BAB 5

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan penelitian keamanan informasi yang dilakukan pada departemen TI dari PT XYZ menggunakan *framework* COBIT 5, maka dapat ditarik kesimpulan sebagai berikut.

1. Kedua *domain* yang menjadi fokus penelitian tidak ada yang mencapai tingkat kapabilitas yang diharapkan departemen TI dengan APO13 mencapai *level* 2 sedangkan DSS05 hanya mencapai *level* 1. Aktivitas-aktivitas dalam *domain* yang dipilih sudah sebagian besar dilakukan perusahaan sehingga rekomendasi bisa dibuat agar *level* target yang diharapkan dapat tercapai.
2. Ditemukan adanya hubungan antara sebagian dari aspek pendekatan atau budaya keamanan informasi perusahaan dengan sebagian hasil pengisian maupun perhitungan kuesioner pada kedua *domain* yang menjadi fokus penelitian, terutama pada APO13.02 (rencana penanggulangan resiko keamanan informasi) dan DSS05.05 (pengelolaan akses fisik ke aset TI). Ini terlihat dari kurang berkembangnya program *training* pada aspek keamanan informasi perusahaan dan kurang diperhatikannya faktor infrastruktur dan lingkungan kerja, serta proses identifikasi sumber daya dan informasi dalam pengelolaan layanan keamanan yang baik secara langsung atau tidak langsung dipengaruhi oleh budaya keamanan informasi perusahaan yang cenderung mempersempit ruang inovasi.

3. Rekomendasi yang disampaikan untuk departemen TI pada PT XYZ dibuat berdasarkan setiap *domain* COBIT 5 yang diuji pada penelitian ini, yaitu APO13 dan DSS05. Tujuan rekomendasi ini agar dapat dijadikan paduan departemen TI dalam melakukan perbaikan pada setiap kelemahan yang ditemukan pada tata kelola keamanan informasi perusahaan sehingga dapat mencapai tingkat kapabilitas keamanan informasi yang diharapkan pada audit berikutnya.

5.2 Saran

Dari penelitian yang dilakukan ada beberapa saran yang dapat diberikan untuk PT XYZ dalam memperkuat sistem keamanan informasinya, yaitu:

1. Mengevaluasi ulang budaya dan pendekatan keamanan informasi perusahaan yang selama ini diterapkan untuk mencari dan menemukan hal-hal apa saja yang perlu direvisi atau diubah untuk memperkuat kapabilitas keamanan informasi dan sistem TI perusahaan secara bertahap sampai pada tingkat dimana kapabilitas keamanan informasi perusahaan telah beroperasi menurut batasan-batasan yang telah terdefinisi pada APO13 dan DSS05 untuk mencapai hasil yang optimal (*predictable process*).
2. Melakukan pengukuran terhadap kapabilitas keamanan informasi perusahaan menggunakan *framework* atau standar lain yang lebih eksklusif pada keamanan informasi (cth: ISO27000 *series*) agar dapat memperoleh hasil yang lebih terperinci mengenai keamanan informasi perusahaan.