Bab V Penutup

V.1 Kesimpulan

Dari pengauditan yang dilakukan di DISKOMINFO Bandung dapat disimpulkan:

Sudah ada upaya melakukan kelola terhadap penjagaan aset infrastruktur DISKOMINFO dengan baik. Tetapi jika dikaitkan dengan standar COBIT, kekuatan kontrolnya masih memerlukan peningkatan.

V.2 Saran

1. *Configuration Repository and Baseline for Infrastructure* (Kontrol objektif DS9.1)
   - Sebaiknya diadakan sistem untuk penyimpanan konfigurasi untuk memonitor dan perubahan semua aset juga untuk *checkpoint* yang diinginkan bila ingin mengembalikan konfigurasi awal.
2. *Identification and Clasification of Problems* (Kontrol objektif DS10.1)
   - Sebaiknya DISKOMINFO memiliki SOP dengan *work instruction* yang lebih jelas.
   - Sebaiknya ada kategori untuk *incident management*, dampak, *urgency ,*dan prioritas.
3. *Site Selection and Layout* (Kontrol objektif DS 12.1)
   - Ada baiknya ruangan server diperbesar, dan DISKOMINFO memiliki *backup data server* di tempat terpisah, untuk mencegah hal- hal yang tidak terduga. Jadi berdasarkan penempatan bidang masing-masing dan jauh dari jangkauan pengunjung (kerusakan oleh manusia) juga terbebas banjir dan dekat dengan ruang *video conference*, tempatnya luas perencanaan letak telah diatur dengan baik .

- Sedangkan standar COBIT yang belum terpenuhi oleh perusahaan, yaitu DISKOMINFO tidak memiliki rancangan desain tata letak atau *layout* dalam menentukan lokasi peletakkan infrastruktur, juga peta evakuasi gempa belum dibuat yang baru. Sehingga peletakkan infrastruktur IT dilakukan masih di sembarang tempat dan tidak mempertimbangkan undang– undang dan peraturan yang relevan, seperti kesehatan dan peraturan keselamatan. Saran adalah meningkatkan kontrol terhadap desain tata letak atau *layout* untuk menentukan peletakkan infrastruktur IT.

4. *Physical Security Measures* (Kontrol objektif DS 12.2)
   - Dinas mungkin bisa menambah alat-alat keamanan seperti: *smart card, token, or biometric scan* untuk memasuki ruangan, CCTV, dan penyimpanan *record.*
   - DISKOMINFO harus memiliki spesifikasi ukuran yang harus dicapai untuk mencapai keberhasilan dari proses yang dijalankan. Dalam hal kontrol untuk kontrol objektif *Physical Security Measures*, maka langkah-langkah yang ada harus mampu mencegah secara efektif, mendeteksi, dan mengurangi risiko yang berkaitan dengan pencurian, suhu udara, kebakaran, asap, air, getaran, teror, vandalisme, mati lampu, bahan kimia, atau bahan peledak. Sebaiknya pengaturan internal DISKOMINFO dibuat lebih spesifik.
5. *Physical Access* (Kontrol objektif DS 12.3)
   - Dinas sebaiknya menambah jumlah resepsionis, karena terkadang meja resepsionis dibiarkan kosong.
   - Ada baiknya penjagaan terhadap *hardware* ditambah, dan dibuat prosedur tertulis. (Lampiran B , SOP Pemeliharaan Sistem Informasi)
   - Sebaiknya ada pemberian otorisasi untuk orang yang masuk ke gedung DISKOMINFO. Dalam hal kontrol untuk mengakses ke tempat-tempat tersebut harus diterapkan untuk semua orang yang memasuki tempat, termasuk staf, staf sementara, klien, vendor, pengunjung atau pihak ketiga lainnya. DISKOMINFO harus memiliki

spesifikasi ukuran yang harus dicapai untuk mencapai keberhasilan dari proses yang dijalankan.

6. *Protection Against Environmental Factors* (Kontrol objektif DS 12 .4)
   - Sebaiknya ditambah keamanan bekerja sama dengan lingkungan sekitar dan pihak DISKOMINFO. (Lampiran B, SOP Kemananan Sistem Jaringan)
   - Dinas seharusnya mempunyai bidang yang khusus mengatur dokumentasi penyimpanan atau perubahan konfigurasi yang berkaitan dengan keamanan. Penambahan penjaga perlu ditambah, memasang tambahan *camera surveillance*, ataupun memasang tambahan tabung pemadam kebakaran, bahkan staf khusus yang memonitor *camera surveillance*.
   - Pengetatan aturan bagi larangan dilarang merokok.
7. *Physical Facilities Management* (Kontrol objektif DS 12.5)
   - Sebaiknya pemeliharaan aset DISKOMINFO dibuat pengaturan lebih spesifik beserta pemeliharaan berkalanya. (Lampiran B, SOP Pemeliharaan Sistem Informasi)
   - DISKOMINFO harus memiliki spesifikasi ukuran yang harus dicapai untuk mencapai keberhasilan dari proses yang dijalankan sehingga memperkecil risiko, contoh : *work instruction,* pedoman keselamatan dalam mengelola fasilitas IT.
8. *Infrastructure Resource Protection and Availability* (Kontrol objektif AI 3.2)
   - DISKOMINFO sebaiknya melengkapi dokumentasi SOP terhadap semua kegiatan IT yang dilakukan ataupun tanggung jawab infrastruktur mendetail dan implementasi konfigurasi sistem IT untuk menghindari ketergantungan terhadap satu personel dan untuk mempermudah setiap personel ataupun personel baru dalam melakukan kegiatan IT. Secara keseluruhan SOPnya harus lebih spesifik, misalnya: dilengkapi dengan *work instruction/ WBS*.
   - Sebaiknya DISKOMINFO harus memiliki staf yang bertanggung jawab untuk memeriksa infrastruktur IT setiap hari.