KEAMANAN DAN KONTROL

A. PENTINGNYA KONTROL

- Salah satu tujuan CBIS adalah untuk memberi dukungan kepada manajer dalam mengontrol area operasinya

B. HUBUNGAN KONTROL DENGAN KEAMANAN

- Keamanan adalah proteksi/perlindungan sumber-sumber fisik dan konseptual dari bahaya alam dan manusia.
- 6 cara untuk menembus keamanan data dan informasi

Accidental	International
1. Modification	4. Modification
2. Destruction	5. Destruction
3. Disclosure	6. Disclosure

C. PROPERTI SISTEM INFORMASI YANG MEMBERIKAN KEAMANAN ISI DATA DAN INFORMASI

1. Integritas Fungsional

   Kemampuan untuk melanjutkan operasi jika salah satu / lebih komponen tidak berfungsi

2. Audibilitas (Kemampuan dapat terdengar)

   Mudah untuk diperiksa, diverifikasi atau didemonstrasikan penampilannya berarti harus lulus dalam pengujian Accountability & Visibility

3. Daya kontrol

   Penghambatan pengaruh terhadap sistem yaitu dengan membagi sistem menjadi subsistem yang menangani transaksi secara terpisah

D. TUGAS KONTROL CBIS

- Mencakup semua fase siklus hidup, selama siklus hidup dibagi menjadi kontrol-kontrol yang berhubungan dengan pengembangan sistem, desain dan operasi

Metode Untuk Mendapatkan dan Memelihara Kontrol CBIS

1. Manajemen dapat melakukan kontrol langsung
2. Manajemen mengontrol CBIS secara tidak langsung dengan terus menerus melalui CIO.
3. Manajemen mengontrol CBIS secara tidak langsung berkenaan dengan proyeknya melalui pihak ketiga

E. KONTROL PROSES PENGEMBANGAN

- Untuk memastikan bahwa CBIS yg diimplementasikan dpt memenuhi kebutuhan pemakai atau berjalan sesuai rencana

1. Fase Perencanaan
   - Mendefinisikan tujuan dan kendala
2. Fase Analisis & Disain
   - Mengidentifikasi kebutuhan informasi
   - Menentukan kriteria penampilan
   - Menyusun disain dan standar operasi CBIS
3. Fase Implementasi
   - Mendefinisikan program pengujian yang dapat diterima
   - Memastikan apakah memenuhi kriteria penampilan
   - Menetapkan prosedur utk memelihara CBIS
4. Fase Operasi & Kontrol
   - Mengontrol CBIS selagi berevolusi selama fase SLC
   - Memastikan bahwa CBIS yang diimplementasikan dapat memenuhi kebutuhan

F. KONTROL DISAIN SISTEM

- Tujuan untuk memastikan bahwa disainnya bisa meminimalkan kesalahan, mendeteksi kesalahan dan mengoreksinya.
- Kontrol tidak boleh diterapkan jika biayanya lebih besar dari manfaatnya. Nilai atau manfaat adalah tingkat pengurangan resiko.

I *Permulaan Transaksi (T*ransaction Origination)

- Perekaman satu elemen data/lebih pada dokumen sumber

1. Permulaan Dokumentasi Sumber
    - Perancangan dokumentasi
    - Pemerolehan dokumentasi
    - Kepastian keamanan dokumen
2. Kewenangan
    - Bagaimana entry data akan dibuat menjadi dokumen dan oleh siapa
3. Pembuatan Input Komputer
    - Mengidentifikasi record input yang salah dan memastikan semua data input diproses

4. Penanganan Kesalahan
    - Mengoreksi kesalahan yang telah dideteksi dan menggabungkan record yg telah dikoreksi ke record entry
5. Penyimpanan Dokumen Sumber
    - Menentukan bagaimana dokumen akan disimpan dan dalam kondisi bagaimana dapat dikeluarkan

II *Entri Transaksi*

- Entri Transaksi mengubah data dokumen sumber menjadi bentuk yang dapat dibaca oleh komputer.

1. Entri Data
    - Kontrol dalam bentuk prosedur tertulis dan dalam bentuk peralatan inputnya sendiri. Dapat dilakukan dengan proses offline/online
2. Verifikasi Data
    a. Key Verification (Verifikasi Pemasukan)
    Data dimasukkan ke sistem sebanyak 2 kali
    b. Sight Verification (Verifikasi Penglihatan)
    Melihat pada layar sebelum memasukkan data ke sistem

3. Penanganan Kesalahan
    - Merotasi record yang telah dideteksi ke permulaan transaksi untuk pengoreksian
4. Penyeimbangan Batch
    - Mengakumulasikan total setiap batch untuk dibandingkan dengan total yang sama yang dibuat selama permulaan transaksi

III *Komunikasi Data*

- Tanggungjawab manajer jaringan dengan menggabungkan ukuran keamanan ke dalam sistem dan memonitor penampilan untuk memastikan keamanan telah dilakukan dgn baik
    ii. Kontrol Pengiriman Data
    iii. Kontrol Channel Komunikasi
    iv. Kontrol Penerimaan Pesan
    v. Rencana Pengamanan Datacom Secara Keseluruhan

IV *Pemrosesan Komputer*

- Dikaitkan dengan input data ke komputer dan dibanguun dalam program dan database

i. Penanganan Data

ii. Penanganan Kesalahan

iii. Database dan Perpustakaan Software

Password # Direktori Pemakai

Direktori Field # Enkripsi

V *Output Komputer*

- Komponen subsistem ini bertanggung jawab untuk mengirimkan produk jadi kepada pemakai

i. Distribusi

- Kontrol pada distribusi laporan berusaha untuk memastikan ketepatan orang yang menerima output.

ii. Penyeimbangan Departemen Pemakai

- Bila departemen pemakai menerima output dari komputer, maka keseluruhan kontrol dari output dibandingkan dengan total yang sama yang telah ditetapkan pada waktu pertama kali data input dibuat.

iii. Penanganan Kesalahan

- Kelompok kontrol tertentu dapat ditetapkan didalam area pemakai dengan menjalankan prosedur formal untuk mengoreksi kesalahan.

iv. Penyimpangan Record

- Tujuan komponen kontrol yang terakhir ini adalah untuk memelihara keamanan yang tepat terhadap output komputer dan untuk mengontrol penyelesaian yang sia-sia.

v. Penyeimbangan Operasi Komputer

- Kontrol ini memungkinkan pelayanan informasi untuk memverifikasi bahwa semua batch dan transaksi yang diterima dari departemen pemakai telah diproses.

G. KONTROL THDP PENGOPERASIAN SISTEM

- Kontrol pengoperasian sistem dimaksudkan untuk mencapai efisiensi dan keamanan.
- Kontrol yang memberikan kontribusi terhadap tujuan ini dapat diklasifikasikan menjadi 5 area :

1. Struktur organisasional

- Staf pelayanan informasi diorganisir menurut bidang spesialisasi. Analisis, Programmer, dan Personel operasi biasanya dipisahkan dan hanya mengembangkan ketrampilan yang diperlukan untuk area pekerjaannya sendiri.

2. Kontrol perpustakaan

- Perpustakaan komputer adalah sama dengan perpustakaan buku, dimana didalamnya ada pustakawan, pengumpulan media, area tempat penyimpanan media dan prosedur untuk menggunakan media tersebut. Yang boleh mengakses perpustakaan media hanyalah pustakawannya.

3. Pemeliharaan Peralatan

- Orang yang tugasnya memperbaiki komputer yang disebut Customer Engineer (CE) / Field Engineer (FE) / Teknisi Lapangan menjalankan pemeliharaan yang terjadwal / yang tak terjadwal.

4. Kontrol lingkungan dan keamanan fasilitas

- Untuk menjaga investasi dibutuhkan kondisi lingkungan yang khusus seperti ruang komputer harus bersih keamanan fasilitas yang harus dilakukan dengan penguncian ruang peralatan dan komputer.

5. Perencanaan disaster

i. Rencana Keadaan darurat

Prioritas utamanya adalah keselamatan tenaga kerja perusahaan

ii. Rencana Backup

Menjelaskan bagaimana perusahaan dapat melanjutkan operasinya dari ketika terjadi bencana sampai ia kembali beroperasi secara normal.

iii. Rencana Record Penting

Rencana ini mengidentifikasi file data penting & menentukan tempat penyimpanan kopi duplikat.

iv. Rencana Recovery

Rencana ini mengidentifikasi sumber-sumber peralatan pengganti, fasilitas komunikasi dan pasokan-pasokan.

MENGAMANKAN SUMBER DAYA INFORMASI

- Perusahaan melakukan investasi besar dalam sumber daya informasinya
- Sumber daya tersebar di seluruh organisasi dan tiap manajer bertanggungjawab atas sumbe daya yang berada di areanya, membuat mereka aman dari akses yang tidak sah

KEAMANAN SISTEM

Tujuan Keamanan Sistem (System Security)

1. Kerahasiaan

   Perusahaan berusaha melindungi daa dan informasi dari pengungkapan kepada orang-orang yang tidak berhak
2. Ketersediaan

   Tujuan CBIS adalah menyediakan data dan informasi bagi mereka yg berwenang untuk menggunakannya terutama bagi subsistem CBIS yang berorientasi informasi SIM, DSS dan SP
3. Integritas

   Semua subsistem CBIS harus menyediakan gambaran akurat dari sistem fisik yang diwakilinya

ANCAMAN KEAMANAN

1. Pengungkapan tidak sah dan pencurian

   Jika database dan software tersedia bagi orang-orang yang tidak berwenang untuk mendapatkan aksesnya, hasilnya dapat berupa kehilangan informasi

2. Penggunaan tidak sah

   Orang-orang yang biasanya tidak berhak menggunakan sumber daya perusahaan

3. Penghancuran tidak sah dan penolakan jasa

   Orang dapat merusak/menghancurkan hardware dan software menyebabkan terhentinya operasi komputer perusahaan

4. Modifikasi tidak sah

   Jenis modifikasi yang sangat mencemaskan disebabkan oleh sotware yang merusak yang terdiri dari program lengkap/segmen kode yg melaksanakan fungsi yang tidak dikehendaki pemilik sistem

Dasar untuk keamanan terhadap ancaman oleh oang-orang yang tidak berwenang adalah pengendalian akses karena jika orang tidak berwenang ditolak aksesnya ke sumber daya informasi, perusakan tidak dapat dilakukan

PENGENDALIAN AKSES

1. Identifikasi pemakai (User Identification)

   Pemakai mula-mula mengidentifikasi diri sendiri dengan menyediakan sesuatu yang diketahuinya seperti kata sandi

2. Pembuktian keaslian pemakai (User Authentication)

   Pemakai membuktikan haknya atas akses dengan menyediakan sesuatu yang menunjukkan bahwa dialah orangnya seperti tanda tangan

3. Otorisasi pemakai (User Authorization)

User Identification dan User Authentication

menggunakan profil pemakai / penjelasan mengenai pemakai yang berwenang

User Authorization

menggunakan file pengendalian akses yang menentukan tingkat-tingkat akses yang tersedia untuk tiap pemakai

Suatu AUDIT LOG disimpan untuk semua kegiatan pengendalian akses seperti tanggal, jam serta identifikasi terminal. LOG digunakan untuk menyiapkan laporan keamanan