Pengendalian Sistem Informasi Berdasarkan Komputer

Oleh:
Wahyu Nurjaya WK, S.T., M.Kom.

Empat Prinsip Keandalan Sistem

1. Ketersediaan. Sistem tersebut tersedia untuk dioperasikan ketika dibutuhkan.
2. Keamanan. Sistem dilindungi dari akses fisik maupun logis yang tidak memiliki otorisasi.
3. Dapat dipelihara. Sistem dapat diubah apabila diperlukan tanpa mempengaruhi ketersediaan, keamanan, dan integritas sistem.
4. Integritas. Pemrosesan sistem bersifat lengkap, akurat, tepat waktu, dan diotorisasi.

Kriteria yang Digunakan Untuk Mengevaluasi Prinsip-Prinsip Keandalan

- Bagi setiap prinsip keandalan di atas, tiga kriteria berikut ini dikembangkan untuk mengevaluasi pencapaian prinsip-prinsip tersebut :
  1. Entitas mempunyai tujuan kinerja, kebijakan dan standar yang telah ditetapkan, didokumentasikan, dan dikomunikasikan, dan yang telah memenuhi tiap prinsip keandalan .
  2. Entitas menggunakan prosedur, people, software, data, and infrastructure to achieve each principle in accordance with established policies and standards.
  3. Entitas mengawasi sistem dan mengambil tindakan untuk mencapai kesesuaian dengan tujuan, kebijakan, dan standar, untuk setiap prinsip keandalan.

Pengendalian yang Berhubungan dengan Beberapa Prinsip Keandalan

- Perencanaan strategis dan penganggaran
- Mengembangkan rencana keandalan sistem
- Dan melaksanakan dokumentasi

Pengendalian yang Berhubungan dengan Beberapa Prinsip Keandalan

- Dokumentasi dapat diklasifikasikan menjadi tiga kategori dasar, yaitu:
  - Dokumentasi administratif: Mendeskripsikan standar dan prosedur untuk pemrosesan data.
  - Dokumentasi sistem : Mendeskripsikan setiap sistem aplikasi dan fungsi utama pemrosesannya.
  - Dokumentasi operasional: Mendeskripsikan hal apa yang dibutuhkan untuk menjalankan sebuah program.

Ketersediaan

- Ketersediaan
  - Meminimalkan waktu kegagalan sistem
    - Pemeliharaan untuk pencegahan
      - Sistem pasokan tenaga listrik yang stabil
      - Batas toleransi kesalahan
    - Rencana pemulihan dari bencana
      - Meminimalkan gangguan, kerusakan, dan kerugian
      - Memberikan cara alternatif memproses informasi untuk sementara waktu
      - Meneruskan jalannya operasi normal sesegera mungkin

Ketersediaan

- Melatih dan memperkenalkan personil dengan operasi perusahaan secara darurat.
- Prioritas proses pemulihan
- Jaminan
- Data dan file program cadangan
  - » Pengaman elektronis
  - » Konsep rekonstruksi bertingkat
  - » Prosedur pengulangan
- Penugasan khusus
- Fasilitas cadangan komputer dan telekomunikasi
- Uji dan revisi periodik
- Dokumentasi yang lengkap

Mengembangkan rencana keamanan

- Mengembangkan dan memperbarui terus menerus rencana keandalan yang komprehensif, adalah salah satu pengendalian penting yang dapat diidentifikasi oleh perusahaan.
  - Pertanyaannya adalah kebutuhan apa yang diminta ?
  - *Siapa yang dapat mengakses informasi* ?
  - *Kapan mereka membutuhkan* ?
  - Pada sistem yang mana informasi berada ?

Pemisahan Tugas dalam Fungsi Sistem

- Di dalam sistem informasi yang sangat terintegrasi, prosedur yang dahulu dilakukan oleh beberapa orang, kini digabungkan.
- Siapapun yang memiliki akses tak terbatas ke komputer, program komputer, dan data, dapat memiliki kesempatan untuk melakukan kejahatan dan menyembunyikan penipuan.
- Dalam rangka memerangi ancaman ini, organisasi harus mengimplementasikan prosedur pengendalian yang sesuai, seperti pemisahan tugas yang efektif dalam fungsi sistem informasi.

Pemisahan Tugas dalam Fungsi Sistem

- Otoritas dan tanggung jawab harus dengan jelas dibagi di antara fungsi-fungsi berikut ini :

1. Administrasi sistem (Systems administration)
2. Manajemen jaringan (Network management)
3. Manajemen pengamanan (Security management)
4. Manajemen perubahan (Change management)
5. Pemakai (Users)
6. Analisis sistem (Systems analysis)
7. Pemrograman (Programming)
8. Operasi komputer (Computer operations)
9. Perpustakaan sistem informasi (Information system library)
10. Pengendalian data (Data control)

Pemisahan Tugas dalam Fungsi Sistem

- Merupakan hal yang penting untuk diketahui bahwa orang-orang yang melakukan fungsi-fungsi ini haruslah orang-orang yang berbeda.
- Mengizinkan seseorang untuk melakukan dua atau lebih pekerjaan, akan menghadapkan perusahaan pada kemungkinan terjadinya penipuan.

Pengendalian atas Akses Secara Fisik

- Bagaiman keamanan akses secara fisik dapat dicapai ?
  - Tempatkan perlengkapan komputer di ruang terkunci dan batasi akses hanya untuk personil yang memiliki otoritas saja
  - Memiliki hanya satu/dua jalan masuk ke ruang komputer
  - Meminta ID pegawai yang sesuai
  - Meminta pengunjung untuk menandatangani sebuah daftar tamu ketika mereka memasuki dan meninggalkan lokasi
  - Gunakan sistem alarm keamanan
  - Batasi akses atas saluran telepon pribadi dan tidak terdeteksi, atau atas terminal dan PC yang memiliki otoriasasi.
  - Pasang kunci ke PC dan peralatan komputer lainnya.
  - Batasi akses ke program, data, dan perlengkapan off-line
  - Tempatkan hardware dan komponen penting sistem lainnya jauh dari bahan yang berbahaya atau mudah terbakar.
  - Pasang detektor asap dan api serta pemadam kebakaran, yang tidak merusak perlengkapan komputer

Pengendalian atas Akses Secara Logis

- Para pemakai harus diizinkan untuk hanya mengakses data yang diotorisasikan pada mereka, dan mereka hanya melaksanakan fungsi tertentu yang diotorisasikan pada mereka.
- Apa sajakah pengendalian atas akses secara logis itu ?
  - Password (passwords)
  - Identifikasi melalui kepemilikan fisik
  - Identifikasi biometris
  - Uji kesesuaian

Perlindungan PC dan Jaringan Klien/Server

- Banyak kebijakan dan prosedur untuk pengendalian komputer utama dapat diaplikasikan untuk jaringan PC.
- Pengendalian berikut ini juga merupakan pengendalian yang penting:
  - Latihlah pemakai mengenai pengendalian yang berkaitan dengan PC serta arti pentingnya.
  - Batasi akses dengan menggunakan kunci di PC dan apabila mungkin.
  - Buatlah kebijakan dan prosedur.

Perlindungan PC dan Jaringan Klien/Server

- PC yang mudah dibawa tidak boleh disimpan dalam mobil .
- Simpanlah data yang sensitif dalam lingkungan yang seaman mungkin.
- Instal software yang secara otomatis akan mematikan terminal atau komputer yang termasuk dalam jaringan setelah tidak digunakan dalam waktu yang telash ditentukan .
- Buatlah cadangan hard drive secara teratur.
- Enkripsi atau lindungi file dengan password.
- Buatlah dinding pelindung di sekitar sistem operasi.
- Memastikan bahwa PC harus di boot dalam sistem pengamanan.
- Gunakan pengendalian password berlapis untuk membatasi akses pegawai ke data yang tidak sesuai.
- Gunakanlah spesialis atau program pengaman untuk mendeteksi kelemahan dalam jaringan.

Pengendalian Internet dan E-commerce

- Berikut ini adalah alasan-alasan mengapa perhatian harus diberikan ketika menjalankan bisnis melalui internet.
  - Ukuran dan kompleksitas internet sangat besar
  - Internet menawarkan variabilitas yang sangat besar dalam hal kualitas, kompatibilitas, kelengkapan, dan stabilitas produk dan pelayanan jaringan

Pengendalian Internet dan E-commerce

  - Akses pesan ke yang lain
  - Banyak Website yang pengamanannya salah
  - Hacker tertarik pada Internet
- Beberapa pengendalian efektif dapat digunakan untuk mengamankan kegiatan internet, seperti :
  - Password
  - Teknologi enkripsi
  - Prosedur verifikasi routing

Pengendalian Internet dan E-commerce

- Pengendalian lain adalah dengan cara memasang firewall, hardware and software yang mengendalikan komunikasi antara jaringan internal perusahaan, yang kadang-kadang disebut sebagai jaringan yang dipercaya, dan jaringan luar/ jaringan yang tidak dipercaya.
  - Firewall adalah pembatas antar jaringan yang menghalangi keluar masuknya informasi yang tidak diinginkan dalam jaringan yang dipercaya.
- Amplop elektronik dapat melindungi pesan e-mail

Keterpeliharaan

- Dua kategori pengendalian yang membantu memastikan keterpeliharaan sistem adalah:
  - Pengembangan proyek dan pengendalian akuisisi
  - Perubahan pengendalian manajemen

Pengembangan Proyek dan Pengendalian Akuisisi

- Pengembangan proyek dan pengendalian akuisisi mencakup elemen-elemen utama berikut ini:
  - Rencana utama strategis
  - Pengendalian proyek
  - Jadwal pemrosesan data
  - Pengukuran kinerja sistem
  - Peninjauan pasca implementasi

Perubahan Pengendalian Manajemen

- Perubahan pengendalian manajemen mencakup hal-hal berikut :
- Peninjauan secara berkala terhadap semua sistem untuk mengetahui perubahan yang dibutuhkan
- Semua permintaan diserahkan dalam format yang baku
- Pencatatan dan peninjauan permintaan perubahan dan penambahan sistem dari pemakai yang diotorisasi
- Penilaian dampak perubahan yang diinginkan terhadap tujuan, kebijakan, dan standar keandalan sistem

Perubahan Pengendalian Manajemen

- Pengkategorian dan penyusunan semua perubahan dengan menggunakan prioritas yang ditetapkan
- Implementasi prosedur khusus untuk mengatasi hal-hal yang mendadak
- Pengkomunikasian semua perubahan ke manajemen
- Permintaan peninjauan, pengawasan, dan persetujuan dari manajemen TI terhadap semua perubahan hardware, software dan tanggung jawab pribadi
- Penugasan tanggung jawab khusus bagi semua yang terlibat dalam perubahan dan awasi kerja mereka.

Perubahan Pengendalian Manajemen

- Pengontrolan hak akses sistem untuk menghindari akses data dan sistem yang tidak memiliki otorisasi
- Pemastian bahwa semua perubahan melewati semua langkah yang sesuai
- Pengujian semua perubahan hardware, infrastruktur
- Pemastian adanya rencana untuk melindungi semua perubahan sistem yang kritis, untuk menjaga kemungkinan adanya sistem yang tidak bekerja atau tidak berjalan dengan sesuai
- Implementasi fungsi kepastian kualitas
- Pembaruan semua dokumentasi dan prosedur ketika perubahan diimplementasikan.

Integritas

- Perusahaan merancang pengendalian umum untuk memastikan bahwa lingkungan pengendalian berdasarkan komputer dari organisasi stabil dan dikelola dengan baik.
- Pengendalian aplikasi adalah untuk melindungi, mendeteksi, dan mengoreksi kesalahan dalam transaksi ketika mengalir melalui berbagai tahap dalam program pemrosesan data.

Integritas:
Pengendalian Sumber Data

Perusahaan harus membentuk prosedur pengendalian untuk memastikan bahwa semua dokumen sumber memiliki otorisasi, akurat, lengkap, jelas, dan masuk kedalam sistem atau dikirim ke tujuannya dengan tepat waktu. Pengendalian data sumber berikut ini mengatur integritas input :

Integritas:
Pengendalian Sumber Data

- Desain formulir
- Pengujian urutan nomor formulir
- Dokumen berputar
- Pembatalan dan penyimpanan dokumen
- Otorisasi dan pemisahan tugas
- Visual scanning
- Verifikasi digit pemeriksaan
- Verifikasi kunci

Integritas:
Rutinitas Validasi Input

Rutinitas validasi input adalah program yang memeriksa integritas data input pada saat data dimasukkan ke dalam sistem.
Rutinitas validasi input mencakup:

- Pemeriksaan urutanPemeriksaan jangkauan
- Pemeriksaan batasan
- Pengujian kelogisan
- Pemeriksaan data yang redundan
- Pemeriksaan field
- Pemeriksaan tanda
- Pemeriksaan validitas
- Pemeriksan kapasitas

Integritas:
Pengendalian Entri Data On-Line

Sasaran dari pengendalian entri data on-line adalah untuk memastikan integritas data transaksi yang dimasukkan dari terminal on-line dan PC dengan mengurangi kesalahan dan penghilangan. Pengendalian entri data on-line mencakup :

Integritas:
Pengendalian Entri Data On-Line

- Pemeriksaan field, batasan, jangkauan, kelogisan, tanda, validitas, dan data yang redundan
- Nomor ID pemakai
- Pengujian kompatibilitas
- Jika memungkinkan, sistem harus memasukkan data transaksi secara otomatis
- Pemberitahuan
- Prapemformatan
- Pengujian kelengkapan
- Verifikasi closed-loop
- Catatan transaksi
- Pesan kesalahan
- Data yang dibutuhkan untuk mereproduksi dokumen entri data on-line harus disimpan seperlunya untuk memenuhi persyaratan legal

Integritas: Pengendalian Pemrosesan dan Penyimpanan Data

Pengendalian-pengendalian umum yang membantu mempertahankan integritas pemrosesan data dan penyimpanan data adalah sebagai berikut :

- Kebijakan dan Prosedur
- Fungsi pengendalian data
- Prosedur rekonsiliasi
- Rekonsiliasi data eksternal
- Pelaporan penyimpangan

Integritas: Pengendalian Pemrosesan dan Penyimpanan Data

- Pemeriksaan sirkulasi data
- Nilai default
- Pencocokan data
- Label file
- Mekanisme perlindungan penulisan
- Mekanisme perlindungan database
- Pengendalian konversi data
- Pengamanan data

Pengendalian Output

- Fungsi pengendalian data seharusnya meninjau kelogisan dan kesesuaian format semua output
- Dan merekonsiliasi total pengendalian input dan output yang berkaitan setiap hari
- Mendestribusikan output komputer ke departemen pemakai yang sesuai

Pengendalian Output

- Mewajibkan pemakai untuk meninjau secara hati-hati kelengkapan dan ketepatan semua output komputer yang mereka terima
- Menyobek atau menghancurkan data yang sangat rahasia.

Pengendalian Transmisi Data

- Untuk mengurangi resiko kegagalan transmisi data, perusahaan seharusnya mengawasi jaringan (network).
- Kesalahan transmisi data diminimalkan dengan menggunakan :
  - Menggunakan enkripsi data
  - Prosedur verifikasi routing
  - Pemeriksaan kesamaan
  - Dan teknik pengetahuan pesan

Pengendalian Transmisi Data

Pengendalian transmisi data memberikan nilai tambah bagi organisasi yang menggunakan electronic data interchange (EDI) atau electronic funds transfer (EFT) dalam mengurangi resiko akses yang tidak memiliki otorisasi terhadap data perusahaan.

Pengendalian Transmisi Data

- Dalam lingkungan seperti ini, pengendalian internal yang baik dapat dicapai dengan menggunakan sejumlah prosedur pengendalian:
  1. Akses fisik ke fasilitas network harus dikendalikan secara ketat.
  2. Identifikasi elektronik harus diwajibkan untuk semua terminal network yang memiliki otorisasi.
  3. Prosedur pengendalian akses logis yang ketat merupakan hal yang penting, dengan password dan nomor telepon penghubungdiubah secara berkala..

Pengendalian Transmisi Data

Prosedur pengendalian, Lanjutan

4 Enkripsi harus digunakan untuk mengamankan data yang disimpan serta data yang dikirim.

5 Rincian semua transaksi harus dicatat yang ditinjau ulang secara berkala untuk mengetahui jika ada transaksi yang tidak valid.

Thank You...!!!

Created by Wahyu Nurjaya WK