BAB 2

LANDASAN TEORI

2.1 Teori-teori Umum

2.1.1 Sistem Informasi

2.1.1.1 Pengertian Sistem

Menurut Mcleod, Jr. (2001, p.9), *"A system is a group of elements that are integrated with the common purpose of achieving a objective"*, yang berarti sistem didefinisikan sebagai sekelompok elemen yang terintegrasi dengan maksud yang sama untuk mencapai tujuan.

Menurut Romney (2004, p.2), sistem adalah rangkaian dari dua atau lebih komponen-komponen yang saling berhubungan, yang berinteraksi untuk mencapai suatu tujuan.

Dari pengertian di atas dapat disimpulkan bahwa sistem merupakan kumpulan elemen yang saling berhubungan untuk mencapai tujuan tertentu.

2.1.1.2 Pengertian Informasi

Menurut McLeod, Jr. (2001, p.15), informasi adalah data yang telah diproses, atau data yang memiliki arti.

Menurut Romney (2004, p.11), informasi adalah data yang telah diatur dan diproses untuk memberikan arti bagi orang yang menerimanya.

Dari pengertian di atas dapat disimpulkan bahwa informasi merupakan data yang telah diolah menjadi suatu bentuk yang lebih berguna bagi yang menerimanya.

2.1.1.3 Karakteristik Informasi

Menurut Mukhtar (1999, p.4), agar suatu informasi bisa berguna haruslah memiliki beberapa karakteristik berikut ini :

1. *Reliable* (dapat dipercaya). Informasi harus bebas dari kesalahan dan harus akurat dalam mempresentasikan suatu kejadian atau kegiatan dari suatu organisasi.
2. *Relevant* (cocok atau sesuai). Informasi yang relevan harus memberikan arti kepada pembuat keputusan. Informasi ini bisa mengurangi ketidakpastian dan bisa meningkatkan nilai dari suatu keputusan.
3. *Timely* (tepat waktu). Informasi yang disajikan tepat waktu pada saat dibutuhkan dan bisa mempengaruhi proses pengambilan keputusan.
4. *Complete* (lengkap). Informasi yang disajikan berisi data yang relevan dan tidak mengabaikan kepentingan yang diharapkan oleh pembuat keputusan.
5. *Understandable* (dimengerti). Informasi yang disajikan hendaknya dalam bentuk yang mudah dimengerti oleh si pembuat keputusan.

2.1.1.4 Pengertian Sistem Informasi

Menurut Alter (1999, p.42), sistem informasi adalah tipe khusus dari sistem kerja yang menggunakan teknologi informasi untuk memperoleh, mengirim, menyimpan, mengambil, memanipulasi, dan menampilkan informasi, dengan demikian mendukung satu atau lebih sistem kerja yang lain.

Menurut Mukhtar (1999, p.3), sistem informasi dapat diartikan sebagai suatu pengorganisasian peralatan untuk mengumpulkan, memasukkan, memproses, mengatur, mengontrol, dan melaporkan informasi untuk pencapaian tujuan perusahaan.

Jadi, dapat disimpulkan bahwa sistem informasi merupakan suatu kesatuan komponen yang saling berinteraksi untuk mengumpulkan, mengolah, menyimpan, dan melaporkan informasi kepada pengguna untuk pencapaian tujuan perusahaan.

2.1.2 Auditing

2.1.2.1 Pengertian Audit

Menurut Arens dan Locbbecke (2001, p.1), *auditing* adalah proses pengumpulan dan pengevaluasian bahan bukti tentang informasi yang dapat diukur mengenai suatu entitas ekonomi yang dilakukan oleh orang yang kompeten dan independen untuk dapat menentukan dan melaporkan kesesuaian antara informasi yang dimaksud dengan kriteria yang telah ditetapkan.

Menurut Mukhtar (1999, p.116), audit adalah suatu proses yang sistematis dan memiliki objektif yang ditujukan untuk mendapatkan dan mengevaluasi bukti-bukti yang berhubungan dengan kegiatan dan kejadian ekonomi untuk meyakinkan hubungannya dengan hasil yang diinginkan pemakai. Dengan kata lain, audit melibatkan pengumpulan, review, dan pendokumentasian semua bukti-bukti pemeriksaan, dan akhirnya merekomendasikan, dimana rekomendasi ini digunakan pemeriksa untuk dasar evaluasi terhadap suatu sistem.

Jadi, dapat disimpulkan bahwa audit adalah suatu proses sistematik untuk memperoleh dan mengevaluasi bukti secara objektif mengenai pernyataan-pernyataan tentang kegiatan dan kejadian ekonomi, dengan tujuan untuk menetapkan tingkat kesesuaian antara pernyataan-pernyataan tersebut dengan kriteria yang telah ditetapkan, serta penyampaian hasil-hasilnya kepada pemakai yang berkepentingan.

2.1.2.2 Jenis Audit

Menurut Arens dan Loebbecke (2001, pp.4-5) pada umumnya audit diklasifikasikan dalam tiga jenis, yaitu :

1. Audit laporan keuangan

   Audit laporan keuangan bertujuan apakah laporan keuangan secara keseluruhan yang merupakan informasi terukur yang akan diverifikasi telah disajikan sesuai dengan kriteria-kriteria tertentu. Umumnya, kriteria-kriteria itu adalah prinsip akuntansi yang berlaku umum.

2. Audit operasional

   Audit operasional merupakan penelaahan atas bagian manapun dari prosedur dan metode operasi suatu organisasi untuk menilai efisiensi dan efektivitasnya. Umumnya, pada saat selesainya audit operasional, auditor akan memberikan sejumlah saran kepada manajemen untuk memperbaiki jalannya operasi perusahaan.

3. Audit kepatuhan

   Audit ketaatan bertujuan mempertimbangkan apakah auditi (klien) telah mengikuti prosedur atau aturan tertentu yang telah ditetapkan pihak yang memilki otoritas lebih tinggi.

2.2 Teori-teori Khusus

2.2.1 Audit Sistem Informasi

2.2.1.1 Pengertian Audit Sistem Informasi

Menurut Weber (1999, p.10), audit sistem informasi adalah proses pengumpulan dan pengevaluasian bukti untuk menentukan apakah sistem komputer dapat melindungi

aset atau kekayaan, memelihara integritas data, memungkinkan tujuan organisasi untuk dicapai secara efektif dan menggunakan sumber daya secara efisien.

Sedangkan menurut Romney (2004, p.434), audit sistem informasi merupakan tinjauan pengendalian umum dan aplikasi atas suatu sistem informasi akuntansi, untuk menilai pemenuhan kebijakan dan prosedur pengendalian internal serta keefektivitasannya untuk menjaga aset.

Berdasarkan pengertian di atas, dapat disimpulkan bahwa audit sistem informasi adalah suatu proses pengumpulan dan pengevaluasian bahan bukti audit untuk menentukan apakah sistem komputer perusahaan telah menggunakan aset sistem informasi secara tepat dan mampu mendukung pengamanan aset tersebut memelihara kebenaran dan integritas data dalam mencapai tujuan perusahaan secara efektif dan efisien.

2.2.1.2 Jenis Audit Sistem Informasi

Menurut Gondodiyoto (2003, p.151) audit sistem informasi dapat digolongkan dalam jenis-jenis audit sebagai berikut :

1. Audit laporan keuangan (*financial statement audit*)

   Audit ini dilakukan untuk mengetahui tingkat kewajaran atas laporan keuangan yang disajikan oleh perusahaan (sesuai dengan standar akuntansi keuangan dan tidak ada salah saji materialitas). Apabila sistem akuntansi perusahaan tersebut merupakan sistem akuntansi berbasis komputer, maka berarti dilakukan audit terhadap sistem informasi akuntansi tersebut apakah proses / mekanisme sistem dan program komputer sudah benar, pengendalian umum sistem memadai dan apakah data substantif (yang ada di dalam *file* / media komputer) sesuai.

2. Audit operasional (*operational audit*)

   a. Audit terhadap aplikasi komputer

      1) Audit setelah implementasi *(post implementation)*

         Auditor memeriksa apakah sistem-sistem aplikasi komputer yang telah diimplementasikan pada suatu organisasi / perusahaan telah sesuai dengan kebutuhan penggunanya (efektif) dan telah dijalankan dengan sumber daya optimal (efisien). Auditor mengevaluasi apakah sistem aplikasi tertentu dapat terus dijalankan karena sudah berjalan dengan baik dan sesuai dengan kebutuhan *user*nya, atau perlu dimodifikasi dan bahkan perlu dihentikan. Pelaksanaan audit ini dilakukan oleh auditor dengan menerapkan pengalamannya dalam pengembangan sistem aplikasi, sehingga auditor dapat mengevaluasi apakah sistem yang sudah diimplementasikan perlu dimuktahirkan atau diperbaiki atau bahkan dihentikan apabila sudah tidak sesuai kebutuhan atau mengandung kesalahan.

      2) Audit secara bersama-sama (*concurrent audit*)

         Auditor merupakan anggota dari tim pengembang sistem. Mereka membantu tim dalam meningkatkan kualitas dari pengembangan untuk sistem yang dibangun oleh para sistem analis designer dan programmer dan akan di implementasikan. Dalam hal ini, auditor mewakili pimpinan proyek dan manajemen sebagai *quality assurance*.

   b. Audit umum (*general audit*)

      Auditor mengevaluasi kontrol pengembangan sistem secara keseluruhan. Kemudian melakukan audit untuk menentukan apakah mereka dapat mengurangi waktu dari test substantive yang perlu dilakukan. Untuk memberikan opini audit

tentang pernyataan keuangan (sebagai tuntutan dari manajemen) ataupun tentang keefektifan dan keefisienan sistem.

2.2.1.3 Tujuan Audit Sistem Informasi

Tujuan audit sistem informasi menurut Weber (1999, p.11) secara garis besar terbagi menjadi empat, antara lain :

1. Meningkatkan objektifitas keamanan aset perusahaan

   Aset informasi suatu perusahaan seperti perangkat keras (*hardware*), perangkat lunak (*software*), sumber daya manusia, data (*file*) harus dijaga oleh suatu sistem pengendalian internal yang baik agar tidak terjadi penyalahgunaan aset perusahaan. Dengan demikian sistem pengamanan aset perusahaan merupakan suatu hal yang sangat penting dan harus dipenuhi oleh perusahaan.

2. Meningkatkan objektifitas integritas data

   Integritas data adalah salah satu konsep dasar sistem informasi. Data memiliki atribut-atribut tertentu seperti kelengkapan, kebenaran, dan keakuratan. Jika integritas data tidak terpelihara, maka suatu perusahaan tidak akan lagi memiliki hasil atau laporan yang benar bahkan perusahaan dapat menderita kerugian.

3. Meningkatkan objektifitas efektifitas sistem

   Efektivitas sistem informasi perusahaan memilki peranan penting dalam proses pengambilan keputusan. Suatu sistem informasi dapat dikatakan efektif bila sistem informasi tersebut telah sesuai dengan kebutuhan *user*.

4. Meningkatkan objektifitas efisiensi sistem

   Efisien menjadi hal yang sangat penting ketika suatu komputer tidak lagi memiliki kapasitas yang memadai. Jika cara kerja dari sistem aplikasi komputer menurun

maka pihak manajemen harus mengevaluasi apakah efisiensi sistem masih memadai atau harus menambah sumber daya manusia, karena suatu sistem dikatakan efisien jika sistem informasi dapat memenuhi kebutuhan *user* dengan sumber daya manusia yang minimal.

2.2.1.4 Metode Audit Sistem Informasi

Menurut Weber (1999, p.55), metode audit meliputi :

1. *Auditing around the computer*

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 masukan dan keluaran dari sistem komputer. Diasumsikan bahwa jika masukan benar akan diwujudkan pada keluaran, sehingga pemrosesan juga benar dan tidak melakukan pengecekan terhadap pemrosesan komputer secara langsung.

Karakteristiknya, yaitu :

a. Sistem sederhana dan berorientasi *batch*.
b. Sistem komputer yang diterapkan masih menggunakan *software* yang umum digunakan, dan telah diakui, serta dugunakan secara masal.
c. Menitikberatkan pada *user* daripada *computer controls* untuk melindungi aset, memelihara integritas data, dan mencapai sasaran yang efektif dan efisien.

Keunggulan dari pendekatan ini adalah pelaksanaan audit lebih sederhana dan auditor yang memiliki pengetahuan minimal di bidang komputer dapat dilatih dengan mudah untuk melaksanakan audit.

Kelemahan dari pendekatan ini adalah jika lingkungan berubah, maka kemungkinan sistem itupun berubah dan perlu penyesuaian sistem, sehingga auditor tidak dapat menilai apakah sistem berjalan dengan baik.

2. *Auditing through the computer*

Auditing through the computer merupakan suatu pendekatan audit yang berorientasi pada komputer dengan membuka *black box*, dengan 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 didcteksi. Sebagai akibatnya, 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.

Kelemahannya 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. Membutuhkan keahlian teknik yang lebih mendalam untuk memahami cara kerja sistem.

3. *Auditing with the computer*

Auditing with the computer merupakan suatu pendekatan audit dengan menggunakan komputer dan *software* untuk membantu melaksanakan langkah-langkah audit.

2.2.1.5 Tahapan Audit Sistem Informasi

Menurut Weber (1999, pp.47-55), tahapan audit sistem informasi terdiri dari :

1. Perencanaan audit (*planning the audit*)

Planning the audit merupakan fase pertama dalam pemeriksaan audit bagi auditor eksternal berarti menyelidiki dari awal atau melanjutkan yangada untuk menentukan apakah pemeriksaan tersebut dapat diterima, penempatan staf audit yang sesuai, melakukan pengecekan informasi latar belakang klien, mengerti kewajiban utama dari klien, menganalisa memajukan bisnis klien dan mengidentifikasikan area resiko. Sedangkan bagi auditor internal berarti mengerti obyek pendukung dalam pemeriksaan, penyediaan informasi pendukung staf yang handal dan mengidentifikasi area resiko.

2. Pengujian pengendalian (*tests of controls*)

Biasanya dalam fase ini diawali memusatkan pada pengendalian manajemen, apabila hasil menunjukkan tidak sesuai dengan harapan maka pengendalian manajemen tidak berjalan sebagaimana mestinya. Bila auditor menemukan kelemahan serius pada pengendalian manajemen mereka akan mengemukakan opini atau mengambil keputusan dalam pengujian transaksi dan saldo untuk hasilnya.

3. Pengujian transaksi (*tests of transactions*)

   Pengujian transaksi yang termasuk pengecekan jurnal yang masuk dari dokumen utama, menguji nilai kekayaan dan ketepatan komputasi. Komputer sangat berguna dalam pengujian ini dan auditor dapat menggunakan piranti lunak (*software*) audit yang umum untuk mengecek apakah pembayaran bunga dari bank telah di kalkulasi secara tepat.

4. Pengujian saldo perkiraan atau hasil keseluruhan (*tests of balances or overall results*)

   Auditor melakukan *tests of balances or overall results* agar bukti penting dalam penilaian akhir kehilangan atau pencatatan yang keliru yang menyebabkan fungsi sistem informasi gagal dalam memelihara data secara keseluruhan dan mencapai sistem yang efektif dan efisien. Untuk lebih mengerti pendekatan dalam fase ini, mementingkan pengamanan aset dan data integritas obyektif. Beberapa pengujian substansi dari saldo digunakan sebagai konfirmasi keuntungan, inventarisasi fisik barang dan mengkalkulasi kembali aktiva yang menyusut.

5. Pendapat auditor (*completion of the audit*)

   Hasil akhir dari tahap audit adalah pernyataan pendapat untuk melengkapi sistem informasi auditnya. Jenis-jenis pendapat auditor adalah :

   a. Pernyataan tidak memberikan pendapat (*disclaimer of opinion*)

      Auditor tidak menyatakan pedapat atas laporan keuangan yang diaudit.

   b. Pendapat tidak wajar (*adverse opinion*)

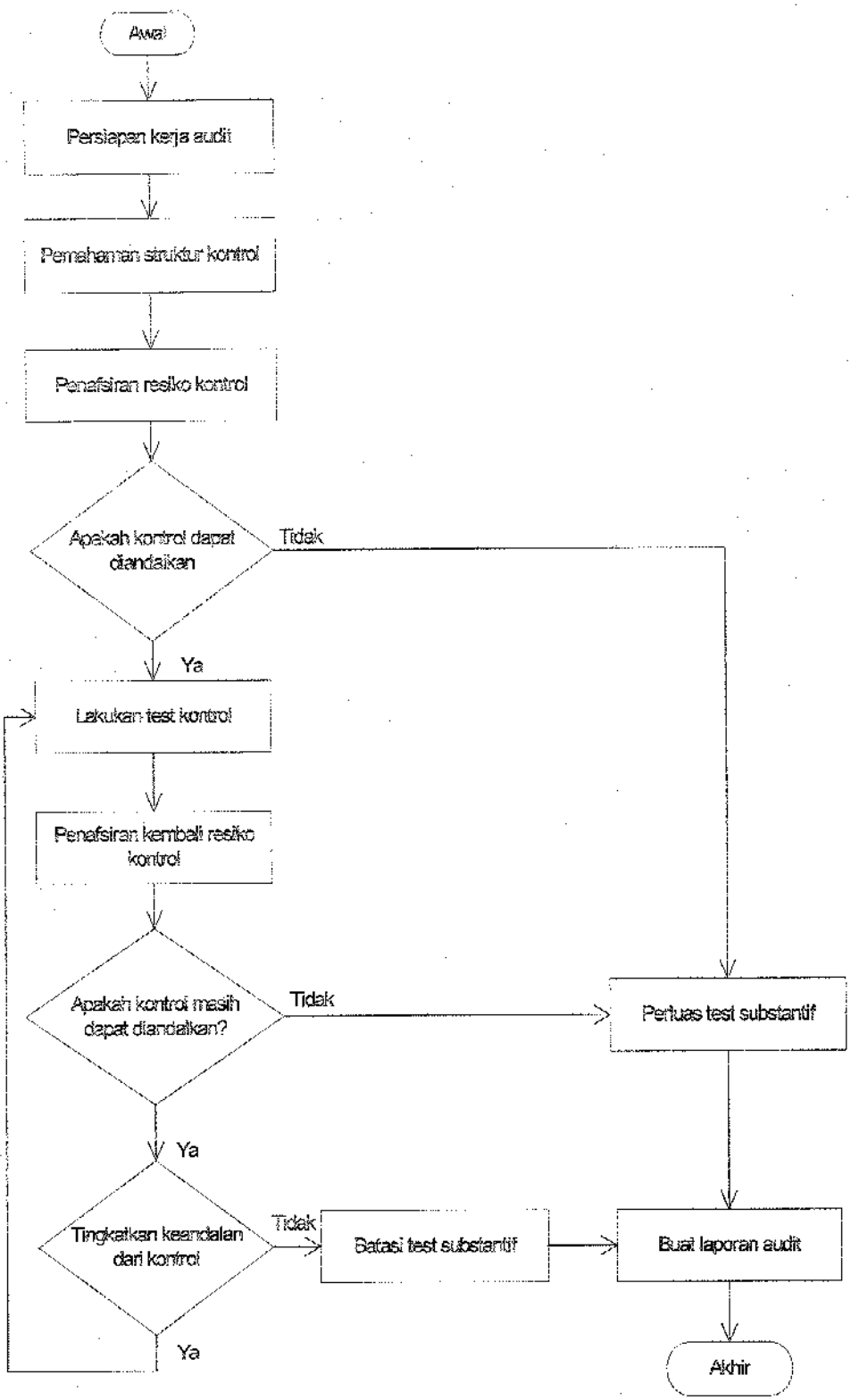
      Auditor memberikan pendapat tidak wajar jika laporan keuangan yang diberikan tidak disusun berdasarkan prinsip akuntansi secara umum.

c. Pendapat wajar dengan pengecualian (*qualified opinion*)

Auditor menyatakan bahwa laporan keuangan yang disajikan salah, tetapi tidak yang mempengaruhi dari laporan keuangan.

d. Pendapat wajar tanpa pengecualian (*unqualified opinion*)

Auditor menyimpulkan tidak ada kehilangan / penyelewangan material atau pencatatan akuntansi.



Gambar 2.1 Flowchart Tahapan Audit Sistem Informasi

2.2.2 Sistem Pengendalian Internal

2.2.2.1 Pengertian Pengendalian Internal

Menurut Weber (1999, p.35), pengendalian adalah suatu sistem untuk mencegah, mendeteksi, dan mengoreksi kejadian yang timbul saat transaksi dari serangkaian pemrosesan tidak terotorisasi secara sah, tidak akurat, tidak lengkap, mengandung redundansi, 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 di atas maka pengendalian dikelompokkan menjadi tiga bagian, yaitu :

1. *Preventive control*

   Pengendalian ini digunakan untuk mencegah masalah sebelum masalah tersebut muncul.

2. *Detective control*

   Pengendalian ini digunakan untuk menemukan masalah yang berhubungan dengan pengendalian segera setelah masalah tersebut timbul.

3. *Corrective control*

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

Menurut Mukhtar (1999, p.41), pengendalian internal merupakan perencanaan organisasi guna mengkoordinasikan metode atau cara pengendalian dalam suatu

perusahaan untuk menjaga aset perusahaan guna meningkatkan tingkat kepercayaan dan akurasi data, serta menjalankan operasional perusahaan secara efisien.

2.2.2.2 Komponen Pengendalian Internal

Menurut Weber (1999, p.49), pengendalian internal 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 kinerja.

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*, perlindungan aset dan *record*, pengecekan kinerja, dan penilaian dari jumlah *record* yang terjadi.

4. *Information* dan *communication*

   Komponen dimana operasi 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.

2.2.2.3 Pengertian Sistem Pengendalian Internal

Menurut Mulyadi (2001, p.163), sistem pengendalian intern meliputi struktur organisasi, metode, dan ukuran-ukuran yang dikoordinasikan untuk menjaga kekayaan organisasi, mengecek ketelitian dan keandalan data akuntansi, mendorong efisiensi dan dipatuhinya kebijakan manajemen.

Menurut Romney (2004, p.229), sistem pengendalian intern adalah rencana organisasi dan metode bisnis yang dipergunakan untuk menjaga aset, memberikan informasi yang akurat dan andal, mendorong dan memperbaiki efisiensi jalannya organisasi, serta mendorong kesesuaian dengan kebijakan yang telah ditetapkan.

Jadi sistem pengendalian intern adalah suatu pengendalian yang dilakukan oleh manajemen dan memastikan bahwa segala kebijakan dan peraturan dilaksanakan dengan baik sehingga sasaran dan tujuan perusahaan dapat tercapai.

2.2.2.4 Jenis Pengendalian Internal

Menurut Weber (1999, p.67), ruang lingkup pengendalian dibedakan atas dua jenis, yaitu kerangka kerja pengendalian manajemen (*management control framework*) dan kerangka kerja pengendalian aplikasi (*application control framework*).

2.2.2.4.1 Pengendalian Manajemen

Pengendalian manajemen dilakukan untuk meyakinkan bahwa pengembangan, pengimplementasian, pengoperasian, dan pemeliharaan sistem informasi telah diproses sesuai dengan rencana dan telah terkendali. Pengendalian ini berguna untuk menyediakan infrastruktur yang stabil sehingga sistem informasi dapat dibangun, dioperasikan, dan dipelihara secara berkesinambungan.

Pengendalian manajemen berupa :

1. Pengendalian top manajemen

   Top manajemen berfungsi mengontrol peranan manajemen dalam perencanaan kepemimpinan dan pengawasan fungsi sistem. Top manajemen harus memastikan bahwa fungsi sistem informasi diatur dengan baik. Top manajemen bertanggung jawab terutama untuk keputusan jangka panjang tentang bagaimana sitem informasi akan digunakan di dalam organisasi.

2. Pengendalian manajemen sistem informasi

   Manajemen sistem informasi bertanggung jawab terhadap keseluruhan perencanaan dan pengendalian dari seluruh kegiatan sistem informasi, serta memberikan saran kepada top manajemen dalam hubungannya untuk pengambilan keputusan kebijaksanaan jangka panjang dan mewujudkan kebijaksanaan jangka panjang dalam tujuan dan sasaran jangka pendek.

3. Pengendalian manajemen pengembangan sistem

   Manajemen pengembangan sistem bertanggung jawab untuk perancangan, pengimplementasian, dan pemeliharaan sistem aplikasi.

4. Pengendalian manajemen pemrograman

   Manajemen pemrograman berfungsi mengontrol pelaksanaan setiap tahap dari daur hidup program (*program life cycle*). Manajemen pemrograman bertanggung jawab untuk pemrograman sistem baru, pemeliharaan sistem lama, dan menyediakan software yang mendukung sistem pada umumnya.

5. Pengendalian manajemen sumber data

   Manajemen sumber data berfungsi mengontrol peranan dan fungsi dari *data administrator* atau *database administrator*. Manajemen sumber data bertanggung

jawab untuk perencanaan dan persoalan pengendalian dalam hubungannya dengan penggunaan data organisasi.

6. Pengendalian manajemen keamanan

   Manajemen keamanan berfungsi mengidentifikasi ancaman utama terhadap fungsi sistem informasi dan perancangan, pelaksanaan, pengoperasian, dan pemeliharaan terhadap pengontrolan yang dapat mengurangi kemungkinan kehilangan dari ancaman ini sampai pada tingkat yang dapat diterima. Manajemen keamanan bertanggung jawab untuk kontrol akses dan keamanan fisik dari fungsi sistem informasi.

7. Pengendalian manajemen operasi

   Fungsi utama dari manajemen operasi bertanggung jawab untuk perencanaan dan pengendalian operasi sistem informasi secara terus menerus. untuk meyakinkan bahwa pengoperasian sehari-hari dari fungsi sistem informasi diawasi dengan baik. Manajemen operasi bertanggung jawab untuk perencanaan dan pengendalian operasi sistem informasi secara terus menerus.

8. Pengendalian manajemen jaminan kualitas

   Fungsi utama yang harus dilakukan oleh manajemen jaminan kualitas (*quality assurance management*) untuk meyakinkan bahwa pengembangan, pelaksanaan, pengoperasian, dan pemeliharaan dari sistem informasi sesuai dengan standar kualitas.

2.2.2.4.2 Pengendalian Aplikasi

Pengendalian aplikasi dilakukan dengan tujuan untuk menentukan apakah pengendalian internal dalam sistem yang terkomputerisasi pada aplikasi komputer

tertentu sudah memadai untuk memberikan jaminan bahwa data dicatat, diolah, dan dilaporkan secara akurat, tepat waktu, dan sesuai dengan kebutuhan manajemen.

2.2.2.4.2.1 Pengendalian *Boundary*

Menurut Weber (1999, p.370) pengendalian *boundary* adalah menetapkan alat penghubung antara *user* dengan sistem komputer. Ketika seorang *user* duduk pada suatu terminal terpasang, dan memulai prosedur awal dengan suatu sistem operasi, fungsi *boundary* dilakukan. Hal ini sama seperti ketika seorang nasabah menuju mesin ATM (*Automatic Teller Machine*) untuk menarik uang tunai, memulai dengan memasukkan kartu ATM, dan melakukan *input* kode PIN (Personal Identification Number) lalu baru dapat berinteraksi dengan sistem untuk melakukan penarikan jumlah uang tunai.

Pengendalian di dalam *boundary* memiliki tiga tujuan utama, yaitu :

1. Untuk menetapkan keaslian identitas *user* terhadap suatu sistem komputer, sistem harus memastikan bahwa *user* adalah asli.
2. Untuk menetapkan keaslian identitas *resource* yang digunakan oleh *user*.
3. Untuk membatasi tindakan yang diambil oleh *user* dalam menggunakan *resource computer*, maka untuk masing-masing *user* diberikan fasilitas komputer dan berhak untuk mengoperasikannya dalam batasan yang telah ditetapkan.

Pengendalian batas-batas sistem aplikasi (*boundary controls*) adalah bahwa dalam suatu sistem aplikasi komputer diperlukan desain dan hal ini mencakup :

1. Ruang lingkup sistem adalah suatu sistem komputerisasi harus jelas ruang lingkupnya seperti apakah dokumen lingkupnya, dari mana sumbernya, tujuan pengolahan data dan siapa penggunanya (*user*), siapa sponsornya (pemegang kewenangannya).

2. Subsistem keterkaitan adalah sistem yang terdiri dari subsistem, modul, program, dan perlu kejelasan ruang lingkupnya (*boundary controls*), dan keterkaitan (*interfaces*) antara subsistem-subsistem dan modul-modul.

Pengendalian akses dilakukan untuk membatasi penggunaan *resource* sistem komputer hanya kepada *user* yang mendapatkan otorisasi, pembatasan aksi *user* yang mendapat otorisasi dapat menggunakan sumber daya ini dan menjamin bahwa *user* hanya mendapatkan sumber daya sistem komputer yang otentik (*authentic*).

Sistem komputer terkini didesain dengan memungkinkan banyak *user* untuk saling berbagi *resource*. Tujuan ini dicapai dengan memiliki sistem komputer tunggal untuk mensimulasi beberapa sistem komputer. Masing-masing komputer yang tersimulasi dinamakan *virtual machine*. *Virtual machine* memungkinkan penggunaan sumber daya yang lebih efisien dengan mengurangi tingkat nyata gangguan sistem komputer.

Dalam lingkungan *resource* yang dapat dibagi, auditor harus menekankan dua permasalahan tentang pengendalian akses, yaitu :

1. Auditor perlu untuk menentukan seberapa baik mekanisme pengendalian akses mampu mengamankan aset dan menjaga integritas data.
2. Atas kemampuan mekanisme pengendalian akses yang ada untuk masing-masing sistem aplikasi auditor harus menentukan apakah pengendalian akses yang dipilih untuk sistem tersebut adalah cukup.

User harus melakukan identifikasi pada mekanisme pengendalian akses dengan memberikan informasi yang ditetapkan. Informasi identifikasi memungkinkan mekanisme untuk memilih *file* informasi otentifikasi yang telah disimpan dan berbagai hal yang berhubungan dengan diri *user* sebagai pelaku.

Masing-masing jenis informasi memiliki berbagai kelemahan. Permasalahan utama atas otentifikasi yang menggunakan informasi yang diingat adalah lupa. Akibatnya *user* akan cenderung untuk memilih informasi yang mudah ditebak oleh pihak lain (*user* lain), untuk mengingat, *user* menuliskan pada tempat-tempat tertentu yang tidak sepenuhnya aman.

Berikut ini terdapat beberapa permasalahan dengan *password*, seperti :

1. Untuk mengingat *password*, *user* sering menuliskannya di dekat terminal yang digunakan oleh *user* sendiri.
2. *User* memilih *password* yang mudah ditebak oleh orang lain, misalnya : nama anggota keluarga, bulan kelahiran dan lain-lain.
3. *User* tidak mengubah *password* setelah waktu yang ditentukan untuk pengubahan *password* terlewati.
4. *User* tidak memahami dan menghargai pentingnya *password*.
5. *User* menjelaskan *password*nya kepada teman atau keluarganya.
6. Beberapa mekanisme pengendalian akses mengharuskan *user* untuk mengingat beberapa *password*.
7. Mekanisme pengendalian akses menyimpan data-data *password* dalam bentuk yang tidak terenc*rypt*.
8. *Password* tidak dihapus ketika *user* keluar dari organisasi.
9. *Password* ditransmisikan melalui jalur komunikasi dalam bentuk *cleartext*.

Sebagaimana dikutip Weber (1999, p.381) dari Barton and Barton (1984), menawarkan panduan bagaimana cara memilih *password* yang aman dan mudah diingat, yaitu:

1. Cobalah dari satu judul lagu yang menjadi lagu favorit. Dari lagu yang favorit tersebut, pilihlah penggalan lirik yang demikian mudah diingat, misalnya : DON'T KNOW WHAT I'VE GOT THESE INFORMATION SYSTEM AUDIT BLUES.
2. Selanjutnya, *password* disusun dengan memilih huruf pertama dari tiap-tiap kata, sehingga *password*-nya adalah DKWIGTISAB.
3. Untuk menjadikan *password* lebih aman, tempatkan satu tanda khusus, misalnya setiap tiga huruf. Sebagai contoh ditempatkan tanda & (*ampersand*) dan * (*asterisk*) secar bergantian, sehingga *password*-nya adalah DKW&IGT*ISA&B.
4. Ketika memasukkan *password* ke dalam mekanisme pengendalian akses, ingatlah sebuah lagu favorit dan ketiklah huruf pertama dari lirik lagu tersebut, jangan lupa menambahkan tanda-tanda khusus pada tempat yang telah ditentukan.

Berhubungan dengan manajemen *password, U.S National Bureau of Standard* (1985) dan *U.S Department of Defense* (1985), sebagimana sikutip oleh Weber (1999,p382), mengeluarkan prinsip-prinsip manajemen password yang baik, yaitu:

1. Jumlah *password* yang ada seharusnya dapat diterima oleh mekanisme pengendalian akses.
2. Mekanisme pengendalian akses seharusnya tidak menerima *password* yang panjangnya lebih pendek dari jumlah digit yang diisyaratkan.
3. Mekanisme pengendalian akses seharusnya tidak memungkinkan *user* untuk memilih *password* yang buruk, seperti : kata-kata yang ditemukan dalam kamus atau kata-kata yang memiliki variasi sebaran huruf minimal.
4. *User* seharusnya diarahkan untuk mengubah *password* secara periodik.
5. *User* seharusnya tidak memungkinkan untuk menggunakan kembali *password* yang sama dalam jangka waktu tertentu (misalnya satu tahun).

6. *Password* seharusnya dienkripsi dengan sekali jalan saat akan disimpan atau ditransmisikan.
7. *User* seharusnya diperkenalkan dan mempelajari tentang arti pentingnya keamanan *password* dan prosedur yang dapat digunakan untuk memilih *password* yang aman dan prosedur yang harus diikuti untuk menjaga agar *password* tetap aman.
8. *Password* harus segera diubah bila terdapat indikasi bahwa *password* telah dikompromikan.
9. Mekanisme pengendalian akses seharusnya membatasi berapa kali *user* boleh memasukkan *password* yang salah, dan adanya sanksi bilamana jumlah gagal akses yang telah dilakukan.

Permasalahan utama untuk otentifikasi yang menggunakan obyek adalah kemungkinan obyek tersebut dicuri oleh orang lain. Hal ini mengakibatkan *user* tidak dapat melakukan akses selama obyek yang bersangkutan tidak ada pada dirinya. Permasalahan utama untuk otentifikasi dengan menggunakan karakteristik pribadi adalah mahalnya peralatan yang digunakan untuk membaca media otentifikasi. Namun demikian, dengan menggunakan metode ini kemungkinan obyek otentifikasi tercuri sangat kecil bahkan tidak mungkin.

2.2.2.4.2.2 Pengendalian *Input*

Menurut Weber (1999, p.420) komponen dalam subsistem *input* bertanggung jawab dalam membawa baik data maupun instruksi ke dalam sistem aplikasi. Kedua tipe *input* harus disahkan, dan kesalahan-kesalahan yang terdeteksi harus dikontrol supaya *input* akurat, lengkap, unik, dan tepat waktu.

Pengendalian input sangat penting dilakukan, karena :

1. Dalam sistem informasi, pengendalian terbesar ada dalam subsistem *input*, jadi auditor akan menghabiskan banyak waktu untuk menilai apakah pengendalian *input* dapat dipercaya.
2. Aktivitas subsitem *input* terkadang melibatkan besarnya rutinitas, campur tangan manusia yang monoton, sehingga mudah terjadi kesalahan.
3. Subsistem *input* sering menjadi sasaran tindak kejahatan, banyak keanehan telah ditemukan yang melibatkan penambahan, pengurangan, atau perubahan *input* transaksi.

2.2.2.4.2.2.1 Metode Data *Input*

Menurut Weber (1999, p.421) metode data *input* meliputi :

1. *Keyboarding*, contoh: *Personal Computer* (PC)
2. *Direct Reading*, contoh: *Optical Character Recognition* (OCR), *Automatic Teller Machine* (ATM).
3. *Direct Entry*, contoh: *touch screen, joystick, mouse.*

2.2.2.4.2.2.2 Perancangan Dokumen Sumber

Tujuan dari pengendalian terhadap perancangan dokumen sumber antara lain: mengurangi kemungkinan kesalahan pencatatan data, meningkatkan kecepatan pencatatan data, mengontrol alur kerja, menghubungkan pemasukan data ke sistem komputer, meningkatkan kecepatan dan ketepatan pembacaan data, dan sebagai alat referensi untuk mengecek urutan-urutan pengisian.

Dasar-dasar yang perlu diperhatikan untuk penilaian dari perancangan dokumen sumber yang baik adalah:

1. Karakteristik dari medium kertas yang akan digunakan untuk dokumen sumber, meliputi: pemilihan panjang dan lebar kertas, kualitas kertas, banyaknya rangkap yang dibuatkan untuk setiap transaksi.
2. *Layout* dan *sytle* yang akan digunakan untuk dokumen sumber.

2.2.2.4.2.2.3 Perancangan Layar Entri Data

Dasar-dasar yang perlu diperhatikan untuk penilaian dari perancangan layar entri data adalah:

1. Layar digunakan untuk pemasukan data secara langsung atau digunakan untuk memasukkan data dari dokumen sumber.
2. Layar masukan harus mencerminkan bagaimana cara pemasukkan *field* data.
3. Layar masukan harus mencerminkan dokumen sumber.

2.2.2.4.2.2.4 Pengendalian Kode Data

Sistem pengkodean terdiri dari beberapa tipe, yaitu:

1. *Serial codes*

   Memberikan urutan nomor atau alphabet sebagai suatu objek, terlepas dari kelompok objek tersebut. Maka, dapat dikatakan bahwa *serial codes* secara unik mengidentifikasi suatu objek. Keuntungan utama dari pengkodean ini adalah kemudahan untuk menambahkan item baru dan juga pengkodean ini ringkas dan padat.

2. *Block sequence codes*

   Pengkodean dengan *block sequence* memberikan satu blok dari nomor-nomor sebagai suatu kategori khusus dari sebuah objek. Kelompok utama dari objek dalam satu kategori harus ditentukan dan disertai dengan satu blok dari nomor-nomor untuk masing-masing nilai dari kelompok tersebut. Keuntungan dari pengkodean ini adalah dalam memberikan nilai *mnemonic* (mudah diingat). Kesulitan yang dihadapi adalah dalam menentukan ukuran / panjang dari kode.

3. *Hierarchical codes*

   Hierarchical codes membutuhkan pemilihan serangkaian nilai kelompok dari suatu objek yang akan dikodekan dan diurutkan berdasarkan tingkat kepentingannya. *Hierarchical codes* lebih berarti dibanding *serial* atau *block sequence* karena pengkodean ini mendeskripsikan lebih banyak kelompok dari objek.

4. *Association codes*

   Dengan *association codes*, kelompok dari objek yang akan diberi kode dipilih, dan kode yang unik diberikan untuk masing-masing nilai dari kelompok tersebut. Kode tersebut dapat berupa numerik, alphabet atau alphanumerik. *Association codes* mempunyai nilai *mnemonic* yang tinggi. Pengkodean ini lebih cenderung salah jika tidak ringkas atau terdiri dari banyak campuran alphabet atau karakter numerik.

Dasar-dasar yang perlu diperhatikan untuk penilaian dari pengkodean data adalah:

1. Panjang dari kode

   Kode yang lebih panjang lebih mudah salah, maka pengkodean tersebut dikelompokkan dalam bagian-bagian kecil dengan memberikan *hypen* (-), *slash* (/), atau spasi untuk mengurangi kesalahan.

2. Penggabungan alphabet dan numerik

   Pengkodean dengan menggunakan penggabungan alphabet dan numerik dilakukan dengan mengelompokkan ke dalam bagiannya masing-masing untuk mengurangi tingkat kesalahan. Selain itu juga membantu dalam pemasukan kode.

3. Pilihan dari karakter

   Pilihan dalam penggunaan karakter juga harus diperhatikan terutama karakter yang memiliki kemiripan dengan huruf dan angka.

4. Penggunaan huruf besar dan huruf kecil

   Pemakaian huruf besar dan kecil secara bersamaan akan memperlambat pemasukan dan meningkatkan kemungkinan terjadinya kesalahan. Demikian juga dengan penggunaan karakter spesial serta bantuan tombol *shift* sebaiknya dihindarkan.

5. Urutan karakter yang dapat diperkirakan

   Penggunaan urutan karakter yang sudah umum lebih baik dibandingkan dengan penggunaan urutan yang tidak umum.

2.2.2.4.2.2.5 *Check Digit*

Pengecekan yang dilakukan dengan menggunakan *check digit* hanya dilakukan pada *field* yang bersifat kritis. Pengecekan ini hanya dapat dilakukan dengan menggunakan mesin pada saat memasukkan atau dengan program *input*.

2.2.2.4.2.2.6 *Batch Controls*

Batching adalah proses pengelompokan transaksi yang memiliki hubungan satu dengan yang lainnya. Ada dua tipe *batch* yang digunakan yaitu *physical batch* dan

logical batch. *Physical batch* adalah kelompok transaksi yang terdiri dari unit *physical*. *Logical batch* adalah kelompok transaksi yang disatukan atas dasar persamaan *logical*.

Penilaian terhadap *batch controls* dapat dilakukan dengan mengacu pada :

1. *Batch cover sheet*

   Batch cover sheet terdiri dari nomor *batch* yang unik, total kontrol untuk *batch*, data yang umum dari berbagai transaksi dalam *batch*, tanggal ketika *batch* dipersiapkan, informasi dari kesalahan yang terdeteksi dalam *batch*, serta tanda tangan dari personil yang bertanggung jawab dalam penanganan *batch*.

2. *Batch control register*

   Batch control register merekam perpindahan *physical batch* antara berbagai lokasi dalam satu organisasi.

2.2.2.4.2.2.7 Validasi Data *Input*

Untuk pengecekan validasi data *input* terdiri dari empat jenis, yaitu :

1. *Field checks*

   Validasi yang dilakukan tidak bergantung pada nilai dari *field* yang lain pada *record input*.

2. *Record checks*

   Validasi yang dilakukan bergantung pada *field* lain dari *record input*.

3. *Batch checks*

   Validasi dilakukan dengan memeriksa kesamaan karakteristik *batch* dari *record* yang akan dimasukkan dengan *record batch* yang sudah tercatat

4. *File checks*

   Validasi yang dilakukan dengan memeriksa kesamaan karakteristik dari *file* yang digunakan dengan karakteristik dari *file* yang sudah terekam.

2.2.2.4.2.2.8 Instruksi *Input*

Dalam memasukkan instruksi ke dalam sistem aplikasi sering terjadi kesalahan karena adanya instruksi yang bervariasi dan kompleks, sehingga perlu menampilkan pesan kesalahan. Pesan kesalahan yang ditampilkan harus dikomunikasikan pada *user* dengan lengkap dan jelas.

Ada enam cara untuk memasukkan instruksi ke dalam sistem informasi, yaitu:

1. *Menu-driven languages*

   Sistem menyajikan serangkaian pilihan kepada *user* dan *user* dapat memilih dengan beberapa cara, yaitu dengan mengetikkan angka atau huruf yang mengidentifikasikan pilihan mereka, meletakkan kursor pada pilihan kemudian menekan tombol *Enter* atau dengan mengklik *mouse*, menggunakan *light pen* atau *touch screen*.

2. *Question-answer dialog*

   Sistem aplikasi menyajikan pertanyaan tentang nilai dari beberapa item data dan *user* meresponnya.

3. *Command languages*

   Membutuhkan *user* untuk memberikan perintah tertentu dalam meminta beberapa proses dan sekumpulan argumen yang secara spesifik memberitahukan bagaimana proses tersebut seharusnya dijalankan.

4. *Forms-based languages*

   Membutuhkan *user* untuk memberikan perintah dan data tertentu yang terdapat dalam form *input* maupun output.

5. *Natural languages*

   User memberikan instruksi pada sistem aplikasi melalui *recognition device.*

6. *Direct manipulation interface*

   User memasukkan instruksi dalam sistem aplikasi melalui manipulasi langsung obyek pada layar.

2.2.2.4.2.3 Pengendalian Komunikasi

Mengontrol pendistribusian pembukaan komunikasi subsistem, komponen fisik, kesalahan jalur komunikasi, aliran dan hubungan, kontrol topologi, kontrol akses hubungan, kontrol atas ancaman subversif, kontrol *internetworking*, dan kontrol arsitektur komunikasi.

2.2.2.4.2.4 Pengendalian Proses

Menurut Porter dan Perry (1996, p.200), pengendalian proses mencakup pengendalian terhadap kemungkinan kehilangan data atau tidak diprosesnya data, perhitungan aritmatik, dan keakuratan pemrograman.

2.2.2.4.2.5 Pengendalian *Database*

Menurut Porter dan Perry (1996, p.204), pengendalian *database* digunakan untuk menjaga integritas data dalam suatu database. Pengendalian yang dilakukan untuk menjaga integritas data tersebut mencakup kontrol terhadap pelaporan kemacetan,

sistem kamus data, sistem kamus data yang terintegrasi, tanggung jawab unsur data, pengendalian data berbareng, dan pemecahan hambatan.

2.2.2.4.2.6 Pengendalian *Output*

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

Pengendalian *output* yang dilakukan berupa :

1. Mencocokkan data *output* (khususnya total pengendali) dengan total pengendali yang sebelumnya telah ditetapkan yang diperoleh dalam tahap *input* dari siklus pemrosesan.
2. Mereview data *output* untuk melihat format yang tepat yang terdiri dari :
   a. Judul laporan
   b. Tanggal dan waktu pencetakan
   c. Banyaknya copy laporan untuk masing-masing pihak yang berwenang
   d. Periode laporan
   e. Nama program (termasuk versinya yang menghasilkan laporan)
   f. Nama personil yang bertanggung jawab atas dikeluarkannya laporan tersebut
   g. Masa berlaku laporan
   h. Nomor halaman
   i. Tanda akhir halaman
3. Mengendalikan data *input* yang ditolak oleh komputer selama pemrosesan dan mendistribusikan data yang ditolak itu ke personil yang tepat.

4. Mendistribusikan laporan-laporan *output* ke departemen pemakai tepat pada waktunya.

2.2.3 Sistem Informasi Penjualan

2.2.3.1 Pengertian Sistem Penjualan

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

1. Kegiatan penjualan kredit

   Dalam transaksi penjualan kredit, jika order dari pelanggan telah dipenuhi dengan pengiriman barang atau penyerahan jasa, untuk jangka waktu tertentu perusahaan memiliki piutang kepada pelanggannya. Kegiatan penjualan secara kredit ini ditangani oleh perusahaan melalui sistem penjualan kredit.

2. Kegiatan penjualan tunai

   Dalam transaksi penjualan secara tunai, barang atau jasa baru diserahkan oleh perusahaan kepada pembeli jika perusahaan telah menerima kas dari pembeli. Kegiatan penjualan secara tunai ini ditangani oleh perusahaan melalui sistem penjualan tunai.

Menurut Sidharta (1996, p.46) sistem penjualan adalah struktur interaksi antara manusia, peralatan, metode-metode, dan kontrol-kontrol yang disusun untuk mencapai tujuan tertentu dalam menyediakan aliran informasi yang mendukung :

1. Rutinitas kerja dalam bagian order penjualan, bagian kredit, dan bagian pengiriman (yaitu dengan menangkap dan mencatat data yang berhubungan dengan penjualan).
2. Pembuatan keputusan untuk personil-personil yang mengatur fungsi penjualan dan fungsi pemasaran.

2.2.3.2 Jaringan Prosedur Sistem Penjualan

Jaringan prosedur yang membentuk sistem penjualan menurut Mulyadi (2001, p.219) adalah :

1. 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 lain untuk memungkinkan fungsi tersebut memberikan kontribusi dalam melayani order dari pembeli.

2. Prosedur persetujuan kredit

   Dalam prosedur ini, fungsi penjualan meminta persetujuan kredit kepada pembeli tertentu dari fungsi kredit.

3. Prosedur pengiriman

   Dalam prosedur ini, fungsi pengiriman mengirimkan barang kepada pembeli sesuai dengan informasi yang tercantum dalam surat order pengiriman yang diterima dari fungsi pengiriman.

4. Prosedur penagihan

   Dalam prosedur ini, fungsi penagihan membuat faktur penjualan dan mengirimkannya kepada pembeli. Dalam metode tertentu faktur penjualan dibuat oleh fungsi penjualan sebagai tembusan pada waktu bagian ini membuat surat order pengiriman.

5. Prosedur pencatatan piutang

   Dalam prosedur ini, fungsi akuntansi mencatat tembusan faktur penjualan ke dalam kartu piutang atau dalam metode pencatatan tertentu mengarsipkan dokumen tembusan menurut abjad yang berfungsi sebagai catatan piutang.

6. Prosedur distribusi penjualan

   Dalam prosedur ini, fungsi akuntansi mendistribusikan data penjualan menurut informasi yang diperlukan oleh manajemen.

7. Prosedur pencatatan harga pokok penjualan

   Dalam prosedur ini, fungsi akuntansi mencatat secar periodik total harga pokok produk yang dijual dalam periode akuntansi tertentu.

2.2.3.3 Pengertian Sistem Retur Penjualan

Menurut Mulyadi (2001, p.226) transaksi retur penjualan terjadi jika perusahaan menerima pengembalian barang dari pelanggan. Pengembalian barang oleh pelanggan harus diotorisasi oleh fungsi penjualan dan diterima oleh fungsi penerimaan.

2.2.3.4 Jaringan Prosedur Sistem Retur Penjualan

Menurut Mulyadi (2001, p.234), jaringan prosedur yang membentuk sistem retur penjualan adalah :

1. Prosedur pembuatan memo kredit

   Berdasarkan pemberitahuan retur penjualan dari pembeli, dalam prosedur ini fungsi penjualan membuat memo kredit yang memberikan perintah kepada fungsi penerimaan untuk menerima barang dari pembeli tersebut dan kepada fungsi akuntansi untuk mencatat pengurangan piutang kepada pembeli yang bersangkutan.

2. Prosedur penerimaan barang

   Dalam prosedur ini, fungsi penerimaan menerima barang dari pembeli berdasarkan perintah dalam memo kredit yang diterima dari fungsi penjualn. Atas penerimaan barang tersebut fungsi penerimaan membuat laporan penerimaan barang untuk melampiri memo kredit yang dikirim ke fungsi akuntansi.

3. Prosedur pencatatan retur penjualan

   Dalam prosedur ini, transaksi berkurangnya piutang dagang dan pendapatan penjualan akibat dari transaksi retur penjualan yang dicatat oleh fungsi akuntansi ke dalam jurnal umum atau jurnal retur penjualan dan ke dalam buku pembantu piutang. Dalam prosedur ini pula berkurangnya harga pokok penjualan dan bertambahnya harga pokok persediaan dicatat oleh fungsi akuntansi ke dalam jurnal umum dan dalam buku pembantu persediaan.