BAB 2
OPERASI KOMPUTER

Tujuan Pembelajaran:

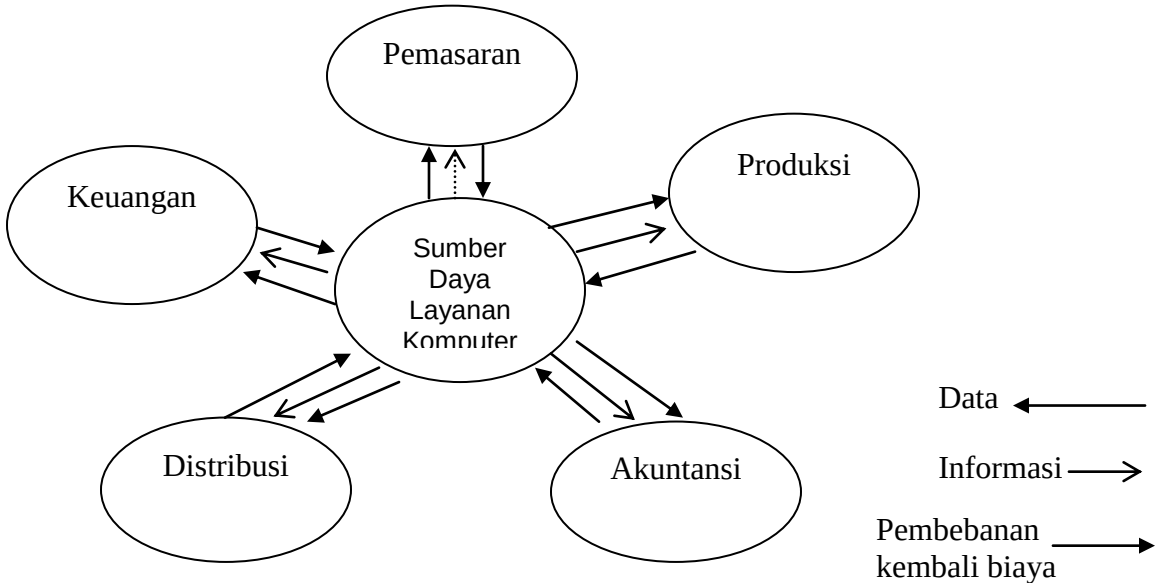
1. Memahami isu pengendalian dan audit TI dan berbagai pendekatannya
2. Mengetahui pengendalian pusat komputer dan prosedur yang digunakan untuk mengujinya
3. Memahami peran penting dan elemen dasar pemulihan dari bencana
4. Memahami peran sistem operasi pada SPI perusahaan dan mengetahui berbagai risikonya
5. Mengetahui teknik pengendalian yang digunakan untuk pengamanan sistem operasi
6. Memahami tujuan dan prosedur audit yang diaplikasikan pada audit operasional
7. Memahami risiko khusus dalam lingkungan IT dan pengendalian yang diperlukan untuk mengatasinya

STRUKTURISASI FUNGSI TEKNOLOGI INFORMASI

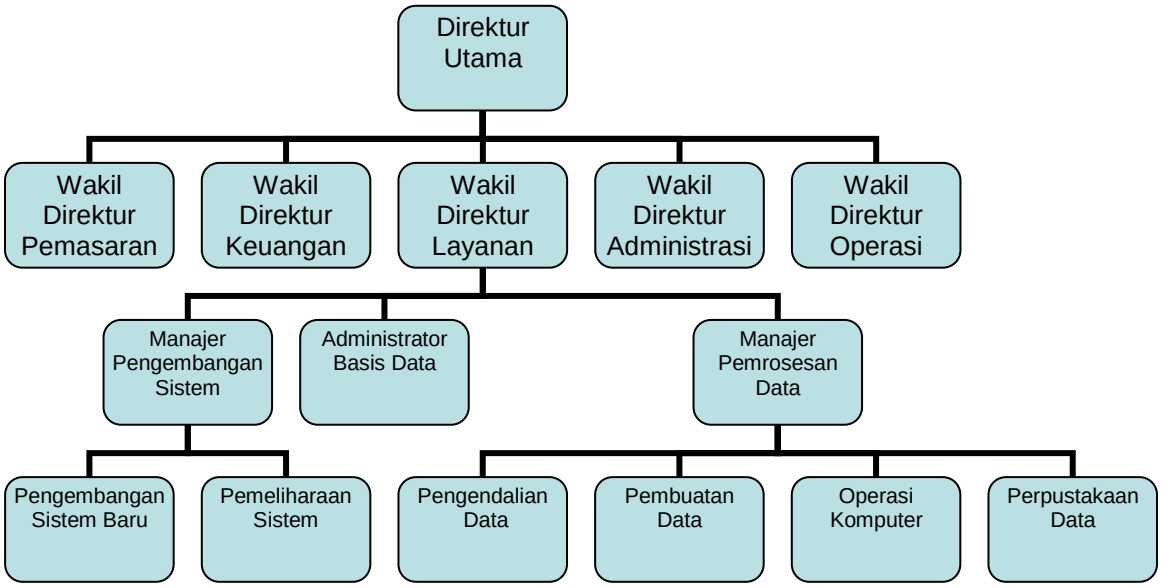
Fungsi teknologi informasi (IT) suatu organisasi merupakan kesimpulan-kesimpulan dasar dari pengendalian internal perusahaan, dimana, ini akan memberikan implikasi untuk proses audit. Bagian ini dimulai dengan membahas proses-proses dasar dan kemudian menentukan model organisasi utama yaitu pendekatan sentralisasi dan pendekatan distribusi.

PEMROSESAN DATA TERPUSAT

Menurut model *Centralized Data Processing*, semua proses data dijalankan oleh satu atau unit komputer yang lebih besar pada sebuah *central site* yang akan membantu para pemakainya dalam organisasi. Gambar berikut ini menjelaskan pendekatan ini, dimana kegiatan-kegiatan pelayanan komputer digabungkan dan diatur sebagai sebuah bagian sumber organisasi. Para pemakai akhir bersaing untuk sumber-sumber tersebut untuk kebutuhan dasarnya. Fungsi pelayanan komputer biasanya diperlakukan sebagai suatu pusat biaya yang mengoperasikan biaya-biaya yang akan dibebankan kembali kepada pemakai akhir.



Gambar di bawah ini menjelaskan suatu sentralisasi suatu pelayanan komputer dan menunjukkan area-area pelayanan utamanya: administrasi pusat data, proses data, pemeliharaan dan pengembangan sistem. Gambaran dari setiap fungsi-fungsi utama dari setiap area adalah sbb:



Administrasi Basis Data (*Database Administration*)

Fungsi ini menjelaskan bahwa perusahaan memelihara sumber data mereka di dalam sebuah lokasi terpusat yang nantinya akan didistribusikan kepada para pemakai akhir. Dalam susunan pembagian data berikut ini, sebuah kelompok independen yaitu DBA yang dikepalai oleh administrator pusat data adalah pihak yang bertanggung jawab untuk keamanan dan kelengkapan pusat data.

Pemrosesan Data (*Data Processing*)

Kelompok data processing mengatur sumber-sumber komputer yang digunakan untuk melakukan proses transaksi dari hari ke hari. Ini terdiri dari fungsi-fungsi yang ada dalam organisasi seperti pengendalian data, perubahan data, operasional komputer, dan perpustakaan data.

- Pengendalian Data (*Data Control*)
  Banyak organisasi memiliki suatu kelompok pengendalian data sebagai *liaison* antara pengguna akhir dan prosessing data, dan juga sebagai suatu fungsi pengendalian untuk operasional yang terkomputerisasi. Pengendalian data bertanggungjawab untuk menerima sekelompok dokumen-dokumen transaksi untuk diproses dari pengguna akhir dan kemudian didistribusikan sebagai output komputer (dokumen dan laporan) dan kembali ke pemakai.
- Konversi Data (*Data Conversion*)
  Fungsi dari pengubah data adalah menulis data transaksi dari sumber dokumen-dokumen kertas kedalam input komputer. Contohnya, perubahan data dapat di *keypunching* dari

order-order penjualan ke dalam suatu aplikasi order penjualan dengan sistem yang modern, atau menulis data ke dalam media magnetic seperti tape atau disk. Dan sumber-sumber dokumen aslinya dikembalikan ke pemakai.

- Operasi Komuter (*Computer Operation*)
  Merupakan file elektronik yang di buat kemudian oleh pusat komputer, dimana hal ini akan di atur oleh kelompok-kelompok operasional komputer. Aplikasi-aplikasi akuntansi biasanya dilakukan berdasarkan sebuah jadwal yang tepat bahwa ini dikendalikan oleh sistem operasi pusat komputer.
- Perpustakaan Data (*Data Library*)
  Merupakan sebuah ruangan yang berdekatan dengan pusat komputer yang menyediakan tempat penyimpanan yang aman untuk *off-line data files.* File-file tersebut dapat di *backup* termasuk data file saat ini. Sebagai contoh, perpusatakaan data dapat digunakan untuk menyimpan *backup-an* data dalam suatu DVD, CD-ROM, tape, bentuk penyimpanan lainnya. Ini juga bisa digunakan untuk menyimpan file lama dan file-file saat ini dalam tape magnetic dan *removable disk packs.* Untuk tambahan, perpustakaan data bisa juga digunakan untuk menyimpan copian asli dari perangkat-perangkat lunak yang diperdagangkan dan lisensi nya untuk keamanan. Suatu pemimpin perpustakaan data adalah yang bertanggang jawab untuk penerimaan, penyimpanan, perbaikan dan pemeliharaan file data, akses pengendalian untuk perpustakaan. Masalah-masalah *librarian* file data untuk operator-operator komputer dalam memenuhi permintaan program dan mengambil file-file ketika prosessing dan backup telah selesai. Beberapa tahun terakhir ini, arah penggunaan *real-time processing* ditingkatkan sedangkan akses langsung ke file dukurangkan bahkan dihilangkan peranannya pada perpustakaan data oleh sebagian besar organisasi. Bagaimanapun, fungsi ini masih bisa menjadi suatu pengendalian efektif untuk aplikasi-aplikasi yang diperdagangkan, lisensi, dan *on-site backup.*

PEMISAHAN PEKERJAAN YANG TIDAK SALING BERHUBUNGAN

Tujuan pemisahan pekerjaan yang tidak saling berhubungan adalah:

1. Sistem-sistem Pengembangan dan Pemeliharaan

Sistem-sistem informasi dibutuhkan oleh pemakainya untuk memenuhi dua fungsi yang berhubungan: sistem pengembangan dan sistem pemeliharaan. Kelompok pembentuk adalah yang bertanggungjawab untuk menganalisis kebutuhan pemakai dan untuk membuat sistem baru untuk memuaskan kebutuhannya. Yang turut ambil bagian dalam kegiatan pengembangan sistem meliputi *systems professional*, pemakai akhir dan para *stakeholder*.

System professional meliputi para analist sistem, perancang pusat data, dan programmer yang merancang dan membuat sistem. *Systems professional* mengumpulkan fakta-fakta tentang masalah para pemakai, menganalisis fakta tersebut dan menentukan solusinya. Hasil dari usaha mereka adalah sebuah sistem informasi yang baru. Satu faktor utama untuk keberhasilan suatu sistem adalah partisipasi dan input dari para pemakai akhir.

Pemakai akhir adalah pihak-pihak untuk siapa sistem itu dibuat. Mereka merupakan pengelola atas laporan-laporan yang diterima dari sistem dan pihak-pihak yang beroperasi dan menggunakan sistem secara langsung sebagai bagian dari tanggungjawab mereka sehari-hari.

Stakeholders merupakan pihak-pihak didalam atau diluar perusahaan yang memiliki suatu kepentingan atas sistem, tetapi mereka bukan merupakan pemakai akhir. Mereka meliputi

akuntan, auditor internal, auditor eksternal, dan pihak lainnya yang mengawasi perkembangan sistem. Bagaimanapun, auditor internal dan eksternal membutuhkan kehati-hatian untuk tidak melanggar indepedensi seperti yang telah ditentukan oleh standar professional, atau Sarbanes-Oxley yang dibutuhkan untu SEC dengan aturan-aturannya.

Ketika sebuah sistem baru telah dirancang dan diimplementasikan, kelompok pemeliharaan sistem diasumsikan bertanggungjawab untuk kelancarannya terhadap kebutuhan pemakai. Proses kehidupan suatu sistem (untuk beberapa tahun) sekitar 80 hingga 90 persen dari total biayanya akan dikeluarkan untuk kegiatan pemeliharaan.

PEMISAHAN FUNGSI-FUNGSI IT YANG BERTENTANGAN

Pemisahan fungsi-fungsi yang bertentangan adalah hal yang kurang penting dalam lingkungan IT dibandingkan lingkungan manual. Ketika tugas-tugas tersebut berbeda, namun teorinya sama. Berikut ada tiga tujuan fundamental dari pemisahan tugas seperti yang telah didiskusikan pada Bab 1:

1. Pemisahan tugas atas pengesahan transaksi dari pemrosesan transaksi
2. Pemisahan antara pemegang laporan dengan pemegang aktiva
3. Membagi tugas-tugas pemrosesan transaksi antar individual untuk menghindari terjadinya kolusi antar dua individu atau lebih

Dalam lingkungan IT, suatu aplikasi baik pengesahan, pemrosesan dan pencatatan merupakan semua sudut pandang dari sebuah transaksi. Dengan demikian, fokus pemisahan pengendalian mulai dari tingkat operasional (tugas-tugas pemrosesan transaksi saat ini dilakukan dengan program komputer) hingga tingkat yang paling tinggi dalam suatu organisasi berhubungan dengan fungsi pelayanan komputer.

Pemisahan Sistem-sistem Pengembangan dari Operasi-operasi Komputer

Pemisahan sistem-sistem pengembangan (antara pengembangan sistem baru dengan pemeliharaan) dan kegiatan-kegiatan operasional merupakan hal yang sangat penting. Hubungan antara kelompok-kelompok tersebut harus kuat dan tanggungjawab mereka tidak boleh disatukan. Para ahli sistem pengembangan dan pemeliharaan harus membuat dan memelihara sistem-sistem tersebut untuk para pemakainya dan tidak boleh terlibat dalam memasukkan data, atau menjalankan aplikasi (ex; operasional komputer). Staf operasional harus menjalankan sistem mereka dan tidak melibatkannya dalam rancangan mereka. Fungsi-fungsi tersebut merupakan satu kesatuan yang bertentangan dan gabungan dari mereka akan menimbulkan kesalahan-kesalahan dan kecurangan. Dengan pengetahuan yang detail tentang ilmu-ilmu aplikasi dan *control parameters* dan akses untuk mengoperasikan sistem komputer dan kugunaan-kegunaannya, merupakan suatu keistimewaan bagi seseorang yang tidak berhak untuk mengubah aplikasi selama aplikasi tersebut digunakan. Perubahan tersebut bisa bersifat sementara dan akan hilang ketika aplikasi-aplikasi tersebut diakhiri.

Sebagai contohnya, hal ini akan lebih mudah bagi para programmer untuk menipu sistem dibandingkan para operator karena mereka mengetahui kodenya. Mereka mengetahui bagaimana mendapatkan hal-hal tertentu, atau yang paling banyak adalah menguasai pengendalian-pengendaliannya. Belum lagi, ada beberapa programmer yang dengan sengaja mendapatkan kode program dan mengendalikan mereka dan membiarkan mereka melakukan kecurangan.

Pemisahan Fungsi Administrasi Pusat Data dengan Fungsi-fungsi Lainnya

Hal penting lainnya dalam pengendalian organisasi adalah pemisahan administrasi pusat data (DBA) dari fungsi pusat komputer lainnya. Fungsi DBA adalah bertanggungjawab untuk sejumlah tugas-tugas yang kritis termasuk keamanan pusat data, yang meliputi skema rancangan database dan data-data pemakai, menentukan akses yang sah ke database dari pemakai, memonitor database, dan merencanakan pengembangan di masa yang akan datang. Mengutus pertanggungjawaban tersebut untuk fungsi-fungsi lainnya yang menunjukkan tugas-tugas yang bertentangan yang dapat mengancam database.

Pemisahan Pengembangan dan Pemeliharaan Sistem Baru

Beberapa perusahaan menyusun fungsi pengembangan system *in-house* mereka ke dalam dua kelompok; analisis sistem dan pemrograman (lihat gambar 2-3). Kelompok analisis sistem bekerja dengan para pemakainya untuk membuat rancangan-rancangan sistem-sistem baru. Sedangkan kelompok pemrograman membuat kode-kode program menurut spesifikasi rancangannya. Sesuai pendekatan ini, programmer yang membuat kode program-program original juga memelihara sistem selama tahap pemeliharaan dalam siklus pengembangan sistem. Walaupun ini suatu pendekatan yang popular, pendekatan ini berhubungan dengan dua tipe masalah pengendalian; dokumentasi yang tidak mencukupi dan potensial atas kecurangan program.

- *PERBAIKAN DOKUMENTASI*, miskinnya sistem dokumentasi merupakan sebuah masalah kronis bagi banyak perusahaan. Ini terutama terjadi dalam perusahaan yang tidak menggunakan CASE dengan bentuk-bentuk dokumentasi otomatis. Ada dua penjelasan untuk fenomena ini; pertama, sebuah sistem dokumentasi tidak menarik dalam merancang, menguji dan menerapkannya. Para ahli sistem lebih banyak memilih untuk berpindah pada proyek-proyek baru daripada mendokumentasikan satu hal dan men yelesaikannya. Tekanan dari para pemakai yang menginginkan sistem baru membuat keputusan untuk lebih cepat berpindah pada sesuatu yang lebih mudah.

  Alasan yang kedua untuk ketidakcukupan dokumentasi adalah keamanan pekerjaan. Ketika sebuah sistem kekurangan dokumentasi, ini akan mempersulit untuk menginterpretasi, menguji dan *debug.* Oleh Karena itu, programmer yang mengerti dengan sistem (salah satu pembeuat kode) memiliki suatu posisi yang kuat dan relative tidak dapat dihindari. Bagaimanapun, ketika dia meninggalkan perusahaan, programmer baru harus memelihara sistem.
- *MENGHINDARI KECURANGAN.* Ketika programmer asli dari sebuah sistem juga mempertahankan tanggungjawabnya, kecurangan potensial akan meningkat. Kecurangan program meliputi mengubah secara tidak sah modul-modul program untuk tujuan yang illegal. Programmer asli mungkin berhasil menyembunyikan kode kecurangan antara ribuan kode yang sah dan ratusan modul yang disusun oleh sebuah sistem. Bagaimanapun, untuk berhasilnya suatu kecurangan, programmer harus melanjutkan dan membatasi akses ke dalam program tersebut. Untuk mengendalikan situasi ini, programmer harus melindungi penggelapan kode oleh programmer lainnya (selama pemeliharaan) atau oleh auditor. Oleh karena itu, elemen penting dalam memelihara duplikasi program-program merupakan tanggung jawab utama. Dengan adanya wewenang dalam memlihara, maka programmer memiliki kebebasan dalam mengakses sistem, menghilangkan kode kecurangan selama proses audit, dan mengembalikan kode ketika pekerjaan telah selesai.

Pemisahan Data Library dari Operations

Data library biasa merupakan suatu tempat yang ada pada pusat komputer yang menyediakan tempat yang aman untuk file-file data yang *off-line* seperti tape magnetic dan *removable disk packs pada legacy-type systems.* Librarian harus secara mendetail memasukkan log setiap file, meliputi nama, nomor serial, isi, tanggal pembuatan, dan tanggal penyimpanan. Masalah-masalah librarian misalnya membongkar tape-tape bekas untuk operator-operator komputer yang cocok dengan permintaan sistem-sistem. Ketika program telah lengkap, operator kembali ke file-file librarian untuk penyimpanan. Pemisahan librarian dari kegiatan operasional adalah sangat penting untuk pengaman fisik file data *off-line.*

Operator-operator yang mengerjakan tugas-tugas library harus mengerti terhadap pentingnya tanggungjawab yang jelas. Manajemen harus dengan teliti mengendalikan orang yang menjalankan fungsi *library* untuk memastikan bahwa mereka tidak memikul tanggungjawab operator-operator lain selama periode sibuk. Pembukaan yang potensial dapat diilustrasikan pada tiga scenario berikut ini.

1. Pusat komputer menjadi sangat berfungsi saat ini.
2. Tidak berpengalamannya individu yang mengisi posisi librarian selama periode-periode sibuk memungkinkan kesalahan pada lokasi penyimpanan dalam library.
3. Librarian bertanggungjawab langsung untuk menerapkan kebijakan *scratch* perusahaan

Audit objectives

1. Menetapkan suatu penafsiran risiko yang menghargai pengembangan sistem, pemeliharaan, dan operasi-operasi.
2. Verifikasi individu-individu pada area-area yang berbeda sesuai dengan tingkat risiko potensial.
3. Verifikasi bahwa pemisahan telah dilakukan dengan cara mempromosikan suatu lingkungan pekerjaan secara lebih formal,ada hubungannya antara tugas-tugas yang bertentangan.

Audit procedure

1. Mendapatkan dan mereview kebijakan perusahaan dalam *computer security*→ memverifikasi bahwa kebijakan keamanan dikomunikasikan pada tanggungjawab karyawan dan supervisor.
2. Mereview dokummentasi yang relevan, yang meliputi chart organisasi saat ini, pernyataan misi dan deskripsi pekerjaan untuk fungsi-fungsi kunci, menentukan jika terdapat individu atau kelompok yang menjalankan fungsi yang berlawanan.
3. Mereview sistem dokumentasi dan pemeliharaan catatan-catatan sebagai sebuah contoh aplikasi-aplikasi.
4. Selama observasi, menentukan kebijakan-kebijakan yang terpisah harus diikuti dengan praktik.
5. Mereview pemakai yang jelas dan pantas untuk memverifikasi programmer yang sesuai dengan deskripsi pekerjaannya.

THE DISTRIBUTED MODEL

Sebuah alternative untuk model sentralisasi data adalah *distributed data processing* (DDP). DDP meliputi jasa pengaturan ulang komputer ke unit IT yang lebih kecil yang terletak pada pengawasan di bawah user terakhir. Unit IT didistribusikan kepada fungsi bisnis, lokasi geografi,

atau kedua-duanya. Seluruh aktivitas komputer pada figure 2-2 bisa saja didistrubusikan. Tingkatan IT didistrusikan tergantung pada tujuan dan filosofi dari management perusahaan. Figure 2-4 menunjukkan 2 alternatif EDP. Alternatif A merupakan model sentralisasi sedangkan alternatif B menunjukkan adanya network connection dalam pendistribusian data dari unit satu ke unit lainnya. Pada figure 2-5, menunjukkan struktur/jenjang pendsitribusian data yang mungkin terjadi dalam pendistribusian data dari task awal ke end user.

Figure 2-4:

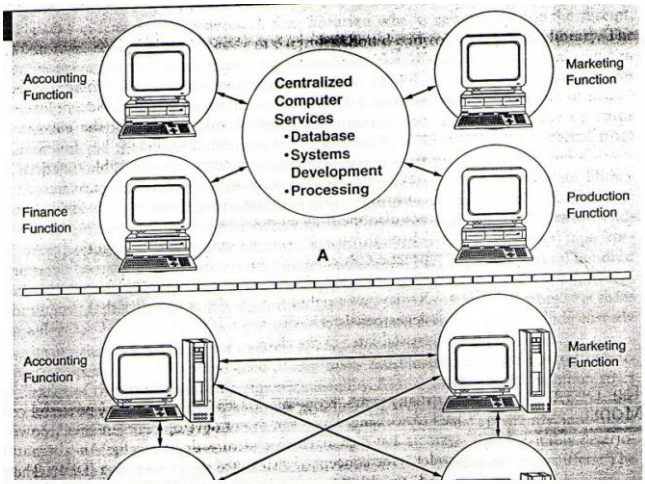
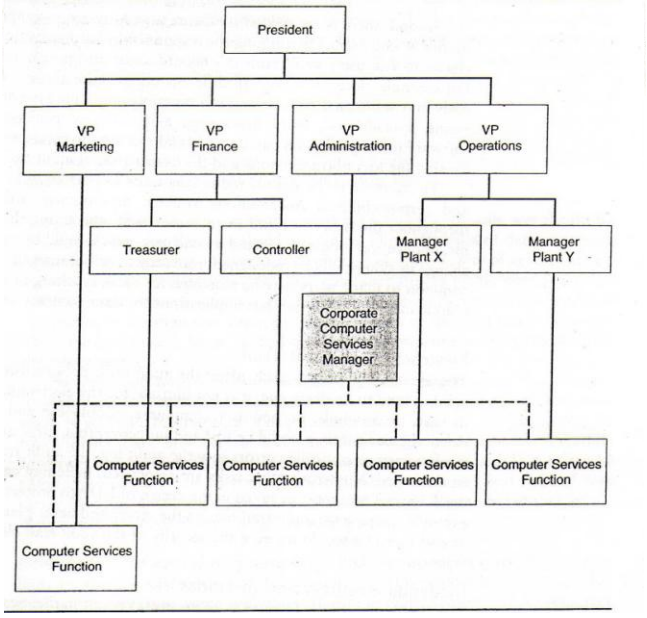


Figure 2-5:



Resiko DDP

- Penggunaan sumber daya yang tidak efisien.
- Pemisahan tugas yang tidak cukup.
- Meningkatkan potensi error dan kegagalan program.
- Pengurangan standar (standar sistem dokumentasi dan pengembangan, pemilihan bahasa program, evaluasi performa, dsb).

Manfaat DDP

- Pengurangan biaya.
- Memperbaiki pertanggung jawaban pusat biaya.
- Meningkatkan kepuasan pengguna.
- Fleksibilitas system *backup*.

PENGENDALIAN LINGKUNGAN DDP

Perencanaan seksama dan implementasi pengendalian dapat mengurangi resiko yang baru saja didiskusikan. Bagian ini mereview persoalan pengendalian dan audit yang berhubungan dengan DDP.

Need for Careful Analysis

DDP membawa ketajaman utama tertentu nilai prestise bahwa, selama analisis pro dan kontra nya, mungkin (dapat) meliputi pertimbangan penting manfaat ekonomi dan kelayakan operasional. Beberapa organisasi telah membuat tindakan (langkah) menuju DDP tanpa pertimbangan dengan sepenuhnya apakah stuktur organisasi yang terdistribusi akan lebih baik mencapai tujuan bisnis mereka. Banyak inisiatif DDP telah membuktikan bahwa untuk tidak efektif, dan tetap *counterproductive* (tidak produktif), karena para pembuat keputusan melihat pada kebaikan sistem ini yang lebih simbolik dan riil.

Implement a Corporate IT Function

Model yang terpusat dengan lemgkap dan model yang terdistribusi menyajikan kembali posisi ekstrim pada sebuah rangkaian alternatif-alternatif struktural. Kebutuhan sebagian besar perusahaan jatuh pada suatu tempat berkisar antara titik akhir ini. Bagi sebagian besar perusahaan, masalah pengendalian kita telah menguraikan dapat dinyatakan langsung (dialamatkan) dengan pengimplementasian sebuah *corporate IT function* seperti yang digambarkan pada gambar 2-5.

Fungsi ini sangat dikurangi dalam ukuran dan kedudukan dari yang mana model yang terpusat ditunjukkan dalam gambar 2-2. Corporate group *IT* menetapkan perkembangan sistem dam manajemen *database* untuk kesatuan sistem yang luas disamping nasihat bersifat teknis dan keahlian khusus untuk *IT community* yang terdistribusi. Peran laporan ini disajikana kembali oleh garis yang ditandai dalam gambar 2-5.

- *Central Testing of Commercial Software and Hardwere*
  Corporate group *IT* mampu secara lebih baik untuk mengevaluasi mutu vendor software dan hardware yang bersaing. Sebuah pusat, secara teknis group yang pandai seperti ini dapat mengevaluasi fitur-fitur sistem, pengendalian, dan kesesuaian dengan industri dan standar-standar organisasi yang paling (scara)efisien. Oleh karena itu, organisasi harus memusatkan perolehan, pengujian, dan pengimplementasian software dan hardare pada *corporate IT function*.
- *User Services*
  Sebuah fitur yang bernilai dari corporate group adalah fungsi jasa penggunanya. Aktivitas ini menyediakan bantuan bersifat teknis kepada para pengguna selama instalasi software baru dan selama pemcarian dan pemecahan masalah hardware dan software.
- *Standard-Setting Body*

Lingkungan pengendalian yang kurang baik secara relatif yang diberlakukan oleh model DDP dapat dikembangkan dengan penetapan beberapa petunjuk pusat (central). *Corporate group* dapat menyumbang untuk tujuan ini dengan penetapan dan pendistribusian kepada pengguna area-area standar yang sesuai untuk pengembangan sistem, pemrograman dan dokumentasi.

- *Personnel Review*
  Corporate group kemungkinan besar lebih baik diperlengkapi daripada para pengguna sampai mengevaluasi mandat (surat kepercayaan) secara teknis dari bakal (prospektif) sistem profesional. Walaupun sistem profesional akan menjadi bagian yang sebenarnya dari *group* pengguna, keterlibatan *corporate group* dalam keputusan pekerjaan dapat memberikan sebuah jasa yang bernilai kepada organisasi.

Audit Objectives

- Mengadakan sebuah penilaian resiko fungsi-fungsi DDP IT
- Menverifikasi bahwa unit-unit IT yang terdistribusi mempergunakan kesatuan standard yang luas dari kinerja yang mempromosikan kesesuaian diantara hardware, software aplikasi dan data.

Audit Procedures

- Memverifikasikan bahwa kebijakan *corporate* dan standar-standar untuk rancangan sistem, dokumentasi, dan perolehan hardware dan software dipublikasikan dan diedarkan ke unit-unit IT yang terdistribusi.
- Mereview bagan organisasi (organizational chart), pernyataan misi, dan *job descriptions* bagi fungsi-fungsi kunci (penting) untuk menetapkan apakah individu-individu atau kelompok-kelompok sedang melakukan tugas-tugas yang tidak sesuai (bertentangan).
- Memverifikasi bahwa pengendalian kompensasi (compensating control) seperti supervisi dan pemantauan manajemen dipergunakan ketika pemisahan tugas-tugas yang tidak sesuai (bertentangan) dari segi ekonomi tidak menguntungkan.
- *Review* dokumentasi sistem untuk memverifikasi bahwa aplikasi, prosedur, dan database dirancang, dan berfungsi sesuai dengan *corporate standards*.
- Memverifikasi bahwa individu-individu diberikan hak (istimewa) akses sistem ke program dan data dengan cara (macam) yang konsisten dengan *job descriptions* mereka.

PUSAT KOMPUTER

Tujuan dari bagian ini adalah menyajikan pengendalian pusat komputer yang membantu menciptakan lingkungan yang aman. Diskusi akan dimulai dengan sebuah pandangan padapengendalian yang dirancang untuk mencegah dan mendeteksi ancaman-ancaman terhadap pusat komputer. Meskipun demikian, bukan persoalan berapa banyak yang diinvestasikan dalam pengendalian, beberapa bencana atau perpecahan terhadap ketersediaan sistem sama sekali tidak dapat diantisipasi dan dicegah. Apa yang dilakukan sebuah perusahaan untuk menyiapkan dirinya terhadap peristiwa demikian? Bagaimanakah perusahaan akan terpulihkan? Pertanyaan-pertanyaan ini adalah pada kemauan rencana pemulihan bencana organisasi.

PENGENDALIAN PUSAT KOMPUTER
Physical Location

Lokasi fisik pusat komputer secara langsung mempengaruhi resiko bencana dan ketidaktersediaan. Untuk batas yang mungkin (dapat diterima), pusat komputer harus jauh dari buatan manusia dan bahaya yang alami, seperti pemrosesan pabrik, gas, dan pipa air, airports, area-area yang tinggi kriminalitas, banjir daratan, keretakan pada lapisan permukaan bumi secara geologi. Lokasi tersebut harus jauh dari arus lalu lintas normal sebanyak yang dapat diterima (mungkin), seperti lantai tertinggi dari sebuah bangunan, atau memisah, bangunan yang dapat menampung diri sendiri. Menyadari bahwa lokasi pusat komputer dalam basement sebuah bangunan mungkin menciptakan sebuah pembongkaran (exposure) untuk resiko bencana seperti banjir.

Constraction

Menurut teori, sebuah pusat komputer harus ditempatkan pada sebuah bangunan tingkat (lantai) satu dari konstruksi yang kokoh dengan akses yang dikendalikan. *Utility* (power dan telepon) dan saluran komunikasi harus di bawah tanah (underground). Jendela-jendela bangunan tidak harus terbuka. Sebuah sistem *filtration* udara harus ditempatkan yang mana mampu mengeluarkan (meniadakan) serbuk sari, debu, debu tungau. Jika pusat komputer harus ditempatkan pada bangunan berlantai banyak, pusat komputer harus ditempatkan pada lantai atas, jika mungkin.

Access

Akses ke pusat komputer harus dibatasi untuk para operator dan karyawan-karyawan lainnya yang bekerja disana. Pengendalian fisik, seperti pintu-pintu yang terkunci, harus dipergunakan untuk batasan akses ke pusat. Pintu (jalan masuk) utama ke pusat komputer harus melewati satu pintu yang terkunc (mudah dicapai hanya dengan menggunakan sebuah *keypad* atau *swipe card*, terutama). Untuk mencapai tingkat keamanan yang lebih tinggi, akses harus dimonitor dengan *closed-circuit cameras* dan sistem *video recording*. Pusat komputer juga harus menggunakan *sign-in logs* untuk para programmer dan analis yang membutuhkan akses untuk membenarkan kesalahan program.

Air Conditioning

Fungsi terbaik komputer pada sebuah lingkungan yang dilengkapi dengan alat pendingin. Untuk komputer-komputer *mainframe*, menyediakan pengaturan suhu udara seringkali merupakan sebuah persyaratan jaminan *vendor*. Komputer beroperasi paling baik pada kisaran temperatur 70 sampai 75 derajat Fahrenheit dan kelembaban relatif 50 persen. Sekelompok PC akanmenghasilkan banyak panas, jadi ruangan yang dipenuhi dengan PC membutuhkan pengaturan suhu udara yang khusus.

Fire Supression

Sebagian besar bencana alami yang biasa mengancam bagi peralatan komputer perusahaan adalah dari kebakaran. Sebagian perusahaan yang menderita kebakaran keluar (mati) dari bisnis karena kehilangan catatan bersifat kritis (penting), seperti piutang dagang. Implementasi sistem penumpasan kebakaran yang efektif memerlukan konsultasi dengan spesialis. Beberapa fitur utama sebuah sistem penumpasan kebakaran tercakup sebagai berikut:

- Alarm otomatis dan manual harus ditempatkan pada lokasi strategis disekitar instalasi
- Ini harus ada sebuah sistem pemadaman kebakaran otomatis yang menyalurkan jenis *suppressant* yang sesuai untuk lokasi tersebut.

- Alat pemadam kebakaran manual harus ditempatkan pada lokasi strategis.
- Bangunan harus memiliki konstruksi yang kuat untuk menahan kerusakan air disebabkan oleh peralatan penekanan kebakaran.
- Pintu keluar kebakaran harus diberi tanda yang jelas dan diberi penjelasan selama kebakaran.

Power Supply

Secara komersial daya listrik menyajikan beberapa masalah yang dapat mengganggu operasi pusat komputer, termasuk total kegagalan (melemahnya) daya, fluktuasi daya, dan frekuensi variasi (selisih). Peralatan yang digunakan untuk mengendalikan masalah-masalah ini termasuk alat pengatur voltase (voltage regulators), pelindung gelombang (surge protectors), generator, dan baterai. Luas dan konfigurasi peralatan pengendalian yang diperlukan akan tergantung pada kemampuan perusahaan untuk menahan (melawan) sejenis gangguan dan daya catatan perusahaan untuk menyediakan jasa yang dapat diandalkan (reliable). Keputusan mengenai pengendalian daya dapat menjadi salah satu keputusan yang mahal, dan biasanya memerlukan nasihat dan analisa para ahli.

Audit Objectives

Tujuan keseluruhan memperhatikan pengendalian pusat komputer adalah untuk mengevaluasi pengendalian yang memerintah keamanan pusat komputer. Secara khusus, auditor harus memverifikasi bahwa:

- Keamanan pengendalian fisik sesuai untuk melindungi secara masuk akal organisasi dari pembukaan (exposures) fisik.
- Ulasan asuransi atas peralatan sesuai untuk mengganti kerugian organisasi untuk perusakan, atau kerusakan (bencana), terhadap pusat komputernya.
- Dokumentasi operator sesuai untuk perjanjian terhadap kegagalan sistem.

Audit Procedures

Berikut ini merupakan pengejian fisik pengendalian keamanan:

- Test of Physical Construction

  Auditor harus menentukan bahwa pusat komputer dibangun dengan kokoh dari bahan tahan api. Dalam hal ini, harus disesuaikan proses pengaliran dibawah lantai yang timbul untuk membiarkan air mengalir jauh dalam peristiwa kerusakan air dari sebuah kebakaran pada lantai yang lebih tinggi atau dari beberapa sumber yang lainnya. Dan juga auditor harus mengevaluasi lokasi fisik pusat komputer. Fasilitas harus ditempatkan pada area yang memperkecil pembukaannya (exposure) dari kebakaran, kerusuhan warga, dan bahaya lainnya.
- Tests of the Fire Detection System

  Auditor harus menetapkan bahwa peralatan deteksi dan penumpasan kebakaran, keduanya manual dan otomatis, ditempatkan dan diuji secara teratur. Sistem deteksi kebakaran harus mendeteksi asap, panas, dan gas yang mudah terbakar.
- Tests of Access Control

  Auditor harus menetapkan bahwa akses rutin ke pusat komputer dibatasi untuk karyawan-karyawan yang diberi otorisasi. Rincian mengenai akses pengunjung (melalui programmer dan yang lainnya) seperti waktu kedatangan dan keberangkatan, tujuan dan frekuensi akses, dapat diperolah dengan mereview *access log*. Untuk menentukan kebenaran dokumen ini, auditor dapat mengobservasi secara tersembunyi proses dimana

akses diizinkan, atau mereview *videotapes* dari kamera pada titik akses, jika mereka sedang digunakan mereka.

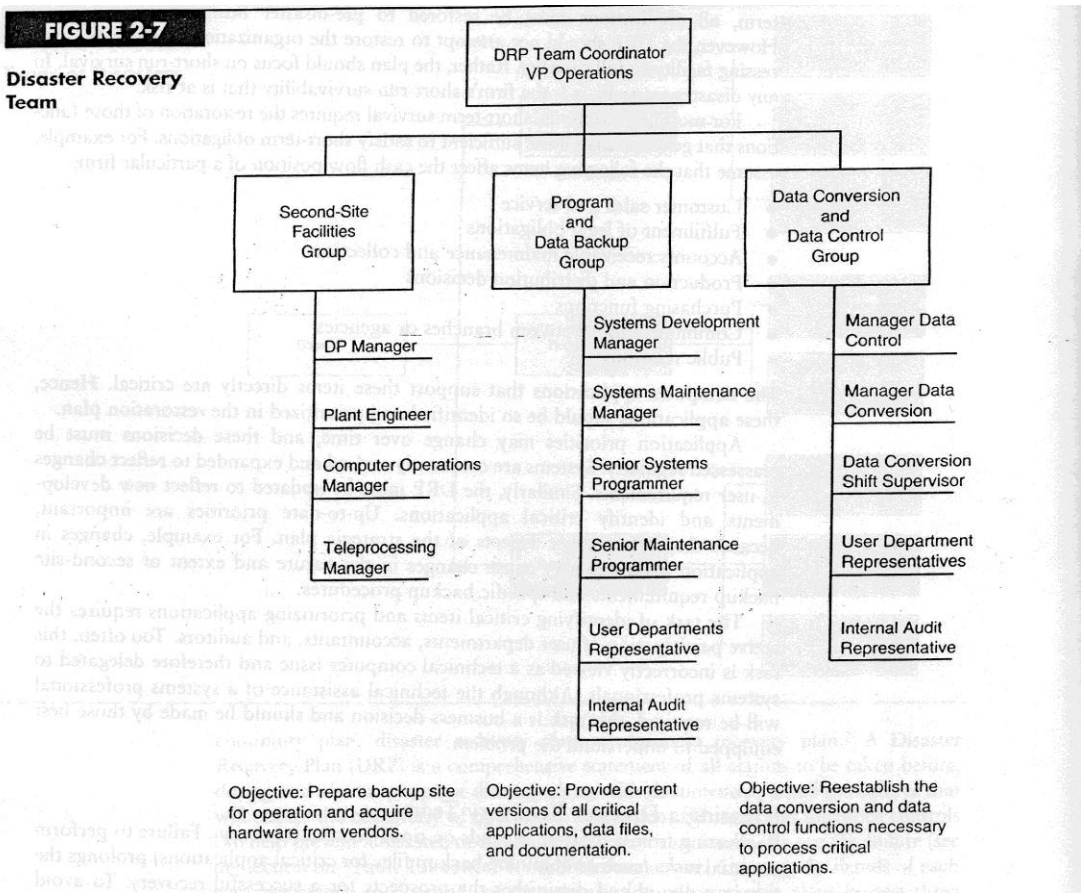
- Tests of Backup Power Supply
  Pusat komputer harus melaksanakan pengujian periodik *backup power supply* untuk memastikan bahwa ia memiliki kapasitas yang cukup untuk menjalankan komputer dan pengaturan suhu udara. Ini merupakan pengujian yang secara ekstrim penting dan hasil pengujian harus dicatat dengan resmi.
- Tests for Insurance Coverage
  Auditor setiap tahun harus mereview ulasan asuransi organisasi atas hardware, software, dan fasilitas fisik komputernya. Perolehan-perolehan baru harus dicatat atas kebijakan dan peralatan usang dan software yang harus dihapuskan.
- Tests of Operator Documentation Controls
  Auditor harus menverifikasi bahwa sistem dokumentasi, seperti system *flowchart*, *logic flowcharts*, dan *program code listings*, bukan merupakan bagian dari dokumentasi operasi. Auditor harus menentukan bahwa dokumentasi pengguna yang sesuai tersedia, atau sebuah fungsi *help desk* di tempatkan, untuk mengurangi jumlah kesalahan dalam pengoperasian sistem.

PERENCANAAN PEMULIHAN BENCANA

Figure 2-6 menggambarkan 3 tipe kejadian yang dapat mengganggu sistem informasi dan komunikasi. Yakni bencana alam, bencana yang disebabkan oleh manusia dan kegagalan sistem. Bencana alam seperti: banjir, angin topan, gempa bumi, dan dapat menghancurkan pusat komputer dan SI walaupun kemungkinannya kecil. Kadang-kadang kejadian bencana alam tidak dapat dihindari. Dengan perencanaan yang hati-hati akibat bencana alam dapat dikurangi dan organisasi dapat pulih kembali. Bencana yang dibuat oleh manusia seperti sabotase dan error dapat menghancurkan. Kegagalan sistem seperti kekurangan listrik sangat jarang terjadi tapi cukup menghancurkan. Berikut beberapa pencegahan untuk mengantisipasi bencana:

1. Indetifying critical applications

2. Membuat tim pemulihan bencana



3. Providing Site Backup

   Hal yang penting dalam DRP adalah menyediakan duplikat fasilitas pemrosesan data jika terjadi bencana. Dari banyak pilihan yang tersedia salah satunya adalah hotsite (Recovery Operations Center), cold site (empty shell) back up yang tersedia secara internal dan yang lainnya.

   - Hot Site/ Recovery Operation Center

     Salah satu pendekatan untuk membuat situs beckup adalah melengkapi dengan Hot side atau recovery operation center. Karena investasi yang besar, hot site biasanya dibagi dengan perusahaan lain. Perusahaan-perusahaan ini membeli saham atau menjadi pelanggan hot site, membayar biaya bulanan. Pendekatan ini memiliki resiko apabila bencana alam yang luas akan mempengaruhi banyak perusahaan dalam area geografis yang sama. Jika beberapa perusahaan berbagi ROC yang sama, banyak perusahaan yang akan terpengaruh.

     Kelebihan hot site dibanding cold site adalah waktu pemulihan yang jauh lebih singkat. Hot site memiliki fasilitas, furniture, hardware dan bahkan sistem operasi. Apabila terjadi masalah besar, pelanggan(perusahaan) dapat memiliki aset-asetnya dan dalam beberapa jam dapat melanjutkan proses aplikasi peting.

   - Cold site/empty shell

     Dalam model ini hanya beberapa perusahaan menyewa atau membeli gedung dan menjadikannya tempat komputer tapi tanpa komputer dan perlengkapannya.

Sebagai contoh, shell biasanya dilengkapi dengan lantai tinggi dengan AC. Jika terjadi bencana, shell tersedia dan siap untuk menampung hardware untuk menjalankan sistem operasi data yang penting.

- Mutual Aid Pact

  Adalah perjanajian antara dua atau lebih organsisasi (dengan fasilitas komputer yang komaptibel) untuk saling membantu dengan pemrosesan data yang mereka butuhkan pada saat terjadi bencana. Ketika terjadi bencana, perusahaan host harus memutus jadwal pemrosesannya untuk memproses aplikasi penting perusahaan yang terkena musibah. Hal ini berdampak pada perusahaan host harus memposisikan diri dalam mode daurat (dan memotong pemrosesan aplikasi prioritas rendah) untuk mengakomodasi peningkatan permintaan sumber daya IT yang tiba-tiba.

  Perjanjian timbala balik seperti ini merupakan pilihan yang populer. Karena relatif cost-free (selama tidak terjadi bencana) dan nyaman secara psikologis.

- Internally Provided Backup.

  Organisasi yang besar dengan pusat pemrosesan data yang banyak lebih memilih membuat sendiri dengan membuat internal excess capacity. Pilihan ini memungkinkan perusahaan untuk mengembangkan susunan hardware dan software standar yang akan memastikan kecocokan fungsi antarpusat pemrosesan data dan meminimisasi masalah ketika terjadi bencana. Pada dasarnya, internally provided backup mirip dengan mutual aid pact tapi antar cabang dalam entitas yang sama.

- Hardware Backup. Jika menggunakan metode cold site, entitas harus memastikan hardware komputer tersedia ketika keadaan darurat.
- Software Backup: Operating System. Jika menggunakan metode cold site yang tidak yang tidak menyertakan operating system (O/S), maka DRP harus menyediakan prosedur untuk membuat copy-an sistem operasi entitas yang siap di akses ketika terjadi bencana.
- Bacup Backup: Applications. Berdasarkan tahap aplikasi-aplikasi kritis DRP harus terdiri dari suatu prosedur untuk menyediakan copyan atau cetakan dari sofware aflikasi-aflikasi kritis. Sekali lagi prosedur ini dapat diselesaikan dengan menyediakan copy an yang cukup untuk aplikasi-aplikasi kritis atau pada tempat backup.
- Back up Data File. Data base harus dicopy setiap harinya dengan kapasitas yang besar, media kecepatan tinggi seperti CD/DVD. Bahkan dalam suatu gangguan, rekonstruksi dari data base diterima dengan update terbaru. Demikian dengan file induk dan file transaksi harus dilindungi.
- Backup Dokumentasi. Sistem untuk dokumentasi aflikasi-aflikasi penting harus di backup dan disimpan didata lain dengan perlakuan yang sama. Jumlah bahan yang besar dan revisi aplikasi secara terus menerus membuat tugas menjadi rumit. Proses dapat menjadi lebih efisien dengan menggunakanalat dokumentasi CASE. DRP harus menyediakan provisi untuk copy-an panduan pengguna agar tersedia.
- Backup Supplies and Source Documents. Perusahaan harus menyediakan backup inventori supplies dan sumber dokumen yang digunakan dalam aplikasi penting. Contoh supplies penting adalah saham, faktur, order pembelian dan formulir untuk tujuan tertentu yang tidak bisa diperoleh dengan cepat.

- Testing the DRP. Sebagaian besar aspek perencanaan contigancy yang diabaikan adalah pengujian rencana. Akan tetapi kemudian DRP penting dan harus dilaksanaakan secara periodik. Pengujian mengukur ksiapan personel dan mengidentifikasikan penghapusan *atau bottlenecks* dalam rencana.

Audit Objective:

- Menverifikasi bahwa rencana pemulihan bencana (DRP) organisasi sesuai untuk memenuhi kebutuhan organisasi dan pengimplimasiannya menguntungkan dan praktis.

Audit Procudures:

- Menverifikasi bahwa DRP manajemen merupakan sebuah solusi yang realistis untuk perjanjian terhadap bencana alam yang dapat menghalangi organisasi dari sumberdaya komputernya. Fokus pengujian berikut pada perhatian area-area yang paling besar.

PENGENDALIAN TOLERANSI KEGAGALAN

Fault tolerance adalah kemampuan sistem untuk meneruskan (continue) operasi ketika bagian dari sistem gagal disebabkan oleh kegagalan, aplikasi program yang eror, atau kesalahan operator. Berbagai tingkatan toleransi kesalahan dapat dicapai dengan mengimplementasikan komponen sistem yang berlebihan (redudant):

1. *Redudant arrays of inexpensive (or independent) disks* (RAID). Ada beberapa jenis konfigurasi RAID. Pada dasarnya, setiap metode meliputi penggunaan parallel disks yang berisi elemen data redudant (yang berlebihan) dan aplikasi-aplikasi.
2. *Uninterruptible power supplies.* Pada peristiwa kekurangan (outage) daya, jangka waktu baterai yang pendek daya *backup* disediakan untuk membenarkan sistem untuk berhenti bekerja (shut down) pada cara yang dikendalikan.
3. *Multiprocessing.* Penggunaan yang simultan (bersamaan) dari dari dua atau lebih *prossecors* meningkatkan *throughput* dibawah operasi normal.

Pengimplementasian pengendalian toleransi kesalahan yang tidak ada satu titik kegagalan sistem yang potensial. Total kegagaglan dapat terjadi hanya pada kejadian kegagalan komponen-komponen *multiple*.

Audit Objective

- Memastikan bahwa organisasi (sedang) menggunakan tingkat toleransi kesalahan yang sesuai.

Audit Procedures

- Sebagian besar sistem yang menggunakan RAID menyediakan sebuah pemetaan grafik (graphical mapping). Dari pemetaan ini, auditor harus menentukan apakah tingkat RAID ditempatkan sesuai untuk organisasi, tingkatan resiko bisnis yang telah ditentukan berhubungan dengan kegagalan disk.
- Jika organisasi tidak (sedang) menggunakan RAID, potensial untuk satu titik kegagalan sistem yang ada. Auditor harus mereview dengan administrator sistem prosedur-prosedur alternatif untuk pemulihan dari sebuah kegagalan disk.
- Menentukan behwa salinan-salinan *boot disks* telah dibuat untuk setiap server dalam jaringan pada kejadian kegagalan sektor *boot.*

PENGENDALIAN SISTEM OPERASI DAN PENGENDALIAN SISTEM KESELURUHAN

Operating system (OS) adalah program pengendalian komputer. OS membenarkan pengguna untuk membagi dan mengakses sumberdaya komputer yang umum, seperti *processors*, *main memory*, *database*, dan *printers*. Akuntan modern butuh untuk mengakui peran *operating system* dalam keseluruhan gambaran pengendalian untuk menaksir resiko-resiko dengan tepat yang mengancam sistem akuntansi.

Operating system melaksanakan tiga tugas utama. Pertama, OS menerjemahkan bahasa tingkat tinggi, seperti COBOL, BASIC, C languages, dan SQI, kedalam bahasa tingkat mesin yang mana komputer dapat execute (melaksanakan suatu instruksi). Kedua, OS mengalokasikan sumberdaya komputer ke para pengguna, *workgroups*, dan aplikasi-aplikasi. Ketiga, OS mengatur (manages) tugas-tugas penjadwalan pekerjaan dan banyak pemrograman (multiprogramming).

Untuk melaksanakan tiga tugas secara konsisten dan dapat diandalkan, operating system harusmencapai lima tujuan pengendalian fundamental:

1. Operating system harus melindungi dirinya sendiri dari para pengguna
2. Operating system harus melindungi para pengguna dari satu sama lain
3. Operating system harus melindungi para pengguna dari diri mereka sendiri
4. Operating system harus dilindungi dari dirinya sendiri
5. Operating system harus dilindungi dari lingkungannya

KEAMANAN SISTEM OPERASI

Operating system security meliputi kebijakan, prosedur dan pengendalian yamg menentukan siapa yang dapat mengakses operating system, yang mana sumberdaya (files, programs, printers) yang dapat mereka akses, dan tindakan apa yang dapatmereka ambil. Berikut ini komponen-komponen yang ditemukan pada operating system yang aman:

Logon Procedure

Sebuah logon procedure yang formal adalah garis pertahanan (defense) pertama operating sistem terhadap akses yang tidak diotorisasi. Ketika pengguna memulai proses, dia disajikan dengan sebuah kotak dialog yang meminta ID dan *password* pengguna. Sistem tersebut membandingkan ID dan *password* ke *database* sah pengguna.

Access Token

Jika usaha logon sukses, operating sistem menciptakan sebuah tanda (bukti) yang berisi informasi kunci mengenai pengguna, temasuk ID pengguna, password, user group, dan hak istimewa yang diberikan kepada pengguna. Informasi dalam tanda (bukti) akses yang digunakan untuk mengesahkan semua tindakan yang diusahakan oleh pengguna selama session (pembahasan).

Access Control List

Akses ke sumberdaya sistem seperti *directories*, *files*, *programs* dan *printers* dikendalikan oleh sebuah daftar (catatan) akses pengendalian yang ditugaskan ke setiap

sumberdaya. Ketika pengguna berusaha untuk akses sumberdaya, sistem membandingkan ID nya dan hak istimewa yang terkandung pada tanda (bukti) akses dengan yang terkandung pada catatan (list) aksespengendalian.

Discretionary Access Control

Administrator pusat sistem biasanya menentukan siapa yang memberikan akses ke sumberdaya khusus dan mempertahankan catatan akses pengendalian. Dalam sistem yang terdistribusi, meskipun demikian, sumberdaya dapat dikendalikan oleh pengguna akhir. Para pemilik sumberdaya pada *setting* ini dapat diberikan akses pengendalian yang bebas untuk menentukan, yang membenarkan mereka untuk memberikan akses hak istimewa ke para pengguna yang lainnya.

ANCAMAN-ANCAMAN TERHADAP INTEGRITAS SISTEM OPERASI

Sasaran sistem operasi terkadang tidak tercapai dikarenakan adanya ancaman sistem operasi itu sendiri, baik secara disengaja maupun tidak disengaja.

- *Accidental threats*
  Contoh: kegagalan hardware yang menyebabkan sistem operasi error
- *Intentational threats*
  Ancaman yang disengaja seperti akses data illegal atau melanggar privacy pemakai untuk keuntungan financial.

Intentational threat dapat datang dari 3 sumber, yaitu:

1. Individu yang memliki hak akses istimewa menyalahgunakan hak istimewa yang mereka miliki.
2. Individu yang mengotak-atik sistem operasi dengan tujuan merusak sistem keamanan operasi.
3. Individu yang sengaja memasukkan virus atau bentuk lainnya yang dapat merusak program sistem operasi.

PENGENDALIAN KESELURUHAN SISTEM

Membahas mengenai pengendalian sistem.

PENGENDALIAN HAK AKSES

Merupakan hak istimewa untuk mengakses tugas invidual atau seluruh tugas yang diotorisasi oleh sistem. Hak istimewa meliputi petunjuk, file, aplikasi dan berbagai sumber-baik akses ke individu maupun secara keseluruhan. Manajemen harus memastikan bahwa individu telah melakukan segala sesuatu yang merupakan tugasnya. Misalnya saja, juru tulis diberi kuasa untuk mengakses dan diperbolehkan melakukan perubahan dalam piutang dagang.

Audit Objective:

- Memeriksa bahwa hak istimewa telah diberikan secara konsisten dengan kebutuhan untuk pemisahan fungsi dan sejalan dengan kebijakan organisasi.

Audit procedure:

- Meninjau ulang kebijakan-kebijakan organisasi untuk memisahkan fungsi-fungsi yang bertentangan dan memastikan bahwa fungsi-fungsi tersebut layak.

- Meninjau ulang hak istimewa dari suatu pemilihan grup pengguna dan individu untuk menentukan jika hak akses mereka sesuai dengan diskripsi tugas dan posisi-posisi mereka. Auditor harus memeriksa bahwa individu yang memiliki hak istimewa mengakses data dan program sebatas yang mereka perlu ketahui.
- Meninjau ulang catatan personalia untuk menentukan apakah karyawan yang memiliki hak istimewa telah menjalani izin keamanan intensive yang cukup dalam memenuhi kebijakan perusahaan.
- Meninjau ulang catatan personal untuk menentukan apakah pegguna secara formal pada umumnya memahami adanya tanggung jawab untuk/ memelihara kerahasiaan data perkumpulan.
- Meninjau ulang pemberian izin. Pemberian izin harus sesuai dengan tugas yang sedang dikerjakan.

PENEGNDALIAN PASSWORD

Password adalah kode rahasia yang dimasukkan oleh pemakai untuk dapat mengakses sistem, aplikasi, file data, atau sebuah jaringan server. Apabila pemakai tidak dapat memberikan password yang benar, sistem operasi akan menunda akses. Walaupun password dapat memberikan keamanan, bila membebankan pada nonsecurityminded pemakai, prosedur password dapat mengakibatkan kesulitan dalam akses sistem operasi itu sendiri. Keadaan yang sering terjadi berkaitan dengan penggunaan password:

1. Password lupa dan sistem menjadi terkunci
2. Terlalu sering mengganti password dapat menjadi kelemahan
3. Setelah syndrome, dengan bantuan password sama dengan menulis dan menunjukkan untuk dilihat
4. Password dapat dengan mudah mengantisipasi kejahatan dengan menggunakan komputer.

Reusable Password

Metode yang paling banyak digunakan untuk pengawasan password adalah *reusable password*. Pemakai menetapkan password sekali kepada sistem dan kemudian digunakan kembali untuk mendapat akses di masa datang. Sistem operasi yang sering digunakan hanya mengatur standar utama untuk menerima password. Kualitas dari keamanan ditetapkan oleh reusable password tergantung pada kualitas password itu sendiri. Alternatif penggunaan reusable password adalah one-time password.

One time password

Pemakai on-time password hanya memasukkan password sekali. Salah satu teknologi yang menggunakan one time password adalah smart card.

Password policy

Eksekutif manajemen dan manajemen information sistem sebaiknya memikirkan kebijakan password yang efektif berdasar pada resiko dan pengawasan. Kebijakan dimulai dengan komunikasi yakni manajemen harus yakin semua pekerja dan pemakai mengetahui tentang kebijakan password. Panjang password harus ditentukan,

Audit objectives

Memastikan bahwa organisasi memiliki kebijakan password yang memadai dan efektif untuk pengaturan akses ke sistem operasi.

Audit procedures

- Memeriksa apakah semua pemakai telah memiliki password
- Memeriksa apakah pemakai baru telah diajarkan cara penggunaan password dan pentingnya pengaturan password.
- Menentukan prosedur-prosedur yang ditempatkan untuk mengidentifikais kelemahan passwords
- Menilai kecukupan standar password seperti lamanya dan waktu berakhirnya
- Mereview kebijakan dan prosedur akun *lokout.*

PENGENDALIAN TERHADAP OBYEK YANG MERUSAK DAN RISIKO E-MAIL

Surat elektronik (e-mail) merupakan fungsi internet yang paling popular, dan jutaan surat berputar ke seluruh dunia tiap hari.Kebanyakan organisasi menerima e-mail, walaupun mereka tidak memiliki servers e-mail sendiri. Tetapi e-mail memberikan resiko yang melekat hal itulah yang harus dipertimbangkan oleh auditor. Resiko yang paling rentan menyerang perusahaan adalah munculnya virus atau worm. Penyebaran virus biasa melalui attachments ke e-mail. Virus bertanggungjawab atas kerugian perusahaan yang mencapai jutaan dollar tiap tahunnya. Kerugian terjadi karena virus merubahan dan menghancurkan data, menurunkan performa komputer, rusaknya hardware, pelanggaran rahasia, dan menyediakan waktu untuk memperbaiki kerusakan.

Virus

Virus komputer merupakan program komputer yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menyisipkan salinan dirinya ke dalam program atau dokumen lain. Virus komputer dapat dianalogikan dengan virus biologis yang menyebar dengan cara menyisipkan dirinya sendiri ke sel makhluk hidup. Virus komputer dapat merusak (misalnya dengan merusak data pada dokumen), membuat pengguna komputer merasa terganggu, maupun tidak menimbulkan efek sama sekali.

Virus komputer umumnya dapat merusak perangkat lunak komputer dan tidak dapat secara langsung merusak perangkat keras komputer dengan cara memuat program yang memaksa over process ke perangkat tertentu misalnya VGA, Memory bahkan Procesor. Efek negatif virus komputer terutama adalah perbanyakan dirinya sendiri, yang membuat sumber daya pada komputer (seperti *CPU Time*, penggunaan memori) menjadi berkurang secara signifikan. Serangan virus dapat dicegah atau ditanggulangi dengan menggunakan perangkat lunak antivirus. Jenis perangkat lunak ini dapat juga mendeteksi dan menghapus virus komputer, asalkan basis data virus komputer yang dimiliki oleh perangkat lunak antivirus telah mengandung kode untuk menghapus virus tersebut. Contoh virus antara lain Worm, Trojan, dll. Contoh antivirus yang bisa diandalkan dan menangkal virus adalah KasperSky, AVG, AntiVir, PCMAV, Norton, Norman, dan McAfee.

Worm

Worm atau cacing komputer dalam keamanan komputer, adalah sebutan untuk sebuah program yang menyebarkan dirinya di dalam banyak komputer, dengan menggandakan dirinya

dalam memori setiap komputer yang terinfeksi. Sebuah worm dapat menggandakan dirinya dalam sebuah sistem komputer sehingga dapat menyebabkan sistem tersebut mengalami *crash* sehingga mengharuskan server harus di-*restart*. Beberapa worm juga menghabiskan *bandwidth* yang tersedia. Worm merupakan evolusi dari virus komputer.

Virus komputer memang dapat menginfeksi berkas-berkas dalam sebuah sistem komputer, tapi worm dapat melakukannya dengan lebih baik. Selain dapat menyebar dalam sebuah sistem, worm juga dapat menyebar ke banyak sistem melalui jaringan yang terhubung dengan sistem yang terinfeksi. Beberapa worm, juga dapat mencakup kode-kode virus yang dapat merusak berkas, mencuri dokumen, e-mail, atau melakukan hal lainnya yang merusak, atau hanya menjadikan sistem terinfeksi tidak berguna.

Beberapa contoh dari worm adalah sebagai berikut:

- ADMw0rm: *Worm* yang dapat melakukan ekspolitasi terhadap layanan jaringan Berkeley Internet Name Domain (BIND), dengan melakukan *buffer-overflow*.
- Code Red: *Worm* yang dapat melakukan eksploitasi terhadap layanan Internet Information Services (IIS) versi 4 dan versi 5, dengan melakukan serangan *buffer-overflow*.
- LoveLetter: Worm yang menyebar dengan cara mengirimkan dirinya melalui e-mail kepada semua akun yang terdaftar dalam Address Book Microsoft Outlook Express/daftar kontak dalam Microsoft Outlook dengan cara menggunakan kode Visual Basic Script (VBScript).
- Nimda
- SQL-Slammer

LOGIC BOMB

Salah satu program jahat yang ditempelkan pada program komputer agar memeriksa suatu kumpulan kondisi di sistem. Ketika kondisi-kondisi yang dimaksud ditemui, logic bomb mengeksekusi suatu fungsi yang menghasilkan aksi-aksi tak diotorisasi. Logic bomb menempel pada suatu program resmi yang diset meledak ketika kondisi-kondisi tertentu dipenuhi. Contoh kondisi-kondisi untuk memicu logic bomb adalah ada atau tidak adanya file tertentu, hari tertentu dari minggu atau tanggal, atau pemakai menjalankan aplikasi tertentu. Begitu terpicu, bomb mengubah atau menghapus data atau seluruh file, menyebabkan mesin berhenti, atau mengerjakan perusakan lain.

BACKDOOR/TRAP DOOR

Trapdoor adalah kode yang menerima suatu barisan masukan khusus atau dipicu dengan menjalankan ID pemakai tertentu atau barisan tertentu. Trapdoor menjadi ancaman ketika digunakan pemrogram jahat untuk memperoleh pengaksesan tak diotorisasi.

TROJAN HORSE

Trojan Horse adalah sebuah program komputer yang dibalik fungsinya/kegunaan yang terlihat juga memiliki fungsi tambahan tersembunyi (sengaja disembunyikan oleh pembuatnya) yang akan mengeksploitasi komputer yang menggunakannya serta secara signifikan akan menurunkan tingkat keamanan komputer. Program trojan horse digunakan untuk melakukan fungsi-fungsi secara tidak langsung dimana pemakai tak diotorisasi tidak dapat melakukannya

secara langsung. Contoh untuk dapat mengakses file-file pemakai lain pada sistem dipakai bersama, pemakai dapat menciptakan program trojan horse. Trojan horse ini ketika program dieksekusi akan mengubah ijin-ijin file sehingga file dapat dibaca oleh sembarang pemakai. Program trojan horse yang sulit dideteksi adalah kompilator yang dimodifikasi sehingga menyisipkan kode tambahan ke program-program tertentu ketika dikompilasi, seperti program login. Kode menciptakan Trapdoor pada program login yang mengijinkan pencipta log ke sistem menggunakan password khusus. Trojan horse ini tak pernah dapat ditemukan jika hanya membaca program sumber. Motifasi dari trojan horse adalah penghancuran data. Program muncul sebagai melakukan fungsi-fungsi berguna, seperti kalkulator, tapi juga secara diam-diam menghapus file-file pemakai. Trojan horse biasa ditempelkan pada program-program atau rutin-rutin yang diambil dari BBS, internet, dan sebagainya.

Spoofing

Pemalsuan IP Address untuk menyerang sebuah server di internet, kegiatan ini biasanya dilakukan oleh para hacker/cracker.

Spamming

Spamming adalah pengiriman mail yang mungkin tidak diinginkan/tidak disukai penerima email. Posting yang sering mengakibatkan SPAMMING, misalnya: berita warning virus, media buyer, multi level marketing, surat berantai, surat yang tidak berarti (junk mail), bomb mail (mengirim email sama berulang-ulang) dan hoax email (email bohong, dari sumber yang tidak jelas). Tujuan dari Spamming merupakan kegiatan "nakal" lainnya di Internet seperti hacking, cracking, carding.

Chain letters

Surat berantai, yaitu surat yang dikirimkan kepada seseorang untuk dikirim lagi ke penerima yang lain. Surat berantai sebagian besar berisi berita-berita yang tidak dapat dipertanggungjawabkan isinya. Cara penyebarannya surat berantai dalam surat berantai biasanya menawarkan ganjaran uang atau keberuntungan yang akan kita terima jika kita meneruskan email tersebut kepada orang kita kenal. Mereka menakuti kita dengan ancaman “bad luck” dan konsekuensi yang akan kita terima kalau kita tidak meneruskan surat tersebut.

Urban Legends

Contoh dari urban legends adalah percakapan antara kapten kapal dengan kapal lain yang ia kira berada dalam jalur tabrakan. Masing-masing meperdebatkan siapa yang harus keluar dari jalur. Akhirnya orang kedua menginformasikan kepada kapten kapal bahwa dia bukanlah kapten kapal melainkan penjaga mercusuar.Pada umumnya cerita ini menarik, dan baris terakhir pada pesan menganjurkan penerima untuk mengirim pesan tersebut kepada teman-temannya.

Hoax Virus Warning

Pada dasarnya hoax memiliki kesamaan dengan chain letters perbedaannya dalam hoax tidak memberikan ganjaran uang atau keberuntungan yang akan diterima bila mengirimkan pesan kepada orang yang dikenalnya. Trik dari hoax virus warning adalah memberikan peringatan tentang konsekuensi yang serius akibat virus, dan pada akhir pesan membuat seruan untuk memberitahukan semua teman sebelum mereka terinfeksi. Dengan membuat pernyataan tersebut penulis mempunyai tujuan untuk mengedarkan pesannya ke seluruh duniia

Flamming

Kelakuan manusia dalam internet tidak dapat dibatasi untuk melakukan interaksi. Karena itu, kebanyakan melakukan atau menulis sesuatu yang tidak mereka lakukan di depan umum. Flamming adalah pesan yang dibuat penulis untuk menyerang partisipan lain dengan sangat kasar dan sering menyangkut hubungan perorangan. Flamming juga memasukkan kata-kata yang menghina orang lain atau suatu organisasi. Resiko dari flaming lebih serius karena undang-undang federal mengatur mengenai pokok persoalan seperti pelecehan seksual. Pengawasan akan memasukkan pendidikan dan kebijakan melarang flaming dengan konsekuensinya.

Audit Objective

- Memeriksa efektifitas kebijakan manajemen dan prosedur untuk mencegah pengenalan dan penyebaran tujuan untuk merusak.

Audit Prosedures

- Melakukan tanya jawab dengan personil operasi, memastikan mereka telah mengerti tentang virus komputer dan mengetahui resiko menggunakan komputer serta penyebaran virus dan program jahat lainnya.
- Memeriksa prosedur operasi untuk memastikan jika CD yang rutin digunakan untuk memindahkan data antar kelompok kerja tidak berisi virus.
- Membuktikan bahwa sistem pengelola rutin melakukan scan workstation pada file server, email server dari serangan virus.
- Membuktikan software yang baru telah diperikasa sesuai standalone yang diimplementasikan pada host atau network server.
- Membuktikan bahwa software antivirus telah diperbaharui dengan jarak yang teratur dan didownload untuk pusat kerja per-individu.

PENGENDALIAN JEJAK AUDIT ELEKTRONIK

Audit trails adalah logs yang dapat dirancang untuk catatan aktivitas pada sistem, aplikasi dan tingkat pengguna. Ketika diimplementasikan dengan tepat, audit trail menyediakan pengendalian detektif untuk membentu mencapai tujuan kebijakan keamanan. Audit trail terdiri dari dua jenis audit *logs*, yaitu: (1) detailed logs of individual keystrokes, dan (2) event-orientd logs.

Keystroke Monitoring

Keystroke monitoring meliputi pencatatan *keystrokes* pengguna dan respon system. Bentuk log ini dapat digunakan setelah bukti (fact) untuk merekonstruksi rincian kejadian atau sebagai pengendalian *real-time* untuk memonitor atau mencegah instruksi yang tidak diotorisasi.

Event Monitoring

Event Monitoring meringkaskan aktivitas kunci berkaitan dengan pengguna, aplikasi dan sumberdaya sistem. Event logs khususnya mencatat ID semua pengguna yang mengakses sistem; wakti dan durasi *session* pengguna; program yang dijalankan selama *session*; dan *file-file*, *database*, *printer* dan sumberdaya yang diakses lainnya.

Audit Trail Objectives

Audit trail dapat digunakan untuk mendukung tujuan keamanan dalam tiga cara:

1. Mendeteksi akses ke sistem yang tidak diotorisasi
2. Menfasilitasi rekonstruksi kejadian-kejadian
3. Mempromosikan akuntabilitas *personal*

Implementing an Audit Trail

Informasi yang terkandung pada *audit logs* berguna bagi akuntan dalam mengukur potensial bencana dan kerugian finansial yang berhubungan dengan eror, penyalahgunaan wewenang, atau akses yang tidak diotorisasi oleh pengganggu luar. *Audit logs*, bagaimanapun juga dapat menghasilkan data pada *overwhelming detail*.

Audit Objective

- Memastikan bahwa pengauditan pengguna dan kejadian memadai untuk mencegah dan mendeteksi penyalahgunaan, rekonstruksi kejadian-kejadian kunci yang mendahului kegagalan sistem dan merencanakan alokasi sumberdaya.

Audit Procedures

Sebagian besar sistem operasi menyediakan beberapa bentuk fungsi-fungsi manajer audit untuk menentukan kejadian-kejadian yang diaudit. Auditor harus menverifikasi bahwa kejadian audit *trail* telah diaktifkan sesuai dengan tujuan organisasi.

- Banyak sistem operasi yang menyediakan sebuah *audit log viewer* yang membenarkan auditor untuk *scan log* untuk aktivitas yang tidak biasa.
- *Security group* organisasi memiliki memonitor dan melaporkan pelanggaran-pelanggaran keamanan. Auditor harus memilih sebuah contoh kasus pelanggaran keamanan dan mengevaluasi *disposition* mereka untuk mengakses keefektifan *security group.*

SISTEM KOMPUTER PERSONAL

Bagian dari chapter ini memeriksa resiko , pengendalian, dan poko persoalan audit yang berkaitan dangan *personal computer enviroment*. *PC environment* memiliki fitur-fitur yang signifikan.

SISTEM OPERASI PC

Operating system di *boot* dan berada pada *memory* utama komputer selama OS dinyalakan. *Operating system* memiliki beberapa fungsi. OS mengendalikan CPU, accesses, RAM, menjalankan program, menerima input dari *keyboard* atau alat input lainnya, mendapatkan kembali dan meyimpan data ke dan dari *secondary storage devices*, menampilkan data pada monitor, mengendalikan *printer*, dan melaksanakan fungsi-fungsi lainnya yang mengendalikan sistem hardware.

Operating system terdiri dari dua jenis instruksi. *System-resident commands* aktif pada *memory* utama pada seluruh waktu untuk mengkoordinasikan permintaan input/output dan melaksanakan program. *Disk resident commands* berada pada sebuah *secondary storage device* sampai permintaan dibuat untuk melaksanakan *special purpose utility programs* ini.

RISIKO DAN PENGENDALIAN SISTEM PC

Ada banyak resiko yang baru dan berbeda yang berhubungan dengan PC:

Risk Assessment
PC memperkenalkan banyak tambahan resiko atau resiko yang berbeda. Oleh karena itu, auditor harus menganalisis semua aspek-aspek PC untuk memastikan resiko spesifik untuk organisasi sebagai subyek, berhubungan dengan PC. Pada beberapa hal, resiko berhubungan dengan lingkungan PC akan tersisa suatu pembukaan (exposure), karena tak satu pun *cost effective* dapat dibuat mengenai resiko.

Inherent Weaknesses
PC hanya menyediakan keamanan minimal lebih dari (pada) *file-file* data dan program. Kelemahan pengendalian ini merupakan bawaan dibalik filosofi rancangan sistem operasi PC. Pada mulanya diperuntukkan sebagai sistem pengguna tunggal, mereka dirancang untuk membuat penggunaan komputer mudah dan untuk memudahkan akses, tidak membatasinya. Filosofi ini sewaktu diperlukan untuk mempromosikan *end-user computing,* kadang-kadang ke arah perbedaan dengan tujuan pengendalian internal.

Weak Access Control
Keamanan software yang meyediakan prosedur logon tersedia untuk PC. Sebagian besar program, bagaimanapun, menjadi aktif hanya ketika komputer di boot dari *hard drive.* Kejahatan komputer berusaha untuk menghindari (mengakali) prosedur logon yang dapat dilakukan dengan memaksa komputer untuk *boot* dari A: drive, atai CD-ROM drive, dengan jalan sebuah sistem operasi yang tidak dikendalikan dapat di *load* kedalam *memory* komputer. Pemilikan jalan pintas sistem operasi komputer yang tersimpan dan paket keamanan, kejahatan memiliki akses yang tidak terbatas ke data dan program pada *hard disk drive.*

Inadequate Segregation of Duties (Ketidaksesuaian pemisahan tugas)
Dalam lingkunga PC, terutama perusahaan-perusahaan kecil, seorang karyawan dapat memiliki akses ke banyak aplikasi yang memproses transaksi yang tidak sesuai. Sebagai contoh, satu orang individu dapat dipercaya untuk mencatat semua data transaksi, termasuk order penjualan, penerimaan kas, faktur-faktur, dan *disbursements*. Khususnya, buku besar dan rekening pembantu diperbaharui secara otomatis dari sumber-sumber input ini. Pembukaan (exposure) bertambah ketika ketika operator juga dipercaya untuk pengembangan (programming) aplikasi yang dia jalankan. Pada operasi perusahaan kecil, mungkin ada sdikit yang bisa dilakukan untuk mengeliminasi konflik bawaan dari tugas-tugas ini. Akan tetapi, pengendalian multilevel password bisa mengurangi resiko tersebut.

Multilevel Password Control
Pengendalian multilevel password digunakan untuk membatasi karyawan-karyawan yang berbagi komputer yang sama untuk direktori khusus, program-program dan file data. Karyawan diharuskan untuk menggunakan password yang lainnya pada tingkat sistem berbeda yang sesuai untuk memperoleh akses. Teknik ini menggunakan tabel-tabel otorisasi yang tersimpan untuk batasan lebih lanjut sebuah akses individu untuk hanya membaca, data input, modifikasi data, kemampuan pencoretan (deletion) data.

Risk of Physical Loss

Karena ukurannya, PC merupakan obyek pencurian. Kemudahan Laptop untuk dibawa menempatkannya pada resiko tertinggi. Prosedur-prosedur harus ditempatkan untuk pegangan para pengguna yang bertanggungjawab untuk pengembalian laptop.

Risk of Data Loss
Terdapat resiko kehilangan data karena kegagalan sistem, sabotase, hackers/crackers,dan lain-lain. Perhatian penuh harus dialihkan untuk melindungi data sebagai asset.

End User Risks
Pengguna akhir terhubung sistem jaringan yang memiliki peluang untuk dengan sengaja menghapus *hard drives*, korup atau sabotase nilai-nilai data, mencuri data dan dengan cara lain menyebabkan kejahatan serius terhadap data perusahaan pada lingkungan PC. Perhatian harus dialihkan untuk membatasi resiko ini dengan pengendalian seperti training dan menciptakan kebijakan efektif atas penggunaan komputer, termasuk menyatakan hukuman untuk pencurian atau penghilangan (penghancuran) data.

Inadequate Backup Procedures Risk
Untuk melindungi (mempertahankan) integritas misi kritis data dan program, organisasi membutuhkan prosedur *backup* formal. Tanggungjawab penyediaan backup pada lingkungan PC jatuh pada pengguna. Seringkali, karena kurangnya pengalaman dan training komputer, pengguna gagal untuk menyadari pentingnya prosedur backup sampai prosedur itu terlambat.
Kegagalan komputer, biasanya kegagalan *disk*, terutama disebabkan hilangnya data yang signifikan pada lingkungan PC. Prosedur formal untuk pembuatan salinan-salinan *backup* file-file data kritis (dan program) dapat mengurangi ancaman ini. Ada sejumlah pilihan yang tersedia berhubungan dengan masalah ini.

- *Local backups on appropriate media*. Media yang dapat digunakan untuk *back up* file-file data pada PC local termasuk floppy disk, CD-R/CD-RW (compact disks), DVDs dan Zip Disks.
- *Dual internal hard drives. Microcomputers* dapat dikonfigurasikan dengan dua *hard disks* fisik internal. Satu disk dapat digunakan untuk menyimpan data yang dihasilkan dan ketika penyimpanan yang lainnya *backup file-file*.
- *External hard drive.* Sebuah pilihan *backup* yang populer adalah *external hard drive* dengan *removable disk cartridge,* yang dapat menyimpan ber-*gigabyte* data per perantaraan (medium). *Medium devices* termasuk CD, DVD, dan *Zip disks*.

Risk Associated with Virus Infection
Dukungan yang tegas terhadap kebijakan dan prosedur organisasi yang terlindungi terhadap infeksi virus adalah kritis untuk pengendalian virus yang efektif. Auditor harus menverifikasi bahwa kebijakan dan prosedur yang ada dan bahwa kebijakan dan prosedur tersebut dipatuhi. Organisasi harus menggunakan pengendalian teknis tambahan dalam bentuk *software* anti virus.
Auditor dapat dapat memperoleh kecukupan bukti pendukung pengendalian virus dengan melaksanakan pengujian berikut ini:

- Auditor harus menverifikasi bahwa organisasi mematuhi kebijakan pembelian sotware hanya dari *vendor* yang memiliki reputasi baik.
- Auditor harus mereview kebijakan organisasi untuk penggunaan software anti virus.
- Auditor harus menverifikasi bahwa hanya software yang diotorisasi yang dipasang pada PC.

Risk of Improper System Development and Maintenance Procedures

Lingkungan *microcomputer* kekurangan fitur-fitur operating system dan pemisahan tugas-tugas yang penting untuk menyediakan pengendalian yang diperlukan. Management harus memberikan kompensasi untuk pembukaan (exposures) bawaan tersebut terhadap yang lainnya, pada teknik-teknik pengendalian yang lebih konvensional.

Perusahaan kecil harus menggunakan prosedur pemilihan software secara formal, yang mencakup langkah-langkah berikut ini :

1. Menyalurkan sebuah analisis formal dari permasalahan dan kebutuhan pengguna.
2. Meminta penawaran dari beberapa vendor.
3. Mengevaluasi produk-produk yang bersaing dengan syarat-syarat kemampuan produk untuk memenuhi kebutuhan yang diidentifikasi.
4. Menghubungi calon pengguna saat ini paket-paket komersial untuk mendapatkan opini mereka tentang produk tersebut.
5. Membuat pilihan.

Audit Objectives

- Menverifikasi bahwa pengendalian disusun untuk melindungi data, program, komputer dari akses yang tidak diotorisasi, manipulasi, perusakan, dan pencurian.
- Menverifikasi bahwa supervisi yang cukup dan prosedur-prosedur operasi yang ada untuk memberikan kompensasi sebagai pengganti lemahnya pemisahan antara fungsi-fungsi (tugas) para pengguna, programmer, dan operator.
- Menverifikasi bahwa prosedur *backup* disusun untuk mencegah hilangnya data dan program karena kegagalan sistem, eror, dan lain sebagainya.
- Menverifikasi bahwa prosedur pemilihan dan perolehan sistem menghasilkan aplikasi-aplikasi yang berkualitas tinggi, dan terlindungi dari perubahan yang tidak diotorisasi.
- Menverifikasi bahwa sistem tersebut bebas dari virus-virus dan cukup terlindungi untuk meminimalkan resiko menjadi terinfeksi dengan virus atau objek yang sejenis.

Audit Procedures

- Auditor harus menverifikasi bahwa *microcomputers* dan file-file mereka secara fisik terkendali.
- Auditor harus menverifikasi mulai dari bagan organisasi, *job descriptions*, dan observasi bahwa aplikasi-aplikasi programmer menjalankan fungsi-fungsi signifikan secara keuangan juga tidak mengoperasikan sistem tersebut.
- Auditor harus mengkonfirmasikan bahwa laporan-laporan transaksi yang diproses, catatan-catatan rekening yang diperbaharui, dan jumlah pengendalian yang disiapkan, didistribusikan, dan mencocokkan dengan manajemen yang sesuai pada interval yang teratur dan tepat waktu.
- Auditor harus menentukan bahwa pengendalian multilevel password digunakan untuk membatasi akses ke data dan aplikasi.
- Jika *removable hard drives* digunakan, auditor harus menverifikasi bahwa *drives* dipindahkan dan disimpan pada lokasi yang aman ketika tidak digunakan.
- Dari pemilihan contoh file-file backup, auditor dapat menverifikasi bahwa prosedur backup sedang ditelusuri. Dengan membandingkan nilai-nilai data dan tanggal-tanggal pada *backup*

disks untuk pembuatan file, auditor dapat menilai frekuensi dan kecukupan prosedur-prosedur backup.

- Auditor harus menverifikasi bahwa aplikasi kode sumber secara fisik aman (seperti pada peti besi yang terkunci) dan hanya versi yang tersusun disimpan pada *microcomputer*.
- Dengan mereview pengendalian pemilihan dan perolehan sistem, auditor harus menverifikasi bahwa paket software komersial digunakan pada *microkomputer* yang dibeli dari *vendor* yang bereputasi baik.
- Auditor harus mereview teknik-teknik pengendalian virus.