MODUL PERKULIAHAN

EDP Audit

DASAR-DASAR SISTEM KOMPUTER

(*Basic of Computing Systems*)

Abstract

Modul ini berisi tentang pembahagasn dasar-dasar komputer. Pengenalan terhadap komponen-komponen sebuah komputer.

Kompetensi

Mahasiswa mampu pememahami dan mengenali tetantang komponen komponen dasar sebuah perangkat komputer

Pengantar

Sebelum melakukan audit sistem komputasi atau menilai kecukupan audit yang dilakukan pada sistem komputasi, ada beberapa dasar yang salah satunya adalah harus memahami tentang bagaimana fungsi sistem komputasi. Sistem komputasi pada dasarnya terdiri dari tiga komponen dasar, yaitu unit pemroses sentral, sistem operasi, dan program aplikasi. Banyak sistem yang juga memiliki sistem keempat dimana data berada dan dikelola. Ini disebut sistem manajemen database. Masing-masing komponen ini dijelaskan dalam bagian berikut dari Modul ini.

Dasar-dasar Komputer

Sebelum melakukan audit sistem komputasi atau menilai kecukupan audit yang dilakukan pada sistem komputasi, ada beberapa dasar yang salah satunya adalah harus memahami tentang bagaimana fungsi sistem komputasi. Sistem komputasi pada dasarnya terdiri dari tiga komponen dasar, yaitu unit pemroses sentral, sistem operasi, dan program aplikasi. Banyak sistem yang juga memiliki sistem keempat dimana data berada dan dikelola. Ini disebut sistem manajemen database. Masing-masing komponen ini dijelaskan dalam bagian berikut dari Bab ini.

UNIT PEMROSES SENTRAL

Unit pemroses sentral (CPU) pada dasarnya adalah sebuah kotak yang saling berhubungan pada rangkaian elektronik. Ada ribuan CPU di dunia saat ini. Mereka termasuk mikrokomputer yang berdiri sendiri seperti keluarga komputer pribadi IBM dan klon mereka, keluarga mikrokomputer Apple Macintosh, komputer mini dan mid-range seperti IBM AS/400 dan Keluarga Compaq Alpha, mainframe komputer seperti IBM sistem serial 390, dan bahkan superkomputer eksperimental. Otak CPU ini adalah chip komputer. Antara lain hal-hal, chip menentukan kecepatan dan efisiensi dimana komputer beroperasi. Untuk chip komputer, kecepatan operasional biasanya diukur dalam megahertz (MHz) dan baru-baru ini dalam gigahertz (GHz) dan teraflops. Satu MHz setara satu juta operasi per detik. Satu GHz setara dengan satu miliar operasi per detik. Satu teraflop setara dengan operasi satu triliun per detik. Ada ratusan produsen chip komputer, baik besar maupun kecil. Beberapa produsen chip yang sangat terkenal termasuk IBM, Sun, Intel, Motorola, Hewlett Packard, Advanced Micro Devices, NEC, Hitachi, Compaq, Mitsubishi, dan Apple. Salah satu produsen chip computer yang paling banyak dikenal adalah Intel, pembuat keluarga chip Pentium® yang dipasang di banyak komputer pribadi dan file server. Chip Pentium 4 memungkinkan komputer pribadi untuk berjalan pada kecepatan lebih dari 2.5 GHz.

Sejarah Pengolahan Kecepatan

Pada Januari 1997, Intel meluncurkan chip komputer Pentium MMXTM, yang disebut-sebut untuk menjalankan program yang ada 10 sampai 20 persen lebih cepat daripada kecepatan prosesor yang sama sebelumnya. Program yang ditulis untuk mengambil keuntungan dari teknologi multimedia peningkat baru dilaporkan bisa

menjalankan 60 persen lebih cepat.[1] Di Juli 1997, Laptop Apple PowerBook® 3400 dilaporkan mampu berjalan dengan kecepatan hingga 235 MHz.[2]

Chip komputer dipasang di komputer komersial yang lebih canggih yang mencapai kecepatan di kisaran 300 sampai 500 MHz pada tahun 1997. Sebagai contoh, dalam Mei 1997, Intel memperkenalkan Pentium II®, prosesor generasi keenam yang dapat berjalan pada 300 MHz dan juga menggabungkan teknologi MMX. Chip ini didasarkan pada Pentium Pro®, sebuah chip penggunaan komersial yang kuat.[3] Pada tahun 1996, Digital diperkenalkan komputer menengah baru Alpha®. Chip Alpha, yang Sit-up 64 bit data pada satu waktu,[4] mampu mengolah pada 440 MHz. Pada Oktober 1996, pembuat chip komputer kecil mengumumkan bahwa telah mengembangkan sebuah chip yang dimaksudkan dapat mengoperasikan software Apple Macintosh hingga 533 MHz.[5]

Pada Desember 1996, berita dirilis dari sebuah superkomputer yang dikembangkan bersama oleh Intel dan Departemen Energi AS dapat berjalan dengan kecepatan melebihi satu teraflop, atau satu triliun operasi per detik.[6] Ini hampir tiga kali lebih cepat daripada rekor komputasi sebelumnya yang dipegang oleh Hitachi dari Jepang. Komputer $55 juta terutama untuk digunakan oleh para ilmuwan pemerintah di Sandia Laboratories di Albuquerque, New Mexico, untuk mensimulasikan tes senjata nuklir yang sekarang dilarang oleh perjanjian internasional.[7] Aplikasi ini mengurangi kebutuhan untuk meledakkan bahan peledak nuklir hidup untuk menilai kekuatan yang merusak mereka. Ini juga menghilangkan risiko kerusakan untuk manusia dan lingkungan, dan dengan demikian menghindari banyak konsekuensi politik yang terkait dengan pengujian nuklir hidup. Teknologi dapat diterapkan untuk aplikasi komersial yang memerlukan perhitungan berkecepatan tinggi. Contoh seperti aplikasi termasuk prakiraan cuaca dan pemetaan genetik. Kecepatan yang luar biasa dari superkomputer dicapai dengan mengelompokan 7,264 chip komputer highend Pentium Pro ke modul, menggunakan teknik yang disebut "komputasi paralel secara besar-besaran." Sistem akhirnya termasuk 9,200 chip komputer dan mampu beroperasi pada 1.4 teraflops. Menggunakan teknologi ini, Intel berharap dapat mengkonfigurasi jaringan untuk memanfaatkan kekuatan pemrosesan chips lebih jauh daripada sebelumnya, sehingga sangat jauh meningkatkan daya komputasi mereka. Pada tahun 2000, Intel berharap superkomputer mampu memecahkan batas tiga teraflop.

Sejak tahun 1997, produsen chip komputer terus mengikuti Hukum Moore, yang menegaskan bahwa kecepatan pemrosesan komputer akan berganda setiap 18 bulan. Salah seorang pendiri Intel, Gordon Moore berprediksi pada tahun 1965 bahwa masing-masing memori chip baru dapat melakukan proses dua kali lebih banyak seperti pendahulunya, dan setiap chip yang baru akan dirilis dalam waktu 18-24 bulan dari chip sebelumnya. Potongan artikel berikut mengenai teorema ini:

- Pada bulan Juni 2002, National Centers for Enviromental Prediction, sebuah divisi dari National Weather Service, memesan komputer IBM $224 juta yang akan mampu berjalan pada 100 teraflops.[8]
- Pada bulan April 2002, komputer Jepang NEC Earth Simulator memiliki 5,104 prosesor yang bisa mencapai kecepatan 35.6 teraflops. Ini mengalahkan rekor kecepatan komputer yang ada dari 7.2 teraflops yang dicapai oleh komputer ASCI White-Pasifik di Lawrence Livermore National Laboratory di California dengan menggunakan 7,424 processors.[9]
- Pada tahun 2002 IBM membuat microchip tunggal tercepat di dunia, yang berjalan lebih dari 100 GHz.[10]
- Pada tahun 2001 Intel merancang struktur baru untuk transistor (chips) yang menghilangkan masalah pembatasan kecepatan dari konsumsi daya dan panas. Chip dilaporkan dapat beroperasi pada satu terahertz, atau satu triliun operasi per detik.[11]
- Britain membeli sebuah superkomputer yang dibuat oleh Sun Microsystems yang memiliki memori setara dengan 11.000 CD-Rom dan berjalan pada 10 GHz.[12]
- Intel memperkenalkan dua chip tercepatnya, yang berjalan pada 1.8 dan 1.6 GHz, dan menawarkan sebuah chip 2 GHz pada kuartal ketiga tahun 2001.[13]
- Intel telah mengembangkan apa yang dikatakannya yaitu transistor tercepat dan terkecil yang pernah ada. Transistor baru hanya 20 nanometer, atau 0.02 mikron, dalam perbandingan ukuran chip 0.18 mikron yang digunakan saat ini. Terobosan ini berarti silikon dapat digunakan untuk membuat chip sampai setidaknya tahun 2007 dan akan membuat mikroprosesor yang munkgin mengandung hampir 1 miliar transistor yang berjalan pada 20 GHz pada tahun itu. Ini juga berarti bahwa hukum Moore akan tetap pada buku-buku sampai setidaknya 2007.[14]
- Advanced Micro Devices, Inc, memperkenalkan dua chip Athlon baru yang berjalan pada 1.2 dan 1.0 GHz.[15]
- Intel memperkenalkan prosesor yang lama ditunggu-tunggu, Pentium 4 yang berjalan pada 1,7 GHz.[16]
- Intel luncurkan chip Pentium 3 untuk laptop, yang berjalan pada 1 GHz.[17]
- Intel memperkenalkan dua chip Celeron yang berjalan pada 766 MHz dan 733 MHz.[18]
- Ilmuwan IBM berencana untuk menghabiskan lima tahun untuk membuat komputer tercepat di dunia. Komputer "Gen biru" akan 500 kali lebih cepat dari apa yang ada saat ini.[19]

- Apple meluncurkan komputer iMac baru yang berjalan pada 400 MHz dan 350 MHz.[20]
- IBM meluncurkan komputer mainframe baru berkecepatan tinggi yang berjalan pada 1.6 GHz. Komputer tersebut akan digunakan untuk memetakan gen manusia.[21]
- IBM telah mengembangkan dunia komputer tercepat yang mampu berjalan pada 3.9 teraflops untuk mensimulasikan peledakan nuklir.[22]

Masa Depan Pengolahan

Potensi kecepatan pemrosesan super komputer, dan nantinya komersial dan komputer konsumen, hanya dibatasi oleh jumlah ruang yang tersedia di dalam rumah komputer dan ukuran bahan yang digunakan untuk membuat chip. Teknologi konvensional menggunakan chip berbasis silikon. Namun, chip ini diproyeksikan mencapai potensi ukuran maksimal pada tahun 2010-2015. Yang baru, menjanjikan teknologi yang didasarkan pada teknologi quantum. Teknologi ini menggunakan atom-atom individu sebagai semikonduktor.

Hal ini menarik untuk mencoba memahami kemampuan potensi robot dan mesin berbasis komputer lainnya, yang dalam waktu dekat, bisa memiliki beberapa chip komputer berkecepatan tinggi yang dikumpulkan dengan cara yang memungkinkan kecepatan pengolahan lebih dari satu kuadriliun operasi per detik atau lebih. Hal ini hanya masalah waktu sebelum banyak peristiwa fiksi yang digambarkan dalam produksi seperti *Star Trek* dan *Star Wars* yang tidak lagi fiksi. Teleporting sudah mulai bereksperimen. Seperti kecepatan komputer yang semakin tinggi yang terlaksana di tempat kerja, auditor perlu memahami kemampuan potensi mereka dan bersiap untuk mengevaluasi kontrol dan keamanan atas mereka. Auditor juga perlu membantu organisasi memaksimalkan manfaat dari kemampuan pemrosesan komputer ini. Pemerintah perlu meminimalkan risiko-risiko dari teknologi seperti ini. Bayangkan kekacauan yang bisa terjadi dalam pertempuran dimana musuh dapat memindahkan bom dan bahkan pasukan di belakang garis masing- masing dan bahkan ke markas masing-masing. Perlombaan untuk teknologi yang benar- benar aktif.

Memori Komputer

Komponen CPU lain menentukan jumlah memori yang tersedia dalam komputer tertentu. Memori biasanya diukur dalam hal jumlah byte data yang dapat disimpan dalam memori pada satu waktu. Dua tipe utama dari memori yang biasanya berkaitan dengan komputer adalah memori pengolahan dan memori penyimpanan. Memori pengolahan sering

disebut sebagai *random access memory* (RAM) atau memori sementara. Jumlah RAM yang tersedia di komputer biasanya dinyatakan dalam megabyte (MB). Pada tulisan ini, komputer rumah ritel baru membanggakan ukuran RAM yang tersedia hingga 512 MB. Manfaat lebih RAM komputer, semakin banyak aplikasi akan dapat memproses secara bersamaan, sehingga memungkinkan pengguna untuk beralih dari satu aplikasi ke yang lain tanpa perlu keluar dari aplikasi sebelumnya. Setelah komputer dimatikan atau kekuatan terganggu, sebagian besar informasi yang berada dalam RAM tidak ditahan, maka diistilahkan memori sementara. Banyak yang telah menemukan hal ini dengan cara yang sulit ketika sistem mereka turun dan mereka tidak menyimpan pekerjaan yang baru saja dikerjakan. Setelah beberapa contoh kehilangan jam kerja karena saya tidak menyimpan, saya mengembangkan kebiasaan untuk menyimpan setiap 5 sampai 10 menit baik hard drive dan disket atau CD baca-tulisan (CD-RW) di drive eksternal. Berbagai aplikasi secara permanen dapat berada dalam RAM. Contoh, ada paket perangkat lunak keamanan yang berada dalam RAM dan mengharuskan pengguna untuk memasukkan sandi sebelum komputer dapat melanjutkan proses inisialisasi.

Perangkat lunak ini dapat mencegah pengguna yang tidak sah dari menginisialisasi komputer dengan menempatkan disket inisialisasi ke drive eksternal, seperti drive A. Pengguna yang tidak sah dapat menggunakan teknik ini untuk menginisialisasi komputer, menghindari aplikasi keamanan masuk yang kurang canggih yang tidak berada dalam RAM, dan kemudian mengakses hard drive dari drive eksternal. Sayangnya, banyak virus komputer yang juga dapat berada dalam RAM. Mereka biasanya dapat menetap ketika pengguna tidak curiga mengakses file yang terinfeksi. Sekali virus tinggal di RAM komputer, mereka dapat menginfeksi komputer lain dan file server dengan menginfeksi sebuah disket yang diakses oleh komputer lain dan perjalanan melalui intranets dan internet. Sebagai contoh, melampirkan file yang terinfeksi untuk pesan e-mail dapat menyebabkan penerima komputer menjadi terinfeksi. Untuk memerangi virus, banyak aplikasi pengecek virus telah dikembangkan dan dipasarkan. Beberapa tersedia dari produsen komputer atas pembelian peralatan komputer dan sistem operasi sementara yang lain tersedia di berbagai toko. Pengecek virus terbaik dapat diset untuk menguji file data masuk untuk virus dalam inventaris mereka, terlepas dari sumber, menghapus file yang terinfeksi, dan memberitahu pengguna atau administrator sistem keamanan dari setiap virus yang terdeksi. Jelas, inventaris virus perlu diperbarui secara berkala seperti virus baru yang teriidentifikasi. Beberapa pengembang aplikasi virus menawarkan layanan yang menyediakan pelanggan dapat memperbarui inventaris virus secara periodik (misalnya, setiap hari). Virus dibahas lebih detail dalam Bab 13.

Memori penyimpanan mengacu pada jumlah byte data yang dapat disimpan di hard drive komputer. Bagian hard drive identik dengan bagian hard disk, fixed disk dan fixed

drive. Memori penyimpanan meningkat di titik dimana biasanya dinyatakan dalam gigabyte (GB). Pada tahun penulisan buku ini, pengecer mengiklankan komputer rumah baru dengan kapasitas hard drive hingga 100 GB. Tidak seperti RAM, memori penyimpanan ditahan bahkan setelah daya dimatikan atau terganggu. Sehingga, memori penyimpanan terkadang disebut sebagai memori permanen. Namun, hal ini hanya tetap sampai informasi telah dihapus sepenuhnya. Perhatikan bahwa tindakan menghapus file tidak benar-benar menghapus data. Itu hanya menghilangkan referensi lokasi file. Data tetap pada media penyimpanan sampai ditimpa. Karena kebanyakan komputer menyimpan data secara berurutan, dapat memakan waktu beberapa minggu, bulan, atau tahun untuk menimpa file yang sebelumnya dihapus, tergantung pada jumlah data yang telah disimpan dan dihapus dan ukuran media penyimpanan. Banyak organisasi memiliki program penyimpanan data cadangan untuk membantu memastikan pemulihan data jika terjadi bencana. Tergantung pada frekuensi rotasi dan periode penyimpanan media cadangan, data dapat bertambah tanpa batas. Untuk alasan ini, terutama ketika bekerja dengan informasi rahasia, atau rahasia yang sangat sensitive, sangat penting untuk secara memadai mengamankan akses ke media penyimpanan komputer.

Perusahaan forensik komputer baru saja muncul untuk mencari melalui tambang data yang ada di hampir semua bisnis, pemerintah, dan organisasi lainnya. Perusahaan-perusahaan forensik ini menyediakan berbagai layanan. Mereka dapat disewa oleh penggugat dalam gugatan terhadap organisasi. Setelah melakukan proses hukum yang diperlukan, mereka dapat mengamankan surat penggeledahan, yang memberikan kewenangan pengadilan untuk memperoleh kendali atas semua sumber daya komputer sebuah organisasi, terlepas dari ukuran, untuk mencari bukti yang memberatkan. Perusahaan forensik komputer juga dapat dipekerjakan oleh organisasi untuk membantu dalam mengembangkan penyimpanan data dan pengambilan kebijakan dan prosedur yang membantu meminimalkan atau memaksimalkan kejadian peyebaran data, tergantung pada tujuan organisasi. Aparat penegak hukum juga telah memanfaatkan jasa perusahaan komputer forensik untuk membantu memulihkan data dari penyitaan peralatan komputer dan media penyimpanan yang diperoleh selama pembersihan. Untuk informasi tambahan, lihat Bab 12 pada forensik komputer. Konsep utama yang perlu diingat ketika menilai kontrol atas komputer adalah bahwa tidak peduli seberapa besar fisiknya atau seberapa cepat ia beroperasi, semua komputer berfungsi pada dasarnya dengan cara yang sama. Dengan demikian, pendekatan audit dan banyak kontrol yang dapat diterapkan yang umumnya sama.

SISTEM OPERASI

Unit pengolahan pusat biasanya terhubung ke berbagai perangkat periferal yang membantu dalam menyimpan, mengakses dan mentransmisi data dan juga dalam produksi keluaran informasi. Contoh perangkat periferal termasuk disk drive eksternal, satu CD-ROM dan drive CD-RW, beberapa drive CD-ROM (kadang-kadang disebut "jukebox"), drive pita perekan suara, paket disk, printer, router, jembatan, gateway, pengendali, monitor visual, keyboard, terminal, dan lain-lain. Perangkat ini secara kolektif disebut sebagai perangkat keras komputer.

Sistem operasi adalah program yang diperlukan untuk membuat perangkat keras berfungsi. Mereka biasanya dimasukkan ke komputer selama proses pembuatan. Sistem operasi biasanya mencakup bermacam-macam program utilitas yang membantu dalam fungsi, pemeliharaan, dan keamanan dari berbagai perangkat keras. Sistem operasi dan utilitas secara kolektif disebut sebagai sistem perangkat lunak. Contoh sistem operasi umum termasuk DOS, Windows, OS/2, NetWare, OSX, Unix, VMS, dan OS/390.[23] Fitur tertentu dalam sistem perangkat lunak dapat disesuaikan oleh pembeli. Sebagai contoh, sistem operasi paling canggih memiliki fitur kontrol akses sistem yang memungkinkan pembeli secara memadai melindungi sistem terhadap akses yang tidak sah. Produsen biasanya mengatur parameter kontrol akses sistem untuk membolehkan akses yang hampir tak terbatas selama instalasi awal. Hal ini diperlukan agar pengguna yang melakukan instalasi awal dapat mengatur pengguna lain, mengkonfigurasi sistem, dan menyesuaikan pengaturan parameter sistem yang tersedia. Namun, karena terbuka luasnya sistem yang baru diinstal, sangat penting bahwa fitur kontrol akses sistem secara benar dikerahkan sesegera mungkin setelah instalasi. Walaupun produsen komputer biasanya membantu dalam penginstalasian awal pada sistem yang kompleks, mereka cenderung lebih berkonsentrasi pada pembuatan sistem operasional daripada memastikan bahwa itu cukup aman. Pada kenyataannya, banyak teknisi penjual biasanya membuat identifikasi pengguna (ID) untuk diri mereka sendiri, yang memiliki hak istimewa yang sama sebagai administrator sistem keamanan. Sering mereka tidak menghapus ID pengguna setelah mereka menyelesaikan instalasi. Akibatnya, organisasi berisiko mejadi subjek akses yang tidak sah oleh para teknisi instalasi. Ini adalah salah satu alasan penting untuk auditor berpartisipasi dalam proyek-proyek implementasi sistem yang baru. Hal ini dan masalah lainnya akan dibahas secara lebih rinci dalam buku.

PROGRAM APLIKASI

Program aplikasi yang diperlukan untuk membuat CPU dan sistem perangkat lunak yang melakukan fungsi bisnis. Banyak program aplikasi dirancang untuk melakukan tugas-tugas umum seperti pengolah kata (misalnya, Word, WordPerfect), spreadsheet (misalnya, Excel, Lotus 1-2-3), dan analisis data (misalnya, Access, Paradoks). Banyak aplikasi lain yang telah dirancang untuk melakukan fungsi spesifik bisnis di berbagai industri (misalnya, aplikasi pinjaman dan deposit di lembaga keuangan, aplikasi kartu kredit di perusahaan pengeluaran kartu, aplikasi desain komputer di perusahaan pembuatan mobil dan pesawat, dan aplikasi pengolahan klaim di perusahaan asuransi). Ada beberapa aplikasi perencanaan sumber daya perusahaan (ERP) yang membantu melakukan fungsi bisnis umum seperti akuntansi keuangan, hutang, sumber daya manusia, penggajian, manajemen aset tetap, dan sebagainya. Contoh aplikasi ERP ini adalah PeopleSoft, SAP, Oracle, Baan, J.D. Edwards, dan Lawson. Secara harfiah jutaan aplikasi lain telah dikembangkan secara internal oleh perusahaan dan eksternal oleh vendor untuk melakukan berbagai fungsi bisnis, beberapa dari mereka menggunakan berbagai bahasa. Masing-masing aplikasi mungkin atau tidak mungkin memiliki fitur kontrol yang dirancang untuk membantu mencegah akses otorisasi kepada mereka. Untuk menilai kecukupan kontrol atas aplikasi ini, pengetahuan rinci tentang fitur kontrol yang tersedia dalam aplikasi tertentu saat ini digunakan dalam organisasi harus diperoleh.

SISTEM MANAJEMEN DATABASE

Sistem manajemen database (DBMS) biasanya terdiri dari seperangkat program yang digunakan untuk menentukan, mencari, mengamankan, dan biasanya mengatur besar volume data. Memiliki data yang terletak di DBMS terpisah menawarkan beberapa manfaat, termasuk fleksibilitas untuk mengubah aplikasi tanpa mempengaruhi data, kemampuan untuk menghilangkan redundansi data sebelumnya diperlukan oleh aplikasi terbuka bebas, dan kemampuan untuk mengamankan lebih baik dan memantau data.

Beberapa aplikasi melakukan tugasnya tidak memerlukan sebuah DBMS. Sebagai contoh, sebuah aplikasi khusus yang mengontrol kenaikkan dan penurunan batang pendingin dalam sebuah tanaman kekuatan nuklir tidak membutuhkan database. Namun, data tentang peningkatan dan penurunan perlu direkam, dipantau, dan dianalisa, kemungkinan oleh aplikasi lain. Tergantung pada jumlah dan kompleksitas data yang direkam, sebuah DBMS mungkin diperlukan.

Pada kenyataannya, mayoritas aplikasi komputasi yang kompleks memiliki beberapa macam DBMS yang terkait dengan aplikasinya. Dalam beberapa kasus, aplikasi dirancang untuk fungsi sebuah DBMS tertentu dan hanya mengandalkan DBMS untuk penerapan keamanan. Dalam kasus lain, aplikasi yang dirancang berfungsi dari berbagai DBMS berbeda dan memiliki fitur keamanan dalam aplikasi perangkat lunak sebaik DBMS. Contoh umum DBMS termasuk Microsoft SQL Server, Oracle, dan IBM DB2.

KONTROL KEAMANAN FISIK

Hardware komputer meliputi CPU dan semua perangkat periferal. Dalam sistem jaringan, perangkat ini termasuk semua jembatan, router, gateway, switch, modem, hub, media telekomunikasi, dan perangkat lain yang terlibat dalam bentuk fisik transmisi data. Bagian-bagian peralatan harus cukup terlindungi terhadap kerusakan fisik yang dihasilkan dari bencana alam, seperti gempa bumi, angin topan, tornado, banjir, dan bahaya lain, seperti bom, kebakaran, lonjakan daya, pencurian, perusakan, dan gangguan lain. Kontrol yang melindungi terhadap ancaman ini disebut kontrol keamanan fisik. Contoh-contoh kontrol keamanan fisik termasuk berbagai jenis kunci (misalnya, konvensional kunci, tanda akses elektronik, kunci biometrik, kunci cipher); asuransi atas perangkat keras dan biaya untuk membuat data kembali; prosedur untuk melakukan backup harian sistem perangkat lunak, program aplikasi dan data; bentuk tempat penyimpanan dan rotasi media cadangan (misalnya, pita perekam suara, disk, disk compact [CD]) untuk lokasi aman; dan program- program pemulihan bencana saat ini dan telah diuji.

KONTROL KEAMANAN LOGIS

Sistem komputer juga harus cukup terlindungi dari akses yang tidak sah dan perusakan yang disengaja atau tidak disengaja atau perubahan sistem program perangkat lunak, aplikasi program dan data. Perlindungan terhadap ancaman ini dicapai melalui penggunaan kontrol keamanan logis. Kontrol keamanan logis adalah membatasai kemampuan akses pengguna sistem dan mencegah pengguna yang tidak sah mengakses sistem. Kontrol keamanan Logis mungkin ada dalam sistem operasi, sistem manajemen database, aplikasi program, atau di ketiganya.

Jumlah dan jenis kontrol keamanan logis bervariasi dengan masing-masing sistem operasi, sistem manajemen database, aplikasi, dan banyak jenis dari perangkat telekomunikasi. Beberapa yang dirancang dengan susunan yang luas dari pilihan kontrol keamanan logis dan parameter yang tersedia untuk keamanan sistem administrator.

Termasuk user id, password dengan persyaratan panjang minimum dan dibutuhkan digit dan karakter, suspensi ID pengguna setelah usaha berturut-turut gagal sign-on, pembatasan akses daftar dan file, pembatasan waktu dan hari, dan pembatasan penggunaan terminal khusus. Sistem operasi lainnya dan aplikasi dirancang dengan sangat sedikit pilihan kontrol. Untuk sistem ini, kontrol keamanan logis sering terlihat ditambahkan sebagai renungan, mengakibatkan pengaturan kontrol yang lebih lemah daripada apa yang cukup diinginkan, bahkan ketika pembatasan akses maksimum yang tersedia telah dilaksanakan.

Banyak sistem diprogram dengan kontrol yang setara dengan tingkat risiko yang terkait dengan fungsi yang dilakukan oleh sistem. Sebagai contoh, sistem pengolahan transaksi transfer bank berisiko tinggi di lembaga keuangan harus memiliki kontrol yang secara signifikan lebih luas daripada sistem pencatatan transaksi rendah risikon pada lembaga yang sama. Namun, waspada sistem berisiko tinggi dengan kontrol buruk. Banyak sistem berisiko tinggi yang telah diprogram dengan tidak memadai mengontrol fitur atau memiliki fitur kontrol yang memadai tetapi fitur yang diimplementasikan tidak memadai. Masalah dapat terjadi ketika programmer dan/atau pemilik proses tidak menyadari satu atau lebih risiko yang signifikan dihadapi organisasi selama pemakaian sistem.

LOKASI FISIK DAN KONTROL KEAMANAN LOGIS

Tampilan 1.1 secara visual menggambarkan konsep dasar sistem komputasi dan lokasi kontrol keamanan fisik dan logis. Kontrol keamanan fisik berkaitan dengan unit pemroses sentral dan terhubung dengan perangkat keras dan peralatan periferal. Kontrol keamanan logis ada di tingkat sistem operasi dan dalam sistem manajemen database dan program aplikasi. Model dasar ini dapat diterapkan untuk hampir semua jenis sistem komputasi. Sebagai contoh, Tampilan 1.2 menyajikan model konseptual dari salah satu cara untuk melihat kontrol keamanan fisik dan logis dari sebuah sistem yang mempunyai tiga aplikasi, masing-masing dengan CPU sendiri. Dalam konfigurasi ini, redundansi data dapat dihilangkan jika dikelola dengan baik karena aplikasi 1 dan 2 yang mampu bertukar data melalui aplikasi middleware. Firmware termasuk chip memori yang sering digunakan yang berisi program operasi dan data sehingga mereka dapat diproses lebih cepat daripada jika program harus dimuat dan dieksekusi di RAM. Tidak seperti RAM, program dan data tidak terhapus ketika CPU dimatikan.

Firmware secara khusus melakukan pemrosesan komputer dan dengan demikian memiliki kontrol keamanan logis yang terkait dengan itu. Langkah-langkah audit untuk menguji kontrol keamanan fisik dan logis atas komputasi sistem disajikan dalam program audit di Bab 3. Setiap langkah audit dibahas lebih rinci pada bab-bab berikutnya. Bab ini

harus memberikan pembaca memahami dasar-dasar bagaimana sistem komputasi beroperasi dan jenis-jenis kontrol keamanan fisik dan logis yang mungkin tersedia. Langkah berikutnya adalah untuk mengidentifikasi sistem komputasi dalam sebuah organisasi.

AUDITOR SISTEM INFORMASI

DESKRIPSI PEKERJAAN

Ringkasan pekerjaan: Di bawah arahan dari Chief Audit Executive (CAE) dan manajemen audit internal, audit, ulasan, tes, dan mengevaluasi aplikasi berbasis IT dan kontrol, prosedur, dan ulasan keamanan elektronik atas perusahaan jaringan layanan TI.

KARAKTERISTIK PEKERJAAN TUGAS DAN TANGGUNG JAWAB

Mungkin termasuk dan/salah satu atau semua hal berikut:

1. Desain berbasis audit pendekatan teknologi; menganalisa dan mengevaluasi perusahaan yang diproses untuk menilai kontrol internal and meminimalkan risiko; melakukan analisis risiko infrastruktur perusahaan teknologi informasi dan jaringan layanan; mengevaluasi kemungkinan resiko yang ada di berbagai sistem komputer; mempersiapkan laporan mendokumentasikan temuan dan penilaian risiko; mengevaluasi tanggung jawab dan penilaian risiko manajemen.
2. Bekerja secara mandiri atau dengan anggota lain dari audit internal untuk meninjau kontrol internal perusahaan, mengikuti kerangka kontrol internal COSO.
3. Menguji efektivitas kebijakan dan prosedur keamanan informasi; mengidentifikasi kekurangan yang ada dalam keamanan program dan mungkin tindakan yang akan diambil.
4. Mengembangkan dan menerapkan audit berbantuan alat dan teknik komputer (CAATTs) untuk membantu keseluruhan upaya audit internal dan melakukan tes lain yang berhubungan dengan kontrol, yang sesuai.
5. Mengembangkan dan menyajikan pelatihan lokakarya untuk staf audit pada kontrol keamanan dan konsep risiko.
6. Melakukan dan mengawasi penyelidikan dari penggunaan komputer yang tidak berwenang.
7. Melakukan proyek-proyek khusus dan tugas-tugas lain seperti yang ditetapkan; memberikan masukan pada kegiatan departemen administratif.

PENGETAHUAN, KETERAMPILAN, KEMAMPUAN, DAN KARAKTERISTIK PRIBADI

- ✓ Pengetahuan auditing, sistem informasi dan keamanan jaringan

- ✓ Penyelidikan dan kemampuan analisis proses aliran
- ✓ Keterampilan hubungan interpersonal manusia
- ✓ Keterampilan verbal dan komunikasi tertulis
- ✓ Kemampuan untuk melakukan penilaian yang baik
- ✓ Kemampuan untuk menjaga kerahasiaan
- ✓ Kemampuan untuk menggunakan alat desktop kantor, alat analisis kerentanan, dan alat-alat IT lain

KUALIFIKASI MINIMUM

Pendidikan dan pengalaman setara dengan:

- ✓ Gelar sarjana dalam ilmu komputer, pemrograman komputer atau akuntansi
- ✓ Kredensial bersertifikat informasi Systems Auditor (CISA) atau calon
- ✓ Auditor Internal bersertifikat credential pilihan

CATATAN

1. Walter S. Mossberg, “MMX Has Much to Offer, but Less Than Hype Suggests,” *Wall Street Journal* (February 13, 1997): B1.
2. Paul Salzman, “P.S. The Mac: I’m Back!” *Computer Source Magazine* (July 1997): 25.
3. “Intel to Introduce Sixth-Generation Pentium Chip,” *KIRO Radio News Fax* (May 5, 1997): National Business page.
4. Don Clark and Jon G. Averbach, “Microsoft, H-P to Unveil Broad Alliance over Windows NT, Business Computing,” *Wall Street Journal* (March 18, 1997): B4.
5. “Fastest Chip to Be Shown,” *KIRO Radio News Fax* (October 22, 1996): National Business page.
6. Bill Richards, “Intel, U.S. Build Most-Powerful Computer Yet,” *Wall Street Journal* (December 17, 1996): B6.
7. Rajiv Chandrasekaran, “New Supercomputer Breaks Record, Using Chips from Desktop,”*Seattle Times* (December 17, 1996): A9.
8. “Business Briefs,” *Seattle News Fax* (June 3, 2002): 5.
9. “Japanese Own Fastest Computer,” *Seattle News Fax* (April 22, 2002): 5.
10. “IBM Unveils Fastest Microchip,” *Seattle News Fax* (February 26, 2002): 5.
11. “Intel Touts New Transistors,” *Seattle News Fax* (November 26, 2001): 5.
12. “Supercomputer May Unlock Origins of Universe,” *Seattle News Fax* (August 1, 2001): 5.

13. “Intel Introduces Fast Chips,” *Seattle News Fax* (July 3, 2001): 5.
14. “Intel Develops Fastest, Smallest Transistor Ever,” *Seattle News Fax* (June 11, 2001):
    5.
15. “Business Briefs,” *Seattle News Fax* (June 6, 2001): 5.
16. “Intel Unveils 1.7 GHz Processor,” *Seattle News Fax* (April 2, 2001): 5.
17. “Intel Rolls Out 1 Gig Laptop Chip,” *Seattle News Fax* (March 19, 2001): 5.
18. “Business Briefs,” *Seattle News Fax* (November 13, 2000): 5.
19. “‘Blue Gene’ Will Dwarf All Other Computers,” *Seattle Times* (June 5, 2000): A1.
20. “Apple Computer Unveils New iMac hardware,” *KIRO Radio News Fax* (October 7, 1999): 6.
21. “Business Briefs,” *KIRO Radio News Fax* (May 4, 1999): 5.
22. “Fastest Computer Developed,” *KIRO Radio News Fax* (October 28, 1998): 2.
23. Daftar produsen komputer dan sistem operasi termasuk tujuan ilustrasi dan tidak berarti dimaksudkan untuk menjadi pelengkap. Yang terdaftar hanya dimaksudkan untuk memberikan pembaca gambaran umum mengenai jumlah dan jenis komputer dan sistem operasi yang ada sekarang.

Daftar Pustaka

1. More information on the total roles and responsibilities of internal audit in today’s enterprise can be found in Robert Moeller, Brink’s Modern Internal Auditing, 7th ed. (Hoboken, NJ: John Wiley & Sons, 2009).
2. Statement on Auditing Standards No. 1, Codification of Auditing Standards and Procedures, AICPA, Professional Standards.
3. National Commission on Fraudulent Financial Reporting, Report of the National Commission on Fraudulent Financial Reporting (1987).
4. Internal Control—Integrated Framework, www.coso.org/publications.htm Note: This reference is for the COSO internal controls report, which can be ordered through the AICPA at www.cpa2biz.com.
5. AICPA-published COSO internal control standards are described in the Statement on Auditing Standards (SAS) numbers 103, 105, 106, 107, 109, 110, and 112.
6. See Robert Moeller, Sarbanes-Oxley Internal Controls: Effective Auditing with AS5, CobiT, and ITIL (Hoboken, NJ: John Wiley & Sons, 2008).

7. COSO, Guidance on Monitoring Internal Control Systems (2009). www.coso.org/documents/ COSO_Guidance_On_Monitoring_Intro_online1.pdf.
8. Here we are presenting only a high-level summary of SOx requirements. See Moeller, Sarbanes-Oxley Internal Controls, for much more information.
9. As a public document, the text of the law can be found in many Web locations. One source is http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf.