BAB II

LANDASAN TEORI

2.1 Audit Sistem Informasi

1. Pengertian Audit Sistem Informasi

Menurut *Arens* dan *Loebbecke* audit adalah:

> Proses yang dilakukan oleh orang yang kompeten dan independen dengan cara mengumpulkan dan mengevaluasikan bukti tentang informasi yang dapat diukur atau dihitung yang berhubungan dengan kesatuan ekonomi yang khusus untuk menentukan dan melaporkan tingkat kesesuaian antara informasi yang dapat dihitung dengan kriteria yang ditentukan.

Menurut *Bodnar* dan *Hopwood* Pengolahan Data Elektronik (PDE)/-*Electronic Data Processing* (EDP) adalah:

> Pemanfaatan teknologi komputer untuk melakukan pengolahan data yang berorientasi pada transaksi dalam suatu organisasi, *EDP* adalah aplikasi sistem informasi akuntansi paling mendasar dalam setiap organisasi.

Karena teknologi komputer telah menjadi hal yang biasa, maka istilah pengolahan data (*data processing – DP*) telah mempunyai arti sama dengan istilah *PDE*.

Menurut *Bodnar* dan *Hopwood* sistem informasi akuntansi berbasis komputer adalah:

> Kumpulan sumber daya, seperti manusia dan peralatan, yang dirancang untuk mengubah data keuangan dan data lainnya menjadi informasi yang bermanfaat.

Menurut *Romney* dan *Steinbart* audit sistem informasi adalah:

> Me-*review* pengendalian umum dan aplikasi dari sistem informasi akuntansi untuk menilai pelaksanaan kebijaksanaan dan prosedur pengendalian intern serta efektifitas perlindungan aset.

2. Tujuan Audit Sistem Informasi

Menurut tujuan audit sistem informasi, yaitu:

a. Meningkatkan perlindungan terhadap aset-aset. Aset informasi perusahaan seperti perangkat keras (*hardware*), perangkat lunak (*software*), sumber daya manusia, file, data harus dijaga oleh suatu sistem pengendalian intern yang baik agar tidak terjadi penyalahgunaan aset perusahaan.

b. Menjaga integritas data. Integritas data adalah salah satu konsep dasar sistem informasi, jika tidak terpelihara maka suatu perusahaan tidak akan lagi memiliki hasil atau laporan yang benar atau bahkan perusahaan dapat menderita kerugian.

c. Meningkatkan efektifitas sistem. Efektifitas sistem informasi perusahaan memiliki peranan penting dalam proses pengambilan keputusan. Suatu sistem informasi dapat dikatakan efektif bila sistem tersebut sesuai dengan kebutuhan *user*.

d. Meningkatkan efisiensi sistem. Suatu sistem dapat dikatakan efisien jika sistem informasi dapat memenuhi kebutuhan *user* dengan sumber daya yang minimal.

3. Metode Audit Sistem Informasi

Metode audit sistem informasi meliputi :

a. *Auditing around the computer.* Merupakan suatu pendekatan audit, dimana auditor memperlakukan komputer sebagai *black box*, maksudnya pemrosesan sistem aplikasi tidak diuji secara langsung. Metode ini hanya berfokus pada *input* dan *output* dari sistem aplikasi, dengan mengasumsikan bahwa jika *input* benar dan *output* juga benar, maka proses juga dianggap benar (*given*).

   Pendekatan ini memiliki dua kelemahan utama, yaitu :

   a) tidak dapat digunakan untuk sistem yang kompleks.

   b) tidak memberikan informasi kepada auditor untuk memahami lebih dalam dari sistem.

b. *Auditing through the computer.* Merupakan suatu pendekatan audit, dimana auditor berorientasi pada komputer dengan membuka *black box*, dan secara langsung berfokus pada pemrosesan dalam sistem aplikasi. Dengan asumsi bahwa apabila pemrosesan memiliki pengendalian yang memadai, maka kesalahan dan penyalahgunaan tidak akan terlewat untuk dideteksi, sebagai akibatnya, *output* dapat diterima.

   Keuntungan utama dari pendekatan ini adalah untuk meningkatkan kekuatan terhadap pengujian sistem aplikasi secara efektif, dimana ruang lingkup dan kemampuan pengujian dapat diperluas sehingga tingkat kepercayaan terhadap kehandalan dari pengumpulan dan

pengevaluasian bukti dapat ditingkatkan. Selain itu, dengan memeriksa secara langsung logika pemrosesan dari sistem aplikasi, dapat diperkirakan kemampuan sistem dalam menangani perubahan dan kemungkinan yang akan terjadi pada masa yang akan datang.

Pendekatan ini memilki dua kelemahan, yaitu :

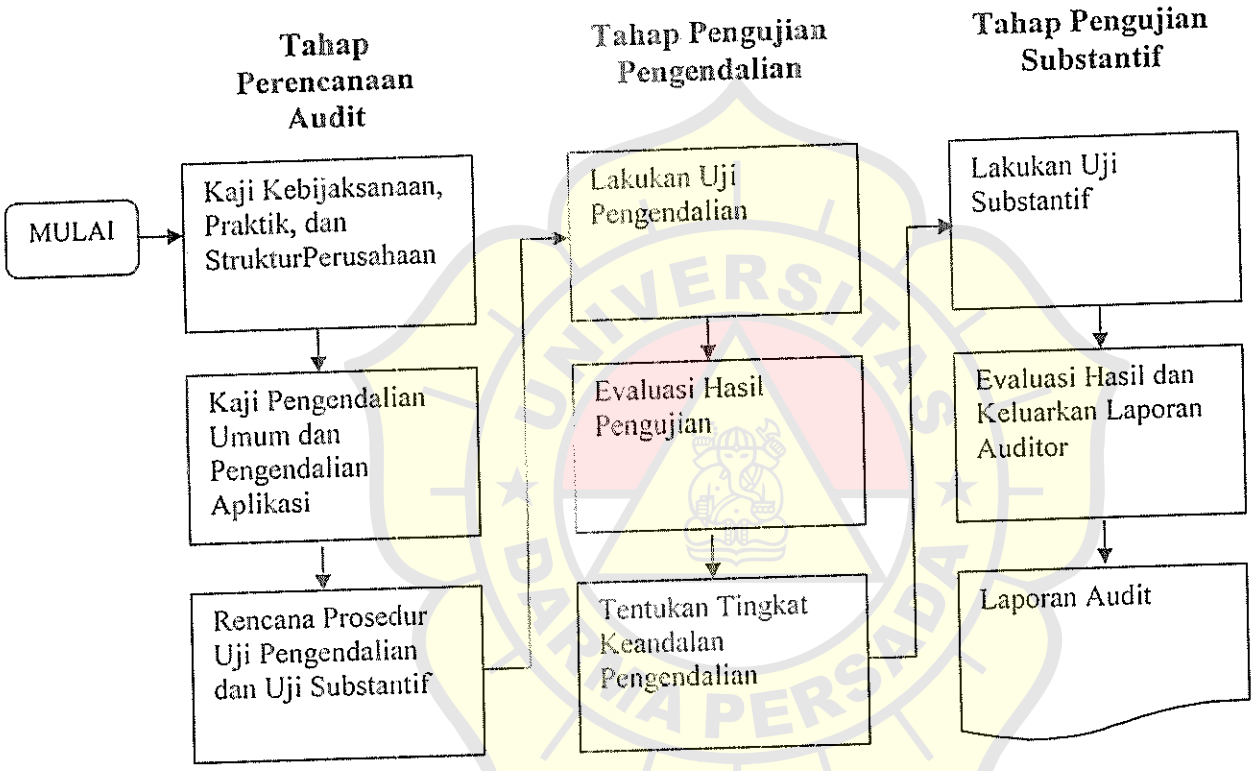
1) biaya yang dibutuhkan relatif tinggi, yang disebabkan jumlah jam kerja yang banyak untuk dapat lebih memahami struktur kontrol intern dari pelaksanaan sistem aplikasi.
2) butuh keahlian teknik yang lebih mendalam untuk memahami cara kerja sistem.

4. Tahapan Audit Sistem Informasi

Tahapan audit sistem informasi digambarkan dalam bentuk *flowchart* sebagai berikut :

Gambar 2.1

Tahapan Audit Sistem Informasi



Sumber : James A. Hall dan Tommie Singleton, *(Audit Teknologi Informasi dan Assuransi (Information Technology Auditing and Assurance)*, buku dua, edisi kedua. Thomson, 2007, hal. 17.

2.2 Pengendalian Internal

Audit internal adalah sebuah penilaian yang sistematis dan objektif yang dilakukan auditor internal terhadap operasi dan *control* yang berbeda-beda dalam organisasi untuk menentukan apakah:

1. informasi keuangan dan operasi telah akurat dan dapat diandalkan.
2. risiko yang dihadapi perusahaan telah diidentifikasi dan diminimalisasir.
3. peraturan eksternal serta kebijakan dan prosedur internal yan bisa diterima telah diikuti.
4. kriteria operasi yang memuaskan telah dipenuhi.
5. sumber daya telah digunakan secara efisien dan ekonomis.
6. tujuan organisasi telah dicapai secara efektif.

semua dilakukan dengan tujuan untuk dikonsultasikan dengan manajemen dan membantu anggota organisasi dalam menjalankan tanggung jawabnya secara efektif.

Dalam kaitannya dengan PDE, AICPA menyebutkan adanya 19 pengendalian pokok dalam kaitannya dengan pengendalian komputerisasi, adalah sebagai berikut:

1. Departement PDE harus dipisahkan dari departemen pemakai.
2. Personil dalam departement PDE harus tidak diijinkan untuk memulai (*originate*) atau mengotorisasikan transaksi, bertanggung jawab terhadap aktiva non PDE ataupun memulai perubahan fail induk (*master file*).
3. Fungsi-fungsi di dalam departemen PDE harus dipisahkan dengan baik.
4. Prosedur-prosedur untuk perancangan sistem, termasuk perolehan paket-paket piranti lunak, harus disertai dengan partisipasi aktif dari wakil-wakil para pemakai, dan bila memungkinkan, partisipasi dari departemen akuntansi dan auditor intern.

5. Masing-masing sistem harus memiliki spesifikasi yang tertulis yang ditelaah dan disetujui oleh manajemen dengan tingkatan yang memadai serta oleh departemen pemakai yang bersangkutan.
6. Pengujian sistem harus merupakan usaha bersama antra pemakai dengan personil PDE, dan harus mencakup fase-fase sistem secara manual maupun yang dikomputerisasikan.
7. Persetujuan akhir harus diperoleh sebelum mengoperasikan sistem yang baru tersebut.
8. Semua konversi fail induk dan fail transaksi harus dikendalikan untuk mencegah timbulnya perubahan yang tidak ada otorisasnya sehingga dapat diperoleh hasil yang akurat dan lengkap.
9. Setelah sistem yang baru berjalan, semua perubahan program harus disetujui sebelum diimplementasikan guna menentukan apakah perubahan-perubahan tersebut ada otorisasinya, diuji dan didokumentasikan.
10. Manajemen harus menetapkan beberapa jenis dokumentasi dan prosedur-prosedur formal untuk mendefinisikan sistem dengan perincian yang cukup.
11. Karakteristik (*feature*) pengendalian yang ada didalam piranti keras komputer, sistem operasi dan piranti lunak pendukung lainnya harus dimanfaatkan semaksimal mungkin untuk mengendalikan pelaksanaanya dan untuk mencegah dan melaporkan ketidakberesan (*malfunctions*) piranti keras.

12. Piranti lunak sistem harus dikendalikan sebagaimana manajemen melakukan pengendalian terhadap pemasangan dan perubahan program-program aplikasi.
13. Akses ke dokumentasi program harus dibatasi hanya kepada personil-personil yang membutuhkannya untuk melaksanakan pekerjaan mereka.
14. Akses ke fail-fail data dan program harus dibatasi hanya kepada personil-personil yang berhak untuk memproses atau memelihara sistem-sistem tertentu.
15. Akses ke piranti keras komputer harus dibatasi hanya kepada personil-personil yang berhak (yang memiliki otorisasi).
16. Suatu fungsi pengendalian harus bertanggung jawab untuk penerimaan data yang akan diproses, untuk pemastian bahwa seluruh data tersebut telah dibukukan, untuk menindaklanjuti kesalahan yang ditemukan selama pengolahan guna melihat bahwa kesalahan-kesalahan tersebut telah dikoreksi dan dikirimkan kembali oleh pihak-pihak yang berwenang, serta utnuk melakukan verifikasi terhadap pendistribusian keluaran yang memadai.
17. Pedoman sistem dan prosedur-prosedur yang tertulis harus dibuat untuk seluruh aktivitas komputer yang memberikan otorisasi khusus atau umum kepada manajemen untuk memproses transaksi.
18. Auditor intern atau kelompok independen lainnya di dalam organisasi harus menelaah dan menilai usulan sistem pada tahap-tahap kritis pengembangan sistem tersebut.

19. Secara rutin auditor intern atau kelompok lainnya di dalam organisasi harus menelaah dan menguji aktivitas pengolahan data.

2.3 Pengendalian Umum

Ikatan Akuntan Indonesia menyatakan bahwa pengendalian umum meliputi unsur-unsur sebagai berikut :

1. Pengendalian organisasi dan manajemen. Pengendalian ini dimaksudkan sebagai alat untuk menciptakan kerangka kerja organisasi PDE.
2. Pengendalian terhadap pengembangan pemeliharaan sistem aplikasi. Pengendalian ini dimaksudkan untuk memperoleh keyakinan yang memadai bahwa sistem PDE telah dikembangkan dan dipelihara secara efisien dan ada otorisasinya.
3. Pengendalian terhadap operasi sistem. Pengendalian ini dimaksudkan untuk memberikan keyakinan bahwa:
   a. Sistem digunakan hanya untuk hal-hal yang telah ada otorisasinya.
   b. Akses ke operasi komputer hanya diijinkan kepada mereka yang telah memiliki otorisasi.
   c. Program yang digunakan hanyalah yang telah ada otorisasinya.
   d. Kesalahan pengolahan dapat dideteksi dan dikoreksi.
4. Pengendalian terhadap perangkat lunak sistem. Pengendalian ini dimaksudkan untuk memperoleh keyakinan yang memadai bahwa perangkat lunak sistem dimiliki atau dikembangkan secara efisien dan diotorisasikan.

5. Pengendalian terhadap entri data dan program. Pengendalian ini dimaksudkan untuk memperoleh keyakinan yang memadai bahwa:
   a. Struktur organisasi telah ditetapkan atas transaksi yang dimasukkan ke dalam sistem.
   b. Akses ke data dan program dibatasi hanya kepada mereka yang memiliki otorisasi.
6. Pengendalian terhadap keamanan PDE. Pengendalian ini dimaksudkan untuk menjaga keamanan PDE lainya yang juga memberikan kontribusi terhadap kelangsungan PDE, seperti misalnya digunakannya salinan cadangan (*backup*) di tempat yang terpisah, prosedur pemulihan (*recovery procedure*) ataupun fasilitas pengolahan di luar perusahaan dalam hal terjadi bencana.

Enam kategori pengendalian umum PDE di atas dapat diklasifikasikan menjadi tujuh jenis pengendalian sebagai berikut:

1. **Pengendalian organisasi dan manajemen.** Metode-metode yang biasanya digunakan oleh manajemen dalam melakukan pengendalian organisasi dan manajemen adalah sebagai berikut :
   a. Memisahkan fungsi departemen PDE dari departemen non PDE.
   b. Memisahkan fungsi-fungsi dalam departemen PDE itu sendiri.
   c. Transaksi yang terjadi harus memperoleh diotorisasi.
   d. Mengadakan pengendalian terhadap seluruh personil.
   e. Membuat perencanaan penganggaran dan sistem pembebanan kepada *user*.

f. Membentuk komisi PDE yang akan berfungsi menetapkan tujuan-tujuan dan kebijakan departemen PDE, menentukan prioritas mana yang harus diambil alih dalam hal.

2. **Pengendalian piranti lunak dan piranti keras**. Tujuan pengendalian piranti lunak dan keras ini antara lain adalah sebagai berikut :

   a. Untuk mendeteksi kesalahan-kesalahan yang terjadi atau ketidakberesan peralatan komputer yang bersangkutan.

   b. Untuk mencegah akses yang tidak ada otorisasinya.

3. **Pengendalian akses**. Kategori pengendalian akses menurut organisasi profesi adalah sebagai berikut :

   a. Akses ke departemen PDE dan piranti keras komputer harus dibatasi.

   b. Akses ke dokumentasi program, program dan fail-fail data harus dikendalikan.

   c. Menggunakan piranti lunak pengendalian akses (*access control software*).

   d. Dengan memasukkan fitur-fitur pengendalian tertentu didalam *software*.

4. **Pengendalian data dan prosedur**. Dapat dikategorikan sebagai berikut:

   a. *Control group*.

   b. Pengendalian fail dan *database*.

   c. Pengamanan terhadap data.

   d. Diefektifkannya fungsi audit intern.

5. **Pengendalian pengembangan sistem baru**. Tujuan pengendalian pengembangan sistem adalah sebagai berikut :

   a. Untuk menjamin bahwa seluruh kegiatan pengembangan sistem telah diotorisasikan, diuji, ditelaah, didokumentasikan, disetujui, dan diterapkan.

   b. Untuk menjamin bahwa standar, kebijakan dan prosedur-prosedur yang ada benar-benar dilaksanakan dalam membantu manajemen mengendalikan sistem dan kegiatan pemrograman.

   Beberapa jenis pengendalian yang dilakukan dalam pengembangan sistem adalah sebagai berikut :

   a. Partisipasi pemakai, manajemen dan auditor.

   b. Pengembangan standar dan pedoman.

   c. Pengujian sistem dan konversi.

   d. Penelaahan setelah pemasangan atau instalasi.

6. **Pengendalian pemeliharaan sistem dan program**. Pengendalian terhadap pemeliharaan sistem meliputi:

   a. Otorisasi untuk melakukan perubahan.

   b. Keterlibatan pemakai.

   c. Persetujuan para pemakai pada waktu perubahan tersebut diuji.

   d. Adanya standar dan pedoman agar mereka yang terlibat dalam perubahan tersebut "dipaksa" untuk mematuhi ketentuan yang ada.

   e. Pengendalian lain yang mengatur mengenai pemprograman dan para personil bagian operasi.

Tujuan dari pengendalian terhadap pemeliharaan program ini adalah sebagai berikut :

a. Untuk menjaga integritas dari sistem yang ada.
b. Untuk mencegah pengrusakan dan kerusakan atau kehilangan program.
c. Untuk mencegah dimasukkannya kesalahan ke dalam program.
d. Untuk mencegah timbulnya perubahan yang tidak ada otorisasinya.

7. **Dokumentasi**. Manfaat dan tujuan pengendalian dokumentasi sebagai berikut :

a. Memberikan sumber informasi bagi personil-personil PDE.
b. Memberikan jaminan bahwa instruksi kepada seluruh personil pengolahan data dan personil pada departemen pemakai telah didokumentasikan secara memadai.
c. Memjamin kelangsungan operasi PDE apabila personil yang berpengalaman meninggalkan departemen PDE atau bahkan keluar dari perusahaan yang bersangkutan.
d. Untuk memberikan jaminan bahwa seluruh program telah didokumentasikan secara memadai.
e. Dokumentasi dapat memberikan jaminan bahwa dokumentasi yang memadai memang benar-benar ada dan dikendalikan secara efektif.
f. Untuk memberikan jaminan bahwa seluruh sistem telah didokumntasikan secara memadai.

2.4 Pengendalian Aplikasi

Jenis pengendalian menurut pengendalian aplikasi :

Tabel 2.1

Klasifikasi Pengendalian Aplikasi

Kategori Pengendalian	Jenis-jenis Pengendalian
Pengendalian masukan	Otorisasi dan Validasi Masukan Transmisi dan Konversi Data Penanganan Kesalahan
Pengendalian Pengolahan	Pemeliharaan Ketepatan Data Pengujian Terprogram atas Batasan dan Memadainya Pengolahan Pengendalian Fail
Pengendalian Keluaran	Rekonsiliasi Keluaran Penelaahan dan Pengujian Hasil Pengolahan Distribusi keluaran *Record Retention*

Sumber : Basalamah, Anies S.M., *Auditing Proses Data Elektronik Dengan Standar IAI*, edisi ketiga. Depok: Usaha Kami, 2003, hal. 220.

1. **Pengendalian atas Masukan.**

   Pengendalian atas masukan menurut IAI dirancang untuk memberikan keyakinan yang memadai bahwa:

   a. Transaksi diotorisasi sebagaimana mestinya sebelum diolah dengan komputer.

b. Transaksi ini diubah dengan cermat ke dalam bentuk yang dapat dibaca mesin dan dicatat dalam file data komputer.
c. Transaksi tidak hilang, ditambah, digandakan, atau diubah tidak semestinya.
d. Transaksi yang keliru ditolak, dikoreksi, dan jika perlu, dimasukkan kembali secara tepat waktu.

Sementara itu pengendalian masukan dalam sistem *online* dirancang untuk memberikan keyakinan bahwa:

a. Transaksi dientri ke terminal yang semestinya.
b. Data dientri dengan cermat.
c. Data dientri ke periode akuntansi yang semestinya .
d. Data yang dientri telah diklasifikasikan dengan benar dan pada nilai transaksi yang sah (*valid*).
e. Data yang tidak sah (*invalid*) tidak dientri pada saat transmisi.
f. Transaksi tidak dientri lebih dari sekali.
g. Data yang dientri tidak hilang selama masa transmisi berlangsung.
h. Transaksi yang tidak berotorisasi tidak dientri selama transmisi berlangsung.

Hal ini disebabkan karena pengendalian atas masukan dimaksudkan untuk menentukan bahwa :

a. Seluruh transaksi telah dicatat dengan baik pada sumber asalnya.
b. Data telah diotorisasikan dengan baik.

c. Seluruh data telah dipindahkan dari tempat pencatatannya ke tempat pengolahan data komputer (secara elektronik).
d. Seluruh data telah dikonversikan ke dalam bentuk yang dapat dibaca oleh mesin.
e. Seluruh data divalidasi melalui proses penyortiran.
f. Seluruh kesalahan dideteksi dan dikoreksi.

Terdapat empat kategori dasar dari masukan sistem PDE yang harus menjadi bagian dari pengendalian atas masukan, adalah sebagai berikut:

a. Jurnal-jurnal atas transaksi.
b. Transaksi pemeliharaan fail (*file maintenance transaction*), seperti misalnya pengubahan harga dalam fail induk.
c. Transaksi untuk megetahui suatu informasi tertentu (*inquiry transactions*), seperti misalnya untuk mengetahui besarnya persediaan yang masih dimiliki.
d. Transaksi perbaikan kesalahan.

Jenis-jenis pengendalian yang termasuk dalam pengendalian atas masukan adalah sebagai berikut:

a. Pengendalian Otorisasi Masukan (*Input Authorization Control*). Dengan adanya otorisasi masukan maka dapat diperoleh jaminan bahwa hanya data yang ada otorisasinya saja yang diproses ke dalam sistem komputer.

Jenis-jenis pengendalian yang termasuk dalam pengendalian otorisasi masukan adalah:

1) Prosedur-prosedur persetujuan.
   a) Bukti otorisasi seperti tanda tangan atau lainnya harus ditelaah oleh *control group*.
   b) Dalam sistem *online*, otorisasi ini sering ditunjukkan dengan digunakannya kata-kata sandi (*password*) dan tabel otorisasi (*authorization table*).
   c) Transaksi-transaksi yang telah dikelompokkan (*batch*) disetuji sebelum proses.
   d) Transaksi pemeliharaan file disetujui oleh penyelia di tempat asal mula transaksi tersebut dibuat.
   e) Batasan-batasan mengenai persetujuan terhadap transaksi-transaksi tertentu, seperti misalnya jumlah kredit maksimum kepada pelanggan.
2) Formulir yang Diberi Nomor Urut (Pra Nomor). Urut-urutan formulir tesebut akan diuji selama pemprosesan berlangsung. Apabila tejadi formulir urut hilang, maka hal tersebut harus ditelaah oleh pejabat yang berwenang di departemen asal formulir tersebut dihasilkan.
3) Penelaahan oleh *Control group*. Transaksi yang diproses dalam bentuk *batch* atau yang harus dilaksanakan oleh departemen PDE harus ditelaah terlebih dahulu oleh *control group*.

4) Sistem Pengawasan Pencatatan Aktivitas. Dengan cara ini semua terminal yang digunakan dicatat dalam tape atau disk.

b. Validasi masukan (*Input Validation Control*). Pengendalian ini telah terprogram dalam sistem, dan dimasukkan untuk memperoleh keyakinan bahwa semua data masukan adalah akurat, lengkap, dan memadai (logis). Pentingnya pengendalian yang telah terprogram ini adalah karena jenis pengendalian ini memiliki beberapa fungsi seperti:

1) Untuk mendeteksi kehilangan data.
2) Untuk menguji perhitungan matematis.
3) Untuk menjamin adanya pembukuan.

Jenis-jenis pengendalian yang termasuk dalam pengendalian validasi masukan ini antara lain adalah sebagai berikut :

1) *Numeric and alphaberic check.*
2) *Logic check.*
3) *Sign check.*
4) *Valid field size check.*
5) *Limit check.*
6) *Valid code check.*
7) *Squence check*

c. Pengendalian Transmisi Data. Tujuan pengendalian trasmisi data adalah untuk mencegah agar data yang akan diproses tersebut tidak hilang, tidak ditambah atau diubah.

Teknik-teknik pengendalian di dalam pengendalian transmisi data antara lain :

1) *Batches logging and tracking.*
2) Program-program aplikasi.
3) Teknik-teknik verifikasi dalam transmisi *online*, antara lain:
   a) *Echo check.*
   b) *Redundancy check.*
   c) *Completeness test.*

d. Pengendalian Konversi Data. Konversi data adalah proses mengubah data dari sumber asalnya ke dalam bentuk yang dapat dibaca oleh mesin (*machine readable form*), misalnya dalam bentuk *punched cards*, pita magnetis, disk atau disket.

Teknik-teknik penegndalian dalam konversi data ini antara lain adalah sebagai berikut :

1) Verifikasi fisik (*Visual verification*).
2) Penggunaan *Check Digit.*
3) Penggunaan *batch control total.*

e. Pengendalian Penanganan Kesalahan. Transaki-transaksi yang salah juga harus dikembalikan sehingga transaksi-transaksi semacam itu tidak diproses. Pengendalian ini mencakup hal-hal sebagai berikut :

1) Identifikasi atas sebab-sebab penolakan serta penelahaan terhadap sebab-sebab penolakan tersebut.

2) Penelaahan dan persetujuan perbaikannya.

3) Memproses kembali (*reentry*) sesegera mungkin kedalam sistem.

Yang termasuk dalam pengendalian ini antara lain adalah sebagai berikut :

1) *Error Log.*

2) *Suspended file*

3) Laporan kesalahan.

2. **Pengendalian atas Pengolahan Data.** Penegendalian atas pengolahan (*processing controls*) dilaksanakan setelah data memasuki sistem dan program-program aplikasi mengolah data tersebut. Menurut IAI, pengendalian ini dimasudkan untuk memperoleh jaminan yang memadai bahwa :

a. Transaksi diolah sebagaimana mestinya oleh komputer.

b. Transaksi tidak hilang, ditambah, digandakan, atau diubah tidak semestinya.

c. Transaksi yang keliru ditolak, dikoreksi, dan jika perlu, dimasukkan kembali secara tepat waktu.

Sedangkan pegendalian pengolahan pada sistem *online* dimaksudkan untuk memperoleh jaminan yang memadai bahwa:

a. Hasil perhitungan telah diprogram dengan benar.

b. Logika yang digunakan dalam proses pengolahan data adalah benar.

c. *File* dan *record* yang digunakan dalam proses pengolahan data adalah benar.
d. Operator telah memasukkan data ke komputer yang *console* semestinya.
e. Tabel pengolahan data selama proses pengolahan data adalah benar.
f. Selama proses pengolahan telah digunakan standar operasi (*default*) yang semestinya.
g. Data yang tidak sah tidak digunakan dalam proses pengolahan.
h. Proses pengolahan tidak menggunakan program dengan versi yang salah.
i. Hasil perhitungan yang dilakukan secara otomatis oleh program adalah sesuai dengan kebijakan manajemen usaha.
j. Data masukan yang diolah adalah data yang berotorisasi.

Dengan adanya pengendalian pengolahan maka pemprosesan data di dalam sistem akan lengkap, akurat, dan kesalahan-kesalahan berikut ini dapat dicegah atau dideteksi :

a. Kegagalan untuk memproses seluruh transaksi masukan atau memproses tidak sebagaimana mestinya (secara salah).
b. Memproses dan memuktahirkan fail yang salah.
c. Memproses masukan yang tidak logis atau tidak wajar.
d. Kehilangan atau distorsi data selama pemprosesan.

Teknik-teknik yang biasa digunakan dalam pengendalian atas pemprosesan adalah sebagai berikut :

a. Dengan mempertahankan keakuratan data, antara lain:
   1) *Batch Control Total*. *Batch control total* dimaksudkan untuk mendeteksi adanya data yang hilang atau data yang tidak terproses.
   2) *Run-to-run control total.*
   3) *Transaction log*
   4) *Fallback procedures.*
   5) *Restart procedure.*
   6) *Recovery procedures.*
b. *Programmed limit and reasonableness tests*, antara lain:
   1) *Zero balancing check*
   2) *Crossfooting check.*
   3) *Overflow check.*
c. Pengendalian atas fail (*file conrols*). Tujuan dari pengendalian atas fail adalah :
   1) Untuk mencegah pemprosesan terhadap fail yang tidak sesuai.
   2) Untuk mendeteksi kesalahan dalam manipulasi fail.
   3) Untuk menunjukkan kesalahan-kesalahan yang disebabkan atau dibuat oleh operator.

Teknik-teknik pengendalian atas fail adalah sebagai berikut :

1) Penggunaan label eksternal.
2) Penggunaan label internal.
3) Teknik *lock out*.
4) Teknik rekonsiliasi.

3. **Pengendalian atas keluaran**. Pengendalian atas keluaran (*output controls*) dimaksudkan untuk menetapkan bahwa data yang diproses adalah lengkap, akurat dan didistribusikan kepada pihak-pihak yang berhak secara tepat waktu. Menurut IAI, pengendalian ini dimaksudkan untuk memberikan keyakinan yang memadai bahwa :

a. Hasil pengolahan adalah cermat.
b. Akses terhadap keluaran dibatasi hanya bagi karyawan yang telah mendapat otorisasi.
c. Keluaran disediakan secara tepat waktu bagi karyawan yang telah mendapat otorisasi semestinya.

Sementara itu pengendalian atas keluaran pada sistem *online* dimaksudkan untuk memberikan keyakinan bahwa:

a. Keluaran yang diterima oleh satuan usaha adalah tepat dan lengkap.
b. Keluaran yang diterima oleh satuan usaha adalah terklasifikasi.
c. Keluaran didistribusikan ke pegawai yang berotorisasi.

Yang termasuk dalam pengendalian atas keluaran antara lain:

a. Rekonsiliasi keluaran dengan masukan dan pengolahan data.
b. Penelaahan dan pengujian hasil-hasil pemprosesan, antara lain:

1) Penelaahan, penyidikan dan pengendalian terhadap laporan-laporan tentang ketidak beresan yang terjadi (laporan pengecualian atau *exception reports*), yang biasanya dilakukan oleh *control group*.
2) Membandingkan keluaran dengan dokumen aslinya.
3) Daftar revisi fail-fail induk harus ditelaah secara hati-hati, yang biasanya mencakup pencarian terhadap pos-pos yang tidak biasa atau tida normal.

c. Pendistribusian keluaran, antara lain:
1) Keluaran hanya dapat didistribusikan kepada para pemakai yang memperoleh otorisasi.
2) Pendistribusian tersebut harus dilakukan secara tepat waktu.
3) Hanya keluaran yang diperlukan saja yang didistribusikan.

d. Pengawasan terhadap catatan (*record retention*), antara lain:
1) Menjaga jangka waktu pencatatan tertentu untuk menjaga keamanan keluaran.
2) Menghindari rekonstruksi yang tidak perlu terhadap fail.
3) Mengurangi biaya perlengkapan (*supplies*) dan bahan bagi departemen EDP.
4) Untuk mengendalikan keluaran-keluaran yang sudah tidak diperlukan lagi (laporan yang sudah tidak dipakai lagi harus dihancurkan).

2.5 Kejahatan Komputer

1. **Pengertian Kejahatan Komputer**. Kejahatan komputer ialah setiap tindakan yang tidak legal dimana pengetahuan tentang teknologi komputer berperan secara cukup dominan dalam pelaksanaan kejahatan komputer tersebut.

   Peranan komputer dalam kejahatan tersebut dalam bentuk sebagai berikut:

   a. Sebagai alat, yaitu pelakunya menggunakan komputer sebagai alat untuk melakukan kejahatan seperti memasukan *input* yang tidak benar.
   b. Sebagai objek, yaitu pelakunya mengarahkan sasaranya pada penghancuran komputer yang digunakan oleh orang, pihak atau oraganisasi lain seperti penggunaan komputer oleh orang yang tidak berhak.
   c. Sebagai subjek, yaitu pelakunya menggunakan komputer untuk menipu seperti mengubah atau merusak data.
   d. Sebagai simbol, yaitu pelakunya menggunakan komputer untuk mengintimidasi seperti mencuri uang kas atau persediaan.

   Kecurangan sebagaimana diwajibkan dalam SA Seksi 316 untuk diungkapkan oleh auditor memiliki kata inti ketidakjujuran, yaitu tindakan penipuan yang disengaja dan direncanakan oleh seseorang kepada orang lain. Sementara itu kecurangan komputer (*computer fraud*) berkaitan dengan setiap pemalsuan yang dilakukan dengan cara

memalsukan program-program komputer, fail-fail data, operasi-operasi komputer, peralatan dan atau komputernya dimanipulasikan.

Delapan belas informasi yang biasa dilanggar dan dapat menimbulkan kerugian bagi suatu perusahaan adalah sebagai berikut:

a. Informasi mengenai gaji dan informasi lain yang berkaitan dengan pegawai.
b. Aplikasi paten dan rahasia-rahasia perdagangan lainnya.
c. Riset pasar dan analisis penjualan.
d. Surat-surat pengaduan (dari pelanggan) kepada perusahaan.
e. Informasi mengenai sistem pengamanan seperti kata sandi, dan sebagainya.
f. Perincian-perincian mengenai aktiva, hutang, pajak, dan masalah finansial lainya.
g. Rencana mengenai produk baru.
h. Rencana mengenai penentuan harga jual (*pricing intention*).
i. Rencana mengenai pemasaran (*marketing intention*).
j. Informasi mengenai tender atau penawaran kompetitif lainnya yang telah atau akan dibuat.
k. Daftar pelanggan perusahaan.
l. Daftar pemegang saham perusahaan.
m. Program-program mengenai aktiva atau kepemilikan.
n. Program-program dan piranti lunak lain.

o. Informasi mengenai rekayasa (*enjiniring*) seperti tempat-tempat peledakan, data mengenai biaya serta perincian-perincian mengenai pabrikasi.

p. Perincian mengenai kepemilikan saham perusahaan.

q. Buku pedoman yang berkaitan dengan produk-produk perusahaan.

r. Buku pedoman mengenai sistem dalam perusahaan serta pernyataan-pernyataan mengenai kebijakan-kebijakan perusahaan.

2. **Pihak-pihak yang mempunyai peluang untuk melakukan pelanggaran**, dapat dikelompokkan sebagai berikut:

a. Para pegawai perusahaan yang bersangkutan. Tanpa adanya suatu struktur pengendalian intern yang memadai, para pegawai departemen PDE akan dengan mudah melakukan pelanggaran. Adanya pengendalian terhadap fisik yang sangat canggih sekalipun pegawai departemen PDE ini akan dengan mudah melakukan pelanggaran karena mereka dapat mengakses untuk memasuki wilayah PDE tanpa kesulitan karena mereka mempunyai otoritas untuk memasuki ruangan PDE.

b. Mantan pegawai. Dengan kelemahan pengendalian yang ada maka mantan pegawai pun memiliki kesempatan yang sama untuk melakukan kejahatan komputer, terlebih mantan pegawai yang berhenti bekerja akibat dikeluarkan karena kondisi yang buruk, seperti akibat PHK.

c. Pihak ketiga. Kategori ini dapat mencakup organisasi atau individu yang bukan orang dalam perusahaan yang bersangkutan, baik dengan cara bekerja sama dengan orang dalam maupun tidak, mereka adalah *Hacker, Phrackers, Crackers*.

3. Metode Pengerusakan Komputer

a. Kerusakan Teknis

1) Dengan memalsukan data (*data diddling*). Pemalsuan data dilakukan dengan cara mengubah fisik dan atau menambah data *input* ataupun *output*.

2) Dengan menyebarkan virus. Virus dalam istilah komputer adalah program-program yang merusak yang biasanya tersembunyi dalam piranti lunak. Beberapa sifat virus adalah sebagai berikut:

a) Virus dapat berkembang biak dengan sendirinya sebagaimana amuba.

b) Virus dapat menghapus atau mengubah fail-fail komputer, atau memenuhi memori dengan hal-hal aneh yang mengakibatkan terganggunya operasi komputer (*operating systems*) yang bersangkutan.

c) Virus dapat menyebar dari satu komputer ke komputer lainnya, melalui disket, flashdisk, transfer lojik melalui saluran telekomunikasi ataupun kontak langsung dengan mesin atau kode yang terinfeksi.

3) Dengan melakukan pembulatan (*rounding down*). Dengan teknik ini para kriminal komputer menyisakan sebagian dari perhitungan dan memindahkan pembulatan tersebut ke akun petugas yang bersangkutan.

4) Dengan menggunakan teknik salami (*salami technique*). Cara ini akan mengurangi sebagian dari nilai transaksi yang sebenarnya dan memindahkannya ke akun petugas yang bersangkutan.

5) Dengan menggunakan teknik yang mengolah datanya dengan kuda troya (*trojan houre*). Dengan cara ini pelakunya menyembunyikan prgram yang tidak bisa diotorisasikan ke dalam program yang ada otorisasinya, dan program tersebut akan dijalankan pada saat program yang ada otorisasinya tersebut dijalankan.

6) Dengan melakukan penyebaran data. Cara ini dilakukan dengan menyebarluaskan informasi ke luar komputer seperti mencetak dalam *print-out* atau dengan mencuri fail dalam media penyimpanan atau mencuri laporan yang diterbitkan.

7) Dengan melakukan penyadapan terhadap saluran telepon. Hal ini dilakukan apabila perusahaan yang mengolah datanya dengan komputer tersebut menggunakan saluran satelit atau saluran komunikasi, yaitu dengan cara menyadap saluran informasi yang tengah dikirim tersebut.

8) Dengan melakukan pemboncengan. Istilah pemboncengan dapat berarti seseorang yang tidak memiliki otorisasi menggunakan komputer yang baru saja ditinggalkan oleh orang yang mempunyai akses atau otorisasi (berwenang menggunakan komputer).

9) Dengan menggunakan penyaruan. Dengan cara ini pelaku tersebut menyaru (memalsu) identitas dan hak-hak orang lain untuk dapat mengakses informasi atau peralatan komuter dan melakukan transaksi yang sebenarnya tidak ada otorisasinya.

10) Dengan melakukan serangan asinkron (*asynchronous attack*). Dengan cara ini orang yang bermaksud merusak atau melakukan kecurangan memanfaatkan arus pergerakan data melalui saluran telekomunikasi yang hanya satu arah untuk suatu waktu tertentu (pergerakan data secara asinkron).

11) Dengan menggunakan pintu jebakan. Dengan cara ini orang yang bermaksud merusak atau melakukan kecurangan memanfaatkan kode-kode yang pada tahap pengembangan program bisa diketahui dengan jelas, tetapi kode-kode tersebut tidak diubah atau dihapuskan dalam tahap penyelesaian pengembangan program yang bersangkutan.

b. Penghentian Ativitas Komputer. Penghentian aktivitas komputer dapat dilakukan melalui terminal atau melalui komputer mikro yang

dihubungkan ke komputer perusahaan (*online* ataupun menggunakan saluran telepon).

Dari metode-metode di atas dapat disimpulkan bahwa kecurangan dan kejahatan komputer mempunyai bentuk sebagai berikut :

1) Penggelapan informasi hasil pengolahan komputer yang seringnya mencakup penghilangan informasi tersebut untuk kepentingan pelakunya.
2) Manipulasi secara sengaja terhadap peralatan ataupun sistem-sistem baik secara sengaja ataupun tidak yang mengakibatkan atau efek sampingnya peralatan tidak dapat digunakan lagi, baik sebagian atau seluruhnya, atau mengakibatkan kerugian lain bagi organisasi.
3) Penggelapan barang-barang, jasa atau uang dengan menggunakan sistem komputer.
4) Manipulasi data akuntansi atau data lainnya untuk alasan kejahatan meskipun tidak melibatkan kehilangan uang secara langsung bagi organisasi yang bersangkutan.

c. Pencegahan Terjadinya Penggelapan dan Kejahatan Komputer. Lima langkah berikut ini dapat digunakan untuk mendetekdi adanya kecurangan :

1) Harus mengetahui *exsposure*-nya (kemungkinan terjadinya). Apa mungkin terjadi kecurangan? Siapa yang melakukannya?

2) Mengetahui gejala kecurangan (*symptomps of fraud*). Hal ini merupakan kunci untuk mendeteksi kecurangan. Familiarisasi dengan apa yang dapat terjadi kesalahan dalam area yang diaudit, serta mempelajari contoh-contoh kecurangan yang pernah terjadi.
3) Berjaga-jaga terhadap terjadinya gejala kecurangan.
4) Mendesain program audit untuk mencari gejala kecurangan.
5) Mengikuti melalui semua gejala kecurangan yang diamati.

Sementara itu *business week* menyebutkan lima cara yang sangat umum digunakan untuk menjaga data komputer, yaitu:

1) Secara regular mengubah kata sandi.
2) Di samping kata sandi, gunakan juga informasi personal lainnya seperti nama pegawai yang bersangkutan, tanggal lahir atau identifikasi lainnya karena akan mempersulit penjahat komputer untuk mengetahui lebih dari satu jenis informasi.
3) Batasi jumlah usaha yang dapat dilakukan oleh seseorang untuk mengakses ke dalam sistem seperti dalam batasan yang diberikan *BIOS setup*, yaitu tiga kali gagal, batal. Artinya, apabila seseorang mengakses secara salah sebanyak tiga kali, maka sistemnya tidak dapat diakses atau menjadi hang sehingga harus di *booting* lagi.

4) Buat catatan mengeai para pengguna sistem (*transaction log*) dan monitor catatan tersebut untuk mendeteksi kalau-kalau ada aktivitas yang tidak biasa atau mencurigakan.

5) Hukum siapa saja yang melanggar ketentuan, baik pegawai maupun pihak ekstern.

2.6 Laporan Keuangan

Menurut IAI tujuan laporan keuangan untuk tujuan umum adalah memberikan informasi tentang posisi keuangan, kinerja dan arus kas perusahaan yang bermanfaat bagi sebagian besar kalangan pengguna laporan dalam rangka memuat keputusan-keputusan ekonomi serta menunjukkan pertanggungjawaban (*stewardship*) manajemen atas penggunaan sumber-sumber daya yang dipercayakan kepada mereka.

Suatu laporan keuangan menyajikan informasi mengenai perusahaan yang meliputi :

1. Aktiva
2. Kewajiban
3. Ekuitas
4. Pendapatan dan beban termasuk keuntungan dan kerugian
5. Arus kas.

Laporan keuangan yang lengkap terdiri dari komponen-komonen berikut ini :

1. Neraca
2. Laporan laba-rugi

3. Laporan perubahan ekuitas
4. Laporan arus kas
5. Catatan atas laporan keuangan.

Laporan keuangan harus menyajikan secara wajar posisi keuangan, kinerja keuangan, perubahan ekuitas, dan arus kas perusahaan. Penilaian atas laporan keuangan dalam laporan audit adalah :

1. Wajar tanpa pengecualian (*Unqualified Opinion*).
2. Wajar tanpa pengecualian dengan paragraf penjelasan atau modifikasi kata.
3. Wajar dengan pengecualian (*Qualified Opinion*).
4. Tidak wajar (*Adverse Opinion*).
5. Tidak memberikan pendapat (*Disclaimer Of Opinion*).

Karakteristik kualitatif pokok laporan keuangan yaitu:

1. Dapat dipahami
2. Relevan
3. Keandalan
4. Dapat dibandingkan

Sistem Informasi Keuangan (SIK) adalah SIM yang menyediakan informasi untuk digunakan oleh fungsi keuangan. SIM (Sistem Informasi Manajemen) menguraikan penggunaan teknologi komputer untuk meyediakan informasi yang berorientasi pada keputusan untuk para manajer.