BAB 2

LANDASAN TEORI

2.1 Sistem Informasi

2.1.1 Pengertian Sistem Informasi

Pengertian sistem informasi menurut Hall yang diterjemahkan oleh A.A.Jusuf (2001, p7) adalah suatu rangkaian prosedur formal di mana data dikumpulkan, diproses menjadi informasi, dan didistribusikan kepada para pengguna.

Sedangkan menurut Laudon (1998, p8), sistem informasi merupakan sekumpulan komponen yang saling berhubungan dan berfungsi untuk mengumpulkan, memproses, menyimpan, dan mendistribusikan informasi untuk membantu manager dalam mengambil keputusan, menganalisis dan menggambarkan masalah yang kompleks dalam suatu organisasi.

Sedangkan O'Brien (2005, p5) mendefinisikan sistem informasi sebagai kombinasi teratur apa pun dari orang-orang, hardware, software, jaringan komunikasi, dan sumber daya data yang mengumpulkan, mengubah, dan menyebarkan informasi dalam sebuah organisasi.

Sedangkan menurut Cushing dan Romney (1994, p6), sistem informasi adalah pengumpulan, pemasukkan, pemrosesan data penyimpanan, pengelolaan, pengendalian serta pelaporan informasi sehingga organisasi dapat mencapai sasaran dan tujuan.

2.1.2 Tujuan Sistem Informasi

Tujuan sistem informasi menurut Hall yang diterjemahkan oleh A.A.Jusuf (2001, p18) dibedakan atas tiga tujuan umum bagi semua sistem, yaitu:

1. Untuk mendukung fungsi kepengurusan (*stewardship*) manajemen. Kepengurusan yang merujuk ke tanggung jawab manajemen untuk mengatur sumber daya perusahaan secara benar.
2. Untuk mendukung pengambilan keputusan manajemen. Sistem informasi memberikan para manajer informasi yang mereka butuhkan untuk melakukan tanggung jawab pengambilan keputusan.
3. Untuk mendukung kegiatan operasi perusahaan. Sistem informasi menyediakan informasi bagi personal operasi untuk membantu kegiatan operasi perusahaan secara efisien dan efektif.

2.1.3 Jenis Sistem Informasi

Jenis sistem informasi menurut Bodnar yang diterjemahkan oleh A.A.Jusuf (2001, p4-p6) antara lain adalah sebagai berikut:

a. Pengolahan Data Elektronik (*Electronic Data Processing*)

   Adalah pemanfaatan teknologi komputer untuk melakukan pengolahan data transaksi-transaksi dalam suatu organisasi. EDP adalah aplikasi sistem informasi paling dasar dalam setiap organisasi.

b. Sistem Informasi Manajemen (*Management Information System*)

   Sistem ini menguraikan penggunaan teknologi komputer untuk menyediakan informasi bagi pengambilan keputusan para manajer.

c. Sistem Pendukung Keputusan (*Decision Support System*)

Sistem ini mensyaratkan penggunaan model-model keputusan dan basis data khusus, dan benar-benar terpisah dari sistem pengolahan data. Sistem pendukung keputusan diarahkan untuk melayani permintaan informasi tertentu, khusus, dan tidak rutin dari manajemen.

d. Sistem Pakar (*Expert System*)

Adalah sistem informasi berbasis pengetahuan yang memanfaatkan pengetahuannya tentang bidang aplikasi tertentu untuk bertindak seperti seorang konsultan ahli bagi pemakainya.

e. Sistem Informasi Eksekutif (*Excecutive Information System*)

Adalah sistem yang dibuat untuk kebutuhan informasi stratejik manajemen tingkat puncak.

f. Sistem Informasi Akuntansi (*Accounting Information System*)

Adalah sistem berbasis komputer yang dirancang untuk mengubah data akuntasi menjadi informasi.

2.2 Sistem Informasi Akuntansi

2.2.1 Pengertian Sistem Informasi Akuntansi

Menurut Bodnard yang diterjemahkan oleh A.A.Jusuf (2000, p23) sistem informasi akuntansi adalah kumpulan sumber daya seperti manusia dan peralatan yang diatur untuk mengubah data menjadi informasi.

Menurut Baridwan (1998, p4) sistem informasi akuntansi adalah suatu komponen organisasi yang mengumpulkan, menggolongkan, mengolah, menganalisa dan komunikasikan informasi keuangan yang relevan untuk pengambilan keputusan

kepada pihak-pihak luar (seperti inspeksi pajak, investor dan kreditur) dan pihak-pihak dalam (terutama manajemen).

2.2.2 Tujuan Dan Fungsi Dari Sistem Informasi Akuntansi

Menurut Bodnard yang diterjemahkan oleh A.A.Jusuf (2000, p23) Tujuan umum penyusunan sistem informasi akuntansi adalah sebagai berikut:

1. Untuk memperbaiki informasi yang diberikan oleh sistem dalam kualitas, ketepatan waktu atau struktur dari informasi tersebut.
2. Untuk memperbaiki pengendalian akuntansi dan pengecekan intern, yang berarti memperbaiki daya andal informasi akuntansi dan menyediakan catatan yang lengkap sebagai pertanggungjawaban dalam melindungi harta perusahaan.
3. Untuk menurunkan biaya dalam menyelenggarakan catatan akuntansi.

Menurut Bodnard yang diterjemahkan oleh A.A.Jusuf (2000, p25) Di dalam organisasi, sistem informasi akuntansi berfungsi untuk :

1. Mengumpulkan dan menyimpan aktivitas yang dilaksanakan di suatu organisasi, sumber daya yang dipengaruhi oleh aktivitas-aktivitas tersebut dan para pelaku aktivitas tersebut.
2. Mengubah data menjadi informasi yang berguna bagi manajemen.
3. Menyediakan pengendalian yang memadai.

2.2.3 Faktor-Faktor Dalam Sistem Informasi Akuntansi

Menurut Bodnard yang diterjemahkan oleh A.A.Jusuf (2000, p25) Penyusunan sistem informasi akuntansi untuk suatu perusahaan perlu mempertimbangkan beberapa faktor penting antara lain:

1. Sistem informasi akuntansi yang disusun harus memenuhi prinsip cepat yaitu sistem informasi akuntansi harus menyediakan informasi yang diperlukan dengan cepat dan tepat waktu serta dapat memenuhi kebutuhan dan kualitas yang sesuai..
2. Sistem informasi yang disusun harus memenuhi prinsip aman yaitu sistem informasi harus dapat membantu menjaga keamanan harta milik perusahaan.
3. Sistem informasi akuntansi yang disusun harus memenuhi prinsip murah yang berarti bahwa biaya untuk menyelenggarakan sistem informasi akuntansi tersebut harus dapat ditekan sehingga relatif tidak mahal.

2.2.4 Siklus Dalam Sistem Informasi Akuntansi

Menurut Romney (2003, p52) Komponen-komponen sistem informasi akuntansi digunakan untuk menangani berbagai transaksi yang ada didalam perusahaan. Transaksi-transaksi yang terjadi didalam perusahaan dapat dikelompokkan menjadi enam kelompok, yaitu :

1. Siklus pengeluaran

Berhubungan dengan usaha mendapatkan sumber-sumber ekonomis yang diperlukan oleh perusahaan, terutama dalam bentuk barang dan jasa. Baik dari pemasok luar maupun dari karyawan didalam perusahaan. Siklus ini meliputi sistem pembelian, sistem hutang dan penggajian. Siklus pengeluaran mempunyai dua sistem utama, yaitu sistem pembelian dan sistem pembayaran kas. Sistem pembelian mencakup pengadaan sumber daya (misalnya barang dagang, suku cadang, alat tulis kantor) dan jasa (misalnya listrik, telpon); sedangkan pembayaran kas meliputi penyiapan pembayaran sampai penyerahan uang kepada pemasok atau penjual.

2. Siklus pendapatan

Berhubungan dengan penditribusian sumber-sumber ekonomi yang telah diubah bentuknya kepada pembeli dan mendapatkan pembayarannya dari mereka. Siklus ini meliputi sistem pemesanan, sistem penjualan & sistem piutang dagang.

3. Siklus produksi

Berhubungan dengan pengumpulan, penggunaan & pengubahan bentuk suatu sumber ekonomi. Siklus ini meliputi sistem produksi dan sistem pengawasan persediaan.

4. Siklus keuangan

Berhubungan dengan pencarian atau pengumpulan dana atau modal dari para pemilik perusahaan dan para kreditur, serta para penggunanya. Dalam hal ini meliputi investasi jangka pendek, sebelum dana tersebut digunakan untuk keperluan operasi, siklus ini juga disebut dengan siklus pengelolaan sumber daya.

5. Siklus perencanaan

Tidak berhubungan langsung dengan transaksi yang terjadi didalam perusahaan. Siklus ini berfungsi untuk menentukan transaksi apa yang akan terjadi pada suatu siklus dan bagaimana siklus transaksi itu akan ditangani dan diawasi. Siklus perencanaan meliputi jangka panjang dan jangka pendek.

6. Siklus pelaporan

Berhubungan dengan pembuatan laporan, baik kepada pihak luar (yaitu pembuatan laporan rutin), maupun pembuat laporan reguler. Laporan untuk kepentingan manajemen memang dapat dimasukkan kedalam siklus pelaporan, tetapi akan lebih cepat dan lebih tepat bila dihasilkan oleh siklus operasi, karena siklus inilah yang langsung berhubungan dengan transaksi dan datanya. Siklus ini sering disebut juga siklus buku besar dan laporan keuangan. Siklus buku besar dan laporan keuangan merupakan muara bagi

semua siklus yang lain. Sistem ini menerima data yang mengalir dari sistem yang lain untuk kemudian menyusun laporan ditiap periode yang telah ditetapkan.

2.3 Sistem Pengendalian Internal

2.3.1 Pengertian Sistem Pengendalian Internal

Menurut Weber (1999, p35), pengendalian adalah suatu sistem untuk mencegah, mendeteksi dan mengoreksi kejadian yang timbul saat transaksi dari serangkaian pemrosesan yang tidak terotorisasi secara sah, tidak akurat, tidak lengkap, mengandung redudansi, tidak efektif dan tidak efisien.

Menurut Mulyadi (1997, p165), sistem pengendalian internal meliputi struktur organisasi, metode dan ukuran-ukuran yang dikoordinasikan untuk menjaga kekayaan organisasi, mengecek ketelitian dan keandalan data akuntansi, mendorong efisiensi dan mendorong dipatuhinya kebijakan manajemen.

Sedangkan menurut Hall yang diterjemahkan oleh A.A.Jusuf (2001, p.150), sistem pengendalian internal merangkum kebijakan, praktik-praktik, dan prosedur-prosedur yang digunakan oleh organisasi untuk mencapai tujuan perusahaan.

2.3.2 Tujuan Pengendalian Internal

Menurut Hall yang diterjemahkan oleh A.A.Jusuf (2001, p.150) Sistem pengendalian internal merangkum kebijakan, praktik, dan prosedur yang digunakan oleh organisasi untuk mencapai empat tujuan utama, yaitu:

1. Untuk menjaga aktiva perusahaan
2. Untuk memastikan akurasi dan dapat diandalkan catatan dan informasi akuntansi
3. Untuk mempromosikan efisiensi operasi perusahaan

4. Untuk mengukur kesesuaian dengan kebijakan dan prosedur yang telah ditetapkan oleh manajemen

2.3.3 Unsur-Unsur Pengendalian Internal

Menurut Mulyadi (1997, p.166), unsur pokok sistem pengendalian internal adalah sebagai berikut:

1. Struktur organisasi yang memisahkan tanggung jawab fungsional secara tegas
2. Sistem wewenang dan prosedur pencatatan yang memberikan perlindungan yang cukup terhadap aset, hutang, pendapatan dan biaya
3. Praktik yang sehat dalam melaksanaan tugas dan tanggung jawab dan fungsi setiap unit organisasi.
4. Karyawan yang mutunya sesuai dengan tanggung jawabnya.

2.3.4 Elemen-Elemen Pengendalian Internal

Menurut Weber (1999, p49), pengendalian internal terdiri dari lima unsur/komponen yang saling berintegrasi, antara lain:

1. Lingkungan Pengendalian (*Control Environment*)

   Komponen ini diwujudkan dengan cara pengoperasian, pembagian wewenang dan tanggung jawab yang harus dilakukan, komite audit berfungsi, dan metode-metode yang digunakan untuk merencanakan dan memonitor kinerja.

2. Penaksiran Resiko (*Risk Assessment*)

   Komponen untuk mengidentifikasi dan menganalisa resiko yang dihadapi oleh perusahaan dan cara untuk menghadapi resiko tersebut.

3. Aktivitas Pengendalian (*Control Activities*)

   Komponen yang dioperasikan untuk memastikan transaksi telah terotorisasi, adanya pembagian tugas, pemeliharaan terhadap dokumen dan *record*, perlindungan aset dan *record*, pengecekan kinerja dan penilaian dari jumlah *record* yang terjadi.

4. Informasi dan Komunikasi (*Information and Communication*)

   Komponen dimana informasi digunakan untuk mengidentifikasi, mendapatkan, dan menukarkan data yang dibutuhkan untuk mengendalikan dan mengatur operasi perusahaan.

5. Pemantauan (*Monitoring*)

   Komponen yang memastikan pengendalian internal beroperasi secara dinamis.

2.3.5 Jenis Pengendalian Internal

Menurut Weber (1999, p67), ruang lingkup pengendalian dibedakan atas dua jenis, yaitu *management control framework* (pengendalian manajemen) dan *application control framework* (pengendalian aplikasi).

1. Pengendalian Manajemen

   Pengendalian manajemen (*management control*) ialah sistem pengendalian internal komputer yang berlaku umum meliputi seluruh kegiatan komputerisasi sebuah organisasi secara menyeluruh. Artinya ketentuan-ketentuan yang berlaku dalam pengendalian tersebut, berlaku untuk seluruh kegiatan komputerisasi di perusahaan tersebut. Pengendalian ini berguna untuk menyediakan infrastruktur yang stabil sehingga sistem informasi dapat dibangun, dioperasikan, dan dipelihara secara berkesinambungan.

a. Pengendalian Top Manajemen (*Top Level Management Control*)

   Mengendalikan peranan manajemen dalam perencanaan kepemimpinan dan pengawasan fungsi sistem.

b. Pengendalian Manajemen Sistem Informasi (*Information System Management Control*)

   Mengendalikan alternatif dari model pengembangan proses sistem informasi sehingga dapat digunakan sebagai dasar pengumpulan dan pengevaluasian bukti.

c. Pengendalian Manajemen Pengembangan Sistem (*System Development Management Control*)

   Mengendalikan tahapan utama dari daur hidup program dan pelaksanaan dari tiap tahap.

d. Pengendalian Manajemen Sumber Data (*Data Resource Management Control*)

   Mengendalikan peranan dan fungsi dari data administrator atau database administrator.

e. Pengendalian Manajemen Jaminan Kualitas (*Quality Assurance Management Control*)

   Mengendalikan fungsi utama yang harus dilakukan oleh *Quality Assurance Management* untuk meyakinkan bahwa pengembangan, pelaksanaan, pengoperasian, dan pemeliharaan dari sistem informasi sesuai dengan standar kualitas.

f. Pengendalian Manajemen Keamanan (*Security Management Control*)

Menurut Weber (1999, p257-266), dapat disimpulkan bahwa pengendalian terhadap manajemen keamanan secara garis besar bertanggung jawab dalam menjamin aset sistem informasi tetap aman. Ancaman utama terhadap keamanan aset sistem informasi:

1. Ancaman kebakaran

   Beberapa pelaksanaan pengamanan untuk ancaman kebakaran:

   a. Memiliki alarm kebakaran otomatis yang diletakkan pada tempat di mana aset-aset sistem informasi berada
   b. Memiliki tabung kebakaran yang diletakkan pada lokasi yang mudah diambil
   c. Memiliki tombol power utama (termasuk AC)
   d. Gedung tempat penyimpanan aset sistem informasi dibangun dari bahan tahan api
   e. Memiliki pintu / tangga darurat yang diberi tanda dengan jelas sehingga karyawan dengan mudah menggunakannya
   f. Ketika alarm berbunyi, signal langsung dikirim ke stasiun pengendalian yang selalu dijaga oleh staf
   g. Prosedur pemeliharaan gedung yang baik menjamin tingkat polusi rendah di sekitar aset sistem informasi yang bernilai tinggi

2. Ancaman banjir

   Beberapa pelaksanaan pengamanan untuk ancaman banjir :

a. Usahakan bahan untuk atap, dinding dan lantai yang tahan air
b. Menyediakan alarm pada titik strategis dimana material aset sistem informasi diletakkan
c. Semua material aset sistem informasi diletakkan di tempat yang tinggi
d. Menutup peralatan *hardware* dengan bahan yang tahan air sewaktu tidak digunakan

3. Perubahan tenaga sumber energi

   Pelaksanaan pengamanan untuk mengantisipasi perubahan tegangan sumber energi listrik, misalnya menggunakan *stabilizer* ataupun *Uninteruptable Power Supply* (UPS) yang memadai yang mampu mengcover tegangan listrik jika tiba-tiba turun.

4. Kerusakan struktural

   Pelaksanaan struktural terhadap aset sistem informasi dapat terjadi karena adanya gempa, angin, dan salju. Beberapa pelaksanaan pengamanan untuk mengantisipasi kerusakan struktural misalnya adalah memilih lokasi perusahaan yang jarang terjadi gempa dan angin ribut.

5. Polusi

   Beberapa pelaksanaan pengamanan untuk mengantisipasi polusi, misalnya situasi kantor yang bebas debu dan tidak memperbolehkan membawa binatang peliharaan. Atau dengan melarang karyawan membawa/meletakkan minuman di dekat peralatan komputer.

6. Penyusupan

   Pelaksanaan pengamanan untuk mengantisipasi penyusup dapat dilakukan dengan penempatan penjaga dan penggunaan alarm.

7. Virus

   Pelaksanaan pengamanan untuk mengantisipasi virus meliputi tindakan:

   a. *Preventive*, seperti meng*install* antivirus dan meng*update* secara rutin, melakukan *scan file* yang akan digunakan
   b. *Detective*, seperti melakukan *scan* secara rutin
   c. *Corrective*, seperti memastikan *backup* data bebas virus, pemakaian antivirus terhadap *file* yang terinfeksi

8. Hacking

   Beberapa pelaksanaan pengamanan untuk mengantisipasi *hacking*:

   a. Penggunaan kontrol logikal seperti penggunaan password yang sulit untuk ditebak
   b. Petugas keamanan secara teratur memonitor sistem yang digunakan
   c. Rencana pemulihan bencana yang terdiri dari empat bagian sebagai berikut:

      i. Rencana Darurat (*Emergency Plan*)
      ii. Rencana *Backup* (*Backup Plan*)
      iii. Rencana Pemulihan (*Recovery Plan*)
      iv. Rencana Pengujian (*Test Plan*)

d. Asuransi

Memiliki asuransi untuk fasilitas peralatan, media penyimpanan, biaya tambahan, gangguan bisnis, dokumen dan kertas yang berharga, dan media transportasi.

g. Pengendalian Manajemen Operasi (*Operations Management Control*)

Menurut Weber (1999, p293-320), secara garis besar pengendalian manajemen operasi (*Operations Management Controls*) bertanggung jawab terhadap hal-hal sebagai berikut:

1. Pengoperasian komputer (*Computer Operations*)

   Tipe pengendalian yang harus dilakukan:

   a. Menentukan fungsi-fungsi yang harus dilakukan operator komputer maupun fasilitas operasi otomatis
   b. Menentukan penjadwalan kerja pada pemakaian *hardware* atau *software*
   c. Menentukan perawatan terhadap *hardware* agar dapat berjalan baik
   d. Pengendalian perangkat keras berupa *hardware controls* dari produsen untuk deteksi *hardware malfunction*

2. Pengoperasian jaringan (*Network Operation*)

   Pengendalian yang dilakukan ialah memonitor dan memelihara jaringan dan pencegahan terhadap akses oleh pihak yang tidak berwenang. Pengendalian sistem komunikasi data antara lain adalah:

a. Jalur komunikasi

b. Hardware

c. Cryptology

d. Software

3. Persiapan dan pengentrian data (*Preparation and Entry Data*)

   Fasilitas-fasilitas yang ada harus dirancang untuk memiliki kecepatan dan keakuratan data serta telah dilakukan terhadap pengentrian data.

4. Pengendalian Produksi (*Production Control*)

   Fungsi yang harus dilakukan untuk pengendalian produksi adalah:

   a. Penerimaan dan pengiriman *input* dan *output*
   b. Penjadwalan kerja
   c. Manajemen pelayanan
   d. Peningkatan pemanfaatan komputer

5. Perpustakaan *File* (*File Library*)

   Fungsi yang harus dilakukan untuk perpustakaan *file* adalah:

   a. Penyimpanan media penyimpanan (*storage of storage media*)
   b. Penggunaan media penyimpanan (*use of strorage media*)
   c. Pemeliharaan dan penempatan media penyimpanan (*maintenance and disposal of storage media*)
   d. Lokasi media penyimpanan (*location of storage media*)

6. Perpustakaan Dokumentasi dan Program (*Documentation and Program Library*)

Orang yang bertanggungjawab atas dokumentasi mempunyai beberapa fungsi yang harus dilakukan yaitu:

a. Memastikan bahwa semua dokumentasi disimpan secara aman
b. Memastikan bahwa hanya orang yang mempunyai otorisasi saja yang bisa mengakses dokumentasi
c. Memastikan bahwa dokumentasi tersebut selalu *up-to-date*
d. Memastikan bahwa adanya *backup* yang cukup untuk dokumentasi yang ada

7. Bantuan dan Dukungan Teknis (*Help Desk/Technical Support*)

   Ada 2 (dua) fungsi utama *help desk/technical support* yaitu:

   a. Membantu *end user* dalam menggunakan *hardware* dan *software* yang berhubungan dengan *end user* seperti *microcomputer, spreadsheet packages, database management packages*, dan *local area networks*
   b. Menyediakan *technical support* untuk sistem produksi dengan dilengkapi suatu penyelesaian masalah yang berhubungan dengan *hardware*, *software* dan *database*

8. Perencanaan Kapasitas dan Pemantauan Kinerja (*Capacity Planning and Performance Monitoring*)

   Tujuan utama dari fungsi sistem informasi ini adalah untuk mencapai tujuan dari penggunaan sistem informasi dengan biaya yang serendah mungkin.

9. Manajemen Operasi *Outsource* (*Management of Outsourced Operations*)

   Saat ini banyak organisasi yang melakukan *outsource* terhadap beberapa fungsi dari sistem informasi mereka. Alasan utama dilakukannya *outsource* karena mereka ingin menfokuskan pada fungsi inti bisnis mereka. Manajemen operasi harus menfokuskan pada 4 (empat) jenis pengendalian dalam hal memantau kegiatan *outsource* antara lain:

   a. Mengevaluasi *outsourcing vendor* yang dilihat dari segi keuangan
   b. Memastikan ketaatan dari kontrak *outsourcing* yang telah disepakati
   c. Memastikan bahwa operasi dari *outsourcing vendor* dapat dijalankan
   d. Memelihara prosedur-prosedur untuk pemulihan bencana dengan *outsourcing vendor*

2. Pengendalian Aplikasi

   a. Pengendalian *Boundary* (*Boundary Control*)

      Mengendalikan sifat dan fungsi pengendalian akses, penggunaan pengkodean dalam pengendalian akses, nomor identifikasi personal (PIN), *digital signatures* dan *plastic cards*. Tujuan dari *boundary control* adalah:

      i. Untuk menetapkan identitas dan otoritas *user* terhadap sistem komputer

ii. Untuk menetapkan identitas dan kebenaran sumber informasi yang digunakan *user*

iii. Untuk membatasi kegiatan *user* dalam mendapat sumber informasi berdasarkan kewenangan

Jenis-jenis pengendalian dalam subsistem *boundary*, yaitu:

i. Pengendalian Kriptografi

Kriptografi merupakan sistem untuk mentransformasikan data menjadi kode (cryptograms) sehingga tidak memiliki arti bagi orang yang tidak memiliki sistem untuk mengubah kembali data tersebut. Tujuannya untuk menjaga kerahasiaan informasi dengan mengacak data.

ii. Pengendalian Akses

Pengendalian akses berfungsi untuk membatasi penggunaan sumber daya sistem komputer, membatasi dan memastikan *user* untuk mendapatkan sumber daya yang mereka butuhkan. Langkah-langkah umum untuk menunjang fungsi tersebut, yaitu:

1. Mengesahkan *user* yang telah mengidentifikasikan dirinya ke sistem
2. Mengesahkan sumber daya yang diminta oleh *user*
3. Membatasi aktivitas yang dilakukan oleh *user* terhadap sistem

b. Pengendalian Input (*Input Control*)

Menurut Weber (1999, pp420-450), komponen pada subsistem *input* bertanggung jawab dalam mengirimkan data dan instruksi ke dalam sistem aplikasi di mana kedua tipe atribut tersebut haruslah divalidasi, selain itu

banyaknya kesalahan yang terdeteksi harus dikontrol sehingga *input* yang dihasilkan akurat, lengkap, unik dan tepat waktu.

Pengendalian *input* merupakan hal yang kritis didasarkan 3 alasan, yaitu jumlah pengendalian yang paling besar pada sistem informasi terhadap kehandalan subsistem *input*, aktivitas pada subsistem *input*, yang bersifat rutin, dalam jumlah besar dan campur tangan ini dapat mengalami kebosanan sehingga cenderung mengalami *error*, subsistem *input* sering menjadi target dari *fraud*. Banyak ketidakberesan yang ditemukan dengan cara penambahan, penghapusan, atau pengubahan transaksi *input*.

c. Pengendalian Proses (*Process Control*)

Menurut Porter dan Perry (terjemahan Widjajanto, Nugroho, 1996, p200), pengendalian proses mencakup pengendalian terhadap kemungkinan kehilangan data atau tidak diprosesnya data, perhitungan aritmatik, dan keakuratan pemrograman.

1. Kemungkinan kehilangan data atau tidak diprosesnya data

   Pengendalian yang dilakukan untuk mendeteksi kehilangan atau tidak diprosesnya data terdiri dari:

   i. Perhitungan *record*

      Perhitungan *record* adalah jumlah *record* yang diproses oleh komputer kemudian total yang dihasilkan dibandingkan dengan suatu perhitungan manual yang telah ditetapkan sebelumnya. Setiap saat *file* diproses, *record* dihitung kembali dan jumlahnya disamakan dengan total awal atau total yang telah disesuaikan.

ii. Total kontrol (*control total*)

Dilakukan terhadap *field* kuantitas atau yang mengandung perhitungan jumlah dalam satu kelompok *record* yang kemudian hasil perhitungan tersebut digunakan untuk mengecek pengendalian yang ditetapkan dalam manual atau pemrosesan komputer sebelumnya atau berikutnya.

iii. Total *hash*

Bentuk lain dari total pengendali yang dibuat dari data dalam suatu *field* non kuantitas di dalam suatu kelompok *record*.

2. Perhitungan aritmatik

Pengendalian yang dilakukan untuk perhitungan atau kalkulasi aritmatik terdiri dari:

i. Pemeriksaan batas (*limit checks*)

Dilakukan dengan mengetes hasil-hasil kalkulasi terhadap batas-batas yang telah ditetapkan terlebih dahulu.

ii. Pemeriksaan saldo jumlah mendatar (*cross-footing balance check*)

Dilakukan terhadap *field-field* yang mempunyai hubungan satu sama lain dan hasil penjumlahannya dicocokkan pada akhir proses.

iii. Tes melimpah (*overflow test*)

Merupakan suatu tes yang digunakan secara luas untuk menentukan apakah ukuran suatu hasil perhitungan melampaui alokasi ukuran yang telah terdaftar dan disimpan.

3. Memastikan keakuratan pemrograman

   Pengendalian yang dilakukan untuk memastikan keakuratan pemrograman berupa:

   i. Dokumentasi yang tepat

      Dokumentasi yang baik akan menempatkan kesalahan pemrograman dan akan memudahkan koreksi.

   ii. Prosedur pengujian program yang ekstensif

      Akan mengurangi kemungkinan gangguan program dan memudahkan pengoperasian sistem yang lancar.

d. Pengendalian *Output* (*Output Control*)

   Pengendalian *output* digunakan untuk memastikan bahwa data yang diproses tidak mengalami perubahan yang tidak sah oleh personil operasi komputer dan memastikan hanya personil yang berwenang saja yang menerima *output*. Pengendalian *output* yang dilakukan berupa:

   1. Mencocokkan data *output* dengan total pengendali sebelumnya yang telah ditetapkan yang diperoleh dalam tahap *input* dari siklus pemrosesan
   2. Meninjau data *output* untuk melihat format yang tepat. Format yang tepat terdiri dari:
      a. *Page heading*
      b. Judul laporan
      c. Tanggal dan waktu pencetakan
      d. Banyaknya *copy* laporan untuk masing-masing pihak yang berwenang

e. Periode laporan
f. Nama program (termasuk versinya yang menghasilkan laporan)
g. Nama personil yang bertanggungjawab atas dikeluarkannya laporan tersebut
h. Masa berlaku laporan
i. Nomor halaman
j. Tanda akhir halaman

3. Mengendalikan data *input* yang ditolak oleh komputer selama pemrosesan dan mendistribusikan data yang ditolak tersebut ke personil yang tepat
4. Mendistribusikan laporan-laporan *output* ke departemen pemakai tepat pada waktunya

e. Pengendalian Database (*Database Control*)

Menurut Porter dan Perry (1996, p204), pengendalian *database* digunakan untuk menjaga integritas data dalam suatu *database*. Pengendalian yang dilakukan mencakup pengendalian terhadap pelaporan kemacetan, sistem kamus data, sistem kamus data yang terintegrasi, tanggungjawab unsur data, pengendalian data bersama dan pemecahan hambatan.

f. Pengendalian Komunikasi (*Communication Control*)

Menurut Weber (1999, p474), pengendalian komunikasi digunakan untuk mengendalikan pendistribusian pembukaan komunikasi subsistem, komponen fisik, kesalahan jalur komunikasi, aliran dan hubungan, pengendalian topologi, pengendalian akses hubungan, pengendalian atas

ancaman subversif, pengendalian *internetworking*, dan pengendalian arsitektur komunikasi.

2.4 Audit Sistem Informasi

2.4.1 Pengertian Audit Sistem Informasi

Menurut Weber (1999, p10), audit sistem informasi adalah proses pengumpulan dan pengevaluasian bukti-bukti untuk memutuskan apakah dengan adanya sistem pengamanan aset yang berbasis komputer dan pemeliharaan integritas data, data dapat mendukung perusahaan untuk mencapai tujuannya secara efektif dan penggunaan sumber daya secara efisien serta mengetahui apakah suatu perusahaan memiliki pengendalian internal yang memadai.

Sedangkan menurut Rommey dan Steinbart (2003, p321), *audit* sistem informasi mengkaji ulang pengendalian sistem informasi akuntansi untuk menilai pemenuhannya dengan kebijakan dan prosedur pengendalian internal dan keefektifan perlindungan terhadap aset.

2.4.2 Tujuan Audit Sistem Informasi

Berdasarkan pendapat Muchtar (1999, p.125), tujuan dari audit sistem informasi adalah untuk mereview dan mengevaluasi pengawasan internal yang digunakan untuk menjaga keamanan dan memeriksa tingkat kepercayaan sistem informasi serta mereview operasional aplikasi. Apabila audit sistem informasi akan dilaksanakan secara lengkap maka auditor harus berusaha untuk memenuhi setiap tujuan berikut ini:

1. Untuk menemukan bahwa sistem keamanan yang ada berfungsi dengan baik untuk memperoleh peralatan, program, file data dari pemakaian dan perubahan oleh yang tidak berhak.
2. Untuk menemukan bahwa desain dan implementasi program aplikasi sesuai dengan spesifikasi dan otorisasi manajemen.
3. Untuk menemukan bahwa semua modifikasi program aplikasi memiliki otorisasi dan persetujuan manajemen.
4. Untuk menemukan akurasi dan integrasi dari proses transaksi, file, laporan, dan record-record lainnya.
5. Untuk menemukan sumber data dari program aplikasi yang tidak akurat dan mengidentifikasikan serta menyesuaikan dengan kebijakan manajemen.
6. Untuk menemukan apakah ada usaha untuk memenuhi syarat akurasi proses data, kelengkapan data, serta tingkat kerahasiaan file data.

2.4.3 Pendekatan Audit Sistem Informasi

Menurut Weber (1999, p55-57), metode audit antara lain adalah:

1. *Auditing around the computer*

   Merupakan suatu pendekatan audit dengan memperlakukan komputer sebagai black box, maksudnya metode ini tidak menguji langkah-langkah proses secara langsung, tetapi hanya berfokus pada input dan output dari sistem komputer. Diasumsikan bahwa jika input benar akan diwujudkan pada output, sehingga pemrosesan juga benar dan tidak melakukan pengecekan terhadap pemrosesan komputer secara langsung.

   Pendekatan ini mengandung berbagai kelemahan antara lain:

a. Umumnya database mencakup jumlah data yang banyak dan sukar untuk ditelusuri secara manual.
b. Tidak menciptakan sarana bagi auditor untuk menghayati dan mendalami lebih mantap liku-liku komputer.
c. Cara ini mengabaikan pengendalian sistem dalam pengolahan komputer itu sendiri, sehingga rawan terhadap adanya kelemahan dan kesalahan yang potensial didalamnya.
d. Kemampuan komputer sebagai fasilitas penunjang pelaksanaan audit menjadi sia-sia.
e. Tidak dapat mencakup keseluruhan maksud dan tujuan penyelenggaraan audit.

2. *Auditing through the computer*

Merupakan suatu pendekatan audit yang berorientasi pada komputer dengan membuka black box, dan secara langsung berfokus pada operasi pemrosesan dalam sistem komputer. Dengan asumsi bahwa apabila pemrosesan mempunyai pengendalian yang memadai, maka kesalahan dan penyalahgunaan tidak akan terlewat untuk dideteksi, sebagai akibat dari keluaran dapat diterima.

Keuntungan utama dari pendekatan ini adalah dapat meningkatkan kekuatan terhadap pengujian sistem aplikasi secara efektif, dimana ruang lingkup dan kemampuan dari pengujian yang dilakukan dapat diperluas sehingga tingkat kepercayaan terhadap keandalan 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 kehilangan yang terjadi pada masa yang akan datang.

Kelemahan dari pendekatan ini adalah sebagai berikut:

a. Biaya yang dibutuhkan relatif tinggi yang disebabkan jumlah jam kerja yang banyak untuk dapat lebih memahami struktur kontrol internal dari pelaksanaan sistem aplikasi.
b. Butuh banyak keahlian teknis yang lebih mendalam untuk memahami cara kerja.

3. *Auditing with the computer*

Pendekatan ini dilakukan dengan menggunakan komputer dan *software* untuk mengotomatisasi prosedur pelaksanaan audit. Pendekatan ini merupakan cara audit yang sangat bermanfaat, khususnya dalam pengujian substantif atas file dan record perusahaan. Software audit yang digunakan merupakan program komputer auditor untuk membantu dalam pengujian dan evaluasi kehandalan data, file dan record perusahaan.

Keunggulan pendekatan ini adalah:

a. Merupakan program komputer yang diproses untuk membantu pengujian pengendalian sistem komputer klien itu sendiri.
b. Dapat melaksanakan tugas audit yang terpisah dari catatan klien, yaitu dengan mengambil copy data atau file untuk dites dengan komputer lain.

Kelemahan dari pendekatan ini adalah dibutuhkan upaya dan biaya yang relatif besar untuk pengembangannya.

2.4.4 Prosedur Audit

Arens dan Loebbecke yang diterjemahkan oleh Jusuf (1996, p.153-158), dalam menentukan prosedur audit digunakan tujuh kategori bahan bukti yang dapat digunakan oleh auditor yaitu:

1. Pemeriksaan Fisik

   Adalah sebagai alat yang langsung digunakan untuk memverifikasi apakah suatu aktiva secara aktual ada, dianggap sebagai salah satu bahan bukti yang paling handal dan berguna.

2. Konfirmasi

   Digambarkan sebagai penerimaan jawaban tertulis maupun lisan dari pihak ketiga yang independen dalam memverifikasi akurasi informasi yang telah diminta oleh auditor.

3. Dokumentasi

   Merupakan bentuk bahan bukti yang digunakan secara luas dalam setiap audit karena biasanya sudah tersedia bagi auditor dengan biaya yang relatif rendah. Seringkali hanya bahan bukti jenis ini yang tersedia.

4. Pengamatan

   Adalah penggunaan perasaan untuk menetapkan aktivitas tertentu. Dalam keseluruhan audit akan ada banyak kesempatan untuk melihat, mendengar, menyentuh, dan mencium untuk mengevaluasi bermacam benda.

5. Pertanyaan

   Adalah mendapatkan informasi tertulis atau lisan dari klien dengan menjawab pertanyaan dari auditor. Meksipun sebagai bahan bukti yang diperhitungkan dapat memperoleh dari klien melalui tanya jawab, biasanya tanya jawab tidak

dapat diperlakukan sebagai kemampuan memberikan kesimpulan, karena didapat dari sumber yang tidak independen dan mungkin memihak kepentingan klien. Dengan demikian, apabila auditor memperoleh bahan bukti tanya jawab, biasanya perlu untuk mendapatkan bahan bukti lain yang menguatkan melalui prosedur yang lain.

6. Pelaksanaan Ulang

   Mencakup pengecekan ulang suatu sampel perhitungan dan perpindahan informasi yang dilakukan klien selama periode yang diaudit.

7. Prosedur Analitis

   Adalah menggunakan perbandingan dan hubungan untuk menentukan apakah saldo akun tersaji secara layak. Prosedur analitis sangat penting sehingga harus dilakukan selama tahap perencanaan dan penyelesaian di setiap audit.

2.4.5 Langkah-langkah Audit Sistem Informasi

Menurut Weber (1999, p47-54), langkah-langkah untuk melakukan kegiatan audit terdiri dari:

1. *Planning the audit*

   Perencanaan merupakan *fase* pertama dari kegiatan audit, bagi eksternal auditor hal ini artinya adalah melakukan *investigasi* terhadap klien untuk mengetahui apakah pekerjaan mengaudit dapat diterima, menempatkan *staff* audit, menghasilkan perjanjian audit, menghasilkan informasi latar belakang klien, mengerti tentang masalah hukum klien dan melakukan analisa terhadap prosedur yang ada untuk mengerti tentang bisnis klien dan mengidentifikasi resiko audit.

2. *Test the controls*

   Auditor melakukan *test controls* ketika mereka menilai bahwa *control* resiko berada pada level kurang dari maksimum, mereka mengandalkan *control* sebagai dasar untuk mengurangi biaya *testing*. Sampai pada *fase* ini auditor tidak mengetahui apakah identifikasi *control* telah berjalan dengan efektif, *test* terhadap *control* oleh karena itu diperlukan evaluasi yang spesifik terhadap materi *control*.

3. *Test the transactions*

   Auditor menggunakan *test* terhadap transaksi untuk mengevaluasi apakah kesalahan atau proses yang tidak biasa terjadi pada transaksi yang mengakibatkan kesalahan pencatatan yang *material* pada laporan keuangan. *Test* transaksi ini termasuk menelusuri atau *trace* jurnal dari sumber dokumen, memeriksa *file* berharga dan mengecek keakuratan perhitungan. Pemakaian komputer sangat membantu pekerjaan ini dan auditor harus menggunakan *software* audit umum untuk mengecek apakah bunga yang dibayar kepada bank telah sesuai perhitungannya.

4. *Tests the balances or overall results*

   Untuk mengetahui pendekatan yang digunakan pada *fase* ini, yang harus diperhatikan adalah tujuan pengamanan harta dan data *integrity*. Beberapa jenis *substantive test* terhadap saldo yang digunakan adalah konfirmasi piutang, perhitungan fisik persediaan, dan perhitungan ulang penyusutan aktiva tetap.

5. *Completion of the audit*

   Pada *fase* akhir audit, eksternal audit akan menjalankan beberapa tes tambahan terhadap bukti yang ada agar dapat dijadikan laporan.

   Terdapat 4 opini yang dapat diberikan terhadap hasil audit oleh eksternal audit, yaitu:

a. *Disclaimer of opinion* (Tidak Memberikan Pendapat), auditor tidak akan memberikan opini.

b. *Adverse opinion* (Pendapat Tidak Wajar), auditor berpendapat bahwa terdapat banyak kesalahan.

c. *Qualified opinion* (Wajar Dengan Pengecualian), auditor berpendapat bahwa terjadi beberapa kesalahan tetapi nilainya tidak *material*.

d. *Unqualified opinion* (Wajar Tanpa Pengecualian), auditor berpendapat bahwa tidak terjadi kesalahan atau *misstatement.*

2.4.6 Teknik Penilaian Resiko dan Pengendalian

Menurut Griffiths (2007, p18) Setelah memperoleh bukti audit yang cukup beserta temuannya dengan menggunakan instrumen pengumpulan bukti, audit dilanjutkan dengan menggunakan matriks penilaian resiko guna merumuskan dan mempertajam analisa terhadap bukti evaluasi dan temuan agar dapat merumuskan dan menyimpulkan opini dengan melakukan perbandingan dan penilaian terhadap tingkat resiko dan pengendalian yang ada.

Matriks penilaian resiko adalah suatu cara untuk menganalisa seberapa besar resiko yang ada dari suatu temuan audit. Hal ini dilakukan dengan cara menganalisa resiko yang ada (*inherent risk*) dan resiko setelah adanya pengendalian (*residual risk*) Griffiths (2007, p18)

2.4.6.1 Matrik Penilaian Resiko

Menurut Griffiths (2007, p20) matrik penilaian resiko adalah metode analisis dengan menghitung aspek tingkat resiko (dampak) dan tingkat terjadinya resiko tersebut, dengan nilai L (*low*) = -1, M (*Medium*) = -2, dan H (*High*) = -3.

Teknik perhitungan dalam matrik penilaian resiko menggunakan fungsi perkalian antara dampak dengan nilai terjadinya. Kriteria penilaian dalam matrik pengendalian terdiri dari :

1. Resiko kecil (*low)* nilainya berkisar antara -1 dan -2, seperti :
    a. Jika dampak *low* (-1) dan terjadinya *low* (-1), maka nilai resiko adalah -1. Artinya, nilai resiko dari dampak dan terjadinya adalah kecil.
    b. Jika dampak *low* (-1) dan terjadinya *medium* (-2), maka nilai resiko adalah -2. Artinya, nilai resiko dari dampak dan terjadinya adalah kecil.
    c. Jika dampak *medium* (-2) dan terjadinya *low* (-1), maka nilai resiko adalah -2. Artinya, nilai resiko dari dampak dan terjadinya adalah kecil.
2. Resiko sedang (*medium*) nilainya berkisar antara -3 dan -4, seperti:
    a. Jika dampak *low* (-1) dan terjadinya *high* (-3), maka nilai resiko adalah -3. Artinya, nilai resiko dari dampak dan terjadinya adalah sedang.
    b. Jika dampak *medium* (-2) dan terjadinya *medium* (-2), maka nilai resiko adalah -4. Artinya, nilai resiko dari dampak dan terjadinya adalah sedang.
    c. Jika dampak *high* (-3) dan terjadinya *low* (-1), maka nilai resiko adalah -3. Artinya, nilai resiko dari dampak dan terjadinya adalah sedang.
3. Resiko tinggi (*high*) nilainya berkisar antara -6 dan -9, seperti:
    a. Jika dampak *medium* (-2) dan terjadinya *high* (-3), maka nilai resiko adalah -6. Artinya, nilai resiko dari dampak dan terjadinya adalah tinggi.

b. Jika dampak *high* (-3) dan terjadinya *medium* (-2), maka nilai resiko adalah -6. Artinya, nilai resiko dari dampak dan terjadinya adalah tinggi.
c. Jika dampak *high* (-3) dan terjadinya *high* (-3), maka nilai resiko adalah -9. Artinya, nilai resiko dari dampak dan terjadinya adalah tinggi.

2.4.6.2 Matrik Penilaian Pengendalian

Menurut Griffiths (2007, p23) matrik Penilaian Pengendalian adalah metode analisis desain (rancangan) dan tingkat efektifitas pengendalian intern. Biasanya tingkat efektifitas dan desain (rancangan) dinyatakan dengan nilai L (*low*) = 1, M (*Medium*) = 2, dan H (*High*) = 3.

Teknik perhitungan dalam matrik penilaian pengendalian menggunakan fungsi perkalian antara efektifitas dengan desain (rancangan). Kriteria penilaian dalam matrik pengendalian terdiri dari:

1. Pengendalian kecil (*low)* nilainya berkisar antara 1 dan 2, seperti:
    a. Jika efektifitasnya *low* (1) dan terjadinya *low* (1), maka nilai pengendaliannya adalah 1. Artinya, nilai pengendalian dari efektifitas dan desain adalah kecil.
    b. Jika efektifitasnya *low* (1) dan terjadinya *medium* (2), maka nilai pengendaliannya adalah 2. Artinya, nilai pengendalian dari efektifitas dan desain adalah kecil.
    c. Jika dampak *medium* (2) dan terjadinya *low* (1), maka nilai pengendaliannya adalah 2. Artinya, nilai pengendalian dari efektifitas dan desain adalah kecil.
2. Pengendalian sedang (*medium*) nilainya berkisar antara -3 dan -4, seperti:

a. Jika efektifitasnya *low* (1) dan terjadinya *high* (3), maka nilai pengendaliannya adalah 3. Artinya, nilai pengendalian dari efektifitas dan desain adalah sedang.
b. Jika efektifitasnya *medium* (2) dan terjadinya *medium* (2), maka nilai pengendaliannya adalah 4. Artinya, nilai pengendalian dari efektifitas dan desain adalah sedang.
c. Jika efektifitasnya *high* (3) dan terjadinya *low* (1), maka nilai pengendaliannya adalah 3. Artinya, nilai pengendalian dari efektifitas dan desain adalah sedang.

3. Pengendalian tinggi (*high*) nilainya berkisar antara 6 dan 9, seperti:
   a. Jika efektifitasnya *medium* (2) dan terjadinya *high* (3), maka nilai pengendaliannya adalah 6. Artinya, nilai pengendalian dari efektifitas dan desain adalah tinggi.
   b. Jika efektifitasnya *high* (3) dan terjadinya *medium* (2), maka nilai pengendaliannya adalah 6. Artinya, nilai pengendalian dari efektifitas dan desain adalah tinggi.
   c. Jika efektifitasnya *high* (3) dan terjadinya *high* (3), maka nilai pengendaliannya adalah 9. Artinya, nilai pengendalian dari efektifitas dan desain adalah tinggi.

Penetapan tingkat efektifitas antara resiko dan pengendalian adalah sebagai berikut :

1. Jika jumlah penilaian resiko dan pengendaliannya adalah 0, maka tingkat pengendalian dan resiko adalah standar. Artinya setiap resiko yang terjadi dapat ditanggulangi oleh pengendalian yang ada.

2. Jika jumlah penilaian resiko dan pengendaliannya adalah positif, maka tingkat pengendalian dan resiko adalah baik. Tapi jika nilai pengendaliannya terlalu tinggi dibanding dengan resiko, maka kemungkinan akan terjadi kelebihan pengendalian (*overcontrol*) yang menyebabkan terjadinya pemborosan dalam operasional.
3. Jika jumlah penilaian resiko dan pengendaliannya adalah negatif, maka tingkat pengendalian dan resiko adalah buruk. Sehingga perlu dilakukan pengingkatan terhadap pengendalian karena resiko yang dihadapi besar.