BAB 2

LANDASAN TEORI

2.1 Sistem Informasi Akuntansi

2.1.1 Pengertian Sistem Informasi Akuntansi

Menurut Bodnar dan Hopwood (2001, p1) Sistem Informasi Akuntansi adalah kumpulan dari sumber daya, seperti manusia dan peralatan yang diatur untuk mengubah data keuangan dan data lainnya menjadi informasi.

Menurut Romney dan Steinbart (2003,p691), Sistem Informasi Akuntansi adalah manusia dan sumber daya di dalam sebuah organisasi yang bertanggung jawab untuk mempersiapkan informasi keuangan dan informasi yang diperoleh dengan mengumpulkan dan memproses transaksi-transaksi perusahaan.

Menurut Jones dan Rama (2003, p4), Sistem Informasi Akuntansi merupakan kumpulan kegiatan yang mendukung aktifitas sistem informasi manajemen, dimana sistem informasi manajemen merupakan sistem yang menangkap data organisasi, menyimpan dan memelihara data tersebut dan menyediakan informasi yang bermanfaat untuk fungsi produksi, pemasaran, sumber daya manusia, akuntansi dan keuangan.

Dari penjelasan tersebut dapat disimpulkan bahwa Sistem Informasi Akuntansi merupakan proses pengolahan data yang kemudian digunakan untuk membuat laporan keuangan untuk fungsi-fungsi yang ada dalam organisasi.

2.1.2 Tujuan atau Kegunaan SIA

Menurut Jones dan Rama (2003, p6-7), Sistem Informasi Akuntansi dalam perusahaan antara lain :

1. Menghasilkan laporan keuangan

   Sistem Informasi Akuntansi yang digunakan untuk menghasilkan laporan khusus untuk memenuhi kebutuhan informasi bagi pihak *investors, creditors,* dan *Tax Collectors, Regulatory Agencies* dan pihak lainnya.

2. Mendukung aktifitas rutin

   Manajer membutuhkan Sistem Informasi Akuntansi untuk menangani aktivitas operasi rutin selama berlangsungnya akivitas operasi perusahaan.

3. Mendukung pengambilan keputusan

   Informasi juga dibutuhkan untuk pengambilan keputusan yang tidak rutin pada semua level yang ada di organisasi.

4. Perencanaan dan pengendalian

   Sistem informasi dibutuhkan untuk perencanaan dan pengendalian aktivitas. Pemusatan informasi pada anggaran dan standar biaya disimpan pada sistem informasi, dan laporan dibuat untuk membandingkan anggaran yang dibuat dengan jumlah yang sebenarnya terjadi.

5. Implementasi Pengendalian Internal

   Pengendalian internal meliputi kebijakan, prosedur, dan sistem informasi yang digunakan untuk melindungi aset perusahaan dari kerugian, pencurian, dan menjaga keakuratan data keuangan. Sehingga dapat membangun pengendalian kedalam sistem informasi akuntansi yang terkomputerisasi untuk membantu pencapaian tujuan organisasi.

2.2 Sistem Informasi Penjualan

2.2.1 Pengertian Sistem Informasi Penjualan

Penjualan merupakan faktor penting dalam kemajuan dan perkembangan perusahaan, karena dari penjualan diperoleh pendapatan untuk membiayai kelangsungan perusahaan, terlebih dalam menghasilkan keuntungan. Oleh karena itu, wajar jika perusahaan mempertimbangkan pentingnya peranan pengendalian intern atas transaksi penjualan yang berkaitan dengan fungsi-fungsi lainnya dalam perusahaan.

Berdasarkan penjelasan di atas, maka dapat disimpulkan bahwa sistem informasi penjualan adalah sistem yang mengalirkan barang dan jasa ke konsumen dengan struktur interaksi yang disusun untuk mencapai tujuan tertentu yang berhubungan dengan kegiatan penjualan.

Menurut Mulyadi (2001, p.202), kegiatan penjualan barang dan jasa dapat dibedakan menjadi 2 jenis yaitu :

- Sistem Penjualan Tunai

  Penjualan secara tunai dilakukan perusahaan dengan cara mewajibkan pembeli melakukan pembayaran terlebih dahulu sebelum barang diserahkan. Setelah uang diterima oleh perusahaan, barang kemudian diserahkan kepada pembeli.

- Sistem penjualan kredit

  Penjualan secara kredit dilaksanakan dengan cara mengirimkan barang dahulu kepada pembeli berdasarkan pesanan, dengan pembayaran ditagih dalam jangka waktu tertentu.

Kegiatan penjualan terdiri dari transaksi penjualan barang atau jasa, baik secara kredit maupun secara tunai, oleh karena itu dibawah ini akan dijabarkan mengenai sistem penjualan tunai.

2.2.2 Sistem Penjualan Tunai

2.2.2.1 Fungsi-fungsi Yang Terkait Dalam Penjualan Tunai

Menurut Mulyadi (2001, p.462), Fungsi-fungsi Yang Terkait Dalam Penjualan Tunai adalah sebagai berikut :

- Fungsi Penjualan

  Fungsi ini bertanggung jawab untuk menerima order dari pembeli, mengisi faktur penjualan tunai, dan menyerahkan faktur tersebut kepada pembeli untuk kepentingan pembayaran barang ke fungsi kas.

- Fungsi Kas

  Fungsi ini bertanggung jawab sebagai penerima kas dari pembeli.

- Fungsi Gudang

  Fungsi ini bertanggung jawab untuk menyiapkan barang yang dipesan oleh pembeli, serta menyerahkan barang tersebut ke fungsi pengiriman.

- Fungsi Pengiriman

  Fungsi ini bertanggung jawab untuk membungkus barang dan menyerahkan barang yang telah dibayar harganya kepada pembeli.

- Fungsi Akuntansi

  Fungsi ini bertanggung jawab sebagai pencatat transaksi penjualan dan penerimaan kas dan membuat laporan penjualan.

2.2.2.2 Prosedur Sistem Penjualan Tunai

Menurut Mulyadi (2001, p.469), jaringan prosedur yang membentuk sistem penjualan tunai adalah sebagai berikut :

- **Prosedur *order* penjualan.**

  Dalam prosedur ini, fungsi penjualan menerima *order* dari pembeli dan menambahkan informasi penting pada surat *order* dari pembeli. Fungsi penjualan kemudian membuat surat *order* pengiriman dan mengirimkannya kepada berbagai fungsi yang lain untuk memungkinkan fungsi tersebut memberikan kontribusi dalam melayani *order* dari pembeli.

- **Prosedur penerimaan kas.**

  Dalam prosedur ini fungsi kas menerima pembayaran harga barang dari pembeli dan memberikan tanda pembayaran (berupa pita register kas dan "cap lunas”pada faktur penjualan tunai) kepada pembeli untuk memungkinkan pembeli tersebut melakukan pengambilan barang yang dibelinya dari fungsi pengiriman.

- **Prosedur penyerahan barang.**

  Dalam prosedur ini fungsi pengiriman menyerahkan barang kepada pembeli.

- **Prosedur pencatatan penjualan tunai.**

  Dalam prosedur ini fungsi akuntansi melakukan pencatatan transaksi penjualan tunai dalam jurnal penjualan dan jurnal penerimaan kas. Disamping itu fungsi akuntansi juga mencatat berkurangnya persediaan barang yang dijual dalam kartu persediaan.

- **Prosedur penyetoran kas ke bank.**

  Sistem pengendalian *intern* terhadap kas mengharuskan penyetoran dengan segera ke bank semua kas yang diterima pada suatu hari. Dalam prosedur ini fungsi kas menyetorkan kas yang diterima dari penjualan tunai ke bank dalam jumlah penuh.

- **Prosedur pencatatan penerimaan kas.**

  Dalam prosedur ini, fungsi akuntansi mencatat penerimaan kas ke dalam jurnal penerimaan kas berdasar bukti setor bank yang diterima dari bank melalui fungsi kas.

- **Prosedur pencatatan harga pokok penjualan.**

  Dalam prosedur ini, fungsi akuntansi membuat rekapitulasi harga pokok penjualan berdasarkan data yang dicatat dalam kartu persediaan. Berdasarkan rekapitulasi harga pokok penjualan ini, fungsi akuntansi membuat bukti memorial sebagai dokumen sumber untuk pencatatan harga pokok penjualan ke dalam jurnal umum.

2.2.2.3 Dokumen Penjualan

Menurut Mulyadi (2001, p214), dokumen yang digunakan dalam penjualan, meliputi :

1. Surat *Order* Pengiriman dan Tembusannya

   Surat *order* pengiriman yang memberikan otorisasi kepada fungsi pengiriman untuk mengirimkan jenis barang dan jumlah barang yang tertera dalam dokumen.

2. Faktur dan tembusannya

   Faktur penjualan diserahkan kepada pelanggan serta tanda bukti bahwa barang telah diterima pelanggan dan perusahaan menggunakannya untuk menagih pada pelanggan dan dipakai sebagai dasar pencatatan timbulnya piutang.

3. Rekapitulasi Harga Pokok Penjualan

   Dokumen yang digunakan untuk menghitung total HPP (Harga Pokok Penjualan) yang dijual selama periode tertentu.

4. Bukti Memorial

   Dokumen sumber untuk dasar pencatatan ke dalam jurnal umum. Pada penjualan kredit, bukti memorial ini merupakan dokumen sumber untuk mencatat HPP (Harga Pokok Penjualan) yang dijual dalam periode tertentu.

2.2.3 *e-Business*

2.2.3.1 Pengertian *e-Business*

Menurut Kalakota (1999, p4) e-business memiliki pengertian yaitu segala aktivitas pertukaran informasi di dalam transaksi bisnis yang memanfaatkan media elektronik yaitu meliputi transaksi penjualan dan pembelian, pelayanan kepada pelanggan, pemberian informasi produk, bekerja sama dengan rekan bisnis dan sebagainya.

2.2.3.2 Manfaat *e-Business*

Beberapa manfaat yang dapat diperoleh dari transaksi e-Business :

- Efisiensi waktu
- *Reduce cost* operasional dan pemasaran
- Melebarkan jangkauan (*global reach*)
- Meningkatkan pendapatan
- Dapat meningkatkan pangsa pasar
- Meningkatkan loyalitas pelanggan

2.3 Audit Sistem Informasi

2.3.1 Pengertian Audit Sistem Informasi

Menurut Arens dan Loebbecke (2003,p1), untuk melaksanakan audit, diperlukan informasi yang dapat diverifikasi dan sejumlah standar atau kriteria yang dapat digunakan sebagai penanganan pengevaluasian informasi tersebut. Supaya dapat diverifikasi, informasi harus dapat diukur.

Menurut Weber (1999,p10) Audit Sistem Informasi adalah proses pengumpulan dan pengevaluasian bukti-bukti untuk menentukan apakah sistem komputer dapat melindungi aktiva-aktiva, menjaga integritas data, mencapai tujuan organisasi secara efektif, dan menggunakan sumber daya secara efisien.

Dapat disimpulkan bahwa pengertian Audit Sistem Informasi adalah proses pengumpulan dan pengevaluasian bukti oleh orang yang kompeten dan independen untuk menetapkan apakah sistem yang dijalankan sesuai dengan kriteria yang telah ditetapkan.

2.3.2 Tahap Audit Sistem Informasi

Menurut Weber (1999, p47), audit terdiri dari lima tahap yaitu :

1. *Planning the audit*

   Selama tahap awal ini, auditor harus memutuskan *level* materiil permulaan yang akan diaudit. Auditor juga harus membuat keputusan akan resiko yang diinginkan. *Level* dari sifat resiko akan bervariasi dalam setiap bagian dari audit.

2. *Test of control*

   Tahap berfokus pada kontrol manajemen. Jika *testing* menunjukkan bahwa kontrol manajemen tidak beroperasi sebagaimana mestinya, baru setelah itu dilanjutkan dengan *testing control* aplikasi

3. *Test of Transaction*

   Auditor menggunakan *test of transaction* untuk mengevaluasi apakah kesalahan atau proyek yang tidak sesuai dengan ketentuan telah mengarah kepada kesalahan material dari informasi keuangan. Biasanya *test of*

transaction meliputi jurnal masukan sampai dokumen sumber, pemeriksaan daftar harga dan pengujian keakuratan penghitungan.

4. *Test of Balance or Overall Result*

   Auditor melakukan *test of balance or overall* untuk mendapatkan bukti yang cukup untuk membuat dan menyampaikan keputusan akhir dari kehilangan atau kesalahan pernyataan laporan yang muncul ketika fungsi sistem informasi gagal untuk menjaga asset-aset, menjaga integritas data, mencapai keefisienan dan keefektifan.

5. *Completion of the Audit*

   Pada tahap akhir, auditor harus merumuskan sebuah opini tentang adanya kehilangan material dan kesalahan pernyataan laporan yang muncul dan membuat sebuah laporan yang muncul.

Standar opini yang berlaku di beberapa negara terdiri dari empat jenis opini yaitu

a. *Disclaimer of opinion*

   Setelah selesai melakukan audit, auditor tidak dapat memberikan sebuah opini.

b. *Adverse Opinion*

   Auditor menyimpulkan bahwa kehilangan material telah muncul atau laporan keuangan telah dinyatakan salah secara materiil.

c. *Qualified Opinion*

   Auditor menyimpulkan bahwa kehilangan telah muncul atau kesalahan laporan secara material telah ada tapi tidak besar atau material.

d. *Unqualified Opinion*

Auditor percaya bahwa tidak ada kehilangan material atau laporan yang salah.

2.3.3 Metode Audit Sistem Informasi

Ada 3 metode Audit Sistem Informasi yang dapat dilakukan oleh auditor, sebagai berikut :

1. *Audit Around the Computer*

Weber (1999, p.56) berpendapat bahwa *Audit Around the Computer* merupakan audit terhadap suatu penyelenggaraan sistem informasi yang berbasis komputer, tanpa menggunakan kemampuan peralatan komputer itu sendiri.

Metode ini merupakan suatu pendekatan dengan memberlakukan komputer sebagai *black box*, maksudnya metode ini tidak menguji langkah-langkah proses secara langsung tetapi hanya berfokus pada masukan dan keluaran dari sistem komputer.

Biasanya *Audit Around the Computer* merupakan pendekatan yang lebih sederhana untuk melakukan proses audit sistem informasi dan dilakukan oleh auditor yang memiliki pengetahuan yang minim terhadap komputer.

Kelemahan dari metode *Audit Around the Computer* adalah :

a. Database biasanya dalam jumlah data yang banyak dan sulit untuk dilacak secara manual.
b. Auditor tidak akan memahami operasional dalam sistem komputer.

c. Adanya pengabaian pada sistem pengolahan komputer sehingga sangat rawan adanya kesalahan potensial di dalam sistem.
d. Kemampuan komputer sebagai fasilitas penunjang pelaksanaan audit menjadi tidak ada.
e. Tidak menyelesaikan maksud dan tujuan proses audit secarara keseluruhan.

Keuntungan dari metode *Audit Around the Computer* adalah :

a. Tidak ada resiko terhadap kemungkinan hancurnya data sesungguhnya.
b. Auditor hanya sedikit memerlukan tambahan pendidikan.
c. Umumnya mudah, sederhana dan dimengerti oleh semua orang.
d. Biaya yang terkait dengan pelaksanaannya kecil.

2. *Audit Through the Computer*

Menurut Weber (1999, p57) pada umumnya para auditor sekarang ini terlibat dengan *Audit Through the Computer*, di mana auditor menggunakan komputer untuk menguji : (1) logika proses dan pengendalian yang ada saat ini pada sistem, (2) prosuksi *record* oleh sistem.

Metode ini merupakan suatu pendekatan yang berorientasi pada komputer dengan membuka *black box* dan secara langsung berfokus pada operasi pemrosesan dalam sistem komputer. Dengan asumsi bahwa apabila sistem pemrosesan mempunyai pengendalian yang memadai, maka kesalahan dan penyalahgunaan tidak akan terlewat untuk dideteksi. Sebagai akibatnya keluaran tidak dapat diterima.

Tujuan dari *Audit Through the Computer* adalah untuk meneliti apakah aplikasi yang diaplikasikan sesuai dengan kondisi yang sesungguhnya. *Audit Through the Computer* dapat juga dilakukan untuk meneliti kelengkapan dan kebenaran akurasi dan validasi *database* atau penelitian *sofware* datanya.

Keuntungan dari pendekatan ini adalah dapat meningkatkan kekuatan terhadap pengujian sistem aplikasi secara efektif, dimana ruang lingkup dan kemampuan pengujian yang dilakukan dapat diperluas sehingga tingkat kepercayaan terhadap kehandalan dari pengumpulan dan evaluasi dapat ditingkatkan, selain itu dengan memeriksa secara langsung logika pemrosesan dari sistem aplikasi dan diperkirakan kemampuan sistem dapat menangani perubahan dan kemungkinan kehilangan yang terjadi pada masa yang akan datang.

Kelemahan dari audit ini yaitu :

a. Biaya yang dibutuhkan relatif tinggi yang disebabkan jumlah jam kerja yang banyak untuk lebih memahami struktur pengendalian *intern* dari pelaksanaan sistem aplikasi.
b. Butuh keahlian teknik yang lebih mendalam untuk memahami cara kerja sistem.

3. *Audit With the Computer*

Menurut Gondodiyoto (2003, p155), *Audit With the Computer* merupakan suatu pendekatan audit dengan bantuan komputer, dimana prosedur auditnya dapat dilaksanakan dengan beberapa cara yaitu:

a. Memproses atau melakukan pengujian dengan sistem komputer klien itu sendiri sebagai bagian dari pengujian pengendalian atau subtantif.
b. Menggunakan komputer untuk melaksanakan tugas audit yang terpisah dari catatan klien, yaitu mengambil *copy* data, *file* atau program milik klien untuk diuji dengan komputer lain (di kantor auditor).
c. Menggunakan komputer sebagai alat bantu dalam audit, menyangkut :
    1. Pengujian program, *file* atau data yang dipergunakan dan dimiliki oleh perusahaan, (sebagai *software* bantu audit).
    2. Menggunakan komputer untuk dukungan kegiatan audit, misalnya untuk administrasi dan surat menyurat, pembuatan tabel atau jadwal, untuk sampling dan berbagai kegiatan *office automation* lainnya.

Metode ini merupakan suatu pendekatan audit dengan menggunakan komputer dan *software* untuk mengotomastisasi prosedur pelaksanaan audit.

2.4 Sistem Pengendalian *Intern*

2.4.1 Pengertian Pengendalian *Intern*

Sistem Pengendalian *Intern* yang terdiri dari kebijakan-kebijakan dan prosedur-prosedur, sangat dibutuhkan oleh suatu perusahaan guna menunjang kegiatan operasinya, salah satu alasan perusahaan menyususun Sistem Pengendalian Internal adalah dalam rangka membantu mencapai sasaran yang diharapkan oleh perusahaan.

Ada beberapa pengertian yang mencoba menjelaskan mengenai Sistem Pengendalian *Intern*. Menurut Weber (1999.p35), pengendalian *intern* 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. Dengan demikian, tujuan dari pengendalian adalah untuk mengurangi resiko atau mengurangi pengaruh yang sifatnya merugikan akibat suatu kejadian (penyebab). Berdasarkan pengertian diatas maka pengendalian dikelompokkan menjadi tiga bagian:

1. *Preventive Control*

   Pengendalian ini digunakan untuk mencegah masalah sebelum masalah itu muncul.

2. *Detective Control*

   Pengendalian ini digunakan untuk menemukan masalah yang berhubungan dengan pengendalian segera setelah masalah itu muncul.

3. *Corrective Control*

   Pengendalian ini digunakan untuk memperbaiki masalah yang ditemukan pada pengendalian *detective*. Pengendalian ini mencakup prosedur untuk menentukan penyebab masalah yang timbul, memperbaiki kesalahan atau kesulitan yang timbul, memodifikasi sistem proses. Dengan demikian dapat mencegah kejadian yang sama di masa yang akan datang.

Menurut Muchtar (1999, p41-42), Pengendalian *Intern* merupakan merupakan perencanaan organisasi guna mengkoordinasi metode atau cara pengendalian dalam suatu perusahaan untuk menjaga aset perusahaan guna meningkatkan tingkat kepercayaan dan akurasi data, serta menjalankan operasional perusahaan secara efisien.

Menurut Mulyadi (2001,p613), Pengendalian *Intern* meliputi struktur organisasi, mengecek ketelitian, dan keandalan data akuntansi, mendorong efisiensi dan mendorong dipatuhinya kebijakan manajemen. Definisi sistem pengendalian *intern* tersebut menekankan tujuan yang hendak dicapai, dan bukan pada unsur-unsur yang membentuk sistem tersebut.

Dari beberapa definisi di atas dapat ditarik kesimpulan bahwa Pengendalian *Intern* adalah suatu kebijakan dan prosedur yang terstruktur di dalam suatu perusahaan dengan tujuan untuk menjaga kekayaan perusahaan, memeriksa keandalan, dan ketelitian data akuntansi, serta mendorong efektivitas dan efisiensi operasi.

2.4.2 Tujuan Pengendalian *Intern*

Menurut Mulyadi (2001,p163) mengungkapkan empat tujuan sistem Pengendalian *Intern*, yaitu untuk :

a. Menjaga kekayaan organisasi
b. Mengecek ketelitian dan kehandalan data akuntansi
c. Meningkatkan efisiensi usaha
d. Mendorong dipatuhinya kebijakan manajemen.

Sedangkan menurut Gondodiyoto (2003,p75), Sistem Pengawasan *Intern* dijalankan bertujuan untuk :

a. Mengamankan aset organisasi
b. Memperoleh informasi yang akurat dan dapat dipercaya

c. Meningkatkan efektifitas dan efisiensi kegiatan

d. Mendorong kepatuhan pelaksanaan terhadap kebijakan organisasi.

Tujuan dari pengendalian intern adalah untuk mengurangi resiko atau mengurangi pengaruh yang sifatnya merugikan akibat suatu kejadian.

2.4.3 Komponen Pengendalian *Intern*

Menurut Weber (1999, p49), Pengendalian *Intern* terdiri dari lima komponen yang saling terintegrasi antara lain :

1. *Control Environment*

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

2. *Risk Assessment*

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

3. *Control Activities*

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

4. *Information and Communication*

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

5. *Monitoring*

   Komponen yang memastikan pengendalian internal beroperasi secara dinamis.

2.4.4. Karakteristik Sistem Pengendalian *Intern*

Menurut pendapat Hartadi (1999,p14-21), karakteristik sistem pengendalian *intern*, yang dapat dipercaya adalah sebagai berikut:

1. Kualitas karyawan sesuai dengan tanggung jawabnya.

   Faktor yang paling sulit dan paling penting dalam pengendalian adalah orang-orang yang dapat menunjang suatu sistem dapat berjalan baik.

   a. Penarikan tenaga kerja

      Manajemen harus mengusahakan seluas mungkin sumber tenaga kerja sehingga akan lebih besar kemungkinannya mendapat calon tenaga kerja yang di kehendaki.

   b. Pengembangan mutu karyawan

      Menyangkut usaha-usaha meningkatkan pengetahuan karyawan dan keahlian atau keterampilannya.

   c. Pengukuran prestasi

      Di maksud untuk menilai pelaksanaan tugas-tugas yang menjadi tanggung jawab masing-masing karyawan.

2. Rencana organisasi yang memisahkan tanggung jawab fungsi secara layak.

   Tujuan adanya pemisahan tanggung jawab adalah tidak ada seorang pun yang harus mengendalikan dua atau tiga tanggung jawab fungsi.

Keuntunganya antara lain:

- Sulit untuk berbuat kecurangan.
- Akan terselengaranya suatu transaksi dikerjakan secara efisien.
- Terhindar dari kesalahan karena adanya saling cek (*cross-check*).

3. Sistem pemberian wewenang, tujuan, tehnik dan pengawasan yang wajar untuk mengadakan pengendalian atas aktiva, utang, penghasilan dan biaya.

   Dalam organisasi setiap transaksi hanya terjadi atas dasar otorisasi dari jabatan yang memiliki wewenang untuk menyetujui terjadinya transaksi tersebut. Oleh karena itu dalam organisasi harus dibuat sistem yang mengatur pembagian wewenang untuk otorisasi atas terlaksananya setiap transaksi. Fomulir merupakan salah satu media yang digunakan untuk merekam penggunaan wewenang untuk memberikan otorisasi terlaksananya transaksi dalam organisasi. Dengan adanya sistem otorisasi tersebut akan menjamin dihasilkannya dokumen pembukuan yang dapat dipercaya, sehingga akan menjadi masukan yang dapat dipercaya bagi proses akuntansi.

4. Pengendalian terhadap penggunaan aktiva dan dokumentasi serta formulir.

   Pengendalian fisik atas aktiva, catatan dan dokumen lainnya harus dibatasi kepada orang-orang tertentu saja yang diberikan wewenang. Hal ini bertujuan untuk menghindari dari kesalahan dan ketidakberesan dari orang-orang yang tidak bertanggung jawab.

5. Perbandingan catatan-catatan aktiva dan utang dengan yang seharusnya ada dan mengadakan tindakan koreksi bila ada perbedaan

   Manajemen harus mengadakan perbandingan secara periodik dengan bukti yang bebas tentang adanya penilaian bahwa transaksi telah dicatat.

2.5 Sistem Pengendalian *Intern* Pada Sistem Berbasis Komputer

Menurut Weber (1999, p38), sebagaimana dikutip oleh Gondodiyoto (2003, p126-127), struktur pengendalian *intern* yang perlu dilakukan pada sistem berbasis komputer adalah sebagai berikut :

1. Pengendalian Umum
2. Pengendalian Aplikasi

2.5.1 Pengendalian Umum

Pengendalian yang berlaku umum, artinya ketentuan-ketentuan yang berlaku dalam pengendalian tersebut, berlaku untuk seluruh kegiatan komputerisasi di dalam pengendalian tersebut. Apabila tidak dilakukan pengendalian ini ataupun pengendaliannya lemah maka berakibat negatif terhadap pengendalian aplikasi.

Pengendalian umum terdiri dari:

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

   Mengendalikan peranan manajemen dalam perencanaan kepemimpinan dan pengawasan fungsi sistem.

2. 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.

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

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

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

   Mengendalikan peranan dan fungsi dari data administrator atau *database* administrator.

5. Pengendalian Manajemen Jaminan Kualtitas *(Quality Assurance Management Control)*

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

6. 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 adalah :

   a. Ancaman kebakaran

      Beberapa pelaksanaan pengamanan untuk ancaman kebakaran :

      - Memiliki *alarm* kebakaran otomatis yang diletakkan pada tempat di mana aset-aset sistem informasi berada.
      - Memiliki tabung kebakaran yang diletakkan pada lokasi yang mudah diambil.
      - Memiliki tombol utama (temasuk *AC*) .
      - Gedung tempat penyimpanan aset informasi dibangun dari bahan tahan api.
      - Memiliki pintu / tangga darurat yang diberi tanda dengan jelas sehingga karyawan mudah menggunakannya.
      - Ketika *alarm* berbunyi, signal langsung dikirim ke stasiun pengendalian yang selalu dijaga oleh staf.
      - Prosedur pemeliharaan gudang yang baik menjamin tingkat polusi sesuatunya telah dirawat dengan baik.

   b. Ancaman banjir

      Beberapa pelaksanaan pengamanan untuk ancaman banjir :

      - Usahakan bahan untuk atap, dinding dan lantai yang tahan air.

- Menyediakan *alarm* pada titik strategis dimana material aset sistem informasi dilakukan.
- Semua material aset sistem informasi diletakkan di tempat yang tinggi.
- Menutup peralatan *hardware* dengan bahan yang tahan air sewaktu tidak digunakan.

c. Perubahan tenaga sumber energi

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

d. 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.

e. Polusi

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

f. Penyusup

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

g. *Virus*

Pelaksanaan pengamanan untuk mengantisipasi *virus* meliputi tindakan :

- *Preventive*, seperti meng*install antivirus* dan meng*update* secara rutin, melakukan *scan* file yang digunakan.
- *Detective*, seperti melakukan *scan* secara rutin.
- *Corrective*, seperti memastikan *back up* data bebas *virus*, pemakaian anti *virus* terhadap *file* yang terinfeksi.

h. *Hacking*

Beberapa pelaksanaan pengamanan untuk mengantisipasi *hacking* :

- Penggunaan kontrol *logical* seperti penggunaan *password* yang sulit untuk ditebak.
- Petugas keamanan secara teratur memonitor sistem yang digunakan.

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

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

a. Pengoperasian komputer (*Computer Operations*)

Tipe pengendalian yang harus dilakukan :

- Menentukan fungsi-fungsi yang harus dilakukan operator komputer maupun fasilitas operasi otomatis.
- Menentukan penjadwalan kerja pada pemakaian *hardware* atau *software*

- Menentukan perawatan terhadap *hardware* agar dapat berjalan baik.
- Pengendalian perangkat keras berupa *hardware controls* dari produsen untuk deteksi *hardware malfunction.*

b. Pengoperasian Jaringan (*Network Operations*)

Pengendalian yang dilakukan ialah memonitor dan memelihara jaringan dan pencegahan terhadap akses oleh pihak yang tidak berwenang. Pengendalian sistem komunikasi data antara lain jalur komunikasi, *Hardware, Cryptology, Software.*

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

Fasilitas-fasilitas yang ada harus dirancang untuk memiliki kecepatan dan keakuratan data serta telah dilakukan terhadap peng*entri*an data.

d. Pengendalian produksi (*Production Control*)

Fungsi yang harus dilakukan untuk pengendalian produksi adalah :

- Penerimaan dan pengiriman *input dan output.*
- Penjadwalan kerja
- Manajemen pelayanan.
- Peningkatan pemanfaatan komputer.

e. *File Library*

Fungsi yang harus dilakukan untuk *file library* adalah :

- Penyimpanan media penyimpanan (*storage of storage media*)
- Penggunaan media penyimpanan (*use of storage media*)

- Pemeliharaan dan penempatan media penyimpanan (*maintenance and disposal of storage media*)
- Lokasi media penyimpanan (*location of storage media*)

f. *Documentation and Program Library*

Orang yang bertanggung jawab atas dokumentasi mempunyai beberapa fungsi yang harus dilakukan yaitu :

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

g. *Help Desk* / *Technical Support*

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

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

h. *Capacity Planning and Performance Monitoring*

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

i. *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 memfokuskan pada fungsi inti bisnis mereka.

2.5.2 Pengendalian Aplikasi

2.5.2.1 Pengendalian *Boundary (Boundary Control)*

Pengendalian *Boundary* menentukan hubungan antara pemakai komputer dengan sistem komputer itu sendiri, ketika pemakai menggunakan komputer maka fungsi *boundary* berjalan.

a. Pengendalian Kriptografi (*Cryptographic Control*)

Pengendalian Kriptografi dirancang untuk mengamankan data pribadi dan untuk menjaga modifikasi data oleh orang yang tidak berwenang, cara ini dilakukan dengan mengacak data sehingga tidak memiliki arti bagi orang yang tidak dapat menguraikan data tersebut.

b. Pengendalian Akses (*Access Control*)

Pengendalian Akses berfungsi untuk membatasi penggunaan sumber daya sistem komputer, membatasi dan memastikan *user* untuk mendapatkan sumber daya yang mereka butuhkan.

Menurut Weber (1999, p380-383), mekanisme pengendalian akses terdiri dari :

1. Identifikasi dan Otentifikasi (*Identification and Authentication*)

   User mengidentifikasi dirinya pada mekanisme pengendalian akses dengan memberi informasi seperti nama atau nomor rekening. Informasi tersebut memungkinkan mekanisme untuk menentukan bahwa data yang masuk sesuai dengan informasi pada *file* otentifikasi. Terdapat tiga bagian yang dapat diisi oleh *user* untuk informasi otentifikasi yaitu :

   a. Informasi yang mudah diingat, contohnya : nama, tanggal lahir, nomor *account, password*, PIN dan lain-lain.
   b. Objek yang berwujud yang dimiliki, contohnya : *Badge, plastic card*, kunci, cincin.
   c. Karakter pribadi, contohnya : sidik jari, ukuran tangan, suara, tanda tangan, pola retina mata.

2. Sumber Daya Objek

   Sumber Daya yang digunakan oleh *user* berdasarkan sistem informasi berbasis komputer dapat dibagi menjadi empat jenis yaitu :

   a. *Hardware*, contohnya : terminal, *printer*, prossesor, *disk*.
   b. *Software*, contohnya : program sistem aplikasi, *storage space*.
   c. Komoditi, contohnya : *Processor time, storage space*
   d. Data, contohnya : *files, groups, data item* (termasuk *images* dan *sound*).

3. Hak Istimewa (*Action Privileges*)

   Hak istimewa diberikan kepada *user* berdasarkan pada tingkatan kewenangan *user* dan jenis sumber daya yang diperlukan oleh *user*.

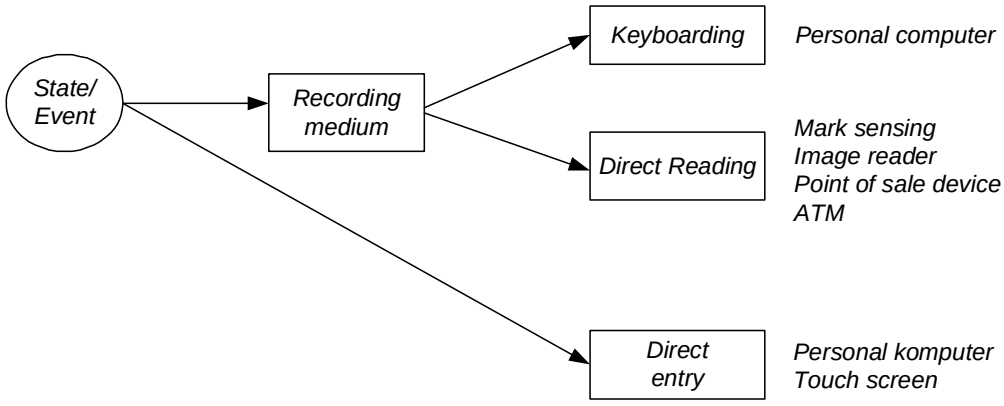
   Contoh hak istimewa ini adalah *user* hanya dapat melakukan akses berupa membaca tetapi tidak bisa mengubah atau menambah (dikenal dengan istilah *read only*), atau *user* hanya memiliki fasilitas menambah data tetapi tidak bisa mengubah atau menghapus data.

2.5.2.2 Pengendalian *Input* (*Input Control*)

Menurut Weber (1999,p420-450), komponen pada subsistem *input*, bertanggung jawab untuk memasukkan data dan intruksi pada sistem aplikasi, kedua jenis *input* tersebut harus divalidasi, setiap kesalahan data harus dapat diketahui dan dikontrol sehingga *input* yang dimasukkan akurat, lengkap, unik dan tepat waktu.

Komponen Pengendalian *Input* terdiri dari 8 komponen antara lain :

a. Metode Data *Input*



Gambar 2.1 Metode Data Input

Sumber : Weber (1999, p.421)

b. Perancangan Dokumen Sumber

Menurut sudut pandang pengendalian, perancangan dokumen sumber yang baik memiliki beberapa tujuan :

1. Mengurangi kemungkinan perekaman data yang *error*.
2. Meningkatkan kecepatan perekaman data.
3. Mengendalikan alur kerja.
4. Memfasilitasi pemasukan data ke sistem komputer.
5. Dapat meningkatkan kecepatan dan keakuratan pembacaan data.
6. Memfasilitasi pengecekan referensi berikutnya.

c. Perancangan Layar Data *Entry*

Jika data dimasukkan melalui monitor, maka diperlukan desain yang berkualitas pada layar tampilan data *entry* agar mengurangi kemungkinan terjadinya kesalahan dan supaya tercapai efisiensi dan efektivitas *entry* data pada subsistem *input*. Auditor harus dapat melakukan penilaian terhadap *layout* rancangan *input* pada komputer agar dapat membuat penilaian terhadap efektivitas dan efisiensi subsistem *input* ini.

d. Pengendalian Kode Data

Tujuan kode data yang unik yaitu untuk mengidentifikasikan entitas sebagai anggota dalam suatu grup atau set, dan lebih rapi dalam menyusun informasi yang dapat mempengaruhi tujuan integritas data,

keefektifan dan keefisienan. Ada lima jenis kesalahan dalam pengkodean data yaitu :

1. *Addition* (penambahan) : sebuah karakter ekstra ditambahkan pada kode, contoh 68573 dikode menjadi 685738.
2. *Transaction* (pemotongan) : sebuah karakter dihilangkan dari kode contoh 55871 dikode menjadi 5571.
3. *Transcription* (perekaman) : sebuah karakter yang salah direkam, contoh 17842 dikode menjadi 14842.
4. *Transposition* (perubahan) : karakter yang berdekatan pada kode dibalik, contoh 87942 dikode menjadi 78942.
5. *Double Transposition* : karakter dipisahkan oleh satu atau lebih karakter yang dibalik, contoh 97942 dikode menjadi 84972.

e. Cek *Digit*

Cek *digit* digunakan sebagai peralatan untuk mendeteksi kesalahan dalam banyak aplikasi, sebagai contoh : tiket pesawat, proses kartu kredit, proses rekening bank, proses pengumpulan *item* bank dan proses lisensi mengemudi.

f. Pengendalian *Batch*

Batching merupakan proses pengelompokan transaksi bersama-sama yang menghasilkan beberapa jenis hubungan antara yang satu dengan yang lainnya. Pengendalian yang bermacam-macam dapat

digunakan pada *batch* untuk mencegah atau mendeteksi *error* atau kesalahan.

g. Validasi *Input* Data

Jenis pengecekan validasi input data :

1. *Field Checks*

   Test validasi dapat diaplikasikan pada *field* yang tidak bergantung pada *field* lainnya dalam laporan *input.*

2. *Record Checks*

   Test validasi dapat diaplikasikan ke *field* berdasarkan hubungan timbal balik yang logis dari suatu *field* dengan *field* lainnya dalam laporan.

3. *Batch Checks*

   Test validasi memeriksa apakah karakteristik laporan *batch* yang dimasukkan sama dengan karakteristik *batch.*

4. *File Checks*

   Test validasi menguji apakah karakteristik penggunaan *file* selama pemasukan data sama dengan rumusan karakteristik *file*.

h. Instruksi *Input*

Dalam memasukkan instruksi ke dalam sistem aplikasi sering terjadi kesalahan karena adanya instruksi yang bermacam-macam dan kompleks. Karena itu perlu menampilkan pesan kesalahan. Pesan

kesalahan yang ditampilkan harus dikomunikasikan kepada *user* dengan lengkap dan jelas.

2.5.2.3 Pengendalian *Output* (*Output Control*)

Menurut Weber (1999, p615-646), subsistem *output* menyediakan fungsi-fungsi yang menentukan isi dari data yang akan disediakan bagi pengguna, cara dimana data dapat diformat dan dipersembahkan bagi pengguna, dan cara dimana data dapat diperbaiki dan dikeluarkan untuk pengguna.

Tipe pengendalian yang berhubungan dengan Pengendalian *Output*:

a. *Inference Control*

   Pengendalian model akses memperbolehkan atau menolak akses terhadap *item* data berdasarkan nama dari data *item*, isi dari data *item* atau beberapa karakteristik dari serangkaian data yang terdapat pada data *item.*

b. *Batch Output and Distribution Control*

   Batch output adalah *output* yang dihasilkan pada beberapa fasilitas operasional dan setelah itu dikirim atau disimpan oleh pemakai *output* tersebut. *Output* ini menggunakan banyak formulir, contohnya, keluaran laporan pengendalian manajemen berisi tabel, grafik atau *image*. Pengendalian terhadap *batch output* dilakukan dengan tujuan untuk memastikan bahwa laporan tersebut akurat, lengkap dan tepat waktu yang hanya dikirim atau diserahkan kepada pemakai yang berhak

c. *Batch Report Design Controls*

Elemen penting untuk melihat pengendalian efektivitas pelaksanaan terhadap produksi, distribusi, laporan keluaran *batch* adalah dengan melihat kualitas dari desainnya. Desain laporan yang baik akan membuat pemakai mudah untuk membaca *output* yang dihasilkan.

d. *Online Output Production and Distribution Controls*

Pengendalian terhadap produksi dan distribusi atas *output* yang dilakukan melalui *online* secara garis lurus, tujuan utamanya adalah untuk memastikan bahwa hanya bagian yang memiliki wewenang saja dapat melihat *output online* tersebut.

e. *Audit Trail Controls*

Pengendalian jejak audit pada subsistem *output* dilakukan untuk menjaga kronologi kejadian yang terjadi dari saat *output* diterima sampai pemakai melakukan penghapusan *output* tersebut karena sudah tidak dipakai atau disimpan lagi.

f. *Existence Controls*

Output dapat hilang atau rusak karena berbagai alasan, seperti *invoice* hilang, *online output* terkirim pada alamat yang salah, *output* terbakar karena kebakaran. *Recovery* terhadap subsistem *output* secara akurat, lengkap dan tepat merupakan hal yang sangat membantu kelangsungan hidup banyak organisasi.

2.6 Penetapan Resiko

Menurut Peltier (2001, p79), resiko didefinisikan sebagai seseorang atau sesuatu yang menyebabkan ancaman.

Menurut Peltier (2001, p79), resiko dibagi menjadi 3 tingkatan yaitu :

1. *High Vulnerability*

   Kelemahan yang sangat besar yang berada di dalam sistem atau rutinitas operasi dan di mana dampak potensial pada bisnis adalah penting, untuk itu harus ada pengendalian yang ditingkatkan.

2. *Medium Vulnerability*

   Beberapa kelemahan yang ada pada sistem dan di mana dampak potensial pada bisnis adalah penting, untuk itu akan ada pengendalian yang perlu ditingkatkan.

3. *Low Vulnerability*

   Sistem telah dibangun dengan baik dan dioperasikan dengan benar. Tidak ada penambahan pengendalian yang diperlukan untuk mengurangi kelemahan (*vulnerability*).

Dari ketiga tingkatan resiko tersebut dibagi lagi menjadi 3 dampak resiko, yaitu :

1. *Severe Impact (high)*

   Memungkinkan untuk perusahaan keluar dari bisnis atau kerusakan yang parah dari kemungkinan bisnis dan perkembangan perusahaannya.

2. *Significant impact (medium)*

   Akan mengakibatkan kerusakan yang berarti dan biaya yang dikeluarkan juga cukup besar sehingga perusahaan akan berjuang untuk mempertahankan.

3. *Minor Impact (low)*

   Tipe dari operasional memberi pengaruh yang kuat pada satu harapan untuk dapat mengatur sebagian dari kehidupan bisnis yang biasa.