PENGELOLAAN PENGENDALIAN SISTEM INFORMASI

Pengelolaan pengendalian-pengendalian (***Managing Controls***) yaitu kegiatan-kegiatan yang dilakukan Manajer Sistem Informasi untuk menyakinkan bahwa pengendalian-pengendalian di dalam sistem teknologi informasi masih tetap dilakukan dan masih efektif dalam mencegah ancaman dan gangguan terhadap sistem informasi.

Tujuan dari sistem informasi tidak akan mengena jika sistem ini terganggu, sehingga sistem informasi harus mempunyai pertahanan terhadap ancaman dan gangguan tersebut, dan pertahanan ini harus dilakukan terus menerus.

Pengendalian di sistem teknologi informasi terbagi menjadi dua kelompok, yaitu :

A. Pengendalian secara umum (*General Controls*)
B. Pengendalian aplikasi (*Application Controls*)

A. PENGENDALIAN SECARA UMUM

Pengendalian secara umum merupakan pengendalian-pengendalian sistem teknologi informasi yang paling luar yang harus dihadapi terlebih dahulu oleh pemakai sistem informasinya.

Pengendalian secara umum terdiri dari :

1. Pengendalian organisasi
2. Pengendalian dokumentasi
3. Pengendalian kerusakan perangkat keras
4. Pengendalian keamanan fisik
5. Pengendalian keamanan data

A. 1. Pengendalian Organisasi

Perencanaan yang baik dan organisasi sistem informasi yang berfungsi seperti yang diharapkan merupakan **pengendalian organisasi** yang baik. Pengendalian organisasi ini dapat tercapai bila ada **pemisahan tugas** dan **pemisahan tanggung jawab** yang tegas.

Pemisahan ini dapat berupa pemisahan tugas dan tanggung jawab di antara departemen dan pemisahan tugas dan tanggung jawab di dalam departemen sistem informasi itu sendiri.

Fungsi-fungsi utama dalam departemen sistem informasi harus dipisahkan tugas dan tanggung jawabnya. Fungsi-fungsi utama yang perlu dipisahkan tugas dan tanggung jawabnya adalah :

1) Bagian pengontrol data
2) Bagian yang mempersiapkan data
3) Bagian operasi komputer
4) Bagian pustaka data
5) Bagian pemrograman dan pengembangan sistem
6) Bagian pusat informasi

- **Bagian pengontrol data (*data control section*)** berfungsi sebagai penengah antara departemen sistem informasi dengan departemen lainnya. Bagian ini berfungsi menerima data dari departemen lainnya, mengagendakannya, membuat *batch control total*, mengawasi jalannya pengolahan data, memonitor koreksi kesalahan selama pengolahan data dan mendistribusikan output kepada pemakai yang berhak.

- **Bagian yang mempersiapkan data (*data preparation section*)** berfungsi untuk mempersiapkan data, melengkapinya (misalnya menambah dangan kode-kode yang diperlukan) dan memverifikasi kebenarannya, sehingga siap untuk dimasukkan ke dalam sistem.

- **Bagian yang mengoperasikan data (*data processing section*)** merupakan bagian yang berfungsi mengolah data sampai dihasilkan laporan. Personil bagian ini disebut ***Computer Operator*** dan bekerja sesuai dengan prosedur yang tertulis di dalam manual pengoperasian.

- **Bagian penyimpan data (*data library section*)** berfungsi menjaga ruangan penyimpanan data yang disebut dengan perpustakaan data. **Perpustakaan data (*data library*)** merupakan tempat dimana data dan program disimpan dalam media simpanan luar. Personil bagian ini disebut **Pustakawan (*Librarian*)**

  Tujuan utama dari fungsi perpustakaan data ini adalah untuk pemisahan tugas dan tanggung jawab antara bagian yang menyimpan data dengan bagian yang akan menggunakannya untuk operasi, sehingga dapat mencegah orang yang tidak berhak untuk mengaksesnya.

- **Bagian pemrograman dan pengembangan sistem** berfungsi didalam pembuatan program dan pengembangan sistem informasi. Personil bagian ini disebut dengan ***Programmer*** dan ***System Analyst***.

  Bagian ini harus dipisahkan dengan bagian operasi dan tidak boleh terlibat dalam pengoperasian secara langsung karena dapat mengubah program yang dipergunakan untuk maksud-maksud negatif.

- **Bagian pusat informasi** dibuat dengan maksud untuk membantu para manajernya membuat program aplikasi sendiri untuk keperluan *end user computing* atau *end user development*.

A.2. Pengendalian Dokumentasi

Lihat penjelasannya di materi Dokumentasi.

A.3. Pengendalian Kerusakan Perangkat Keras

Proses pengolahan data dapat terganggu jika terjadi kerusakan perangkat keras yang dapat menyebabkan kemacetan proses. Untuk mencegah hal ini, maka dapat dilakukan dengan pengendalian perangkat keras, menyediakan perangkat keras cadangan dan membeli asuransi.

Pengendalian perangkat keras komputer merupakan pengendalian yang sudah dipasang di dalam komputer itu (*built in*) oleh pabrik pembuatnya. Pengendalian ini dimaksudkan **untuk mendeteksi kesalahan atau tidak berfungsinya perangkat keras (*hardware malfunction*)**.

Pengendalian perangkat keras dapat berupa :

- **Pemeriksaan pariti (*Parity Check*)**
  RAM mempunyai kemampuan untuk melakukan pengecekan dari data yang disimpannya, yang disebut dengan ***parity check***. Bila data hilang atau rusak, dapat diketahui dari sebuah bit tambahan yang disebut dengan ***parity bit*** atau ***check bit***. Misalnya 1 byte memory di RAM terdiri dari 8 bit, sebagai parity bit digunakan sebuah bit tambahan, sehingga menjadi 9 bit.

- **Pemeriksaan gaung (*Echo Check*)**
  Tujuan dari pengecekan ini adalah untuk menyakinkan bahwa alat-alat input/output seperti misalnya printer, tape drive, disk drive, dsb masih tetap berfungsi dengan memuaskan bila akan dipergunakan.

- **Pemeriksaan baca setelah rekam (*Read after write check*)**
  Tujuan dari pengecekan ini adalah untuk menyakinkan bahwa data yang telah direkam ke media simpanan luar telah terekam dengan baik dan benar. Untuk mengetahui hal ini, setelah data direkam, maka dibaca kembali untuk dibandingkan dengan data yang direkamkan, kalau sama berarti telah direkam dengan benar.

- **Pemeriksaan baca ulang (*Dual read check*)**
  Tujuan dari pengecekan ini adalah untuk menyakinkan apakah data yang telah dibaca, telah dibaca dengan benar. Untuk maksud ini, data yang dibaca, dibaca sekali lagi dan dibandingkan keduanya, bila sama berarti telah dibaca dengan benar tanpa kesalahan.

- **Pemeriksaan validitas (*Validity Check*)**
  Tujuan dari pengecekan ini adalah untuk menyakinkan bahwa data telah dikodekan dengan benar.

Pengendalian kerusakan perangkat keras berikutnya adalah dengan menyediakan perangkat keras cadangan yang akan digunakan jika perangkat keras utama rusak atau macet.

Menyediakan perangkat keras cadangan merupakan hal yang sangat mahal. Sebagai alternatif menggunakan perangkat keras cadangan, beberapa organisasi menggunakan processor cadangan. Jika processor utama rusak, maka processor kedua sebagai processor cadangan akan digunakan, sehingga proses pengolahan data tidak terganggu. Sistem komputer seperti ini disebut ***Dual processor computer*** atau ***Fault tolerant computer***.

Membeli asuransi merupakan pengendalian lainnya untuk menangani perangkat keras yang rusak. Jika perangkat keras rusak, maka pihak asuransi akan bertanggung jawab untuk memperbaiki atau menggantinya.

A.4. Pengendalian Keamanan Fisik

Pengendalian keamanan fisik perlu dilakukan untuk menjaga keamanan terhadap perangkat keras, perangkat lunak, dan manusia di dalam perusahaan.

Pengendalian keamanan fisik dapat dilakukan sebagai berikut :

1) **Pengawasan terhadap pengaksesan fisik**
   Pengawasan ini merupakan proteksi yang berupa pembatasan terhadap orang-orang yang akan masuk ke bagian yang penting.

   Pengawasan ini dapat dilakukan dengan cara :
   - Penempatan satpam
   - Pengisian agenda kunjungan
   - Penggunaan tanda pengenal
   - Pemakaian kartu
   - Penggunaan *Closed-Circuit Television*

2) **Pengaturan lokasi fisik**
   Lokasi ruang komputer merupakan pertimbangan yang penting di dalam perencanaan sekuriti. Pengendalian terhadap lokasi fisik yang baik dari ruang komputer dapat berupa :
   - Lokasi yang tidak terganggu oleh lingkungan
   - Gedung yang terpisah
   - Tersedia fasilitas cadangan

3) **Penerapan alat-alat pengaman**
   Alat-alat pengaman tambahan dapat digunakan untuk mengendalikan hal-hal yang dapat terjadi yang dapat menyebabkan sesuatu yang fatal. Alat-alat pengaman tersebut dapat berupa :
   - Saluran air
   - Alat pemadam kebakaran
   - UPS (*Uninteruptible Power Systems*)

4) **Stabilizer**

5) **AC (*Air Conditioner*)**

6) **Pendeteksi kebakaran**

A.5. Pengendalian Keamanan Data

Menjaga integritas dan kemanan data merupakan pencegahan terhadap keamanan data yang tersimpan di simpanan luar supaya tidak hilang, rusak dan diakses oleh orang yang tidak berhak.

Cara-cara pengendalian keamanan data :

1) Dipergunakan *Data Log*

Agenda (*Log*) dapat digunakan pada proses pengolahan data untuk memonitor, mencatat dan mengidentifikasi data. Kumpulan data yang akan dimasukkan ke departemen sistem informasi seharusnya dicatat terlebih dahulu oleh ***data control group***. File dan program yang dibutuhkan pada operasi pengolahan data juga harus dicatat oleh ***librarian*** di ***library log***. Dengan demikian segala sesuatu yang dapat mempengaruhi perubahan data dapat diketahui, diidentifikasi dan dilacak.

Disamping ***data log***, dapat juga digunakan ***transaction log***, yaitu suatu file yang akan berisi nama-nama pemakai komputer, tanggal, jam, tipe pengolahannya, lokasi, dsb tentang penggunaan sistem informasi yang perlu diketahui.

2) Proteksi File

Beberapa alat atau teknik tersedia untuk menjaga file dari penggunaan yang tidak benar yang dapat menyebabkan rusak atau tergantinya data dengan nilai yang tidak benar, diantaranya adalah :

- Cincin proteksi pita magnetik
- *Write-protect tab*
  Suatu *tab* yang dapat digeser naik atau turun di disket untuk membuat disket hanya dapat dibaca.
- Label ekternal dan label internal
- *Read-only storage*

3) Pembatasan pengaksesan (*access restriction*)

Tujuan sekuriti yang penting adalah untuk mencegah personil yang tidak berwenang untuk dapat mengakses data.
Pengaksesan harus dibatasi untuk mereka yang tidak berhak dengan cara :

- Isolasi fisik
  Data yang penting dapat secara fisik diisolasi dari penggunaan personil-personil yang tidak berhak.

- Otorisasi dan identifikasi
  Tiap-tiap personil yang berhak mengakses data telah diotorisasi dan diberi pengenal (diidentifikasi) dengan memberikan ***password*** kepada personil.

- *Automatic lockout*
  Untuk mencegah seseorang mencoba-coba password berulang-ulang, biasanya mencoba password hanya diberikan kesempatan tiga kali.

- Pembatasan pemakaian
- Mengunci keyboard

4) Data *back-up* dan *recovery*

Pengendalian *back-up* dan *recovery* diperlukan untuk berjaga-jaga jika file atau database mengalami kerusakan, kesalahan data, atau kehilangan data.

Back-up adalah salinan dari file atau database di tempat yang terpisah.
Recovery adalah file /atau database yang telah diperbaiki dari kerusakan, kesalahan atau kehilangan datanya.

Ada 5 tipe penyebab yang dapat mengakibatkan kesalahan, kerusakan atau kehilangan data :
- Disebabkan oleh kesalahan program (*program error*)
- Disebabkan oleh kesalahan perangkat lunak sistem (*systems software error*)
- Disebabkan oleh kegagalan perangkat keras (*hardware failure*)
- Disebabkan oleh kesalahan prosedur (*procedural error*)
- Disebabkan oleh kegagalan lingkungan (*environmental failure*)

B. PENGENDALIAN APLIKASI

Pengendalian aplikasi merupakan pengendalian yang dipasang pada pengolahan aplikasinya.
Pengendalian aplikasi terdiri dari :
1. Pengendalian-pengendalian Masukan (*Input Control*)
2. Pengendalian-pengendalian Pengolahan (*Processing Control*)
3. Pengendalian-pengendalian Keluaran (*Output Controls*)

B.1. Pengendalian-pengendalian Masukan

Pengendalian masukan mempunyai tujuan untuk meyakinkan bahwa data transaksi yang valid telah lengkap, terkumpul semuanya serta bebas dari kesalahan sebelum dilakukan proses pengolahannya.

Data input yang akan dimasukkan ke dalam komputer dapat melibatkan dua tahap, yaitu :

a) ***Data Capture*** **(Penangkapan data)** merupakan proses mengidentifikasikan dan mencatat kejadian nyata yang terjadi akibat transaksi yang dilakukan oleh organisasi.
b) ***Data Entry (Pemasukan data)*** merupakan proses membacakan atau memasukkan data ke dalam komputer.

Pada tahap *data capture* dapat dilakukan pengendalian sbb :

1) Nomor urut tercetak pada dokumen dasar
Dokumen dasar harus diberi nomor urut yang sudah tercetak. Tujuan dari pengendalian ini adalah untuk mengetahui bila ada dokumen yang hilang.

2) Ruang maksimum untuk masing-masing field di dokumen dasar
Dokumen dasar dirancang sedemikian rupa sehingga tidak ada field data yang meleset, yang dapat dilakukan dengan menyediakan ruang maksimum untuk masing-masing field data, sehingga kelebihan digit atau karakter dapat terlihat. Pengendalian ini merupakan pengendalian untuk kebenaran data.

3) Kaji ulang data
Personil yang mengisi dokumen dasar harus mengkaji ulang kembali data yang dicatatnya, dengan cara meneliti kembali kelengkapan dan kebenaran datanya.

4) Verifikasi data
Dokumen dasar yang sudah diisi oleh seorang personil dapat diverifikasi kelengkapan dan kebenarannya oleh personil yang lainnya.

Pengendalian pada tahap pemasukkan data berupa pengecekan yang telah terprogram di dalam program aplikasi dan disebut dengan ***Programmed Check*** **(pengecekan program)**.

Pengendalian yang ada di *programmed check* dapat berupa :

1) Echo check

Data yang diketikkan pada keyboard untuk dimasukkan ke komputer akan ditampilkan (*echo*) pada layar terminal. Dengan demikian operator dapat membandingkan antara data yang diketikkan dengan data yang seharusnya dimasukkan. Program dibuat sedemikian rupa dengan memberikan kesempatan pada operator untuk memperbaiki bila data yang diketikkan salah.

2) Existence check

Kode yang dimasukkan dibandingkan dengan daftar kode-kode yang valid dan sudah diprogram.

3) Matching check

Pengecekan ini dilakukan dengan membandingkan kode yang dimasukkan dengan field di file induk bersangkutan.

4) Field check

Field dari data yang dimasukkan diperiksa kebenarannya dengan mencocokkan nilai dari field data tersebut dengan tipe field-nya, apakah bertipe numerik, alphabetik, atau tanggal.

5) Sign check

Field dari data yang bertipe numerik dapat diperiksa untuk menentukan apakah telah berisi dengan nilai yang mempunyai tanda yang benar, positif atau negatif.

6) Relationship check atau logical check

Hubungan antara item-item data input harus sesuai dan masuk akal. Pengecekan ini berfungsi untuk memeriksa hubungan antara item-item data input yang dimasukkan ke komputer. Kalau tidak masuk akal, maka akan ditolak oleh komputer.

7) Limit check atau reasonable check

Nilai dari input data diperiksa apakah cukup beralasan atau tidak. Contohnya,tanggal transaksi yang terjadi adalah 30 Februari 2000 adalah tidak beralasan.

8) Range check

Nilai yang dimasukkan dapat diseleksi supaya tidak keluar dari jangkauan nilai yang sudah ditentukan.

9) ***Self-checking digit check***

Self-checking digit check adalah pengecekan untuk memeriksa kebenaran dari digit-digit data yang dimasukkan. Pengecekan ini digunakan karena operator cenderung melakukan kesalahan memasukkan digit-digit data.

10) ***Sequence check***

Sequence check memeriksa urutan dari record data yang dimasukkan dengan cara membandingkan nilai field record tersebut dengan nilai field record sebelumnya yang terakhir dimasukkan.

11) ***Label check***

Untuk menghindari kesalahan penggunaan file, maka label internal yang ada di simpanan luar dapat diperiksa untuk dicocokkan dengan yang seharusnya digunakan.

12) ***Batch control total check***

Batch control total check umumnya diterapkan pada pengolahan data dengan metode ***batch processing***.

13) ***Zero-balance check***

Bila transaksi yang dimasukkan merupakan nilai-nilai yang saling mengimbangi, misalnya nilai-nilai debet dan nilai-nilai kredit, maka nilai-nilai tersebut harus imbang atau kalau dikurangkan selisihnya harus nol. *Zero-balance check* akan melakukan pengecekan selisih antara dua sisi tersebut harus imbang.

B.2. Pengendalian-pengendalian Pengolahan

Tujuan dari pengendalian-pengendalian pengolahan adalah untuk mencegah kesalahan-kesalahan yang terjadi selama proses pengolahan data yang dilakukan setelah data dimasukkan ke dalam komputer. Kesalahan pengolahan dapat terjadi karena program aplikasi yang digunakan untuk mengolah data mengandung kesalahan.

Kesalahan-kesalahan yang umumnya disebabkan oleh kesalahan dalam program adalah :

1) ***Overflow***
   Overflow terjadi jika proses pengolahan mengandung perhitungan yang hasilnya terlalu besar atau terlalu kecil, sehingga tidak muat untuk disimpan di memori komputer. Jika terjadi *overflow*, maka hasil dari proses pengolahan data menjadi tidak tepat lagi.

2) **Kesalahan logika program**
   Kesalahan ini merupakan kesalahan yang berbahaya dan sulit untuk dilacak, karena kesalahan logika program tidak dapat ditunjukkan oleh komputer dan tetap akan didapatkan hasilnya, tetapi dengan hasil yang salah.

3) **Logika program yang tidak lengkap**

4) **Penanganan pembulatan yang salah**
   Permasalahan pembulatan terjadi bila tingkat ketepatan yang diinginkan dari perhitungan arithmatika lebih kecil dari tingkat ketepatan yang terjadi.

5) **Kesalahan akibat kehilangan atau kerusakan record.**

6) **Kesalahan urutan data**

7) **Kesalahan data di file acuan (*reference file*)**

8) **Kesalahan proses serentak**
   Kesalahan proses serentak (*concurency*) terjadi jika sebuah file di dalam basis data dipergunakan oleh lebih dari seorang pemakai dalam *network*.

B.3. Pengendalian-pengendalian Keluaran

Keluaran (output) yang merupakan produk dari pengolahan data dapat disajikan dalam bentuk ***hard copy*** dan ***soft copy***. Pengendalian-pengendalian keluaran dimaksudkan untuk diterapkan pada kedua macam bentuk keluaran tersebut.

Dalam bentuk *hard copy* keluaran yang paling banyak dilakukan adalah berbentuk laporan yang dicetak menggunakan printer.

Dalam bentuk *soft copy* yang paling umum adalah berbentuk tampilan di layar terminal.

Untuk menghasilkan laporan yang berbentuk *hard copy* dapat dilakukan melalui beberapa tahapan, yaitu :

1) Tahap menyediakan media laporan
2) Tahap memproses program yang menghasilkan laporan
3) Tahap pembuatan laporan di printer file
4) Tahap pengumpulan laporan
5) Tahap mencetak laporan di media kertas
6) Tahap mengkaji ulang laporan
7) Tahap pemilahan laporan
8) Tahap distribusi laporan
9) Tahap kaji ulang laporan oleh pemakai laporan
10) Tahap pengarsipan laporan
11) Tahap pemusnahan laporan yang sudah tidak diperlukan

Pengendalian-pengendalian keluaran yang dapat dilakukan untuk masing-masing tahap keluaran adalah sebagai berikut :

1) **Pengendalian pada tahap penyediaan media laporan.**
   Pengendalian terhadap penyimpanan media laporan ini dapat dilakukan dengan cara sebagai berikut :
   - Menyelenggarakan sistem penyimpanan media laporan tercetak.
   - Pengendalian terhadap pengaksesannya
   - Pemberian nomor urut
   - Penyimpanan cap pengesahan yang terpisah

2) **Pengendalian pada tahap pemrosesan program penghasil laporan.**
   Pengendalian pada proses program yang digunakan untuk mencetak laporan merupakan pengecekan-pengecekan yang sudah dipasang di dalam program. Pengendalian ini bertujuan untuk menjamin kebenaran dan kelengkapan informasi yang dicetak di dalam laporan.

3) **Pengendalian pada tahap pembuatan printer file.**
   Kemungkinan suatu laporan tidak langsung dicetak ke printer, tetapi direkam terlebih dahulu ke file, karena disebabkan oleh beberapa hal, seperti :
   - Menunggu printer yang sedang digunakan oleh proses yang lain.
   - Bentuk dan isi laporan akan dimodifikasi kembali.

Kalau printer file digunakan, maka harus dilakukan pengendalian-pengendalian sebagai berikut :

- Isi dari pinter file tidak dapat diubah oleh orang lain yang tidak berhak.
- Printer file tidak disalin oleh orang lain yang tidak boleh melihat isi laporan.
- Printer file hanya dicetak untuk keperluan yang sah saja dan dihapus bila sudah tidak diperlukan

4) Pengendalian pada tahap pencetakan laporan.

Pengendalian pada tahap ini mempunyai dua tujuan utama untuk :

- meyakinkan bahwa yang dicetak hanya sejumlah tembusan yang diperlukan saja
- mencegah isi dari laporan tidak terbaca oleh orang lain yang tidak berhak

5) Pengendalian pada tahap pengumpulan laporan.

Setelah laporan dicetak, maka harus dikumpulkan segera oleh staf bagian pengendalian. Semua laporan dapat diletakkan terlebih dahulu di tempat yang khusus dan terkunci sebelum didistribusi-kan. Laporan tidak boleh ditinggal di ruang komputer secara sembarangan, karena dapat hilang atau terbaca oleh orang lain yang tidak berhak.

6) Pengendalian pada tahap kaji ulang laporan.

Sebelum laporan didistribusikan dan digunakan oleh pemakai laporan, maka laporan-laporan tersebut harus bebas dari kesalahan serta harus mencerminkan informasi yang tidak menyesatkan. Untuk itu laporan sebelum didistribusikan harus diperiksa kembali atau dikaji ulang terhadap kesalahan yang tampak, misalnya field yang mengandung nilai yang tidak masuk akal, cetakan yang tidak benar, data yang hilang atau tidak terbaca, dsb.

7) Pengendalian pada tahap pemilahan program.

Jika laporan terdiri dari beberapa halaman atau terdiri dari beberapa macam untuk beberapa pemakai yang berbeda, maka laporan tersebut perlu untuk dipilah dalam kelompok-kelompok tertentu. Staf bagian pengendalian harus turut mengawasi dan mengecek bahwa laporan-laporan tersebut telah lengkap, tidak ada yang hilang dan tidak difotokopi atau disalin. Kemudian laporan yang sudah dipilah harus langsung didistribusikan.

8) **Pengendalian pada tahap distribusi laporan.**
Pengendalian yang dapat diterapkan pada tahap ini adalah :
- Laporan dapat diberi tanggal kapan dibuat, sehingga distribusi yang terlambat dapat diketahui oleh pemakainya.
- Dibuat daftar distribusi siapa-siapa saja yang berhak untuk menerima laporan, sehingga distribusi tidak keliru ke pihak lain yang tidak berhak.
- Untuk laporan yang penting, harus dibuat daftar penerimaan yang ditandatangani oleh si penerima laporan sebagai bukti bahwa laporan telah didistribusikan dan diterima dengan benar dan lengkap.

9) **Pengendalian pada tahap kaji ulang oleh pemakai.**
Penerima laporan sebaiknya mengkaji ulang isi dari laporan yang diterimanya sebelum menggunakannya untuk mendeteksi kesalahan yang mungkin ada. Pemakai laporan harus memberikan umpan balik kepada bagian Sistem Informasi terhadap kesalahan atau ketidaksesuaian serta perbaikan lebih lanjut terhadap laporan yang digunakannya, sehingga untuk di kemudian hari laporan dapat lebih efektif.

10) **Pengendalian pada tahap pengarsipan laporan.**
Jika laporan sudah tidak digunakan lagi oleh pemakai laporan pada suatu saat tertentu, tetapi masih penting untuk digunakan di masa mendatang, maka laporan tersebut harus diarsip dengan baik. Pengarsipan laporan harus aman, tidak mudah dijangkau oleh orang lain yang tidak berhak.

11) **Pengendalian pada tahap pemusnahan laporan.**
Bila laporan sudah tidak digunakan lagi selamanya, maka laporan harus dimusnahkan. Pemusnahan laporan harus benar-benar dilakukan tak berbekas, yang dapat dilakukan dengan dibakar atau dihancurkan dengan alat pengracik kertas.

Laporan yang berbentuk *soft copy*, informasi ditampilkan pada layar terminal. Pengendalian yang dilakukan pada laporan yang berbentuk soft copy meliputi :

1) **Pengendalian pada informasi yang ditansmisikan**
Pengendalian ini dimaksudkan supaya orang yang tidak berhak tidak dapat menyadap di tengah jalur untuk informasi yang dikirimkan.

Kalau transmisi informasi menggunakan jalur telekomunikasi, maka dapat dilakukan dengan **menyandikan** (*encryption*) informasi yang ditransmisikan. Kalau pengiriman informasi sifatnya lokal dengan menggunakan kabel, maka jalur kabel harus diawasi supaya **penyadapan kabel** (***wiretapping***) dapat dicegah.

2) Pengendalian pada tampilan di layar terminal
Pengendalian ini berguna untuk mencegah mereka yang tidak berhak untuk dapat melihat informasi yang ditampilkan di layar terminal.

Pengendalian ini dapat dilakukan dengan beberapa cara :
- Menempatkan masing-masing terminal di ruangan yang terpisah.
- Menampilkan informasi yang penting dan tidak ingin terlihat orang lain dengan tampilan **intensitas rendah** (***low intensity***) di layar terminal, sehingga tidak mudah dibaca dari jarak jauh.
- Meletakkan terminal yang menghadap ke tembok, sehingga tidak mudah terlihat bagi mereka yang lewat.

MEMERIKSA KEEFEKTIFAN PENGENDALIAN-PENGENDALIAN YANG DIPASANG

Salah satu cara untuk menyakinkan bahwa pengendalian-pengendalian telah diterapkan dan beroperasi semestinya dapat dilakukan dengan memeriksa pengendalian-pengendalian yang ada secara rutin. Cara ini disebut dengan **Pemeriksaan Sistem-sistem Informasi** (***Information Systems Audit***)

Pengauditan sistem-sistem informasi didefinisikan oleh **Weber** (1999) sebagai ***: suatu proses mengumpulkan dan mengevaluasi bukti untuk menentukan apakah suatu sistem komputer telah menjaga aktiva-aktiva, menjaga integritas data, membuat sasaran organisasi dicapai secara efektif dan menggunakan sumber-sumber daya secara efisien.***

Pengauditan sistem-sistem informasi mempunyai tujuan untuk :
a. Meningkatkan keamanan dari aktiva-aktiva
b. Meningkatkan integritas data
c. Meningkatkan efektivitas sistem
d. Meningkatkan efisiensi sistem

Pengauditan sistem-sistem informasi menggunakan lima macam prosedur sebagai berikut :

1. **Prosedur-prosedur untuk mendapatkan pemahaman dari pengendalian-pengendalian yang ada.**
   Teknik-teknik yang digunakan adalah bertanya, inspeksi dan observasi untuk mendapatkan pemahaman apakah pengendalian-pengendalian sudah diterapkan.

2. **Pengujian terhadap pengendalian-pengendalian (*Test of controls*).**
   Teknik-teknik yang digunakan adalah bertanya, inspeksi dan observasi untuk menilai apakah pengendalian-pengendalian yang ada sudah beroperasi dengan efektif.

3. **Pengujian terhadap nilai-nilai transaksi secara terinci (*Substantive tests of details of transactions*).**
   Pengujian ini dilakukan untuk mendeteksi kesalahan-kesalahan rupiah di transaksi-transaksi yang dapat mengakibatkan kesalahan di laporan-laporan keuangan.

4. **Pengujian terhadap nilai-nilai di saldo rekening secara terinci (*Substantive tests of details of account balances*).**
   Pengujian ini difokuskan pada saldo-saldo rekening-rekening neraca dan laporan rugi laba.

5. **Prosedur-prosedur kaji analitikal (*Analytical review procedures*).**
   Pengujian ini difokuskan pada hubungan antara item-item data dengan maksud untuk mengidentifikasikan area-area yang membutuhkan pekerjaan audit lebih lanjut.