# BAB 4. SIMPULAN DAN SARAN

## 4.1 Simpulan

Simpulan yang dapat diambil dari hasil analisis berdasarkan kontrol area yang diambil dari ISO 27001:2005 yaitu kebijakan keamanan, organisasi keamanan informasi, pengelolaan aset dan keamanan sumber daya manusia yang ada pada analisis BAB III adalah sebagai berikut:

1. Divisi TI pada PT. Pos Indonesia telah memahami proses-proses dalam mengelola dokumentasi kebijakan keamanan informasi, namun belum dikaji secara utuh dalam satu dokumentasi dan belum adanya pengkajian secara regular dalam interval waktu yang terencana, pengkajian dilakukan masih secara *ad-hoc* atau pada waktu yang dibutuhkan saja. Dokumentasi kebijakan keamanan sudah disetujui oleh dewan direksi dan dapat memastikan kesesuaian, kecakupan, dan keefektifan tetapi belum secara efektif berjalan pada bagian divisi IT pada PT.Pos Indonesia. Hal tersebut sesuai dengan visi dan misi perusahaan untuk menyediakan layanan yang handal dan terpercaya kepada pelanggan dan seluruh pemagku kepentingan. Dengan hasil analisis diatas dapat disimpulkan bahwa *GAP* kesesuaian antara proses pada PT. Pos Indonesia dan proses dalam ISO 27001:2005 menyangkut Kebijakan Keamanan cukup kecil.
2. Divisi TI pada PT. Pos Indonesia telah memahami pengelolaan keamanan informasi baik di dalam maupun diluar organisasi, namun masih kurangnya perhatian terhadap identifikasi resiko terhadap perjanjian kerahasiaan dengan pihak luar. Hal tersebut sesuai dengan visi dan misi perusahaan untuk menyediakan layanan yang handal dan terpercaya kepada pelanggan dan seluruh pemagku kepentingan. Dengan hasil analisis diatas dapat disimpulkan bahwa *GAP* kesesuaian antara proses pada PT. Pos Indonesia dan proses dalam ISO 27001:2005 menyangkut Organisasi Keamanan Informasi cukup kecil.

3. Divisi TI pada PT. Pos Indonesia telah memahami pengelolaan dan pemeliharaan aset serta memberikan perlindungan yang tepat terhadap aset di dalam organisasi, namun penerapannya masih kurang efektif karena belum adanya penilaian terhadap aset-aset organisasi. Hal tersebut sesuai dengan visi dan misi perusahaan untuk menyediakan layanan yang handal dan terpercaya kepada pelanggan dan seluruh pemagku kepentingan. Dengan hasil analisis diatas dapat disimpulkan bahwa *GAP* kesesuaian antara proses pada PT. Pos Indonesia dan proses dalam ISO 27001:2005 menyangkut Pengelolaan Aset Informasi sangat kecil sehingga perbaikan atau perubahan pada proses ini bisa dilakukan paling akhir.
4. Divisi TI pada PT. Pos Indonesia telah memahami pengelolaan sumber daya manusia baik sebelum dipekerjakan, selama bekerja maupun telah berakhir atau terjadi perubahan pekerjaan di dalam organisasi, namun kurang efektif karena kurangnya kepedulian terhadap keamanan informasi. Hal tersebut sesuai dengan visi dan misi perusahaan untuk menyediakan layanan yang handal dan terpercaya kepada pelanggan dan seluruh pemagku kepentingan. Dengan hasil analisis diatas dapat disimpulkan bahwa *GAP* kesesuaian antara proses pada PT. Pos Indonesia dan proses dalam ISO 27001:2005 menyangkut Keamanan Sumber Daya Manusia cukup besar sehingga kepentingan untuk melakukan perbaikan atau perubahan perlu dilakukan terlebih dahulu pada proses ini.

## 4.2 Saran

Penerapan SMKI (Sistem Manajemen Keamanan Informasi) pada PT. Pos Indonesia dapat mengacu pada persyaratan standarisasi sesuai dengan ketentuan pada SMKI ISO 27001:2005 sebagai implementasinya. Untuk itu aspek keamanan harus memenuhi kriteria CIA (*confidentially, integrity, availability*). Untuk mencapai aspek tersebut maka perlu diperhatikan beberapa hal yang penting yaitu adanya kontrol, *monitoring*, *auditing*, dan

pemahaman tentang dampak, ancaman dan vulnerabilitas pada PT. Pos Indonesia. Kontrol pada pada pokok masalah yang diambil adalah kebijakan keamanan, organisasi keamanan informasi, pengelolaan aset dan keamanan sumber daya manusia. Berikut ini adalah saran dari hasil analisis yang dilakukan pada BAB 3. Referensi penulisan dokumen ISO 27001:2005 dapat dilihat pada lampiran U untuk *Policy*, lampiran V untuk *Procedure*, lampiran W untuk *Work Instruction*, dan lampiran X untuk *Record Schedule*.

1. Pembuatan dokumen SMKI 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 yang sesuai dengan kontrol yang diambil:
    A. *Security Policy (Doc 5.1)*
    B. *Internet Acceptable Usage Policy (Doc 7.2)*
2. Pembuatan prosedur dan panduan ini dikembangkan secara internal oleh PT. Pos Indonesia sebagai penyelenggara publik dan memuat cara menerapkan kebijakan yang telah ditetapkan serta menjelaskan penanggung jawab kegiatan. Dokumen ini bersifat operasional. Berikut ini adalah dokumen yang sesuai dengan kontrol yang diambil :
        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 (Doc 6.8)*
        H. *Inventory And Ownership Of Assets (Doc 7.1)*
        I. *Rules For Use Of E-Mail (Doc 7.3)*

J. *Information Security Classification Guideliness (Doc 7.6)*
K. *Telecommunications Procedure (Doc 7.11)*
L. *Personel 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. Dokumen *Record Schedule* berisi bukti objektif yang menunjukan seberapa baik kegiatan yang dilakukan atau apa hasil benar-benar tercapai.