BAB IV SIMPULAN DAN SARAN

4.1 Simpulan

1. Terdapat aset fisik yaitu personel, perangkat keras, fasilitas, dokumentasi, dan penunjang. Terdapat pula aset *logical* seperti data/informasi, *software* aplikasi, dan sistem *software* pada Politeknik X.

2. Aset Politeknik X telah diberi penilaian dengan skala satu sampai sepuluh berdasarkan prioritas untuk pengamanan dengan rata-rata sebagai berikut:

   a. Personel = 10
   b. Perangkat keras = 6
   c. Fasilitas = 7
   d. Dokumentasi = 8
   e. Penunjang = 5
   f. Data/informasi = 9
   g. *Software* aplikasi = 8
   h. Sistem *software* = 7

3. Berbagai sumber ancaman yang mengancam aset sistem informasi Politeknik X adalah bencana alam dan politik, kesalahan manusia, kegagalan perangkat lunak dan perangkat keras, kecurangan dan kejahatan komputer, dan program yang jahat/usil. Sumber ancaman yang paling potensial adalah kesalahan manusia.

4. Kecenderungan ancaman yang terdapat pada Politeknik X adalah keterbatasan sumber daya manusia, personel yang tidak loyal, pencurian aset, masalah pada listrik, keterbatasan sumber daya keuangan, virus, pemalsuan data, penyalahgunaan hak

akses, kesalahan pemasukan data, kegagalan fungsi perangkat keras dan perangkat lunak, dan ketiadaan testing yang serius terhadap perangkat lunak.

5. Kontrol yang ada untuk melindungi aset sistem informasi Politeknik X adalah kontrol administratif, kontrol pengembangan dan pemeliharaan sistem, kontrol operasi, proteksi terhadap pusat data secara fisik, kontrol perangkat keras, kontrol terhadap akses komputer, kontrol terhadap akses informasi, kontrol terhadap perlindungan terakhir, dan kontrol terhadap aplikasi. Dari dua puluh dua ancaman, sebesar 91% (dua puluh ancaman) yaitu kebakaran, runtuhnya bangunan, keterbatasan sumber daya keuangan, keterbatasan sumber daya manusia, kesalahan pemasukan data, pemalsuan data, tidak ada inisatif dari personel, tidak loyal, *training* yang minim, pencurian aset fisik dan logical, listrik padam, korsleting, tegangan listrik yang tidak stabil, kerusakan *access point*, kegagalan fungsi perangkat keras, penyalahgunaan hak akes, sabotase, *hacking*, dan virus telah memiliki kontrol dan 9% (dua ancaman) yaitu gempa bumi dan ancaman belum memiliki kontrol.

6. Kontrol yang diterapkan tidak seluruhnya dapat mengatasi bahaya ancaman. Dari dua puluh ancaman yang mungkin terjadi dan telah memiliki kontrol, hanya sebesar tujuh ancaman atau 35% kontrol yang dapat mengatasi bahaya ancaman, sedangkan tiga belas ancaman atau 65% kontrol lainnya belum mampu menghadapi bahaya dari ancaman tersebut.

7. Dari data dan hasil wawancara yang dianalisis, telah dibuat suatu laporan yang dapat dipergunakan untuk memperbaiki kontrol yang ada agar dapat mengatasi bahaya ancaman. Dalam penanganan ancaman yang paling berisiko, kontrol yang harus diperbaiki terlebih dahulu adalah berdasarkan ancaman dengan urutan berikut ini:

a. Keterbatasan sumber daya keuangan
b. Keterbatasan sumber daya manusia
c. *Training* yang minim
d. Virus
e. Kesalahan pemasukan data
f. Pemalsuan data
g. Pencurian aset fisik dan *logical*
h. Kebakaran
i. Gempa bumi
j. Runtuhnya bangunan
k. Ancaman Bom
l. Sabotase
m. *Hacking*

8. Dari data dan hasil wawancara yang dianalisis, telah dibuat dua contoh prosedur untuk kontrol operasi yaitu penanganan terhadap virus dan kontrol administratif yaitu perekrutan personel.

4.2 Saran

1. Bagi ancaman yang belum memiliki kontrol, sebaiknya disediakan kontrol untuk melindungi aset dari ancaman tersebut. Seperti pada ancaman gempa bumi, Politeknik X membutuhkan kontrol untuk melakukan *back up* terhadap data dan sistem di luar gedung Politeknik X dan mengubah desain ruang server agar lebih tahan gempa. Pada ancaman bom yang yang juga belum memiliki kontrol diberi kontrol untuk melakukan *back up* data dan sistem di luar gedung Politeknik X, mengubah desain ruang *server* agar dipisah dengan ruangan layanan Sisfo, dan menggunakan sistem identifikasi dan autorisasi bagi pihak yang akan masuk ruang Sisfo (misalnya: alat pindai retina atau sidik jari).

2. Sebaiknya semua kontrol memiliki prosedur sebagai tindakan pengamanan aset sistem informasi Politeknik X.