BAB IV SIMPULAN DAN SARAN

4.1 Simpulan

Simpulan yang dapat diambil dari hasil analisis berdasarkan proses kebijakan keamanan, organisasi keamanan informasi, pengelolaan aset dan keamanan sumber daya manusia yang ada pada analisis BAB III adalah sebagai berikut:

1. Unit TI pada PT.KAI telah memahami serta mengetahui proses-proses dalam mengelola dokumentasi kebijakan keamanan informasi, namun dalam mengkaji keamanan informasi belum secara rutin ditetapkan masih secara *ad hoc* atau jika dibutuhkan saja baru dikaji, dokumen kebijakan keamanan informasi sudah dapat memastikan kesesuaian, kecakupan dan keefektifan tetapi belum secara efektif berjalan pada bagian Unit TI di PT.KAI.
2. Unit TI pada PT.KAI telah memahami dalam pengelolaan keamanan informasi di dalam maupun diluar organisasi, namun di dalam organisasi masih belum secara efektif dijalankan sesuai dengan aturan yang ada.
3. Unit TI pada PT.KAI telah memahami dalam pemeliharaan aset serta memberikan perlindungan yang tepat terhadap aset di dalam organisasi. Namun penerapannya masih belum efektif yang diakibatkan kurangnya kepedulian terhadap aset organisasi.
4. Unit TI pada PT.KAI telah memahami pengelolaan sumberdaya manusia sebelum dipekerjakan, selama bekerja maupun yang sudah diberhentikan atau perubahan pekerjaan di dalam organisasi. Namun belum seluruhnya menyangkut tentang keamanan informasi.

4.2 Saran

Penerapan SMKI (Sistem Manajemen Keamanan Informasi) di dalam PT.KAI idealnya dapat mengimplementasi persyaratan standarisasi sesuai dengan ketentuan yang berlaku pada SMKI ISO 27001:2005. Untuk itu prinsip keamanan harus tetap dipenuhi yang dimana aspek persyaratan keamanan yaitu *confidentiality*, *integrity* dan *availability*. Untuk mencapai aspek tersebut maka perlu diperhatikan beberapa hal yang penting yaitu adanya kontrol dan proteksi, monitoring dan auditing, serta pemahaman tentang dampak, ancaman dan vulnerabilitas pada PT.KAI. Penekanan dan penyesuaian terhadap masing-masing kontrol pada pokok masalah yang diambil yaitu kebijakan keamanan, organisasi keamanan informasi, pengelolaan aset dan keamanan sumber daya manusia harus terpenuhi berikut ini adalah saran atau rekomendasi dari hasil analisis pada BAB III, referensi penulisan dokumen ISO 27001:2005 dapat dilihat pada lampiran R untuk *Policy*, lampiran S untuk *Procedure*, lampiran T untuk *Work Instruction*, lampiran U untuk *Record*.

1. Pembuatan dokumen *policy* SMKI, dokumen ini bersifat strategis yang memuat komitmen yang dituangkan dalam bentuk kebijakan, standar, sasaran dan rencana terkait pengembangan (*development*), penerapan (*implementation*) dan peningkatan (*improvement*) sistem manajemen keamanan informasi. berikut ini adalah dokumen sesuai dengan proses atau kontrol yang diambil:
 - A. *Security Policy (Doc 5.1)*
 - B. *Internet Acceptable Usage Policy (Doc 7.2)*
2. Pembuatan prosedur dan panduan yang dikembangkan secara internal oleh PT.KAI sebagai penyelenggara pelayanan publik dan memuat cara menerapkan kebijakan yang telah ditetapkan serta menjelaskan penanggung jawab kegiatan. Prosedur-prosedur dalam dokumen ini meliputi antara lain:
 - A. *Management Review Of The Information Security Policy (Doc 5.2)*

- B. *Information Security Committee (Doc 6.1)*
 - C. *Information Security Co-Ordination (Doc 6.2)*
 - D. *Authorizing New Information Processing Facilities (Doc 6.4)*
 - E. *Confidentiality Agreements (Doc 6.5)*
 - F. *Internal Independent Review Procedure (Doc 6.7)*
 - G. *External Parties (6.8)*
 - H. *Inventory And Ownership Of Assets (7.1)*
 - I. *Rules For Use Of E-Mail (7.3)*
 - J. *Information Security Classification Guidelines (7.6)*
 - K. *Telecommunications Procedure (Doc 7.11)*
 - L. *Personnel Screening Procedure (Doc 8.1)*
3. Pembuatan dokumen petunjuk teknis, instruksi kerja dan formulir yang digunakan untuk mendukung pelaksanaan prosedur tertentu sampai ke tingkatan teknis.
 4. Menyesuaikan sasaran pengendalian dan pengendaliannya, dalam proses ini yang dimaksud adalah Kebijakan Keamanan, Organisasi Keamanan Informasi, Pengelolaan Aset dan Keamanan Sumber Daya Manusia.
 - A. 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.
 - B. Organisasi keamanan informasi

Sasaran dalam proses ini adalah untuk mengelola keamanan informasi didalam maupun diluar organisasi.
 - C. 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.
 - D. 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 kepedulian terhadap ancaman dan masalah di dalam keamanan informasi.