Materi Inisiasi 7

PENGENDALIAN SISTEM INFORMASI

A. PENDAHULUAN

Modul ini akan membahas tentang pengendalian yang harus ada pada sistem informasi. Tujuan dari sistem informasi tidak akan tercapai jika sistem ini mudah terganggung sehingga sistem informasi harus memiliki pertahanan dan pertahanan itu harus dilakukan terus menerus. Pertahanan dari sistem informasi sering disebut sebagai pengendalian dan keamanan sistem informasi (*information system control and security*) untuk menghindari fasilitas dan proses pada komputer dari gangguan-gangguan yang disengaja maupun yang tidak disengaja dan menyebabkan beberapa perubahan, kerusakan atau pencurian sumbersumber daya sistem informasi secara tidak sah.

Sistem informasi mempunyai dua kelompok pengendalian yang perlu dikelola secara terus-menerus selama sistem tersebut dioperasikan, yaitu pengendalian secara umum (*general controls*) dan pengendalian aplikasi (*application controls*).

B. PENGENDALIAN SECARA UMUM

Sistem informasi perlu dipasang dengan perangkat pengendalian sehingga dapat mencegah dan mendeteksi gangguan-gangguan yang akan terjadi. Pengendalian pada sistem informasi adalah pengendalian secara umum (*general controls*) dan pengendalian aplikasi (*application controls*).

Pengendalian secara umum (*general controls*) merupakan pengendalian sistem teknologi informasi yang harus dihadapi terlebih dahulu oleh pemakai sistem informasinya. Jika pengendalian secara umum dapat dilewati maka pengendalian aplikasi dapat diaktifkan. Pengendalian-pengendalian secara umum terdiri dari beberapa bagian, yaitu sebagai berikut ini.

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

PENGENDALIAN ORGANISASI

Perencanaan yang baik dan organisasi sistem informasi yang berfungsi sesuai yang diharapkan merupakan pengendalian organisasi yang baik. Pengendalian organisasi ini dapat tercapai apabila ada pemisahan tugas (*segregation of duties)* dan pemisahan tanggung jawab (*segregation of responsibilities)* yang tegas. Pemisahan ini dapat berupa tugas dan tanggung jawab di antara departemen maupun di dalam departemen sistem informasi itu sendiri. Pemisahan tugas dan tanggung jawab di antara departemen dapat berupa sebagai berikut:

1. Pemisahan tugas dan tanggung jawab antara pemberi wewenang transaksi dengan bagian yang menyimpan aktiva bersangkutan.
2. Pemisahan tugas dan tanggung jawab antara bagian penyimpanan aktiva dengan bagian pelaksanaan.

3. Pemisahan tugas dan tanggung jawab antara bagian pelaksanaan dengan bagian yang melakukan pengolahan data.
4. Pemisahan tugas dan tanggung jawab antara bagian pelaksanaan dengan bagian yang melakukan pengolahan data.
5. Pemisahan tugas antara bagian penyimpanan aktiva dengan bagian pengolahan data.
6. Pemisahan tugas dan tanggung jawab antara yang melakukan koreksi kesalahan transaksi dengan bagian pengolahan data.

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 pemrogram dan pengembangan sistem, dan (6) bagian pusat informasi (*information center*)

Bagian pengontrol data (*data controlsection*) berfungsi sebagai penengah antara departemen-departemen lainnya dengan departemen sistem informasi. Personil-personil bagian ini sering disebut dengan *data control group*. *Data control group*adalah yang menerima data dari departemen-departemen lainnya, mengagendakannya, membuat *batch control total*, mengawasi jalannya pengolahan data, dan mendistribusikan *output* kepada pemakai yang berhak.

Bagian yang mempersiapkan data data (*data preparation section*) berfungsi untuk mempersiapkan data, melengkapinya (misalnya menambah kode-kode yang diperlukan), dan memverifikasi kebenaran data sehingga siap untuk dimasukkan ke dalam sistem. Bagian yang mengoperasikan data (*data processing section*) merupakan bagian yang berfungsi mengolah data sampai sampai menghasilkan laporan. Anggota pada bagian ini disebut *computer operator* dan bekerja sesuai dengan prosedur yang tertulis di dalam manual pengoperasian.

Bagian penyimpanan data (*data library section*) berfungsi menjaga ruangan penyimpanan data yang disebut dengan perpustakaan data. Perpustakaan data (*data libarary*) merupakan tempat di mana data dan program disimpan dalam bentuk media simpanan luar. Anggota bagian ini disebut dengan pustakawan (*librarian*). Tujuan utama dari perpustakaan data ini adalah untuk pemisahan tugas dan tanggung jawab antara bagian yang menyimpan data dengan bagian yang akan menggunakannya untuk pengoperasian sehingga dapat mencegah orang yang tidak berhak untuk mengaksesnya.

Bagian pemrograman dan pengembangan sistem berfungsi untuk membuat program dan mengembangkan sistem informasi. Anggota bagian ini disebut dengan pemrogram (*programmer*) dan analis sistem (*system analyst).* Bagian ini harus dipisah karena tidak boleh terlibat dengan pengoperasian secara langsung yang akibatnya dapat memengaruhi program yang dipergunakan untuk tujuan negatif.

Bagian pusat informasi (*information center* atau disebut juga dengan IC) dibuat dengan tujuan agar para manajernya membuat program aplikasi sendiri untuk keperluan *end user computing (*EUC) atau *end user develompment* (EUD).

PENGENDALIAN DOKUMENTASI

Dokumentasi dapat dianggap sebagai materi yang tertulis atau sesuatu yang menyediakan informasi tentang suatu objek. Dokumentasi dapat berisi tentang deskripsi-deskripsi, penjelasan-penjelasam, bagan alur, daftar-daftar, cetakan hasil komputer, dan contoh-contoh objek dari sistem informasi. Dokumen ini penting untuk keperluan-keperluan sebagai berikut ini.

1. Mempelajari cara mengoperasikan sistem.
2. Sebagai bahan pelatihan.
3. Dasar pengembangan sistem lebih lanjut.
4. Dasar apabila ingin memodifikasi atau memperbaiki sistem di kemudian hari.
5. Materi acuan bagi *auditor.*

Dokumen yang ada di departemen sistem informasi, diantaranya adalah

1) **Dokumentasi Dokumen Dasar.** Merupakan dokumentasi yang berisi kumpulan dokumen-dokumen dasar sebagi bukti transaksi yang digunakan dalam sistem. Misalnya, faktur penjualan, order penjualan, order pembelian, surat pengiriman barang, dan *time card*.
2) **Dokumentasi Daftar Rekening (*Chart of Account*).** Merupakan dokumentasi yang menunjukkan informasi mengenai rekening-rekening yang dipergunakan di dalam transaksi. Daftar rekening berisi daftar dari kode rekening, nama rekening, kalsifikasinya (aktiva, utang, modal, pendapatan pendapatan, dan biaya-biaya), serta petunjuk dari masing-masing rekening bagaimana rekening tersebut dipergunakan.
3) **Dokumentasi Prosedur Manual.** Merupakan dokumentasi yang menunjukka. arus dari dokumen-dokumen besar di dalam perusahaan dan kepada siapa harus ditujukan.
4) **Dokumentasi Prosedur.** Dokumentasi prosedur dapat berisi prosedur-prosedur yang harus dilakukan pada suatu keadaan tertentu, seperti prosedur pengetesan program, prosedur penggunaan file, prosedur pembuatan *back up*dan *restore.*
5) **Dokumentasi Sistem.** Dokumentasi sistem menunjukkan bentuk dari sistem informasi yang digambarkan dalam bagan alur sistem (*system flowchart*). Pada dokumentasi ini dapat terlihat dari *input* yang digunakan, deskripsi *output* yang digunaka dam yang dihasilkan, deskripsi file-file yang digunakan, dan berita kesalahan pengolahan pada tiap sistem pengolahan.
6) **Dokumentasi Program.** Dokumentasi program menggambarkan logika dari program dalan bentuk bagan alur program (*program flowchart*), tabel keputusan (*decision table*), dan bentuk pengendalian program.
7) **Dokumentasi Operasi.** Dokumentasi operasi berisi penjelasan bagaimana cara dan prosedur mengoperasikan program.
8) **Dokumentasi Data.** Dokumentasi data berisi definsi dari item-item data di dalam *database* yang digunakan oleh sistem informasi.

PENGENDALUAN KERUSAKAN PERANGKAT KERAS

Proses pengolahan data dapat terganggu jika terjadi kerusakan pada 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 biasanya sudah terpada didalam komputer untuk mendeteksi kesalahan atau tidak berfungsinya perangkat keras. Pengendalaian perangkat keras dapat berupa pemerikasaan pariti (*parity check*), pemeriksaan gaung (*echo check),* pemeriksaan

baca setelah rekam (*read after write check),* pemeriksaan baca ulang (*dual read check*), dan pemeriksaan validitas (*validity check).*

1) ***Parity Check.*** RAM mempunyai kemampuan untuk melakukan pengecekan data yang disimpannya hal ini disebut juga dengan *parity check.* Apabila daya hilang atau rusak, dapat diketahui dari *bit* tambahan yang disebut dengan *parity bit* atau *check bit.*
2) ***Echo Check.*** Meyakinkan bahwa alat-alat *input/ouput* seperti *printer, tape dirve, disk drive* masih tetap berfungsi dengan baik bila akan digunakan. Apabila alat I/O akan digunakan, CPU mengirim sinyal ke alat tersebut dan alat I/o akan mengirimkan sinyal balik ke CPU tentang statusnya, apalah masih berfungsi atau tidak dan akan tampil berita dilayar terminal.
3) ***Read After Write Check.*** Meyakinkan bahwa data yang telah direkamkan ke media simpanan luar telah terekam dengan baik dan benar. Untuk mengetahui hal ini, setelah data direkamkan makan dibaca kembali untuk dibandingka dengan data yang direkamkan.
4) ***Dual Read Check.*** Tujuan dari pengecekan ini adalah untuk meyakinkan apakah data terbaca dengan benar.
5) ***Validity Check.*** Meyakinkan bahwa data telah dikodekan dengan benar. Pada sistem komputer, angka, dan karakter diwakili dengan suatu kode komputer dalam bentuk digit biner (*binary digit*).

PENGENDALIAN KEAMANAN FISIK

Pengendalian keamanan fisik perlu dilakukan untuk menjaga keamanan terhadap perangkat keras, perangkat lunak, dan manusia didalam perusahaan. Hal-hal yang menyebabkan tidak amannya fisik sistem diantaranya adalah pencuria, sabotase, kegagalan arus listrik yang dapat merusak komponen, dan suhu yang terlalu dingin dapat menyebabkan ruangan menjadi lembab menyebabkan komponen berkarat, debu, dan bencana alam.

Pengendalian keamanan fisik dapat dilakukan dengan cara sebagai berikut.

1) Pengawasan terhadap pengaksesan fisik. Pengawasan ini berupa pembatasan akses terhadap orang-orang yang akan masuk ke bagian yang penting. Apabila keleluasaan untuk dapat keluar masul bagian yang penting selalu diawasi maka kesempatan untuk melakukan hal-hal yang merugikan dapat diminimalisir. Pengawasan ini dapat dilakukan dengan cara sebagai berikut ini.
   a. Penempatan satpam.
   b. Pengisian agenda kunjungan.
   c. Penggunaan tanda pengenal.
   d. Pemakaian kartu.
   e. Penggunaan *closed-Circuit Television.*
   f. Penggunaan pengracik kertas.
   g. Tersedianya pintu arang yang mebuka ke luar.
2) Pengaturan lokasi fisik. Lokasi dari ruang komputer menjadi pertimbangan didalam perencanaan sekuriti, hal ini dapat dilakukan dengan cara sebagai berikut.

a. Lokasi yang tidak terganggu dengan lingkungan.
b. Gedung yang terpisah.
c. Tersedia fasilitas cadangan.

3) Penerapan alat-alat pengaman
   a. Saluran Air
   b. Alat pemadam kebakaran
   c. *Uninterruptible Power Systems (*UPS) untuk mengatasi apabila arus listrik tiba-tiba terputus.
4) Stabilizer
5) Air Conditioner (AC) berfungsi untuk mengatur suhu ruangan.
6) Pendeteksi kebakaran

PENGENDALIAN KEAMANAN DATA

Menjaga integritas dan keamanan data merupakan pencegahan terhadap keamanan data yang tersimpan di simpanan luar agar tidak hilanh, rusak, dan diakses oleh orang lain yang tidak berhak. Beberapa cara pengendalian telah banuak diterapkan untuk maksud ini, diantaranya adalah sebagai berikut ini.

1) Dipergunakan *Data Log.* Agenda (*log*) dapat digunakan pada proses pengolahan data untuk memonitor, mencatat, dan mengidentifikasi data. Disamping *data log* dapat juga dipergunakan *transaction log,* yaitu suatu file yang akan berisi nama-nama pemakai komputer, tanggal, jam, tipe pengolahannya, dan lokasinya.
2) Proteksi File
   Beberapa alat yang digunakan untuk proteksi file diantaranya adalah sebagai berikut ini.
   a. Cincin proteksi pita magnetik dapat memproteksi pita magnetik dari *overwritten*. Apabila cincin dilepas maka tidak dapat direkam dengan datasehingga data yang sudah ada tidak akan tertindih.
   b. *Write-protect tab.* Suatu tab yang dapat digeser naik atau turun di disket untuk membuat disket hanya dapat dibaca.
   c. Label eksternal dan label Internal. Label eksternal merupakan label yang ditampilkan diluar bungkus simpanan luar untuk menunjukkan isi darinya supaya tidak salah megolakasinya datanya. Sedangkan label internal menunjukkan informasi yang direkam di simpanan luar berupa informasi tentang nama dan simpanan luarnya.
   d. *Read-only storage* adalah alat simpanan luar dimana data yang tersimpan didalamnya hanya dapat dibaca saja.
3) Pembatasan Pengaksesan. Memliki tujuan untuk mencegah anggota yang tidak berwewenang untuk dapat mengakses data.
4) Data *Backup* dan *Recovery*. Diperlukan untuk berjaga-jaga bila *file* atau *database* mengalami kerusakan atau kehilangan data atau kesalahan data.

PENGENDALIAN APLIKASI

Pengendalian-pengendalian aplikasi (*application controls*) merupakan pengendalianpengendalian yang dipasang pada pengolahan aplikasinya, yaitu pengendalian-pengendalian pada tahap masukan yang disebut dengan pengendalian-pengendalian masukan (*input controls*),

pengendalian-pengendalian pengolahan (*processing controls*) dan pengendalianpengendalian keluaran (o*utput controls*).

1. PENGENDALIAN-PENGENDALIAN MASUKAN

Pengendalian masukan (*input controls*) mempunyai tujuan untuk meyakinkan bahwa data transaksi yang valid telah lengkap, terkumpul semuanya serta bebas dari kesalahan sebelum dilakukan proses pengolahannya. Pengendalian ini merupakan pengendalian aplikasi yang penting karena input yang salah, *output*-nya juga akan salah. Sampah yang masuk sampah pula yang keluar (GIGO atau singkatan dari *Garbage In Garbage Out*).

Pengendalian pada tahap ini berupa pengecekan yang telah terprogram yang disebut dengan *programmed check*. Berikut ini pengendalian-pengendalian yang terdapat dalam program ini:

a. ***Echo Check.*** Data yang diketikkan pada *keyboard* untuk dimasukkan ke computer akan ditampilkan (*echo*) pada layar terminal. Kesalahan ini tidak dapat dideteksi oleh computer sehingga harus diperiksa oleh operator dimana operator dapat membandingkan antara data yang diketikkan dengan data yang seharusnya dimasukkan.

b. ***Existence Check.*** Kode yang dimasukkan dibandingkan dengan daftar kode-kode yang valid dan sudah diprogram. Contoh penjualan tunai (Kode T) dan penjualan kredit (Kode K).

c. ***Matching Check.*** Pengecekan ini dilakukan dengan membandingkan kode yang dimasukkan dengan *field* di file induk bersangkutan. Apabila kode barang yang dimasukkan dan dicocokkan dengan kode barang di file induk tidak ditemukan berarti kemungkinan kode barang tersebut salah atau tidak ada.

d. ***Field Check.*** Field dari data yang dimasukkan diperiksa kebenarannya dengan mencocokkan nilai dari *field* data tersebut dengan tipe *field*-nya, apakah bertipe numeric, alfabetik, ataukah tanggal. Contoh, tipe *field* numeric harus diisi dengan data numeric. Apabila diisi dengan data bukan numeric berarti salah.

e. ***Sign Check.*** *Field* data yang bertipe numeric dapat diperiksa untuk menentukan apakah telah terisi dengan nilai yang mempunyai tanda yang benar, positif ataukah negatif.

f. ***Relationship Check / Logical Check.*** Pengecekan ini berfungsi untuk memeriksa hubungan antara item-item data *input* yang dimasukkan ke komputer apakah sudah sesuai dan masuk akal. Apabila tidak masuk akal maka akan ditolah oleh komputer.

g. ***Limit Check / Reasonable Check.*** Nilai dari input data diperiksa apakah cukup beralasan atau tidak. Misalnya, tanggal transaksi yang terjadi 30 Februari 1987 adalah tidak beralasan.

h. ***Range Check.*** Nilai yang dimasukkan juga dapat diseleksi supaya tidak keluar dari jangkauan nilai yang sudah ditentukan. Misalnya, suatu organisasi memilki 5 departemen dengan kode A sampai E jika dimasukkan kode G berarti salah karena di luar *range* dari departemen yang ada

i. ***Self-Checking Digit Check.*** Pengecekan untuk memeriksa kebenaran digit-digit data yang dimasukkan. Kesalahan yang sering terjadi:

1) Kelebihan digit atau karakter, contoh 8598 ditulis 85598
2) Pemotongan digit atau karakter, contoh 85988210 ditulis 859210
3) Kesalahan penulisan digit atau karakter, contoh 8598 ditulis 8593
4) Peletakan posisi digit atau karakter yang salah, contoh 8598 ditulis 8958
5) Kesalahan acak digit atau karakter yang merupakan gabungan dari kesalahan-kesalahan
6) di atas, contoh 859882 ditulis 858920

Untuk mendekteksi kesalahan pada *self-checking digit check*, masing-masing posisi digit diberi bobot nilai. Nilai masing-masing digit dikalikan dengan bobotnya dan dijumlahkan kemudian hasilnya dibagi dengan nilai 11 (bilangan ideal untuk cara ini).

2. PENGENDALIAN-PENGENDALIAN PENGOLAHAN

Tujuan dari pengendalian ini adalah untuk mencegah kesalahan-keslahan yang terjadi selama proses pengolahan data yang dilakukan setelah data dimasukkan ke dalam komputer. Kesalahan-kesalaahan yang pada umumnya disebabkan dalam program:

a. ***Overflow.*** *Overflow* terjadi jika proses pengolahan mengandung perhitungan-perhitungan yang hasilnya terlalu besar atau terlalu kecil sehingga tidak muat untuk disimpan di memori komputer.

b. **Kesalahan Logika Program.** Kesalahan ini sering terjadi apalagi bila program tidak diuji dengan teliti. Kesalahan ini merupakan kesalahan yang berbahaya dan sulit dilacak karena kesalahan logika tidak dapat ditunjukkan oleh computer dan tetap akan didapatkan hasilnya, tetapi dengan hasil yang salah.

c. **Logika Program yang Tidak Lengkap.** Walaupun mungkin dalam program tidak ada kesalahan-kesalahan dari logika dan semua kondisi logika telah benar, tetapi mungkin juga ada beberapa kondisi logika yang terlewat.

d. **Penanganan Pembulatan yang Salah.** Permasalahan pembulatan terjadi bila tingkat ketepatan yang diinginkan dari perhitungan aritmatika lebih kecil dari tingkat ketepatan yang terjadi.

e. **Kesalahan Akibat Kehilangan atau Kerusakan *Record.*** Walaupun kelengkapan dan kebenaran dari isi file transaksi ini telah divalidasi di tahap *input*, tetapi pada waktu proses *update* dapat juga terjadi beberapa *record* yang hilang atau mengalami kerusakan data sehingga data yang diproses menjadi tidak benar.

f. **Kesalahan Urutan Proses.** *Record* di file induk akan di- *update* oleh data transaksi. Sebelum dilakukan proses peng*update*-an ini, apabila terjadi penambahan data baru atau penghapusan data atau perubahan perubahan terhadap file induk maka proses-proses ini harus dilakukan terlebih dahulu, kalua tidak maka dapat mengakibatkan terjadinya kesalahan-kesalahan.

g. **Kesalahan Data di File Acuan.** Banyak program yang menggunakan file acuan (*reference file*) atau file table (*table file*) untuk menyimpan data yang relative konstan.

h. **Kesalahan Proses Serentak.** Kesalahan proses serentak (*concurrency*) terjadi apabila sebuah file basis data dipergunakan oleh lebih dari seorang pemakai dalam *network*.

Pengontrolan untuk mengecek kesalahan-kesalahan pengolahan dapat berupa sebagai berikut:

a. ***Control Total Check.*** Pada tahap pengendalian masukan, *control total check* biasanya dilakukan pada *batch processing method* untuk meyakinkan bahwa semua data yang dimasukkan sudah lengkap dan sudah benar. Pada tahap pengolahan, *conrol total check* dapat dipergunakan untuk mendeteksi apakah semua data yang diolah telah lengkap dan benar.

b. ***Matching Check.*** Pada tahap pengolahan data, pencarian data di suatu file yang tidak ketemu harus dapat dideteksi. *Matching check* merupakan pengendalian untuk melakukan hal ini. *Matching check* pada *batch processing method* dapat digunakan juga untuk

mendeteksi kesalahan dari urutan data. Pada *online processing method*, pengecekan ini pada tahap *input* dan pada tahap pengolahan dapat di dalam satu program.

c. ***Reference File Check.*** Kesalahan peggunaaan data yang diambil dari file acuan (*reference file*) dapat dideteksi dengan cara mencetak isi file acuan yang digunakan setelah dilakukannya proses pengolahan. Hasil cetakan isi file acuan kemudian dapat diperiksa kebenarannya. Apabila file acuan cukup besar dan diputuskan untuk tidak mencetak isinya maka dapat dilakukan pengecekan yang lain yaitu *control total* (misalnya *hash total*) dari nilai-nilai di file acuan.
d. ***Limit and Reasonable Check.*** Pada tahap *input*, pengecekan ini ditujukan pada kewajaran dari data *input* yang dimasukkan ke computer, sedangkan pada tahap pengolahan, pengecekan ini ditujukan pada hasil pengolahannya. Pengecekan ini misalnya untuk mengecek saldo akhir kas hasil dari suatu transaksi kas yang tidak boleh negative. Saldo kas yang negative adalah nilai yang tidak wajar. Pengecekan kewajaran ini dapat juga diterapkan untuk pengecekan kesalahan logika program yang tidak benar ang dapat menyebabkan hasil pengolahan menjadi tidak wajar.
e. ***Cross Footing Check.*** Dilakukan dengan menjumlahkan masing-masing item data secara ke samping (horizontal) dan secara independen juga dilakukan penjumlahan secara tegak (vertical). Total penjumlahan ke samping dan total penjumlahan tegak dapat dicocokkan secara menyilang dan harus didapatkan hasil yang sama.
f. ***Record Locking.*** Proses konkurensi terjadi karena *record* yang sama di dalam suatu file dipergunakan oleh lebih dari satu pemakai. Untuk mengatasi konkurensi dapat dilakukan dengan mengunci *record* yang sedang dipergunakan sehingga tidak dapat digunakan oleh pemakai yang lain.

Pengendalian pengolahan yang lainnya yang perlu dilakukan untuk mentranmisikan datadari suatu tempat ke tempat yang lain adalah pengendalian komunikasi. Pengendalian komunikasi dimaksudkan untuk menangani keslahan selama proses mentanmisikan data dan untuk mencegah keamanan dari data selama proses mentransmisikan data dan untuk mencegah keamanan dari data selama pengirman data tersebut. Pengendalian komunikasi dibagi menjadi dua bagian yaitu pengendalian-pengendalian kesalahan transmisi dan pengendalian-pengendalian keamanan dan transmisi. Pengendalian kesalahan transmisi dapat dilakukan dengan teknik pantulan (*echo technique*), pengecekan parity dua kordinat (*twocordinate parity checking*) atau *cycle redundancy checking*.

3. PENGENDALIAN-PENGENDALIAN KELUARAN

Keluaran (*output*) yangmerupakan produk dari pengolahan data dapat disajikan dalam dua bentuk utama, yaitu dalam bentuk *hard copy* dan dalam bentuk *soft copy*. Dalam bentuk *hard copy* yang paling banyak dilakukan adalah berbentuk lapoan yang dicetak menggunakan alat cetak (*printer*) dan dalam bentuk *soft copy* yang paling umum adalah berbetuk tampilan di layar *terminal*.

Untuk menghasilkan laporan yang berbentuk *hard copy* dapat dilakukan melalui beberapa tahapan, dan tiap-tiap tahapan ini perlu dilakukan pengendalian-pengendalian, yaitu sebagai berikut:

a. Pengendalian-pengendalian pada tahap menyediakan media laporan
b. Pengendalian-pengendalian pada tahap memproses program yang menghasilkan laporan
c. Pengendalian-pengendalian pada tahap pembuatan laporan di file (*printer file*)

d. Pengendalian-pengendalian pada tahap pengumpulan laporan
e. Pengendalian-pengendalian pada tahap mncetak laporan di media keras (kertas)
f. Pengendalian-pengendalian pada tahap mengkaji ulang laporan
g. Pengendalian-pengendalian pada tahap penilaian laporan
h. Pengendalian-pengendalian pada tahap distribusi laporan
i. Pengendalian-pengendalian pada tahap kaji ulang laporam oleh pemakai laporan
j. Pengendalian-pengendalian pada tahap pengarsipan laporan
k. Pengendalian-pengendalian pada tahap pemusnahan laporan yang sudah tidak diperlukan