latar Belakang

Teknologi Informasi (TI) adalah teknologi yang tidak hanya fokus pada teknologi komputer (perangkat keras dan perangkat lunak) yang akan digunakan untuk memproses dan menyimpan informasi, melainkan mencakup teknologi komunikasi untuk mengirim atau menyebarkan informasi (Martin, 1999). TI merupakan bidang pengelolaan teknologi dan mencakup berbagai bidang yang termasuk, tetapi tidak terbatas pada hal-hal seperti proses, perangkat lunak komputer, sistem informasi, perangkat keras komputer, Bahasa program, dan data konstruksi. Singkatnya, apa yang membuat data, informasi atau pengetahuan yang dirasakan dalam membuat format visual apapun, melalui setiap mekanisme distribusi multimedia dianggap bagian dari TI. Bagi perusahaan TI memiliki manfaat sebagai pendorong kemajuan bisnis dan memberikan manfaat yang baik bagi keberlangsungan perusahaan tersebut, dan pemanfaatannya sudah menjadi bagian yang penting dalam suatu perusahaan.

Dengan semakin berkembangnya peranan teknologi informasi dalam dunia bisnis, maka menuntut manajemen TI untuk menghasilkan Sistem Informasi yang layak dan mendukung kegiatan bisnis. Untuk itu, dituntut sebuah perubahan dalam bidang manajemen TI. Perubahan yang terjadi adalah dengan diterapkannya Perancangan Strategis Sistem Informasi untuk memenuhi tuntutan menghasilkan SI yang mendukung kegiatan bisnis suatu organisasi. Seiring dengan perkembangan zaman dan dunia bisnis, peningkatan Perencanaan Strategis Sistem Informasi menjadi tantangan serius bagi pihak manajemen TI.

Kemanan informasi dalam perkembangan IT merupakan salah satu aspek penting dari sebuah perusahaan. Kemanan informasi bertujuan untuk menjaga aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*). Sistem Manajemen Kemanan Informasi diperlukan karena ancaman terhadap aspek keamanan informasi semakin lama semakin meningkat. Sistem manajemen

keamanan informasi (SMKI) bukan merupakan suatu produk melainkan suatu proses untuk menentukan bagaimana mengelola, memonitor, dan memperbaiki informasi agar aman. Penerapan sistem manajemen keamanan informasi yang baik akan memberikan perlindungan terhadap proses bisnis organisasi agar dapat terhindar dari kemungkinan risiko yang akan terjadi. ISO/IEC 27001:2013 merupakan standar internasional yang dapat digunakan organisasi sebagai pedoman untuk menerapkan sistem manajemen keamanan informasi.

Dana Pensiun Telkom atau Dapen Telkom, merupakan salah satu yayasan yang didirikan oleh PT. Telkom yang bergerak di bidang Asuransi dan Keuangan Masa Depan. Maksud dibentuknya Yayasan Dana Pensiun Pegawai (YDPP) Telkom saat itu adalah untuk mengelola dan mengembangkan dana guna menjamin dan memelihara kesinambungan penghasilan bagi Pegawai PT. Telkom beserta keluarganya setelah memasuki masa purna tugas. Dana Pensiun Telkom dibentuk dengan tujuan untuk dapat mengelola dana yang didapat dari iuran pendiri, iuran peserta, dan lain-lain serta untuk menyelenggarakan dan menjalankan program Manfaat Pensiun bagi karyawan serta para pensiunannya.

Pada Dapen Telkom terdapat bagian SISFO yang memiliki peran untuk pemenuhan kebutuhan akan informasi dengan pengembangan dan pelayanan TI untuk pengolahan data. Namun berdasarkan observasi didapatkan bahwa belum adanya pedoman yang berhubungan dengan proses pengamanan informasi, serta kurangnya pemahaman tentang risiko kehilangan informasi dan pengendalian terhadap informasi. Dan juga Dapen Telkom masih mengikuti POJK (Peraturan Jasa Keuangan) yang diatur oleh badan OJK negara, sehingga Dapen Telkom belum memiliki dan belum menerapkan suatu standar internasional yang berkaitan dengan keamanan informasi pada internal Dapen Telkom sendiri.

Dari hasil observasi dan wawancara Dapen Telkom belum pernah mengalami serangan yang cukup merugikan perusahaan, tetapi untuk manajemen aset yang ada pada Dapen Telkom belum tertata dengan baik, seperti sistem kabel yang masih berantakan dan belum adanya kontrol akses yang sesuai dengan standar untuk aset

yang penting. Oleh karena itu dilakukan proses perancangan sistem manajemen keamanan informasi sebagai langkah awal untuk mengamankan informasi dengan memberikan gambaran tentang risiko yang terjadi, serta dampak pengendalian terhadap risiko keamanan informasi. Mengingat pentingnya informasi dan adanya kemungkinan risiko gangguan, Dapen Telkom perlu melakukan kegiatan tata kelola keamanan informasi dilingkungkannya. Salah satu standar yang dapat digunakan untuk menganalisa tingkat keamanan informasi pada sebuah organisasi adalah standar ISO/IEC 27001:2013 sesuai dengan insiden yang banyak terjadi. Pengukuran tingkat keamanan informasi diperlukan untuk menganalisa sejauh mana organisasi telah mengamankan informasi dilingkungkannya. Dari analisa tingkat keamanan, sehingga dapat melakukan evaluasi dan perancangan ataupun pembaharuan sistem manajemen keamanan informasi di suatu organisasi.

Tahapan penting dalam proses perancangan sistem keamanan informasi meliputi tahap penentuan ruang lingkup, tahap analisis risiko, dan tahap penentuan obyektif kontrol dan kontrol keamanan yang sesuai dengan standar ISO/IEC 27001:2013. Standar ISO/IEC 27001:2013

Untuk menentukan obyektif kontrol dan kontrol keamanan yang dibutuhkan, penulis melakukan analisis risiko terhadap seluruh aset yang ada pada Dapen Telkom. Dari hasil analisis risiko tersebut akan didapatkan beberapa aset yang memiliki nilai risiko yang tinggi dan membutuhkan sebuah rekomendasi berupa teknis dan non-teknis. Rekomendasi non-teknis berupa obyektif kontrol dan kontrol keamanan yang dapat meminimalisir tingkat risiko aset tersebut.

Setelah didapat obyektif kontrol dan kontrol keamanan, maka obyektif kontrol dan kontrol keamanan tersebut akan diukur dan ditentukan tingkat kedewasaannya. Tingkat kedewasaannya tersebut akan digunakan untuk mengukur sejauh mana Bagian IT Dapen Telkom mampu menerapkan sistem manajemen keamanan informasi yang telah dirancang. Selain itu dengan adanya nilai tingkat kedewasaan dapat ditentukan rekomendasi untuk meningkatkan keamanan informasi pada Bagian SISFO Dapen Telkom. Metode pengukuran tingkat kedewasaan yang akan

digunakan yaitu *System Security Engineering Capability Maturity Model (SSE-CMM)*.

I.2 Perumusan Masalah

Perumusan permasalahan yang akan dibahas dalam penelitian ini adalah sebagai berikut :

1. Bagaimana *maturity level* dan *gap analysis* pada bagian Sistem Informasi Dapen Telkom dengan standar ISO/IEC 27001:2013 pada fase *Plan*?
2. Bagaimana perancangan sistem keamanan informasi berbasis *risk management* menggunakan ISO/IEC 27001:2013 pada fase *Plan* di Bagian Sistem Informasi Dapen Telkom?

I.3 Tujuan Penelitian

Penelitian ini memiliki beberapa tujuan untuk menjawab rumusan masalah diatas, yaitu sebagai berikut :

1. Mengetahui *maturity level* dan *gap* pada kebijakan keamanan bagian Sistem Informasi Dapen Telkom berdasarkan ISO/IEC 27001:2013.
2. Membuat sebuah perancangan sistem keamanan informasi berbasis *risk management* dengan menggunakan ISO/IEC 27001:2013 yang sesuai dengan keadaan bagian Sistem Informasi Dapen Telkom.

I.4 Manfaat Penelitian

Manfaat yang dapat diperoleh dari penelitian ini adalah :

- a. DAPEN TELKOM dapat melakukan evaluasi setelah melihat hasil dari penelitian ini;
- b. Memberikan pedoman bagi DAPEN TELKOM dalam mengambil keputusan untuk mencapai tujuan bisnisnya;
- c. Membantu DAPEN TELKOM dalam meminimilasi dampak risiko TI yang mungkin terjadi melalui rekomendasi perancangan manajemen risiko TI yang diberikan.;

- d. Sebagai gambaran tentang kebijakan manajemen keamanan informasi bagi Dapen Telkom;
- e. Memberikan gambaran kondisi penerapan kebijakan informasi bagi DAPEN TELKOM.

I.5 Batasan Masalah

Adapun batasan – batasan masalah dalam penelitian ini untuk menghindari pembahasan yang menyimpang dalam penelitian ini :

1. Lingkup yang menjadi objek penelitian adalah manajemen aset Dapen Telkom;
2. Penelitian ini hanya mengambil data dari *Annex C* dan *Annex D* pada standar ISO/IEC 27005:2008 sebagai referensi dari daftar tabel ancaman dan daftar tabel kelemahan;
3. Penelitian ini tidak melakukan analisis di fase *Do*, *Check*, dan *Act* pada fase PDCA;
4. Tidak adanya pembangunan aplikasi dalam mendukung proses organisasi.

I.6 Sistematika Penulisan

Penelitian ini diuraikan dengan sistematika penulisan sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini berisi uraian mengenai latar belakang penelitian, perumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini berisi studi literatur yang relevan dengan permasalahan yang diteliti.

BAB III METODE PENELITIAN

Pada bab ini akan dijelaskan langkah-langkah penelitian secara rinci, meliputi penggambaran rinci dari metode konseptual dan sistematika pemecahan masalah. Dimana metode konseptual merupakan gambaran alur, sedangkan untuk sistematika pemecahan masalah, analisis, perancangan, implementasi serta kesimpulan dan saran.

BAB IV PENGUMPULAN, PENGOLAHAN DAN ANALISIS DATA

Bab ini berisi pengumpulan serta pengolahan data digunakan sebagai analisis dalam penilaian terhadap risiko dan juga analisis terhadap kesenjangan.

BAB V PERANCANGAN

Pada bab ini akan dilakukan proses perancangan terhadap rekomendasi berdasarkan hasil analisis kesenjangan yang diperoleh.

BAB VI PENUTUP

Bab ini berisi kesimpulan dan saran untuk penelitian yang dilakukan di Dapen Telkom.