15 Keamanan Komputer

Setelah membaca bab ini anda diharapkan memahami hal-hal sebagai berikut :

- Mengapa penggunaan komputer menjadikan sistem informasi tidak aman
- Menciptakan lingkungan pengendalian
- Pengendalian umum
- Pengendalian aplikasi
- Pemeriksaan sistem informasi

Pendahuluan

Dewasa ini sistem komputer memegang peranan yang sangat penting dalam berbagai kegiatan seperti dalam aktivitas bisnis, pemerintahan dan dalam kehidupan sehari-hari. Banyak organisasi mengandalkan komputer dalam sistem informasinya. Penggunaan komputer dalam sistem informasi selain memberikan manfaat juga mengundang berbagai macam resiko sehingga organisasi-organisasi tersebut harus membuat langkah-langkah khusus untuk melindungi sistem informasinya dan menyakinkan bahwa sistem tersebut tetap aman, akurat dan layak.

Keadaan tersebut di atas mendorong suatu organisasi untuk menyusun standar pengendalian yang dapat meyakinkan bahwa sistem informasi yang dimilikinya benar-benar terkendali. Dengan *data* yang tersimpan dalam bentuk *data* elektronik dan prosedur yang diotomatisasikan, *data* tersebut mudah diubah, rusak dan tidak berfungsi sehingga mendorong terjadinya kecurangan dan kerusakan pada *hardware* atau *software* yang digunakan. Kerusakan atau kesalahan yang dialami oleh sistem informasi yang berbasis komputer akan berdampak sangat parah bila dibandingkan dengan sistem informasi secara manual. *Virus* juga merupakan salah satu ancaman berbahaya yang dapat menyebar tanpa terkendali dari satu sistem ke sistem lainnya, merusak memori komputer atau menghancurkan program dan *data* yang ada.

15.1 Mengapa Penggunaan Komputer Menjadikan Sistem Informasi Tidak Aman

Banyak keuntungan dapat diperoleh bila sistem informasi yang digunakan berjalan dengan aman. Tetapi ketika *data* dalam jumlah besar disimpan secara elektronik, maka sistem informasi menjadi tidak cukup aman lagi untuk digunakan dibandingkan dengan sistem manual.

Ada beberapa masalah didalam sistem informasi manajemen berbasis komputer yang perlu diperhatikan, yaitu:

- Sistem informasi yang kompleks tidak dapat dibuat ulang secara manual.
- *Data-data* dalam program komputer hanya dapat dibaca dengan komputer sehingga bila terjadi perubahan baik disengaja atau tidak, perubahan tersebut tidak dapat dilihat/dibaca secara langsung.
- Prosedur-prosedur program komputer yang di kompile tidak tampak nyata sehingga sulit dipahami atau diaudit.
- Pengembangan dan pengoperasian sistem informasi memerlukan keahlian teknis khusus yang tidak mudah untuk dikomunikasikan kepada operator. Sistem akan menjadi tidak aman bila ditangani oleh teknisi yang tidak memiliki integritas yang baik terhadap organisasi.
- Meskipun peluang terjadinya musibah terhadap sistem informasi lebih kecil daripada sistem manual tapi kalau musibah itu terjadi dampak yang ditimbulkannya akan lebih parah dibandingkan dengan sistem manual.
- Sistem informasi dapat diakses oleh banyak orang. Informasi makin mudah untuk diakses akan makin sulit untuk dikontrol.
- Sistem informasi yang *on-line* sangat sulit untuk dikontrol karena *data* dapat diakses secara cepat dan langsung melalui terminal komputer.

Hecker, orang yang Mengakses sistem informasi secara ilegal dengan tujuan keuntungan dan kejahatan.

Saat ini ketidakamanan penggunaan sistem informasi berbasis komputer bertambah dengan munculnya *hecker* dan *virus*. *Hecker* adalah orang yang dapat mengakses sistem informasi secara ilegal dengan tujuan mendapatkan keuntungan dan kejahatan, sedangkan *virus* adalah program komputer yang dapat menyebar dengan cepat dari satu komputer ke komputer lain. *Virus* akan merusak *data* atau program komputer sehingga merusak proses kerja komputer. *Virus* seringkali sulit untuk dideteksi, bahkan dengan *software antivirus* sekalipun.

Kondisi yang membuat tidak amannya penggunaan sistem informasi manajemen berbasis komputer tersebut, tentunya harus secara khusus mendapat perhatian baik oleh penyusun sistem informasi maupun oleh pemakai.

Virus adalah program komputer yang dapat menyebar dengan cepat dari satu komputer ke komputer lain

Ada tiga faktor utama yang harus betul-betul dipertimbangkan dan diperhatikan oleh pengembang dan pemakai sistem informasi, yaitu musibah, keamanan dan kesalahan administratif.

- **Musibah bisa terjadi setiap saat** - perangkat keras, program, *file-file data* dan peralatan lainnya bisa hancur karena kebakaran, kesalahan arus listrik atau musibah lainnya. Beberapa musibah yang terjadi dapat mengganggu operasional rutin perusahaan dan berakibat pada seluruh aktivitas organisasi, untuk musibah semacam ini mungkin dibutuhkan wakbertahun-tahun dan dana jutaan rupiah untuk memperbaikinya kembali. Pada perusahaan-perusahaan besar yang memiliki sistem jaringan *on-line* diseluruh dunia, maka antisipasi terhadap munculnya musibah tersebut mutlak diperlukan, sehingga aktivitas organisasi tetap dapat berjalan tanpa harus menunggu waktu lama untuk perbaikan jika terjadi musibah yang tak terduga. Salah satunya adalah seperti yang dilakukan oleh Visa USA Inc., salah satu perusahaan besar yang memiliki jaringan diseluruh dunia. Perusahaan ini memiliki satu sistem komputer yang dapat mengantisipasi terjadinya musibah dengan cara membangun *'fault-tolerant computer system'*, yaitu suatu sistem pengamanan untuk sistem informasi berbasis komputer yang terdiri dari perangkat keras dan lunak cadangan, serta komponen tenaga listrik yang dapat mem*backup* sistem agar bisa terus beroperasi. Sistem komputer cadangan ini memiliki ekstra memori *(memory)*, prosesor *(processors)* dan *harddisk*. Sistem ini dapat mendeteksi kesalahan yang terjadi dan mengalihkannya pada sistem cadangan. Sistem ini biasanya digunakan oleh perusahaan besar yang memiliki sistem pengolahan transaksi secara *on-line*.

Fault-tolerant-computer system yaitu suatu sistem yang memiliki perangkat keras, lunak, sumber tenaga listrik cadangan sehingga sistem terus berjalan saat terjadi berbagai kesalahan.

- **Keamanan *(security)* -** adalah serangkaian kebijakan, prosedur dan teknik pengukuran yang digunakan untuk melindungi sistem informasi terhadap akses dari orang yang tidak berwenang, pengubahan, pencurian dan kerusakan fisik. Keamanan dapat dilakukan dengan menyusun satu teknik dan perangkat yang dapat mengamankan perangkat keras dan lunak komputer, jaringan komunikasi dan *data*.

Keamanan adalah serangkaian kebijakan, prosedur, dan teknik pengukuran yang digunakan untuk melindungi sistem informasi manajemen terhadap akses yang tidak berwenang, pencurian dan kerusakan fisik.

- **Kesalahan *(error)* administratif -** pada sistem informasi berbasis komputer dapat terjadi berbagai kesalahan administratif seperti kesalahan pemasukan *data*, kesalahan program, operasional komputer dan sebagainya.

15.2 Menciptakan Lingkungan Pengendalian

Untuk mengurangi resiko kesalahan dan untuk mengantisipasi terjadinya musibah, kejahatan komputer serta rendahnya tingkat keamanan suatu kebijakan dan prosedur khusus harus dimasukkan pada saat merancang dan mengimplementasikan suatu sistem informasi. Gabungan dari sistem manual dan berbasis komputer dapat menjadi acuan untuk mengukur sampai sejauhmana keamanan suatu sistem telah dibuat dan sesuai dengan standar pengendalian manajemen.

Pengendalian *(control)* meliputi semua metode, kebijakan dan prosedur organisasi yang menjamin keamanan harta kekayaan perusahaan, akurasi dan kelayakan *data* manajemen serta standar operasi manajemen lainnya.

Pengendalian *(control)* meliputi semua metode, kebijakan dan prosedur organisasi yang menjamin keamanan harta kekayaan perusahaan, akurasi dan kelayakan *data* manajemen serta standar operasi manajemen lainnya.

Pengendalian terhadap sistem informasi harus dilakukan sedini mungkin dan merupakan bagian penting dalam perancangan. Pengembang dan pemakai harus memberikan perhatian penuh terhadap masalah pengendalian ini mulai dari tahap perancangan hingga pengimplementasiannya.

Sistem informasi berbasis komputer dikendalikan oleh kombinasi dari pengendalian umum *(general control)* dan pengendalian aplikasi *(application control)*.

Pengendalian umum mengontrol rancangan keamanan dan penggunaan komputer serta keamanan dari *file-file data* organisasi secara umum.

- **Pengendalian umum** - mengontrol rancangan, keamanan dan penggunaan *software* sistem informasi serta keamanan dari *file-file data*nya secara umum melalui organisasi. Secara keseluruhan, pengendalian umum ini diterapkan pada semua aplikasi komputer yang merupakan kombinasi dari *software* sistem *(system software)* dan prosedur manual yang diarahkan kepada terciptanya pelaksanaan pengendalian secara menyeluruh.

Pengendalian aplikasi, merupakan pengendalian yang khusus ditujukan bagi setiap aplikasi komputer.

- **Pengendalian aplikasi** - merupakan pengendalian yang khusus ditujukan bagi setiap aplikasi komputer, seperti program aplikasi untuk penggajian, piutang dan pengolahan order. Penerapan pengendalian dilakukan baik terhadap pemakai subsistem informasi tertentu maupun terhadap prosedur penyusunan programnya.

15.2.1. Pengendalian Umum

Pengendalian umum merupakan pengendalian yang menyeluruh yang bertujuan untuk memberikan keyakinan bahwa prosedur yang diprogram *(software)* telah berjalan secara efektif pada seluruh aktivitas bisnis. Pengendalian ini meliputi :

- Pengendalian atas seluruh proses implementasi sistem
- Pengendalian atas *software* yang digunakan
- Pengendalian atas fisik *hardware*

- ❑ Pengendalian atas pengoperasian komputer
- ❑ Pengendalian atas keamanan *data* dan jaringan
- ❑ Pengendalian atas aktivitas administrasi

Pengendalian atas Seluruh Proses Implementasi Sistem

Pengendalian atas implementasi diawali dengan pemeriksaan terhadap proses pengembangan diberbagai bagian untuk meyakinkan bahwa proses benar-benar terkendali dan dikelola dengan baik.

Pengendalian terhadap implementasi diawali dengan pemeriksaan terhadap proses pengembangan di berbagai bagian untuk meyakinkan bahwa proses benar-benar terkendali dan dikelola dengan baik

Pemeriksaan terhadap pengembangan sistem harus menghasilkan suatu *review* formal terhadap seluruh tahap pengembangan sistem informasi di semua bagian sehingga manajemen memiliki informasi untuk menyetujui atau menolak implementasi sistem informasi yang tengah disusun.

Pemeriksaan terhadap pengembangan sistem informasi juga harus mengevaluasi sampai sejauhmana keterlibatan pemakai sistem dalam setiap tahap implementasi dan memeriksa penggunaan azas biaya-manfaat *(cost-benefit)* dalam menetapkan kelayakan pengembangan sistem informasi. Selanjutnya pemeriksa juga harus melihat pelaksanaan pengendalian dan jaminan kualitas teknis *(quality assurance techniques)* untuk setiap tahap pengembangan, konversi dan pengujian.

Hal yang penting juga dalam penyusunan sistem informasi adalah tersedianya dokumentasi yang memperlihatkan bagaimana jalannya sistem informasi baik dari segi teknis maupun pemakai. Suatu sistem informasi tidak akan dapat beroperasi sebagaimana seharusnya dan terpelihara tanpa dukungan dokumentasi yang memadai. Pemeriksaan terhadap pengembangan sistem informasi juga harus ditujukan untuk melihat sampai sejauhmana tingkat kesesuaian antara dokumentasi sistem, pemakai maupun pengoperasiannya dengan standar yang telah ditentukan.

Pengendalian atas Perangkat Lunak (Software)

Pengendalian *software* bertujuan untuk menjamin keamanan dan kelayakan dari *software* yang digunakan

Pengendalian keamanan program dirancang untuk me lindungi dari perubahan yang tidak semestinya pada program yang berada dalam sistem informasi yang siap digunakan.

Pengendalian penting dilakukan bagi setiap kategori *software* yang digunakan dalam sistem informasi berbasis komputer. Pengendalian *software* bertujuan untuk memantau penggunaan *software* sistem informasi dan melindunginya dari akses yang dilakukan oleh pihak yang tidak berwenang.

Pengendalian *software* sistem dilakukan terhadap pengoperasian *software* sistem operasi yang mengatur jalannya program aplikasi. Pengendalian terhadap *software* sistem juga dilakukan terhadap penggunaan kompiler, program utiliti, laporan operasional, setup dan penanganan *file*. Pengendalian *software* sistem merupakan bagian pengendalian yang sangat penting karena mengontrol seluruh fungsi program yang memproses *data*.

Pengendalian keamanan program dirancang untuk melindungi program dari perubahan yang tidak semestinya yang dilakukan oleh orang yang tidak berhak sebelum program tersebut dioperasikan.

Pengendalian atas Perangkat Keras (Hardware)

Pengendalian *hardware* bertujuan untuk menjamin bahwa komputer *hardware* yang digunakan secara fisik aman dan bekerja secara baik.

Pengendalian perangkat keras dilakukan untuk menjamin bahwa *hardware* yang digunakan secara fisik benar-benar aman dan semuanya berfungsi dengan baik. Perangkat keras komputer secara fisik harus benar-benar aman sehingga dapat diakses hanya oleh orang-orang yang berwenang. Akses pada ruang dimana komputer dioperasikan harus benar-benar dibatasi hanya untuk petugas bagian komputer saja. Peralatan komputer juga harus benar-benar aman dan terlindung dari kebakaran dan temperatur yang berlebihan. Bagi organisasi yang menggunakan sistem informasi berbasis komputer dalam seluruh aktivitasnya harus memiliki pengamanan ekstra bagi peralatan komputernya.

Pengendalian Pengoperasian Komputer

Pengendalian pengoperasian komputer, prosedurnya dilakukan untuk menjamin bahwa prosedur pemrograman dilaksanakan secara konsisten dan diterapkan secara tepat untuk memproses dan menyimpan *data*

Pengendalian operasi komputer merupakan pekerjaan bagian komputer untuk meyakinkan bahwa sistem informasi telah dijalankan dengan benar dan konsisten dalam menyimpan dan memproses *data*. Pengendalian ini meliputi pengawasan terhadap seluruh pemrosesan, pengoperasian *hardware* dan *software*, pembuatan *backup* dan prosedur perbaikan yang diterapkan.

Perintah-perintah untuk menjalankan komputer juga harus didokumentasikan, dikaji ulang *(review)* dan disetujui oleh petugas yang berwenang. Pengendalian terhadap pengoperasian *software* meliputi prosedur manual yang dirancang untuk memperbaiki dan mendeteksi adanya kesalahan. Pengendalian ini merupakan gabungan dari instruksi-instruksi pengoperasian *software* yang lebih spesifik, prosedur perbaikan dan pengoperasian kembali, prosedur pemberian label dan penyimpanan *backup* serta prosedur untuk aplikasi yang spesifik.

Software sistem dapat menyimpan rincian *data* aktivitas sistem jaringan komputer selama beroperasi. *Data* ini dapat dicetak untuk di*review* bila diperlukan, sehingga kesalahan fungsi *hardware*, penyelesaian yang tidak normal dan tindakan operator yang salah dapat diteliti. Perintah tertentu untuk membuat *copy* dan perbaikan *data (backup)* dapat dilakukan sehingga bila terjadi kerusakan atau kesalahan pada *hardware* atau *software* tidak menimbulkan perubahan yang berarti pada sistem informasi yang sedang digunakan.

Pengendalian Terhadap Keamanan Data dan Jaringan

Pengendalian terhadap keamanan *data* dilakukan untuk meyakinkan bahwa *backup data* berharga, baik yang berada di disket ataupun di CD terhindar dari penggunakan oleh pihak yang tidak berwenang, perubahan atau kerusakan. Pengendalian *data* sangat mudah dilakukan pada *file data* yang disimpan secara *batch* karena pengendalian dapat difokuskan hanya kepada operator yang menjalankan *file batch* tersebut. Akan tetapi pengendalian sangat sulit dilakukan untuk sistem yang *on-line* atau *'real time'*

karena sistem tersebut dapat diakses melalui terminal dimana saja pada saat sistem tersebut dioperasikan.

Ketika *data* di*input* secara *on-line* melalui sebuah terminal, maka *input* harus benar-benar dijaga dari penggunaan orang yang tidak berhak. Untuk mengatasi masalah ini pengendalian keamanan *data* dapat dilakukan dalam beberapa cara yaitu :

Pengendalian keamanan data dilakukan untuk meyakinkan bahwa *copy data (backup)* berharga, baik yang berada di disket atau pun di CD terhindar dari penggunakan oleh pihak yang tidak berwenang, perubahan atau kerusakan

- **Terminal secara fisik dibatasi** - sehingga hanya petugas yang berwenang saja yang dapat menggunakannya.

- **Lengkapi *software* dengan *password* -** sehingga hanya petugas-petugas yang berwenang saja yang dapat mengakses jaringan komputer sistem informasi.

- **Untuk sistem dan aplikasi khusus** - dapat digunakan *password* dan sistem keamanan tambahan.

Sistem yang dirancang secara *on-line*, harus memiliki *file data* yang benar-benar aman.

Bagi sistem informasi yang dapat diakses melalui *internet* atau *extranet* mengamankannya dapat menggunakan *' irewalls'*, yang berfungsi untuk melindungi *data* dari orang-orang yang tidak berwenang menggunakannya. *'Firewalls'* ini biasanya ditempatkan antara LAN dan WAN atau jaringan eksternal seperti *internet*. Perangkat ini dapat mendeteksi kewenangan user sebelum dapat mengakses ke jaringan.

Untuk menciptakan *'Firewalls'* yang baik, harus ada yang menyusun dan memelihara aturan-aturan internal agar dapat mengidentifikasi orang, aplikasi atau alamat secara terinci yang diperkenankan atau ditolak untuk masuk ke jaringan.

'Firewalls' dapat mencegah tetapi tidak sepenuhnya melindungi jaringan dari pemakai yang tidak berwenang sehingga harus dianggap sebagai salah satu elemen dari seluruh rencana pengamanan sistem informasi berbasis komputer.

Pengendalian Administratif

Pengendalian administratif merupakan standar formal, ketentuan-ketentuan, prosedur dan pengendalian disiplin yang diterapkan untuk menjamin bahwa pengendalian aplikasi dan organisasi secara umum dilaksanakan dengan benar. Hal-hal penting dalam pengendalian administratif adalah adanya: (1) Pemisahan fungsi, (2) Kebijakan dan prosedur tertulis dan (3) Supervisi.

Pengendalian administratif, memformalkan standar, ketentuan, prosedur dan disiplin untuk menjamin bahwa pengendalian organisasi telah dilaksanakan dan diterapkan secara tepat.

- **Pemisahan fungsi -** merupakan prinsip dasar dalam pengendalian intern bagi setiap organisasi. Pemisahan fungsi dirancang untuk meminimumkan risiko terjadinya kesalahan dan kecurangan baik disengaja atau tidak disengaja terhadap harta perusahaan. Karena itu, orang yang bertanggungjawab atas pelaksanaan sistem harus berbeda dengan orang yang men-

Pemisahan fungsi, merupakan prinsip dari pengendalian intern untuk membagi tanggung jawab dan menentukan tugas-tugas diantara orang-orang se hingga fungsi masing-masing tidak saling tumpang tindih dan untuk meminimalkan terjadinya kesalahan dan manipulasi terhadap harta perusahaan.

jalankan. Petugas yang memproses *input* harus dipisahkan dari petugas yang memproses *output*.

- **Kebijakan dan prosedur yang tertulis -** merupakan sarana untuk menetapkan standar formal yang mengendalikan jalannya sistem informasi. Prosedur harus diformalkan secara tertulis dan disahkan oleh pejabat yang berwenang. Tanggung jawab dan pertanggungjawaban harus benar-benar dijelaskan secara rinci dan jelas.

- **Supervisi terhadap personel yang terlibat dalam prosedur pengendalian -** harus menjamin bahwa pengendalian sistem informasi manajemen telah dilaksanakan seperti seharusnya. Dengan supervisi, kelemahan dapat segera diketahui, kesalahan segera dikoreksi dan penyimpangan dari prosedur standar dapat diketahui lebih awal. Tanpa adanya supervisi yang memadai, rancangan penyusunan pengendalian menjadi tidak berguna.

Kelemahan dari setiap poin pengendalian umum dapat berakibat secara luas terhadap prosedur pemrograman dan *data-data* dari seluruh aktivitas organisasi. Tabel 15.1 memperlihatkan kelemahan-kelemahan tersebut dan akibat yang ditimbulkannya.

Tabel 15.1 Kelemahan-kelemahan dalam pengendalian umum.

Kelemahan-kelemahan	Dampak yang ditimbulkan
Pengendalian implementasi sistem	Sistem atau sistem baru yang dimodifikasi akan mengalami kesalahan atau tidak berfungsi seperti yang diharapkan.
Pengendalian Keamanan program	Dapat terjadi perubahan tanpa otorisasi yang dilakukan saat beroperasi, sehingga mengurangi tingkat keyakinan program atau sistem informasi yang telah dirubah tersebut.
Pengendalian *software* sistem	Pengendalian ini tidak memiliki dampak langsung terhadap aplikasi-aplikasi yang dibuat secara terpisah. Kecuali untuk *software* sistem informasi yang terintegrasi, pengendalian umum sangat tergantung kepadanya karena kelemahan pada bagian ini akan merusak pengendalian umum lainnya.
Pengendalian *hardware* secara fisik	*Hardware* mungkin saja tidak dapat berfungsi dengan baik dan menunjukkan berbagai kerusakan (error)

Lanjutan tabel 15.1

Kelemahan-kelemahan	Dampak yang ditimbulkan
Pengendalian pengoperasian komputer	Kesalahan mungkin saja terjadi dalam mengoperasikan sistem informasi, sehingga sistem informasi tidak beroperasi sebagaimana seharusnya
Pengendalian keamanan *data* dan jaringan komputer	Perubahan terhadap *data* yang tersimpan didalam sistem komputer dan akses terhadap informasi penting dapat saja terjadi dan dilakukan oleh orang yang tidak berwenang.
Pengendalian administratif	Seluruh bagian pengendalian akan dilaksanakan tidak sesuai dengan yang seharusnya.

15.2.2. Pengendalian Aplikasi

Otorisasi *input*, *Data* yang dimasukkan ke dalam komputer harus benar-benar diotorisasi, dicatat dan dimonitor sejak dokumen sumber *data* tersebut dibuat

Pengendalian aplikasi merupakan pengendalian khusus terhadap setiap aplikasi komputer yang digunakan, seperti aplikasi penggajian dan pemrosesan *order*. Pengendalian Ini meliputi prosedur-prosedur baik yang diotomatisasi maupun manual yang dilaksanakan untuk menjamin bahwa hanya *data-data* yang sah saja yang diproses secara lengkap dan akurat oleh suatu aplikasi.

Pengendalian bagi setiap aplikasi harus melibatkan semua rangkaian proses, baik secara manual maupun komputer, mulai dari langkah awal persiapan transaksi, pelaksanaan transaksi hingga dihasilkannya *output* dari transaksi yang dilakukan. Pengendalian aplikasi terfokus kepada hal-hal dibawah ini:

- **Kelengkapan *input* dan pemutakhiran *data*** - semua transaksi yang terjadi harus dimasukan dan dicatat ke dalam komputer.

- **Ketepatan *input* dan pemuktahiran *data*** - *data* yang disimpan didalam komputer harus benar-benar akurat dan disimpan pada *file* komputer yang benar.

- **Keabsahan/Validitas** - *data* harus diotorisasi atau setidaknya diperiksa kesesuaiannya dengan transaksi yang terjadi, atau dengan kata lain transaksi harus mencerminkan kejadian yang sebenarnya.

- **Pemeliharaan** - *data* pada komputer harus selalu dimutakhirkan agar sesuai dengan situasi kondisi saat ini.

Pengendalian aplikasi dapat diklasifikasikan menjadi:

(1) Pengendalian *input*/masukan,
(2) Pengendalian pemrosesan dan
(3) Pengendalian *output*/keluaran.

Pengendalian Input

Pengendalian *input* merupakan prosedur untuk memeriksa akurasi dan kelengkapan *data* pada saat dimasukkan pada sistem, termasuk juga otorisasi *input*, konversi *data* dan pemeriksaan ulang.

Pengendalian *input* memeriksa akurasi dan kelengkapan *data* ketika akan dimasukan kedalam sistem informasi. Ada beberapa pengendalian *input* tertentu untuk otorisasi, konversi *data*, perbaikan *data*, dan untuk menangani kesalahan.

- **Otorisasi *input data*** - *data* yang dimasukan ke dalam komputer harus benar-benar diotorisasi, dicatat dan dimonitor sejak dokumen sumber tersebut dibuat. Misalnya dengan menerapkan prosedur formal yang memberikan otorisasi hanya kepada karyawan tertentu dibagian penjualan untuk memasukan *data* pesanan *(order)*. Formulir penjualan harus diberi nomor seri, disusun berdasarkan kelompok dan dicatat sehingga transaksi tersebut dapat dilacak ketika saat selesai dibuat oleh bagian penjualan sampai kepetugas yang berwenang memasukkannya ke dalam komputer. Tumpukan dokumen tersebut harus ditan*data*ngani terlebih dahulu sebelum dimasukan ke dalam komputer.

Konversi data, proses untuk mengubah *data* dari satu bentuk ke bentuk lain pada transaksi komputer.

- **Konversi *data* -** *data* transaksi harus benar-benar dapat dipindahkan ke dalam komputer tanpa ada kesalahan ketika *data* tersebut direkam. Kesalahan perekaman dapat dihindari dengan memasukan *data* transaksi secara langsung dari dokumen ke komputer atau dengan menggunakan *scaner* pada *(Point-of-sales)* yang dapat membaca *data* penjualan secara langsung melalui *bar-code* yang terdapat pada barang yang dibeli. Mengotrol jumlah *data* yang telah masuk dapat dilakukan sebelum transaksi terjadi. Jumlah ini dapat bervariasi mulai dari jumlah dokumen sampai dengan total jumlah penjualan. Pada sistem *on-line* pengendalian *batch* dapat digunakan dengan mengontrol jumlah yang ada di komputer dengan yang ada di dokumen.

- ***Editing* -** berbagai sub program dapat dibuat untuk memperbaiki *data* yang salah dimasukan sebelum *data* tersebut diproses. *Data* yang diedit bila tidak memenuhi kriteria yang ditentukan, *data* tersebut tidak dapat di edit. Sub program untuk editing juga dapat melaporkan kesalahan-kesalahan yang harus diperbaiki. Keuntungan dari sistem '*on-line*' atau *'real time'* adalah editing dapat dilakukan terlebih dahulu saat ditemukan kesalahan sebelum diproses. Program komputer biasanya dipersiapkan untuk mendeteksi kalau ada kesalahan *data* yang dimasukan. Jika terjadi kesalahan yang tidak disengaja, kesalahan tersebut dapat diketahui dan diperbaiki oleh operator yang lainnya.

Tabel 15.2 Pengendalian *input*

Teknik pemeriksaan	Penjelasan	Contoh
Pemeriksaan potensial *(Reasonableness checks)*	Untuk diterima *data* harus sesuai dengan batas waktu yang telah ditentukan atau *data* akan ditolak	Jika transaksi *order* untuk 200 unit dan catatan *order* terbesar adalah 50 unit, maka transaksi akan ditolak.
Pemeriksaan Format *(Format checks)*	Karakteristik dari isi (huruf/angka), panjang dan tanda dari masing-masing *field data* telah diperiksa oleh komputer	Sembilan posisi dari nomor Jaminan Sosial tidak boleh berisi huruf.
Pemeriksaan keberadaan/validasi *(Existence checks)*	Komputer akan membandingkan *data* yang di*input* dengan tabel atau *file* master untuk meyakinkan bahwa codenya sah.	Seorang pegawai dapat memperoleh Standar Ketenagakerjaan jika kodenya 1,2,3,4 atau 5. Nilai lain akan ditolak.
Pemeriksaan ketergantungan *(Dependency checks)*	Komputer akan melakukan pemeriksaan hubungan logis antar *data* dari transaksi yang berhubungan. Bila tidak maka transaksi akan ditolak.	Transaksi kredit kendaraan harus memperlihatkan hubungan logis antara jumlah pinjaman, jumlah pembayaran kredit dan jumlah cicilan.
Pemeriksaan angka *(Checks digit)*	Menyimpan *data* kode angka sebagai referensi untuk mengontrol setiap kode angka yang dimasukkan dikemudian hari.	Mengecek kebenaran angka yang ditulis, apabila angka yang ditulis tidak sesuai dengan standar yang ada maka *data* akan ditolak. Misalnya kode standar 297437, *data* ditulis 29743, maka transaksi ini akan ditolak sampai dimasukan *data* dengan jumlah digit yang sebenarnya.

Pengendalian Pemrosesan

Pengendalian Pemrosesan aktivitas rutin untuk mengetahui bahwa *data* benar-benar lengkap dan akurat pada saat dimutakhirkan.

Pengendalian terhadap proses dilakukan dengan tujuan untuk meyakinkan bahwa *data* benar-benar lengkap dan akurat setelah dilakukan pemutakhiran *data*. Pengendalian terhadap pengolahan *data* ini dilakukan dengan cara mengontrol hasil penjumlahan atau perhitungan apakah telah sesuai dengan yang dirumuskan. Pengendalian terhadap pengolahan/pemrosesan meliputi pengendalian terhadap total, kesesuaian, dan edit

- **Pengendalian penjumlahan -** dilakukan dengan mencocokkan antara jumlah item yang telah di*input* dengan jumlah perubahan yang terjadi karena pemutakhiran *data*. Pemutakhiran dapat di kontrol dengan membandingkan jumlah total

yang muncul di layar atau *hardcopy* selama proses pemutakhiran dengan jumlah total *data* transaksi (kuantitas dan harga) pada dokumen yang dimasukan ke komputer dan dihitung secara manual.

Pencocokan dengan komputer proses pengontrolan menjamin bahwa *data* yang diinput sesuai dengan in*data* yang ada di *file* master.

- **Pengendalian kesesuaian dan editing** - yaitu mencocokan antara *data* yang di*input* dengan *data* yang ada di *file* master atau *file* lainnya, bila *data*nya tidak cocok maka harus dicatat untuk penyelidikan lebih lanjut. Pada umumnya penyesuaian terjadi selama *data* di*input*, tetapi penyesuaian dapat saja dilakukan pada saat pencocokan dilakukan setelah mendapat otorisasi dari yang berwenang untuk menyakinkan kelengkapannya. Dalam sistem informasi penyesuaian dilakukan dengan menggunakan fasilitas editing. Contohnya, mencocokan antara kartu tanda kehadiran karyawan dengan *data* yang ada di *file* master.

Pengendalian Output

Pengendalian *output* menjamin bahwa hasil dari proses komputer akurat, lengkap dan telah didistribusikan dengan tepat.

Pengendalian *output* dilakukan untuk meyakinkan bahwa hasil pemrosesan komputer betul-betul tepat, lengkap dan didistribusikan dengan baik. Umumnya pengendalian *output* terdiri dari :

- Menyamakan total *output* dengan total *input* atas proses yang dilakukannya.
- Me*review* catatan pengolahan komputer untuk meyakinkan bahwa semua pengolahan komputer telah dilakukan dengan benar
- Pemeriksaan terhadap laporan *output* dilakukan untuk meyakinkan bahwa jumlah, format dan rinciannya benar dan telah sesuai dengan *input*nya.
- Prosedur formal dan dokumentasi yang menunjukan hanya yang berhak saja yang telah menerima laporan, atau dokumen penting lainnya.

15.2.3. Keamanan dan e-Commerce (Transaksi secara elektronik)

Keamanan dalam komunikasi secara elektronik merupakan masalah utama bagi perusahaan yang menerapkan transaksi secara elektronik *(e-commerce)*. Bukan hanya masalah keamanan yang harus dipecahkan akan tetapi juga individu dan manajer suatu organisasi harus percaya bahwa masalah ini harus dipecahkan sebelum *e-commerce* benar-benar digunakan sepenuhnya.

Ini penting untuk diketahui bahwa *data* yang berhubungan dengan transaksi pembelian dan penjualan tersimpan secara rahasia ketika *data* tersebut dikirimkan secara elektronik.

Beberapa organisasi menggunakan *'encryption'* untuk melindungi pengiriman informasi rahasianya pada seluruh jaringan. *Encryption* adalah pengkodean dan pengacakan pesan untuk menjaga agar orang yang tidak berwenang tidak dapat mengakses atau memahami data yang sedang atau telah dikirimkan.

'Encryption' juga digunakan untuk melindungi pesan-pesan dalam *internet* dan jaringan umum lainnya karena jaringan tersebut sangat tidak aman. *'Encryption'* membantu melindungi pengiriman *data* pembayaran dan membantu dalam mengatasi masalah keaslian dan kelengkapan pesan. Kebenaran *(authentication)*, mengacu pada kemampuan setiap bagian untuk mengetahui bahwa bagian lain dalam transaksi benar-benar orang yang berhak melakukannnya. Dalam prosedur manual contohnya adalah penggunaan tanda tangan. Kelengkapan pesan *(message integrity)*, adalah kemampuan untuk meyakinkan bahwa pesan-pesan yang dikirim tiba tanpa ditiru atau dirubah.

Encryption adalah pengkodean dan pengacakan pesan untuk menjaga agar orang yang tidak berwenang tidak dapat mengakses atau memahami *data* yang sedang atau telah dikirimkan.

15.2.4. Pengembangan Struktur Pengendalian: Biaya dan Manfaat

Mekanisme pengendalian yang telah diuraikan di atas dapat dilaksanakan pada seluruh sistem informasi, tetapi akan membutuhkan biaya yang sangat mahal dan cukup rumit secara ekonomi atau tidak layak untuk dilaksanakan. Beberapa analisis biaya dan manfaat harus dilaksanakan untuk menentukan mekanisme pengendalian mana yang paling efektif tanpa harus mengorbankan efisiensi biayanya.

Salah satu dari kriteria dalam menentukan berapa luas pengendalian yang harus dilakukan pada suatu sistem informasi, sangat tergantung dari seberapa penting suatu *data* bagi perusahaan. Sistem informasi misalnya harus didahulukan dibanding sistem untuk pelatihan karyawan kalau pengolahan *data* lebih prioritas dari pengendalian.

'Standing data' adalah data yang permanen dan mempengaruhi arus data yang masuk dan keluar dari sistem informasi. Kesalahan dalam *data* transaksi tunggal akan berakibat hanya pada traksaksi itu sendiri. Tetapi kesalahan dalam *data* permanen *(file master)* akan berdampak kepada seluruh transaksi yang terjadi.

Efektivitas biaya pengendalian juga dipengaruhi oleh efisiensi, tingkat kerumitan dan biaya-biaya pada setiap penggunaan teknik pengendalian. Misalnya, pemeriksaan yang melakukan pengujian satu per satu secara lengkap akan memakan waktu yang lama dan secara operasional tidak mungkin dilaksanakan oleh sistem informasi yang memproses bejuta-juta pembayaran harian. Tetapi mungkin saja teknik ini dilaksanakan jika hanya untuk memverifikasi beberapa *data* penting seperti jumlah rupiah dan jumlah rekening tanpa memeriksa nama dan alamat.

Pertimbangan lainnya adalah tingkatan resiko jika aktivitas atau proses yang spesifik tidak terkendali dengan tepat. Penyusun sistem informasi dapat membuat pernyataan adanya resiko

yang menjelaskan masalah yang sering muncul dan kerusakan yang potensial terjadi. Misalnya jika kerusakan itu terjadi kurang dari setahun sekali dengan kerugian maksimum 1 juta rupiah, maka tidaklah layak untuk menghabiskan biaya 2 juta rupiah guna merancang dan memelihara pengendalian untuk melindungi dari kerusakan tersebut.

Pada situasi-situasi tertentu suatu organisasi tidak tahu betul kemungkinan terjadinya kerusakan pada sistem informasinya dan tidak akan dapat menentukan dampak yang mungkin ditimbulkan oleh kerusakan tersebut. Pada kondisi ini menurut Rainer Snyder dan Carr (1991) manajemen harus memilih untuk menerangkan resiko-resiko dan dampak yang ditimbulkannya secara kualitatif.

Untuk memutuskan pengendalian yang bagaimana yang akan digunakan, penyusun sistem informasi manajemen harus mengevaluasi berbagai teknik-teknik pengendalian dan hubungannya dengan efesiensi biaya. Kelemahan suatu pengendalian di satu sisi mungkin dapat ditutupi dengan kelebihan pengendalian pada sisi yang lain.

15.3 Audit Sistem Informasi

Setelah pengendalian diterapkan pada suatu sistem informasi, bagaimana cara untuk mengetahui bahwa pengendalian tersebut berjalan dengan efektif?. Untuk menjawab hal tersebut, suatu organisasi harus menyelenggarakan pemeriksaan/audit secara sistematis dan komprehensif. Organisasi yang besar biasanya memiliki bagian pemeriksaan intern yang bertanggungjawab untuk melaksanakan pemeriksaan terhadap sistem informasi yang diterapkan diperusahaannya.

15.3.1. Ketentuan dalam Audit Proses Pengendalian

Pernyataan adanya resiko ditentukan berdasarkan potensi munculnya masalah dan kerusakan

Pemeriksaan (audit) atas sistem informasi ditujukan untuk mengenali semua pengendalian yang mengatur sistem informasi itu sendiri dan menilai efektivitas pelaksanaannya. Untuk melaksanakan hal tersebut, seorang auditor harus memahami betul operasionalisasi, fasilitas-fasilitas fisik, telekomunikasi, sistem pengendalian, tujuan pengamanan *data*, struktur organisasi, personel, prosedur manual dan penerapan masing-masing aplikasi komputer.

Auditor harus mengumpulkan dan menganalisis semua bahan-bahan tentang sistem informasi yang diterapkan, seperti user dan dokumentasi sistem, contoh-contoh *input* dan *output*, dan dokumen-dokumen yang berhubungan dengan pelaksanaan pengendalian. Auditor biasanya melakukan wawancara dengan petugas yang menggunakan dan mengoperasikan sistem sesuai dengan aktivitas dan prosedurnya. Pengendalian untuk aplikasi yang digunakan, pengendalian secara keseluruhan, dan pengendalian terhadap disiplin. Auditor harus melacak arus sampel tran-

saksi dari sistem yang dipergunakan dan melakukan pengujian jika tersedia *software* untuk audit.

15.3.2. Pemeriksaan Terhadap Kualitas Data

Pemeriksaan kualitas data adalah penelaahan terhadap pemakai, *file-file* dan sampel dari *file* untuk menentukan akurasi dan kelengkapan data dalam sistem informasi manajemen.

Aspek yang terpenting dari pemeriksaan sistem informasi manajemen adalah analisis terhadap kualitas *data*. Pemeriksaan kualitas *data* dilakukan dengan menggunakan metode-metode berikut ini :

- Melakukan survey terhadap user untuk mendapatkan persepsi mereka tentang kualitas data.
- Melakukan survey terhadap seluruh *file-file data*
- Melakukan survey terhadap sampel data dari *file data*

Walapun tidak terlalu umum melakukan pemeriksaan terhadap kualitas *data*, namun organisasi tidak memiliki cara lain untuk mengetahui pada tingkat apa sistem informasi manajemen yang dimilikinya tidak akurat, tidak lengkap atau menyajikan informasi yang tidak jelas.

Data yang tidak akurat, tidak tepat waktu atau tidak konsisten dengan sumber informasinya, dapat menciptakan masalah operasional dan keuangan yang serius bagi aktivitas bisnis. Pada saat *data* yang tidak tepat tidak disimpan, maka akan melahirkan keputusan yang tidak benar, pengembalian produk yang secara umum menimbulkan kerugian bagi perusahaan.

Tidak memadainya kualitas *data* dapat terjadi karena berbagai sebab. Salah satunya disebabkan oleh kesalahan pada saat memasukan *data* atau karena adanya kesalahan dalam sistem informasi itu sendiri dan juga rancangan *database*nya. Menurut Wand dan Wang (1996) Sistem perlu dirancang sedemikian rupa sehingga sesuai dengan apa yang ada dilapangan dan memenuhi kebutuhan user.

Rangkuman

Dewasa ini setiap organisasi memiliki ketergantungan yang sangat tinggi pada sistem informasi berbasis komputer, dengan *data* yang mudah diubah kedalam bentuk-bentuk elektronik, maka otomatisasi semakin mudah terlaksana. Kemudahan ini pada akhirnya membuat *data-data* tersebut menjadi tidak aman dari kerusakan, kesalahan penggunaan, kecurangan dan kerusakan pada *hardware* maupun *software*. Akibat yang ditimbulkan oleh kerusakan sistem informasi manajemen dengan menggunakan komputer akan lebih parah dibandingkan dengan sistem yang disusun secara manual karena semua catatan-catatan dari fungsi-fungsi organisasi mungkin saja hancur atau hilang.

Untuk menghindari atau meminimalisasi kerusakan-kerusakan yang mungkin timbul maka suatu organisasi harus dapat menciptakan alat pengendalian yang efektif terhadap sistem informasi manajemen yang digunakannya. Pengendalian melindungi keamanan sistem informasi manajemen terutama untuk sistem jaringan yang dirancang secara *on-line*. Secara umum ada dua kategori pengendalian utama yaitu pengendalian umum dan pengendalian aplikasi.

Soal

1. Coba jelaskan mengapa sistem informasi berbasis komputer tidak aman.
2. Apa yang dimaksud dengan pengendalian, sebutkan dan jelaskan dua macam pengendalian ?
3. Sebutkan dan jelaskan bagian dari pengendalian umum ?
4. Sebutkan dan jelaskan unsur-unsur dari pengendalian aplikasi ?
5. Jelaskan apa yang dimaksud dengan *virus* dan *Hecker* ?

Tugas

1. Coba jelaskan ide anda untuk mengamnkan sistem informasi berbasis komputer apabila dihadapkan dengan masalah integritas dari SDM.
2. Coba jelaskan ide anda bagaimana menerapkan pengendalian umum di Indonesia bila dihadapkan kepada masalah sosial, ruangan komputer yang terbuka dan pengawasan teradap SDM yang lemah.
3. Coba jelaskan bagaimana penerapan pengendalian aplikasi untuk menghadapi perubahan terhadap *data* oleh pihak yang tidak berwenang.
4. Coba jelaskan dampak dari audit sistem informasi bila dilakukan oleh orang tidak paham komputer dan sistem informasi.
5. Coba jelaskan bagaimana pengamanan sistem informasi berbasis *internet* yang menggunakan *encription* dan *fire wall.*