

BAB I PENDAHULUAN

1.1 Latar Belakang

Informasi merupakan salah satu aset yang sangat penting baik untuk perusahaan, pemerintahan, ataupun organisasi. Dengan perkembangan teknologi informasi yang sangat pesat, kemungkinan terjadinya gangguan terhadap keamanan informasi semakin meningkat. Untuk itu, perusahaan harus dapat menerapkan kebijakan yang tepat untuk melindungi aset informasi yang dimiliki. Salah satu kebijakan yang dapat diambil oleh perusahaan untuk mengatasi masalah gangguan terhadap keamanan informasi adalah dengan menerapkan Sistem Manajemen Keamanan Informasi (SMKI).

Salah satu model pendukung keamanan informasi adalah ISO 27001:2005 dari sekian banyak model yang ada, dimana masing-masing memfokuskan diri pada manajemen keamanan informasi yang berbeda-beda. ISO 27001:2005 itu sendiri merupakan standar model untuk penetapan, penerapan, pengoperasian, pemantauan, pengkajian, pemeliharaan, dan perbaikan Sistem Manajemen Keamanan Informasi (SMKI). Desain dan penerapan SMKI dari suatu organisasi dipengaruhi oleh kebutuhan dan sasaran organisasi. Standar ini dapat digunakan untuk menilai kesesuaian oleh pihak terkait baik internal maupun eksternal.

PT.KAI merupakan perusahaan yang bergerak dalam bidang pelayanan terhadap publik, dimana PT.KAI memiliki proses bisnis yang kompleks sehingga peran TI sangat dibutuhkan dalam mendukung proses bisnis tersebut. Untuk menjamin keamanan aset ataupun TI pada PT.KAI dibutuhkan suatu model dimana ISO 27001:2005 dapat menjadi panduan dalam mengatasi keamanan informasi, khususnya pada Unit TI PT.KAI. Hal ini karena pengguna layanan kereta api sangat banyak sehingga manajemen keamanan informasi dinilai sangat penting pada Unit IT di PT.KAI. Untuk memberikan arahan manajemen dan dukungan keamanan informasi diperlukan adanya dokumen keamanan informasi. Keamanan informasi dibutuhkan oleh unit TI PT.KAI baik didalam maupun diluar organisasi.

PT.KAI juga harus dapat memelihara perlindungan yang sesuai terhadap aset organisasi serta memastikan bahwa informasi menerima tingkat perlindungan yang tepat. Selain itu, PT. KAI juga harus dapat memastikan bahwa pegawai, pengguna sistem, serta pihak-pihak lain yang berkepentingan di dalam pengelolaan atau perbaikan sistem memahami tanggung jawab sesuai dengan perannya yang bertujuan untuk mengurangi resiko pencurian, kecurangan atau penyalahgunaan fasilitas, serta peduli terhadap ancaman dan masalah di dalam keamanan informasi.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dijelaskan pada 1.1, maka rumusan masalah yang akan dikaji dalam Tugas Akhir adalah sebagai berikut:

1. Apakah penerapan dokumentasi kebijakan keamanan informasi sudah dikaji yang mencakup keamanan informasi pada bagian unit TI di PT.KAI?
2. Apakah Unit TI di PT.KAI sudah mengelola dengan baik tentang keamanan informasi di dalam maupun diluar organisasi?
3. Apakah Unit TI di PT.KAI sudah mengelola aset dengan baik di dalam organisasi?
4. Apakah Unit TI di PT.KAI sudah mengelola dengan baik tentang keamanan sumber daya manusia di dalam organisasi?

1.3 Tujuan Pembahasan

Tujuan dari pembahasan dalam Tugas Akhir ini berdasarkan rumusan masalah pada poin 1.2 adalah sebagai berikut:

1. Memahami serta mengetahui proses-proses dalam mengelola dokumentasi kebijakan keamanan informasi, serta dapat memastikan kesesuaian, kecakupan, dan keefektifan yang berkelanjutan pada bagian Unit TI di PT.KAI.
2. Memahami dalam pengelolaan keamanan informasi di dalam maupun diluar organisasi pada bagian Unit TI di PT.KAI.

3. Memahami dalam pemeliharaan aset serta memberikan perlindungan yang tepat terhadap aset di dalam organisasi pada bagian Unit TI di PT.KAI.
4. Memahami pengelolaan sumberdaya manusia sebelum dipekerjakan, selama bekerja maupun yang sudah diberhentikan atau perubahan pekerjaan di dalam organisasi pada bagian Unit TI di PT.KAI.

1.4 Ruang Lingkup Kajian

Ruang lingkup kajian penelitian dilakukan pada Unit TI di PT.KAI, standar yang digunakan dalam tugas akhir ini adalah ISO 27001:2005 yang mendukung perlindungan memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh Unit TI PT.KAI untuk mengevaluasi, mengimplementasikan, dan memelihara keamanan informasi di perusahaan, yang menggunakan 4 kontrol di antaranya adalah:

1. Kebijakan keamanan

Sasaran dalam proses ini adalah untuk memberikan arahan manajemen dan dukungan untuk keamanan informasi menurut persyaratan bisnis dan hukum serta regulasi yang relevan.

2. Organisasi keamanan informasi

Sasaran dalam proses ini adalah untuk mengelola keamanan informasi didalam maupun diluar organisasi.

3. Pengelolaan aset.

Sasaran dalam proses ini adalah untuk mencapai dan memelihara perlindungan yang sesuai terhadap aset organisasi serta memastikan bahwa informasi menerima tingkat perlindungan yang tepat.

4. Keamanan sumber daya manusia

Sasaran dalam proses ini adalah untuk memastikan bahwa pegawai serta pengguna sistem beserta pihak-pihak lain yang berkepentingan di dalam pengelolaan atau perbaikan sistem memahami tanggung jawab sesuai dengan perannya yang bertujuan untuk mengurangi resiko pencurian, kecurangan atau penyalahgunaan fasilitas, serta

peduli terhadap ancaman dan masalah di dalam keamanan informasi.

1.5 Sumber Data

Metode pengumpulan data pada PT.KAI yang dilakukan dalam menyelesaikan tugas akhir ini dibagi menjadi beberapa bagian, yaitu :

1. Wawancara

Metode ini dilakukan dengan cara menanyakan langsung kepada orang yang mempunyai keterkaitan dengan pembahasan penelitian, biasanya dilakukan dengan menyiapkan daftar pertanyaan terlebih dahulu yang kemudian ditanyakan kepada orang yang bersangkutan.

2. Observasi

Merupakan metode penelitian yang langsung turun melakukan interaksi dengan mengamati beberapa proses kerja yang ada.

3. Kuesioner

Metode ini dilakukan dengan cara memberikan sejumlah pertanyaan secara tertulis kepada sejumlah responden yang berguna untuk mendapatkan kesimpulan untuk dapat dianalisis menjadi informasi.

1.6 Sistematika Penyajian

Secara umum, sistem penyajian diuraikan sebagai berikut :

Bab I Pendahuluan

Membahas mengenai Latar Belakang, Rumusan Masalah, Tujuan dan Manfaat Penelitian, Ruang Lingkup, serta Sistematika Penyajian.

Bab II Kajian Teori

Membahas mengenai Kajian Teori yang menjadi acuan dalam menganalisis manajemen keamanan informasi.

Bab III Analisis dan Evaluasi

Bab ini membahas mengenai profil perusahaan serta bagian TI, *Gap Analisis* Manajemen Keamanan Informasi pada bagian Unit TI di PT.KAI menggunakan standar ISO 27001:2005.

Bab IV Simpulan dan Saran

Bab ini membahas mengenai kesimpulan dan saran pengembangan berdasarkan hasil *Gap Analisis* SMKI pada BAB III.