1. Pendahuluan

1.1 Latar Belakang

Informasi merupakan aset yang sangat bernilai bagi organisasi. Sebagaimana aset organisasi yang lain, maka informasi harus dilindungi. Keamanan informasi bertujuan untuk menjaga aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*). Sistem Manajemen keamanan informasi diperlukan karena ancaman terhadap aspek keamanan informasi semakin lama semakin meningkat[3]. Sistem manajemen keamanan informasi (SMKI) bukan merupakan suatu produk melainkan suatu proses untuk menentukan bagaimana mengelola, memonitor dan memperbaiki informasi agar menjadi aman. Penerapan sistem manajemen keamanan informasi yang baik akan memberikan perlindungan terhadap proses bisnis organisasi agar dapat terhindar dari kemungkinan resiko yang terjadi. ISO 27001 merupakan standar internasional yang dapat digunakan organisasi sebagai pedoman untuk menerapkan sistem manajemen keamanan informasi. ISO 27001 menyediakan model yang lengkap terkait dengan bagaimana membangun, menerapkan, operasional, memonitor, mengkaji ulang, memelihara dan mengembangkan sistem manajemen keamanan informasi[9].

Di IT Telkom terdapat UPT sistem informasi (sisfo) yang memiliki peran untuk pemenuhan kebutuhan akan informasi dengan pengembangan dan pelayanan TI untuk pengolahan data[10]. Namun berdasarkan observasi awal didapat bahwa belum adanya pedoman yang berhubungan dengan proses pengamanan informasi, kurangnya pemahaman tentang resiko kehilangan informasi dan pengendalian terhadap informasi. Oleh karena itu dilakukan proses perancangan sistem manajemen keamanan informasi sebagai langkah awal untuk mengamankan informasi dengan memberikan gambaran tentang resiko yang terjadi, dampak serta pengendalian terhadap resiko keamanan informasi. Tahapan penting dalam proses perancangan sistem manajemen keamanan informasi meliputi tahap penentuan ruang lingkup, tahap analisis resiko dan penentuan obyektif kontrol dan kontrol keamanan. Untuk mempermudah melakukan analisis resiko, akan dibangun perangkat lunak yang dapat memfasilitasi tahap analisis resiko.

Setelah didapat objektif kontrol dan kontrol keamanan, maka objektif kontrol dan kontrol keamanan tersebut akan diukur dan ditentukan tingkat kedewasaannya. Tingkat kedewasaan tersebut akan digunakan untuk mengukur sejauh mana UPT Sisfo mampu menerapkan sistem manajemen keamanan informasi yang telah dirancang. Selain itu dengan adanya nilai tingkat kedewasaan dapat ditentukan rekomendasi untuk meningkatkan keamanan informasi pada UPT Sisfo. Metode pengukuran tingkat kedewasaan yang akan digunakan yaitu *System Security Engineering Capability Maturity Model* (SSE CMM)

1.2 Perumusan Masalah

Masalah yang akan dikaji dalam tugas akhir ini adalah:

1. Bagaimana melakukan analisis resiko terhadap aset informasi sehingga dihasilkan daftar resiko yang mungkin terjadi.
2. Bagaimana membangun perangkat lunak yang dapat mempermudah proses analisis resiko.
3. Bagaimana menentukan objektif kontrol dan kontrol berdasarkan ISO 27001 untuk mengurangi resiko pada aset informasi yang sudah teridentifikasi.
4. Bagaimana mengukur tingkat kedewasaan sistem manajemen keamanan informasi menggunakan SSE-CMM.

1.3 Tujuan

Tujuan yang ingin dicapai dalam tugas akhir ini adalah :

1. Menghasilkan daftar resiko terhadap informasi yang mungkin terjadi di UPT Sistem Informasi berdasarkan hasil analisis resiko.
2. Menghasilkan perangkat lunak yang dapat mempermudah dalam proses analisis resiko.
3. Menganalisis resiko berdasarkan aset yang sudah teridentifikasi untuk kemudian menganalisis objektif kontrol dan kontrol keamanan yang sesuai.
4. Menganalisis nilai tingkat kedewasaan sistem manajemen keamanan informasi menggunakan SSE-CMM untuk kemudian dihasilkan usulan rekomendasi peningkatan program keamanan informasi.

1.4 Batasan Masalah

Adapun batasan masalah pada Tugas akhir ini adalah:

1. Proses perancangan sistem manajemen keamanan informasi berdasarkan kondisi UPT Sistem Informasi IT Telkom pada tahun 2011.
2. Proses analisis resiko berdasarkan aset yang berkaitan dengan akademik, karena Road map UPT Sisfo tahun 2011 fokus pada pengembangan sistem akademik.

1.5 Metodologi Penyelesaian Masalah

Dalam penyusunan tugas akhir ini untuk dapat menyelesaikan masalah maka akan dilakukan metodologi sebagai berikut:

a. Identifikasi Masalah

Tahap ini merupakan tahap awal dalam memulai suatu penelitian. Pada tahap ini, penulis melakukan identifikasi terhadap masalah yang akan dibahas. Permasalahan yang akan diangkat dalam penelitian ini adalah keadaan keamanan informasi yang ada di UPT sistem Informasi, serta

bagaimana merancang sebuah sistem keamanan manajemen informasi yang dapat mengurangi resiko terhadap keamanan informasi.

b. Studi Literatur

Studi literatur dilakukan dengan cara mempelajari literatur-literatur baik yang berupa buku (*textbook*), jurnal, dan artikel ilmiah, maupun website yang berhubungan dengan ISO 27001, keamanan informasi, dan proses audit.

c. Pengumpulan data

Dalam tahap ini akan dilakukan pengkajian terhadap resiko keamanan informasi serta ISO 27001 sehingga dihasilkan variabel – variabel apa saja yang dapat digunakan sebagai perancangan keamanan informasi. Serta mencari dan mengumpulkan data yang dapat digunakan untuk proses perancangan terhadap SMKI.

d. Perancangan sistem

Dalam membangun sistem akan digunakan model perancangan *waterfall*.Pertama akan dilakukan analisa kebutuhan sistem, setelah itu akan dilakukan perancangan aplikasi dengan bantual *tools* visio. Kemudian rancangan tersebut akan diimplementasikan ke dalam bahasa yang dikenali computer atau *coding*. Setelah tahapan *coding* akan dilakukan *testing* sebelum akhirnya aplikasi diterapkan.

e. Pengujian dan analisis

Pengujian akan dilakuan terhadap perangkat lunak yang dibangun dan pengujian terhadap hasil perancangan SMKI. Metode pengujian terhadap aplikasi yang digunakan yaitu *black box testing*, dimana focus pengujian terhadap perangkat lunak pada fungsionalitas dan spesifikasi perangkat lunak. Dalam proses analisis akan dilakukan analisa resiko yang terdiri dari identifikasi aset sampai penentuan kontrol keamanan. Dari hasil analisis resiko akan diketahui kemungkinan resiko keamanan informasi yang terjadi di UPT Sisfo.

f. Penyusunan Laporan

Pada tahapan ini dilakukan penyusunan laporan mengikuti kaidah penulisan yang benar dan sesuai dengan ketentun dan sistematika yang ditentukan oleh institusi.