BAB 2

LANDASAN TEORI

2.1 Sistem Infomasi

2.1.1. Pengertian Sistem

Menurut James A. Hall (2007, h6) yang diterjemahkan oleh Dewi Fitriasari dan Deny Arnos Kwary, "Sistem adalah kelompok dari dua atau lebih komponen atau subsistem yang saling berhubungan yang berfungsi dengan tujuan yang sama".

Menurut Mulyadi (2001, h5), "Sistem adalah suatu jaringan prosedur yang dibuat menurut pola yang terpadu untuk melaksanakan kegiatan pokok perusahaan".

Jadi dapat disimpulkan bahwa sistem adalah kumpulan komponen-komponen yang saling berhubungan satu dengan lainnya dengan tujuan yang sama untuk dapat melaksanakan kegiatan pokok perusahaan.

2.1.2. Pengertian Informasi

Menurut Sanyoto Gondodiyoto dan Henny Hendarti (2007, h82), "Informasi adalah data yang telah diolah diubah menjadi suatu bentuk yang sesuai dengan keinginan si penerima".

Menurut James A. O'Brien (2005, h38), yang diterjemahkan oleh Dewi Fitriasari, "Informasi adalah data yang telah diubah menjadi konteks yang berarti dan berguna bagi para pemakai akhir tertentu."

Dapat disimpulkan bahwa informasi merupakan data yang telah diolah diubah menjadi suatu bentuk yang berarti dan berguna bagi para pemakai.

2.1.3. **Pengertian Sistem Informasi**

Menurut James A. Hall (2007, h9) yang diterjemahkan oleh Dewi Fitriasari dan Deny Arnos Kwary, "Sistem informasi (*information system*) adalah serangkaian prosedural formal di mana data dikumpulkan, diproses menjadi informasi dan didistribusikan ke para pengguna.

Menurut James A. O'Brien (2005, h5), yang diterjemahkan oleh Dewi Fitriasari, sistem informasi dapat merupakan kombinasi teratur apa pun dari orang-orang, *hardware*, *software*, jaringan komunikasi, dan sumber daya data yang mengumpulkan, mengubah, dan menyebarkan informasi dalam sebuah organisasi.

Berdasarkan definisi di atas maka dapat ditarik sebuah kesimpulan bahwa sistem informasi adalah serangkaian prosedural formal di mana data dikumpulkan, diproses menjadi informasi dan didistribusikan ke para pengguna dalam sebuah organisasi.

2.1.4. **Tujuan Sistem Informasi**

Tujuan sistem informasi menurut James A. Hall (2007, h21) yang diterjemahkan oleh Dewi Fitriasari dan Deny Arnos Kwary, terdapat tiga tujuan dasar umum didapati di semua sistem, yaitu:

a. Mendukung fungsi kepengurusan (*stewardship*) pihak manajemen. Administrasi mengacu pada tanggung jawab manajemen untuk mengelola dengan baik sumber daya perusahaan.
b. Mendukung pengambilan keputusan manajemen. Sistem informasi memberikan pihak manajer informasi yang di butuhkan untuk melaksanakan tanggung jawab pengambilan keputusan tersebut.
c. Mendukung operasional harian perusahaan. Sistem informasi menyediakan informasi bagi personal operasional untuk membantu mereka melaksanakan pekerjaan hariannya dalam cara yang efisien dan efektif.

2.2 Sistem Pengendalian Internal

2.2.1 Pengertian Pengendalian Internal

Pengendalian internal 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 (2001, h165), sistem pengendalian internal meliputi struktur organisasi, metode dan ukuran-ukuran untuk menjaga kekayaan organisasi, mengecek ketelitian dan keandalan data akuntansi, mendorong efisien dan mendorong dipatuhinya kebijakan manajemen.

Jadi dapat disimpulkan bahwa sistem pengendalian internal adalah suatu sistem untuk mencegah, mendeteksi dan mengoreksi kejadian yang

timbul saat transaksi untuk menjaga kekayaan organisasi, mengecek ketelitian dan keandalan data akuntansi, mendorong efisien dan mendorong dipatuhinya kebijakan manajemen.

2.2.2 **Tujuan Pengendalian Internal**

Pengendalian internal merangkum kebijakan, praktik dan prosedur yang digunakan oleh organisasi untuk mencapai empat tujuan utama:

1. Untuk menjaga aktiva perusahaan.
2. Untuk memastikan akurasi dan dapat diandalkan catatan dan informasi akuntansi.
3. Untuk mempromosikan efisiensi operasi bisnis.
4. Untuk mengukur kesesuaian dengan kebijakan dan prosedur yang telah ditetapkan oleh manajemen.

2.2.3 **Komponen Pengendalian Internal**

Pengendalian internal terdiri dari lima komponen yang saling terintegrasi, antara lain:

1. Lingkungan Pengendalian

   Komponen ini diwujudkan dengan 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. Penilaian Resiko

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

3. Aktivitas Pengendalian

   Komponen yang dioperasikan untuk memastikan transaksi 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

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

5. Pemantauan

   Komponen yang memastikan pengendalian internal beroperasi secara dinamis.

2.2.4 **Jenis Pengendalian Internal**

Pengendalian terdiri dari dua jenis yaitu:

1. Pengendalian Manajemen (*Management Control Framework*)

   Pengendalian manajemen adalah 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, dioperasi, 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 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.

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

   Mengendalikan fungsi utama yang harus dilakukan oleh *Quality Assurance Management Control* untuk meyakinkan bahwa

pengembangan, pelaksanaan, pengoperasian, dan pemeliharaan dari sistem informasi sesuai dengan standar kualitas.

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

Pengendalian terhadap manajemen keamanan secara garis besar bertanggung jawab dalam menjamin aset sistem informasi tetap aman.

g. Pengendalian Manajemen Operasional (*Operational Management Control*)

Mengendalikan fungsi utama dari manajemen operasional untuk menyakinkan bahwa pengoperasian sehari-hari dari fungsi sistem infomasi diawasi dengan baik.

2. Pengendalian Aplikasi (*Application Control Framework*)

Pengendalian aplikasi berfungsi untuk memastikan bahwa setiap sistem aplikasi dapat melindungi aset-aset, menjaga integritas data, dan mewujudkan tujuan secara efektif dan efisien.

a. Pengendalian Batasan (*Boundary Control*)

Pengendalian ini bertanggung jawab untuk menentukan hubungan antara *user* dengan sistem komputer seperti fungsi pengendalian akses, nomor identifikasi personal (PIN), *digital signatures*, dan *plastic cards*.

b. Pengendalian Masukan (*Input Control*)

Komponen pada subsistem *input* bertanggung jawab dalam mengirimkan data dan instruksi ke dalam sistem aplikasi dimana kedua tipe atribut tersebut haruslah divalidasi, selain itu banyaknya kesalahan yang terdeteksi harus dikontrol sehingga *input* yang dihasilkan akurat, lengkap, unik dan tepat waktu.

c. Pengendalian komunikasi (*Communication control)*

Merupakan subsistem komunikasi yang bertanggung jawab untuk pengiriman data ke subsistem yang lain dalam suatu sistem dan untuk mengirimkan data ke penerima data dari sistem yang lain.

d. Pengendalian Proses (*Process control)*

Pengendalian proses terdiri dari komponen yang melakukan kegiatan pengambilan keputusan, perhitungan, pengklasifikasian, memerintah dan meringkas data pada sistem.

e. Pengendalian Database (*Database control*)

Merupakan subsistem database yang menyediakan fungsi-fungsi untuk mendefenisikan, membuat, memodifikasi, menghapus, dan membaca data dalam sistem informasi.

f. Pengendalian Keluaran (*Output control*)

Digunakan untuk memastikan bahwa data yang diproses tidak mengalami perubahan yang tidak sah oleh operator komputer dan memastikan hanya orang yang berwenang saja yang menerima *output.*

Sesuai dengan ruang lingkup evaluasi sistem informasi yang dilakukan maka yang akan dibahas lebih lanjut dalam skripsi ini adalah:

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

   Ancaman utama terhadap keamanan aset sistem informasi adalah:

   a. Kerusakan karena kebakaran (*fire damage*)

      Beberapa cara untuk mengatasi ancaman kebakaran, yaitu:

      1) *Alarm* kebakaran yang manual maupun otomatis diletakkan pada tempat yang strategis.
      2) Pemadam kebakaran diletakkan pada tempat yang strategis.
      3) Bangunan tempat diletakkannya aset sistem informasi dibangun dengan konstruksi spesial yang tahan panas.
      4) Tempat diletakkannya pemadam kebakaran dan arah keluar diberi tanda yang jelas sehingga memudahkan untuk melihat tanda tersebut.
      5) Prosedur kebersihan yang baik dapat memastikan bahwa barang-barang yang mudah menyebabkan kebakaran minimal sekali keberadaannya di ruang sistem informasi.

   b. Kerusakan karena air (*water damage*)

      Beberapa cara penanganan terhadap *water damage* adalah:

      1) Jika memungkinkan, plafon, dinding dan lantai tahan air (*waterproof*).
      2) Pastikan bahwa tersedia sistem drainase yang memadai.

3) Tempatkan *alarm* pada tempat yang strategis dimana harta sistem informasi berada.

4) Pada lokasi yang sering banjir, tempatkan harta sistem informasi pada bangunan yang tinggi.

5) Memiliki *master switch* untuk semua kran air.

6) Gunakan sistem *dry-pipe automatic sprinkler* yang dijalankan oleh *alarm* dan api.

7) Tutup *hardware* dengan kain pengaman ketika tidak digunakan.

c. Naik turunnya voltase listrik (*energy variations*)

Hal ini dapat dicegah dengan menggunakan peralatan yang dapat menstabilkan tegangan listrik seperti pemakaian UPS untuk setiap komputer dan peralatan sistem informasi lainnya.

d. Kerusakaan struktur (*structure damage*)

Kerusakan struktur pada harta bagian sistem informasi dapat terjadi karena terjadi gempa, angin ribut, salju, tanah longsor dan kecelakaan.

e. Polusi (*polution*)

Polusi dapat merusak *disk drive*, *hard disk*, kebakaran dan lain-lain.

f. Gangguan dari orang yang tidak bertanggugjawab (*unauthorized intrusion*)

g. Virus dan *worm* (*viruses and worms*)

Beberapa pelaksanaan pengamanan untuk mengantisipasi virus, antara lain:

1) Tindakan *preventive*, seperti jangan menggunakan domain umum (*shareware software*), lakukan akses *read-only* terhadap *software*, men-*scan* file yang akan digunakan dan lain-lain.

2) Tindakan *detective*, seperti secara berkala menjalankan program *anti virus* untuk mendeteksi ada atau tidaknya virus.

3) Tindakan *corrective*, seperti pastikan ada *backup* yang bersih dan jalankan program *anti virus* untuk me-*remove* file yang terkena virus.

h. Penggunaan yang salah terhadap *software*, data dan jasa komputer (*misuse of software, data, and services*)

2. Pengendalian Manajemen Operasional (*Operational Management Control*)

Pengendalian atas delapan fungsi utama yang menjadi tanggung jawab manajemen operasional, yaitu:

a. Operasional komputer (*computer operasional*)

Kontrol terhadap operasional komputer merupakan aktivitas harian, ada tiga jenis kontrol yang ada, yaitu:

- Kontrol operasional (*operation control*)

  Banyak jenis kegiatan yang harus dilakukan untuk mendukung jalannya program komputer, sebagai contoh program harus dijalankan dan dimatikan, media penyimpan harus tersedia, formulir harus disediakan di *printer* dan informasi yang dihasilkan harus dikirim ke pamakai informasi.

- Kontrol jadwal (*scheduling control*)

  Scheduling controls dilakukan untuk memastikan bahwa komputer digunakan untuk kegiatan yang seharusnya dan menggunakan sumber daya dengan efisien.

- Kontrol pemeliharaan (*maintenance network control*)

  Kegiatan *maintenance* terhadap *hardware* komputer merupakan tindakan preventif yang harus dilakukan agar kerusakan *hardware* dapat dicegah.

b. Jaringan operasional (*network operations*)

Sebuah server memainkan peranan penting untuk mendukung mekanisme kontrol akses data pada *Local Area Network*. Dari sudut pandang operasional, *utilities operating system* yang terletak pada *file server* membuat staf operasional dapat mengelola *day to day* dan operasional jangka panjang jaringan menjadi lebih baik.

c. Persiapan data dan *entry* (*preparation data and entry*)

Secara umum, semua sumber data untuk aplikasi sistem dikirim ke bagian persiapan data untuk diketik dan diverifikasi sebelum dimasukkan ke dalam sistem komputer.

d. Kontrol produksi (*production control*)

Pengendalian pekerjaan operator komputer terdiri dari lima tugas, yaitu:

- Menerima dan mengirim *input* dan *output*
- Menjadwal pekerjaan

- Melakukan perjanjian jasa pelayanan kepada pemakai
- Menetapkan harga
- Memperoleh tambahan pemakaian komputer

e. Perpustakaan file (*file library*)

Fungsi *file library* pada bagian operasional adalah bertanggung jawab untuk mengelola manajemen penyimpanan data.

f. Dokumentasi dan program kepustakaan (*documentation and program library*)

Berbagai jenis dokumentasi diperlukan untuk mendukung fungsi sistem informasi pada suatu organisasi, perencanaan strategis dan operasional, dokumentasi sistem aplikasi program, dokumentasi sistem *software*, dokumentasi database, manual operasional, dan manual standar.

g. *Help desk* (*technical support*)

Fungsi bagian ini pada bagian operasional terdiri dari dua, yaitu:

- Membantu *end user* untuk mendapatkan *hardware* dan *software*.
- Menyediakan dukungan teknis untuk membantu mengatasi masalah.

h. Perencanaan kapasitas dan pengawasan kinerja (*capacity planning and performance monitoring*)

Dengan menggunakan perhitungan statistik pengawasan kinerja, manajer operasional harus membuat tiga keputusan, yaitu:

- Mereka harus mengevaluasi apakah profil kinerja memperlihatkan adanya kegiatan oleh bagian yang tidak berwenang terjadi.

- Mereka harus memastikan bahwa kinerja sistem dapat diterima oleh pemakai.
- *Hardware* dan *sotware* yang diperlukan harus tersedia.

3. Pengendalian Batasan (*Boundary Control*)

Tujuan utama *boundary controls* antara lain:

a. Untuk memastikan bahwa pemakai komputer adalah orang yang memiliki wewenang.
b. Untuk memastikan bahwa identitas yang diberikan oleh pemakai adalah benar.
c. Untuk membatasi tindakan yang dapat dilakukan oleh pemakai untuk menggunakan komputer ketika melakukan tindakan otorisasi.

Jenis *boundary control* antara lain:

a. *Cryptographic control*

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

b. *Access control*

Kontrol akses melarang pemakaian komputer oleh orang yang tidak berwenang, membatasi tindakan yang dapat dilakukan oleh pemakai dan memastikan bahwa pemakai hanya memperoleh sistem komputer yang asli.

c. *Personal Identification Numbers* (PIN)

PIN adalah teknik yang digunakan secara luas untuk mengidentifikasi orang. Sebuah PIN merupakan jenis *password* yang sederhana. Bisa merupakan nomor rahasia seseorang yang berhubungan dengan orang tersebut dan melayani pekerjaan memverifikasi keotentikan seseorang. Terdapat tiga metode untuk membuat PIN:

1) *Derived* PIN

   PIN dibuat berdasarkan nomor *account* pelanggan.

2) *Random* PIN

   PIN dibuat secara random berdasarkan panjangnya karakter.

3) *Customers-selected* PIN

   Memungkinkan pelanggan memilih PIN mereka sendiri.

Prinsip mengatur *password* dengan baik sebagai berikut:

1) Jumlah *password* yang ada seharusnya dapat diterima oleh mekanisme pengendalian akses.
2) Mekanisme pengendalian akses tidak menyetujui apabila panjang *password* kurang dari minimum.
3) Mekanisme pengendalian akses tidak memperbolehkan *user* menggunakan *password* yang kata-katanya mudah dicari di kamus.
4) *User* harus mengganti *password* secara periodik (misalnya sebulan sekali)
5) *User* tidak diperbolehkan menggunakan kembali *password* yang usianya lebih dari 12 bulan.

6) *Password* harus dienkripsi ketika akan disimpan atau ditransmisikan.
7) *User* harus diberi penjelasan mengenai pentingnya keamanan *password*, prosedur yang dapat digunakan untuk memilih *password* yang aman dan prosedur untuk menjaga keamanan *password*.
8) *Password* harus segera diganti, apabila terdapat indikasi bahwa *password* telah dikompromikan.
9) Mekanisme pengendalian akses membatasi *user* untuk memasukkan *password* yang salah.

4. Pengendalian Masukan (*Input Control*)

Komponen pada subsistem *input* bertanggung jawab untuk memasukkan data dan instruksi pada sistem aplikasi, dimana kedua jenis *input* tersebut harus divalidasi. Selain itu, setiap kesalahan data harus dapat diketahui dan dikontrol sehingga *input* yang dimasukkan akurat, lengkap, unik dan tepat waktu.

a. Metode *input* data

Cara *input* data dapat dilakukan dengan metode berikut:

1) *Keyboarding*, contoh: *Personal Computer* (PC)
2) *Directing reading*, contoh: *mark sensing*, *image reader*, *point-of-sale device*, ATM
3) *Direct entry*, contoh: *Personal Computer* (PC), *touch screen*, *joystick or voice or cideo*.

b. Kontrol kode data

Ada empat jenis sistem pengkodean, yaitu:

1) *Serial codes*

Menggunakan angka atau huruf yang berutuan untuk sebuah entitas.

2) *Block sequence codes*

Menggunakan blok angka untuk menentukan kategori *particular* dari entitas.

3) *Hierarchical codes*

Memerlukan satu set atribut pilihan dari entitas yang akan diberi kode dan pemilihan tersebut berdasarkan kepentingan.

4) *Association codes*

Atribut dan entitas yang akan diberi kode dipilih dan kode yang unik diberikan kepada setiap atribut.

c. *Batch controls*

Adalah proses pembentukan grup suatu transaksi yang memiliki hubungan satu dengan yang lain. Ada dua jenis *batch*, yaitu:

1) *Physical batches*

Adalah pengelompokkan transaksi pada unit fisiknya.

2) *Logical batches*

Adalah proses pengelompokkan transaksi dilakukan berdasarkan logika.

d. Validasi *input* data

Ada empat jenis data *input* validasi yang harus dicek ketika data dimasukkan pada terminal, yaitu:

1) *Field check*

Tes validasi yang dilakukan terhadap *field* tidak tergantung pada *field* lain dalam *input record* atau dalam *input record* lainnya.

2) *Record check*

Tes validasi yang dilakukan pada *field* tergantung pada hubungan logika *field* itu dengan *field* yang lain pada *record*.

3) *Batch check*

Tes validasi melakukan pengujian apakah karakteristik dari *batch record* yang dimasukkan sama dengan karakteristik yang telah ditetapkan pada *batch*.

4) *File check*

Tes validasi melakukan pengujian apakah karakteristik pada *file* yang digunakan selama *entry* data adalah sama dengan karakteristik data pada *file*.

5. Pengedalian Keluaran (*Output Control*)

Jenis-jenis pengendalian output adalah:

a. Batch output production and distribution controls

Batch output adalah *output* yang dihasilkan pada beberapa fasilitas operasional dan sesudah itu dikirim atau disimpan oleh *user output* tersebut. Kontrol terhadap *batch output* dilakukan dengan tujuan untuk memastikan bahwa laporan tersebut akurat, lengkap dan tepat waktu yang hanya dikirim atau diserahkan kepada organisasi kepada *user* yang berhak

b. *Batch report design controls*

Desain laporan yang baik harus berisi data-data berikut:

- Nama laporan
- Waktu dan tanggal laporan tersebut dibuat
- Jumlah lembar laporan
- Periode proses pembuatan laporan
- Program yang digunakan untuk pembuatan laporan (versi berapa)
- *Contact person*
- Klasifikasi sekuritas (*confidential* atau biasa)
- Tanggal retensi
- Metode penghancuran laporan
- Halaman

c. Online output production and distribution controls

Tujuan pengendalian ini adalah untuk memastikan bahwa *online output* hanya dapat dilihat oleh bagian yang berwenang dan proteksi terhadap kemungkinan terjadinya dan integritas dari *output* pada saat dilakukan pengiriman melalui media komunikasi.

2.3 Audit Sistem Informasi

2.3.1 Pengertian Audit

Menurut Arens dan Leobbecke (2003, h1), yang diterjemahkan oleh Amir Abadi Jusuf, ”Audit adalah proses pengumpulan dan pengevaluasian bahan bukti tentang informasi yang dapat diukur mengenai suatu entitas

ekonomi yang dilakukan oleh seorang yang kompeten dan independen untuk dapat menentukan dan melaporkan kesesuaian informasi dimana dengan kriteria yang telah ditetapkan".

Menurut Mulyadi & Puradireja (1998, h4), "Audit adalah suatu proses sistematik untuk memperoleh dan mengevaluasi bukti secara obyektif 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".

Secara umum pengertian di atas dapat diartikan bahwa audit adalah proses pengumpulan dan pengevaluasian bahan bukti tentang informasi yang dapat diukur mengenai suatu entitas ekonomi yang dilakukan oleh seorang yang kompeten dan independen untuk menetapkan tingkat kesesuaian antara pernyataan-pernyataan tersebut dengan kriteria yang telah ditetapkan, serta penyampaian hasil-hasilnya kepada pemakai yang berkepentingan.

2.3.2 Jenis-jenis Audit

Menurut Arens dan Leobbecke (2003, h4-5), yang diterjemahkan oleh Amir Abadi Jusuf, audit pada umumnya dibagi menjadi tiga golongan, yaitu audit pada umumnya dibagi menjadi tiga golongan, yaitu:

1. Audit laporan keuangan (*financial statement audit*) adalah untuk menentukan apakah laporan keuangan secara keseluruhan yang

merupakan informasi terukur yang akan diverifikasi telah disajikan sesuai dengan kriteria tertentu.

2. Audit kepatuhan (*compliance audit*) adalah mempertimbangkan apakah klien telah mengikuti prosedur atau aturan tertentu yang telah ditetapkan pihak yang memiliki otoritas lebih tinggi, misalnya pemeriksaan surat perjanjian dengan banyak dan atau kreditur lain untuk memastikan bahwa perusahaan tersebut telah memenuhi ketentuan hukum berlaku.
3. Audit operasional (*operational audit*) adalah penelaahan atas bagian manapun dari prosedur dan metode operasi suatu organisasi untuk menilai efisiensi dan efektifitasnya. Umumnya, pada saat selesainya audit operasional, auditor akan memberikan sejumlah saran kepada manajemen untuk memperbaiki jalannya operasi perusahaan.

2.3.3 Pengertian Audit Sistem Informasi

Audit sistem informasi merupakan proses pengumpulan dan pengevaluasian bukti-bukti untuk menentukan apakah sebuah sistem komputer telah menetapkan sistem pengendalian yang memadai, semua data dilindungi dengan baik atau tidak disalahgunakan serta terjaminnya integritas data, keandalan serta efektifitas dan efisiensi penyelenggaraan sistem informasi.

2.3.4 Tujuan Audit Sistem Informasi

Tujuan audit sistem informasi dapat disimpulkan secara garis besar terbagi menjadi 4 tahap yaitu:

1. Meningkatkan keamanan aset-aset perusahaan

   Aset informasi suatu perusahaan seperti perangkat keras (*hardware*), perangkat lunak (*software*), sumber daya manusia, file data harus dijaga oleh suatu sumber daya informasi yang baik agar tidak terjadi penyalahgunaan aset perusahaan.

2. Meningkatkan 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 laporan yang benar bahkan perusahaan dapat menderita kerugian.

3. Meningkatkan efektifitas sistem

   Efektifitas sistem informasi perusahaan memiliki peranan penting dalam pengambilan keputusan suatu sistem informasi dapat dikatakan efektif bila sistem informasi tersebut telah sesuai dengan kebutuhan *user*.

4. Meningkatkan efisiensi sistem

   Suatu sistem sebagai fasilitas pemrosesan informasi dikatakan efisien jika menggunakan sumber daya seminimal mungkin untuk menghasilkan *output* yang dibutuhkan.

2.3.5 Standar ISACA

Menurut Sanyoto Gondodiyoto dan Henny Hendarti (2007, h202), keahlian dan keterampilan minimal yang harus dilakukan agar dapat memenuhi persyaratan kompetensi profesional minimal dalam melaksanakan tugas audit diatur dalam standar profesional. Adapun standar audit sistem informasi disusun oleh *Information System Audit and Control Association* (ISACA), adalah sebagai berikut:

S1. *Audit Charter*

Perlunya dibuat *Audit Charter* atau *Letter of Engagement* dalam penugasan audit sistem informasi. Hal yang diatur tentang perlunya *audit charter* bagi audit internal (atau *letter of engagement* untuk auditor eksternal), mencakup *Responsibility, Authority, and Accountability*, yaitu meliputi tanggung jawab, otoritas, dan *accountability* dari fungsi audit sistem informasi pada suatu organisasi (perlu didokumentasikan dalam suatu surat keputusan pimpinan/perjanjian).

S2. *Independence*

a. *Pro Professional Independence*

Dalam permasalahan yang berkaitan dengan audit, auditor sistem informasi harus bersikap independen dalam tingkah laku dan tindakannya. Auditor atau Unit/Fungsi Audit harus mempunyai posisi independen terhadap pihak-pihak yang terkait dalam audit. (Untuk menjaga agar tidak terjadi *conflict of interest*).

b. *Organizational Relationship*

Fungsi audit sistem informasi harus berada independen dari area yang diaudit untuk mencapai tujuan objektivitas dari suatu proses audit.

S3. *Professional Ethics and Standards*

Auditor harus selalu mempedomani *professional ethics* dan *standards*.

a. Code of Professional Ethics

Auditor dari sistem informasi harus menghormati dan menaati etika profesional dari *Information System Audit and Control Association*.

b. Due Professional care

Standard auditing profesional harus diterapkan dalam segala aspek dalam pekerjaan yang dilakukan oleh auditor sistem informasi.

S4. *Professional Competence*

Auditor harus memiliki kompetensi yang dibutuhkan untuk melaksanakan tugasnya. Auditor sistem informasi harus memainkan kompetensi teknikal melalui pendidikan profesional berkelanjutan (*Continuing Professional Education*).

S5. *Audit Planning*

Auditor sistem informasi harus merencanakan kegiatan audit, agar tujuan audit tercapai sesuai standar profesional audit. Perencanaan audit (*audit planning*) diperlukan dalam tiap pelaksanaan suatu penugasan audit.

S6. Performance of Audit Work

1. *Supervision*

Staf dari audit sistem informasi harus tepat untuk dapat menjamin tujuan dari audit dijalankan dan *standard auditing professional* dapat terpenuhi. Pentingnya pengukuran kinerja audit *(performance of audit work).*

2. *Evidence*

Selama masa pekerjaan audit, auditor sistem informasi harus mendapatkan bukti yang tepat, dapat dipercaya, relevan dan berguna untuk mencapai tujuan objektif dari suatu audit.

S7. Reporting

Report Content and Form, auditor sistem informasi harus menyediakan *report* dalam bentuk yang tepat pada saat penyelesaian tugas audit. Laporan Audit berupa lingkup, tujuan, periode audit, dan lingkungan dimana audit dijalankan. Laporan audit harus mengidentifikasi permasalahan yang terjadi dalam jangka waktu audit. Laporan audit juga untuk memberikan rekomendasi dari layanan atau kualifikasi yang diberikan auditor terhadap tugas audit yang dijalankan.

S8. Follow Up Activities

Tindak lanjut atas rekomendasi temuan audit, auditor sistem informasi harus meminta dan mengevaluasi informasi yang sesuai dari penemuan yang terdahulu dan rekomendasi yang dihasilkan pada periode audit terdahulu untuk mendefinisikan tindakan yang tepat yang baru harus diimplementasikan dalam satu periode waktu.

S9. Irregularities of Audit Work

Hal-hal yang berkaitan dengan ketidakwajaran dan penyimpangan (*irregularities and illegal acts*).

S10. IT Governance

Hal-hal yang berkaitan dengan tata kelola teknologi informasi pada suatu organisasi/perusahaan, agar TI dikelola secara efektif, efisien, ekonomis, terjamin *integrity, security, availability, reralibility*, dan *continuity*.

S11. Use of Risk Assessment in Audit Planning

Teknik-teknik penaksiran risiko dalam perencanaan audit.

S12. Audit Materiality

Konsep materialitas dalam audit (khususnya audit sistem informasi).

S13. Using the Work of Other Expert

Penggunaan hasil audit lain (*expert* lainnya) dalam pelaksanaan audit.

S14. Audit Evidence

Hal-hal yang berkaitan dengan bukti audit.

2.3.6 COBIT(*Control Objectuves for Information & Related Technology)*

Menurut Sanyoto Gondodiyoto dan Henny Hendarti (2007, h158), COBIT merupakan panduan yang paling lengkap dari praktik-praktik terbaik untuk manajemen TI yang mencakup empat domain, yaitu: perencanaan & organisasi, akuisisi & implementasi, penyerahan & dukungan TI, dan monitor. COBIT *Framework* mencakup tujuan pengandalian yang terdiri dari 4 domain:

1. Perencanaan dan Organisasi (*Planning and Organization*)

   Yaitu mencakup pembahasan tentang identifikasi dan strategi investasi TI yang dapat memberikan yang terbaik untuk mendukung pencapaian tujuan bisnis. Selanjutnya identifikasi dan visi strategi perlu direncanakan, dikomunikasikan, dan diatur pelaksanaannya.

2. Perolehan dan Implementasi (*Acquisition and Implementation*)

   Yaitu untuk merealisasi strategi TI, perlu diatur kebutuhan TI, diidentifikasi, dikembangkan, atau diimplementasikan secara terpadu dalam proses bisnis perusahaan.

3. Penyerahan dan Pendukung (*Delivery and Support*)

   Domain ini lebih dipusatkan pada ukuran tentang aspek dukungan TI terhadap kegiatan operasional bisnis (tingkat jasa layanan TI aktual atau *service level*) dan aspek urutan (prioritas implementasi dan untuk pelatihannya).

4. *Monitoring*

   Yaitu semua proses TI yang perlu dinilai secara berkala agar kualitas dan tujuan dukungan TI tercapai, dan kelengkapannya berdasarkan pada syarat kontrol internal yang baik.

4 domain pada COBiT *Framework* tersebut selanjutnya dirinci menjadi 34 *high level control objectives* (dan selanjutnya dirinci ke dalam 215 *detail control objectives*), sebagai berikut:

1. *Planning and Organization*

1.1. *Define a Strategic IT Plan*

1.2. *Define the Information Architecture*

1.3. *Determine Technological Direction*

1.4. *Define the IT Processes, Organisation and Relationships*

1.5. *Manage the IT Investment*

1.6. *Communicate Management Aims and Direction*

1.7. *Manage IT Human Resources*

1.8. *Manage Quality*

1.9. *Assess and Manage IT Risks*

1.10. *Manage Projects*

2. *Acquisition & Implementation*

2.1. *Identify Automated Solutions*

2.2. *Acquire and Maintain Application Software*

2.3. *Acquire and Maintain Technology Infrastructure*

2.4. *Enable Operation and Use*

2.5. *Procure IT Resources*

2.6. *Manage Changes*

2.7. *Install and Accredit Solutions and Changes*

3. *Delivery & Support*

3.1. *Define and Manage Service Levels*

3.2. *Manage Third-party Services*

3.3. *Manage Performance and Capacity*

3.4. *Ensure Continuous Service*

3.5. *Ensure Systems Security*

3.6. *Identify and Allocate Costs*

3.7. *Educate and Train Users*

3.8. *Manage Service Desk and Incidents*

3.9. *Manage the Configuration*

3.10. *Manage Problems*

3.11. *Manage Data*

3.12. *Manage the Physical Environment*

3.13. *Manage Operations*

4. Monitoring

4.1. *Monitor and Evaluate IT Performance*

4.2. *Monitor and Evaluate Internal Control*

4.3. *Ensure Regulatory Compliance*

4.4. *Provide IT Governance*

Kriteria kerja COBiT meliputi:

- Efektifitas: untuk memperoleh informasi yang relevan dan berkelanjutan dengan proses bisnis seperti penyampaian informasi dengan benar, konsisten, dapat dipercaya dan tepat waktu.
- Efisiensi: memfokuskan pada ketentuan informasi melalui penggunaan sumber daya yang optimal.
- Kerahasiaan: memfokuskan proteksi terhadap informasi yang penting dari orang yang tidak memiliki hak otorisasi.

- Integritas: berhubungan dengan keakuratan dan kelengkapan informasi sebagai kebenaran yang sesuai dengan harapan dan nilai bisnis.
- Ketersediaan: berhubungan dengan informasi yang tersedia ketika diperlukan dalam proses bisnis sekarang dan yang akan datang.
- Kepatuhan: sesuai menurut hukum, peraturan, dan rencana perjanjian untuk proses bisnis.
- Keakuratan informasi: berhubungan dengan ketentuan kecocokan informasi untuk manajemen mengoperasikan entitas dan mengatur pelatihan keuangan dan kelengkapan laporan pertanggungjawaban.

2.3.7 Prosedur Audit

1. Inspeksi

   Merupakan pemeriksaan secara rinci terhadap dokumen dan kondisi fisik sesuatu.

2. Pengamatan (*observation*)

   Pengamatan atau observasi merupakan prosedur audit untuk melihat dan menyaksikan suatu kegiatan.

3. Permintaan Keterangan (*enquiry*)

   Merupakan prosedur audit yang dilakukan dengan meminta keterangan secara lisan.

4. Konfirmasi

   Konfirmasi merupakan bentuk penyelidikan yang memungkinkan auditor memperoleh informasi secara langsung dari pihak ketiga yang bebas.

5. Penelusuran (*tracing*)

   Penelusuran terutama dilakukan pada bahan bukti dokumenter. Dimana dilakukan mulai dari data awal direkamnya dokumen, yang dilanjutkan dengan pelacakan pengolahan data-data tersebut dalam proses akuntansi.

6. Pemeriksaan bukti pendukung (*vouching*)

   Pemeriksaan bukti pendukung merupakan prosedur audit yang meliputi:

   a. Inspeksi terhadap dokumen-dokumen yang mendukung suatu transaksi atau data keuangan untuk menetukan kewajaran dan kebenarannya.
   b. Pembandingan dokumen tersebut dengan catatan akuntansi yang berkaitan.

7. Perhitungan (*counting*)

   Prosedur audit ini meliputi perhitungan fisik terhadap sumber daya berwujud seperti kas, pertangungjawaban semua formulir bernomor urut tercetak.

8. *Scanning*

   Scanning merupakan penelaahan secara cepat terhadap dokumen, cacatan, dan daftar untuk mendeteksi unsur-unsur yang tampak tidak biasa yang memerlukan penyelidikan lebih mendalam.

9. Pelaksanaan ulang (*reperforming*)

   Prosedur audit ini merupakan pengulangan aktivitas yang dilaksanakan oleh klien.

10. *Computer-assisted audit techniques*

Apabila catatan akuntansi dilaksanakan dalam media elektronik maka auditor perlu menggunakan c*omputer-assisted audit techniques* dalam menggunakan berbagai prosedur audit di atas.

http://masgede.wordpress.com/2008/11/21/prosedur-audit-pekerjaan-atestasi/

2.3.8 Tahapan Perencanaan Audit Sistem Informasi

Ada lima tahap dalam Audit Sistem Informasi, yaitu:

1. Perencanaan Audit (*Planning the audit*)

   Perencanaan adalah tahap awal. Pada tahap ini auditor harus menentukan *preliminary* material untuk audit serta mencoba memperoleh pengertian mengenai pengendalian internal yang digunakan dalam organisasi.

2. Pengujian Pengendalian (*Tests of controls*)

   Auditor harus melakukan pengujian atas pengendalian tertentu untuk mengevaluasi apakah mereka beroperasi secara efektif.

3. Pengujian Transaksi (*Tests of transaction*)

   Auditor menjalankan pengujian substantif untuk mengevaluasi apakah ada kesalahan material atau salah penyajian dari akuntansi yang terjadi ataupun yang mungkin terjadi.

4. *Tests of balances or overall results*

   Auditor mencari untuk mendapatkan bukti cukup untuk membuat keputusan akhir tingkat kesalahan atau salah penyajian yang telah terjadi ataupun mungkin terjadi.

5. *Completion of the audit*

   Auditor memberikan opini apakah ada kesalahan material ataupun salah penyajian yang telah terjadi atau yang mungkin terjadi.

2.3.9 Metode Audit

Ada dua macam metode audit, yaitu:

1. *Auditing Around the Computer*

   Cara ini dapat dilakukan bila yang diaudit memenuhi kriteria, yaitu:

   a. Bisnis tersebut resikonya kecil
   b. Logikalnya sederhana; tidak ada rutin spesial yang dikembangkan untuk melakukan proses data.
   c. *Input* transaksi dilakukan dengan metode *batch* dan pengendalian dilakukan dengan metode tradisional, sebagai contoh pembagian tugas dan pengawasan dilakukan oleh pihak manajemen.
   d. Proses utama berisi pengurutan terhadap *input* dan *update master* file dilakukan secara berurutan
   e. Jejak audit jelas; laporan detil disiapkan sesuai dengan sistem
   f. Jenis penugasan relatif tetap dan sistem jarang diubah.

2. *Auditing Through the Computer*

   Auditor yang menggunakan cara ini menggunakan komputer untuk menguji:

   a. Logika proses dan pengendalian yang ada saat ini pada sistem.
   b. Produksi *record* oleh sistem

Audit jenis ini harus digunakan terhadap kasus:

1. Resiko dasar yang berhubungan dengan aplikasi sistem tinggi.
2. Proses aplikasi melibatkan *input* dalam jumlah besar begitu juga *output* yang dihasilkan, pengujian secara langsung terhadap validitas *input* dan *output* sudah dilakukan.
3. Bagian dari pengendalian internal dimasukkan pada sistem komputer, sebagai contoh, pada sistem *on-line* di bank, program komputer melakukan transaksi *batch* untuk setiap setiap *teller* untuk menghasilkan pengendalian total terhadap rekonsiliasi transaksi pada akhir hari.
4. Logika pemrograman pada aplikasi rumit.
5. Karena pertimbangan *cost-benefit*, jarak substantial yang nampak pada jejak audit terlihat pada sistem.

2.3.10 Instrumen Audit

Menurut Sanyoto Gondodiyoto dan Henny Hendarti (2006, h.447) terdapat berbagai teknik pemeriksaan yang bisa diterapkan dalam melaksanakan audit. Teknik-teknik pemeriksaan tersebut sering disebut dengan istilah instrumen audit. Berikut ini adalah contoh-contoh instrumen audit yang dapat digunakan pada saat pelaksanaan audit :

1. Observasi (*Observation*)

Observasi adalah cara memeriksa dengan menggunakan panca indera, terutama mata, yang dilakukan secara berkelanjutan selama kurun waktu tertentu untuk membuktikan suatu keadaan atau masalah.

2. Wawancara (*Interview*)

   Wawancara merupakan teknik pemeriksaan berupa tanya-jawab secara lisan antara auditor dengan *auditee* untuk memperoleh bahan bukti audit. Tanya-jawab dapat dilakukan secara lisan (wawancara) atau tertulis.

3. Kuisioner (*Quetionaire*)

   Teknik ini merupakan teknik pemeriksaan yang mudah dan praktis karena tertulis. Dengan metode ini, responden ditentukan, kemudian dikirimi surat pengantar beserta daftar pertanyaan (*questionaire*) tentang hal-hal yang ditanyakan dengan pedoman pengisian dan tanggal jawab yang ditentukan.

4. Inspeksi Fisik (*Physical Inspection*)

   Inspeksi merupakan cara memeriksa dengan memakai panca indera terutama mata, untuk memperoleh bukti atas suatu keadaan atau suatu masalah pada saat tertentu. Inspeksi merupakan usaha pemeriksaan untuk memperoleh bukti-bukti secara langsung ditempat dimana keadaan atau masalah ingin dibuktikan.

5. Prosedur analisis

   Analisis artinya memecah atau mengurai suatu masalah ke dalam beberapa bagian atau elemen dan memisahkan bagian tersebut untuk

digabungkan dengan keseluruhan atau dibandingkan dengan yang lain. Dengan analisis pemeriksa dapat melihat hubungan penting antara satu unsur dengan unsur lainnya.

6. Penelaahan Dokumen

   Pada teknik ini dilakukan penelaahan pada dokumen yang tersedia pada suatu organisasi, seperti bagan arus, bagan organisasi, manual program, manual operasi, manual referensi, notulen rapat, surat perjanjian dan catatan-catatan historis lainnya. Jika mungkin dokumen-dokumen penting harus ditelaah sebelum wawancara. Dokumentasi yang bermanfaat adalah diagram (*flowchart*/bagan alir) dan DFD (*data flow diagram*/diagram arus data). DFD menekankan pada hubungan arus data dan pemrosesan. DFD sangat sederhana dan mudah digunakan.

2.3.11 Penetapan Matriks Penilaian Resiko

Matriks penilaian resiko adalah suatu cara untuk menganalisa seberapa besar resiko yang ada dari suatu temuan audit. Hal ini dilakukan dengan cara menganalisa pengaruh dan korelasi antara tingkat dampak (*impact*) yang ditimbulkan dari suatu resiko dengan tingkat keterjadian (*likelihood*) dari resiko tersebut. Besarnya tingkatan dampak dan keterjadian suatu resiko dinyatakan sebagai berikut:

		Dampak		
		L ow	*Medium*	*High*
Keterjadian	*High*	3	6	9
	Medium	2	5	8
	Low	1	4	7

Penilaian dari matriks resiko terdiri dari:

- Jika dampak *Low* dan keterjadian *Low*, maka nilai resiko adalah 1.
- Jika dampak *Low* dan keterjadian *Medium*, maka nilai resiko adalah 2.
- Jika dampak *Low* dan keterjadian *High*, maka nilai resiko adalah 3.
- Jika dampak *Medium* dan keterjadian *Low*, maka nilai resiko adalah 4.
- Jika dampak *Medium* dan keterjadian *Medium*, maka nilai resiko adalah 5.
- Jika dampak *Medium* dan keterjadian *High*, maka nilai resiko adalah 6.
- Jika dampak *High* dan keterjadian *Low*, maka nilai resiko adalah 7.
- Jika dampak *High* dan keterjadian *Medium*, maka nilai resiko adalah 8.
- Jika dampak *High* dan keterjadian *High*, maka nilai resiko adalah 9.

2.4 Sistem Informasi Persediaan

2.4.1 Pengertian Sistem Informasi Persediaan

Menurut James A. Hall (2007, h9) yang diterjemahkan oleh Dewi Fitriasari dan Deny Arnos Kwary, "Sistem informasi (*informastion system*) adalah serangkaian prosedural formal di mana data dikumpulkan, diproses menjadi informasi dan didistribusikan ke para pengguna".

Menurut Mulyadi (2001, h112) , "*Inventory* atau persediaan terdiri dari barang dagangan yang dimaksudkan untuk diperjualbelikan serta bahan baku dan bahan pembantu yang dipakai dalam proses produksi barang yang akan dijual".

Dapat disimpulkan bahwa sistem informasi persediaan adalah sebuah rangkaian prosedur formal dimana data dikumpulkan tentang barang dagangan yang dimaksudkan untuk diperjualbelikan, diproses menjadi informasi untuk didistribusikan kepada para pemakai.

2.4.2 Fungsi Persediaan

Menurut Mulyadi (2001, h242) ada lima fungsi dari persediaan, yaitu :

1. Untuk melakukan pembatasan terhadap inflasi dan perubahan harga.
2. Untuk menghindari kekurangan stok yang dapat terjadi karena cuaca, kekurangan pasokan, masalah mutu, atau pengiriman yang tidak tepat.
3. Untuk memberikan suatu stok barang-barang agar dapat memenuhi permintaan yang diantisipasi akan timbul dari konsumen.
4. Untuk mengambil keuntungan dari potongan jumlah, karena pembelian dalam jumlah besar dapat secara substansial menurut biaya produk.
5. Untuk memasangkan produksi dengan distribusi. Misalnya, bila permintaan produknya tinggi hanya pada musim panas, suatu perusahaan dapat membentuk stok selama musim dingin sehingga biaya kekurangan stok dan kehabisan stok dapat dihindari.

2.4.3 Jenis Persediaan

Menurut Mulyadi (2001, h553), dalam perusahaan manufaktur terdapat tiga jenis persediaan, yaitu:

1. Persediaan barang jadi

   Yaitu persediaan yang telah selesai diproses atau diolah dalam pabrik dan siap untuk dipasarkan.

2. Persediaan barang dalam proses

   Yaitu persediaan yang merupakan keluaran dari bagian dalam proses produksi yang telah diolah menjadi suatu bentuk, tetapi perlu diproses lebih lanjut untuk menjadi barang jadi.

3. Persediaan bahan baku

   Yaitu persediaan barang berwujud yang digunakan dalam produksi, barang tersebut diperoleh dari sumber-sumber alam ataupun dibeli dari pemasok atau perusahaan lain.

4. Persediaan bahan penolong

   Yaitu persediaan yang diperlukan dalam proses produksi untuk membantu proses tersebut tetapi bukan merupakan komponen utama.

5. Persediaan suku cadang

   Yaitu persediaan yang terdiri dari suku cadang atau komponen-komponen rakitan yang menunjang proses produksi.

6. Persediaan bahan habis pakai pabrik.

   Yaitu persediaan yang diperlukan untuk menunjang proses produksi berupa sumber daya alam.

2.4.4 Metode Pencatatan Persediaan

Menurut Mulyadi (2001, h126) ada dua macam metode pencatatan persediaan, yaitu:

1. Metode mutasi persediaan (*Perpetual inventory method*)

   Dicatat dalam kartu persediaan, jika persediaan berkurang karena pemakaian tidak dicatat dalam kartu persediaan. Metode ini cocok digunakan dalam penentuan biaya bahan baku dalam perusahaan yang harga pokok produknya dikumpulkan dengan metode harga pokok pesanan

2. Metode persediaan fisik (*Physical inventory method*)

   Tambahan persediaan dari pembelian saja yang dicatat. Metode ini cocok digunakan dalam penentuan biaya bahan baku dalam perusahaan yang harga pokok produknya dikumpulkan dengan metode harga pokok pesanan.

2.4.5 Metode Penilaian Persediaan

Ada tiga metode dalam melakukan penelitian persediaan, yaitu:

1. Metode FIFO (*First in first out*)

   Metode ini didasarkan asumsi bahwa harga yang sudah terjual, dinilai menurut harga pembelian barang yang terdahulu (pertama) masuk. Dengan demikian, persediaan akhir dinilai menurut harga pembelian barang yang terakhir masuk.

2. Metode LIFO (*Last in first out*)

Metode ini didasarkan atas asumsi bahwa harga yang telah terjual dinilai menurut harga pembelian barang yang terakhir masuk sehingga persediaan yang masih ada dinilai berdasarkan harga pembelian barang yang terdahulu.

3. Metode Rata-Rata (*Weight average method*)

   Metode ini didasarkan atas harga rata-rata, dimana harga tersebut dipengaruhi jumlah barang yang diperoleh pada masing-masing harganya. Dengan demikian, persediaan dinilai berdasarkan harga rata-rata.

2.4.6 Fungsi Terkait

Menurut Mulyadi (2001, h581-582), fungsi yang terkait dalam sistem penghitungan fisik persediaan adalah:

1. Panitia penghitungan fisik persediaan.

   Panitia ini berfungsi untuk melaksanakan perhitungan fisik persediaan dan menyerahkan hasil perhitungan fisik tersebut kepada bagian kartu persediaan untuk digunakan sebagai dasar *adjustment* terhadap catatan persediaan dalam kartu persediaan. Seperti telah disebutkan diatas, panitia perhitungan fisik terdiri pemegang kartu, perhitungan, dan pengecekan.

2. Fungsi akuntansi

   Fungsi akuntansi bertanggung jawab untuk mencantumkan harga barang yang dihitung ke dalam hasil perhitungan fisik, mengalikan kuantitas dan harga barang yang tercantum dalam daftar hasil perhitungan fisik, mencantumkan harga total dalam daftar hasil perhitungan fisik,

melakukan *adjustment* terhadap kartu persediaan berdasarkan hasil perhitungan fisik persediaan, membuat bukti memorial untuk mencatat *adjusment* data persediaan dalam jurnal umum berdasarkan hasil perhitungan fisik persediaan.

3. Fungsi gudang.

   Fungsi gudang bertanggung jawab untuk melakukan *adjustment* data kuantitas persediaan yang dicatat dalam kartu gudang berdasarkan hasil perhitungan fisik persediaan

2.4.7 Prosedur Sistem Persediaan

Menurut Mulyadi (2001, h560-580), sistem dan prosedur bersangkutan dengan sistem akuntansi persediaan, yaitu:

1. Prosedur pencatatan produk jadi.

   Prosedur ini merupakan salah satu prosedur dalam sistem akuntansi biaya produksi. Dalam prosedur ini dicatat harga pokok jadi yang didebitkan ke dalam rekening Persediaan Produk Jadi dan dikreditkan ke dalam rekening Barang Dalam Proses.

2. Prosedur pencatatan harga pokok produk jadi yang dijual.

   Prosedur ini merupakan salah satu prosedur dalam sistem penjualan disamping prosedur lainnya, seperti: prosedur order penjualan, prosedur persetujuan kredit, prosedur pengiriman barang, prosedur penagihan, prosedur pencatatan piutang.

3. Prosedur pencatatan harga pokok produk jadi yang diterima kembali dari pembeli.

   Jika produk jadi yang telah dijual dikembalikan oleh pembeli, maka transaksi retur penjualan ini akan mempengaruhi persediaan produk jadi, yaitu menambah kuantitas produk jadi dalam kartu gudang yang diselenggarakan oleh bagian gudang dan menambah kuantitas dan harga pokok produk jadi yang dicatat oleh bagian kartu persediaan dalam kartu persediaan produk jadi.

4. Prosedur pencatatan tambahan dan penyesuaian kembali harga pokok persediaan produk dalam proses.

   Pencatatan persediaan produk dalam proses umumnya dilakukan oleh perusahaan pada akhir periode, pada saat dibuat laporan keuangan bulanan dan laporan keuangan tahunan. Pada awal periode akuntansi berikutnya, dibuat jurnal penyesuaian kembali (*readjusting entry*) untuk membalik jurnal pencatatan persediaan produk dalam proses yang dilakukan pada akhir periode tersebut di atas.

5. Prosedur pencatatan harga pokok persediaan yang dibeli.

   Prosedur ini merupakan salah satu prosedur yang membentuk sistem pembelian. Dalam prosedur ini dicatat harga pokok persediaan yang dibeli.

6. Prosedur pencatatan harga pokok persediaan yang dikembalikan kepada pemasok.

Jika persediaan yang telah dibeli dikembalikan kepada pemasok, maka transaksi retur pembelian ini akan mempengaruhi persediaan yang bersangkutan, yaitu mengurangi kuantitas persediaan dalam kartu gudang yang diselenggarakan oleh bagian gudang dan mengurangi kuantitas dan harga pokok persediaan yang dicatat oleh bagian kartu persediaan dalam kartu persediaan yang bersangkutan.

7. Prosedur permintaan dan pengeluaran barang gudang.

   Dalam prosedur ini dicatat harga pokok persediaan bahan baku, bahan penolong, bahan habis pakai pabrik, dan suku cadang yang dipakai dalam kegiatan produksi dan kegiatan non-produksi.

8. Prosedur pencatatan tambahan harga pokok persediaan karena pengembalian barang gudang.

   Transaksi pengembalian barang gudang mengurangi biaya dan menambah persediaan barang di gudang.

9. Sistem penghitungan fisik persediaan.

   Sistem penghitungan fisik persediaan umumnya digunakan oleh perusahaan untuk menghitung secara fisik persediaan yang disimpan di gudang, yang hasilnya digunakan untuk meminta pertanggungjawaban bagian gudang mengenai pelaksanaan fungsi penyimpanan, dan pertanggungjawaban bagian kartu persediaan mengenai keandalan catatan persediaan yang diselenggarakannya, serta untuk melakukan penyesuaian *(adjustment)* terhadap catatan persediaan di bagian kartu persediaan.

2.4.8 Dokumen yang digunakan

1. Bukti memorial

   Digunakan untuk mencatat tambahan kuantitas dan harga pokok persediaan produk jadi dalam kartu persediaan dan sebagai sumber dalam mencatat transaksi selesainya produk jadi dalam jurnal umum.

2. Surat order pengiriman

   Diterima oleh bagian gudang dari bagian order penjualan. Setelah bagian gudang mengisi surat order pengiriman tersebut dengan kuantitas produk jadi yang diserahkan kepada bagian pengiriman, atas dasar surat order pengiriman dalam kartu gudang.

3. Faktur penjualan.

   Digunakan untuk merekam berbagai informasi yang diperlukan oleh manajemen mengenai transaksi penjualan tunai

4. Memo kredit

   Digunakan oleh bagian kartu persediaan untuk mencatat kuantitas dan harga pokok produksi jadi yang dikembalikan oleh pembeli ke dalam persediaan.

5. Bukti memorial

   Digunakan sebagai dokumen sumber dalam mencatat *readjustment* persediaan harga pokok produk dalam proses.

6. Bukti kas keluar

   Digunakan sebagai dasar pencatatan tambahan kuantitas dan harga pokok persediaan ke dalam kartu persediaan.

7. Memo debit

   Digunakan oleh bagian kartu persediaan untuk mencatat kuantitas dan harga pokok persediaan yang dikembalikan kepada pemasok ke dalam kartu persediaan

8. Bukti permintaan dan pengeluaran barang gudang

   Digunakan oleh bagian gudang untuk mencatat pengurangan persediaan karena pemakaian intern dan sebagai dokumen sumber dalam pencatatan pemakaian persediaan ke dalam jurnal pemakaian bahan baku atau jurnal umum.

9. Bukti pengembalian barang gudang

   Digunakan oleh bagian gudang untuk mencatat tambahan kuantitas persediaan ke dalam kartu gudang, dipakai oleh bagian kartu persediaan untuk mencatat tambahan kuantitas dan harga pokok persediaan ke dalam kartu persediaan, untuk mencatat berkurangnya biaya ke dalam kartu biaya, dan untuk mencatat pengembalian barang gudang tersebut ke dalam jurnal umum

10. Kartu penghitungan fisik (*Inventoty Tag*)

    Digunakan untuk merekam hasil penghitungan fisik persediaan.

2.4.9 Informasi yang diperlukan

1. Laporan produk selesai

   Digunakan oleh bagian gudang untuk mencatat tambahan kualitas produk jadi dalam kartu gudang.

2. Laporan penerimaan barang

   Digunakan oleh bagian gudang untuk mencatat produk jadi yang diterima dari pembeli ke dalam kartu gudang dan sebagai dasar pencatatan tambahan kuantitas barang dari pembelian ke dalam kartu gudang.

3. Laporan pengiriman barang

   Digunakan oleh bagian gudang untuk mencatat kuantitas persediaan yang dikirimkan kembali kepada pemasok ke dalam kartu gudang.

4. Daftar hasil penghitungan fisik (*Inventory Summary Sheet)*

   Digunakan untuk meringkas data yang telah direkam dalam bagian ke-2 kartu penghitungan fisik.

2.4.10 Tujuan Audit Persediaan

Menurut Mulyadi & Puradireja (1998, h257) tujuan audit terhadap persediaan antara lain :

1. Memperoleh keyakinan tentang keandalan catatan akuntansi yang bersangkutan dengan persediaan.
2. Membuktikan asersi keberadaan persediaan yang dicantumkan di neraca dan keterjadian transaksi yang berkaitan dengan persediaan.
3. Membuktikan asersi kelengkapan transaksi yang berkaitan dengan persediaan yang dicatat dalam catatan akuntansi dan kelengkapan saldo persediaan yang disajikan di neraca.
4. Membuktikan asersi hak kepemilikan klien atas persediaan yang dicantumkan di neraca.

5. Membuktikan asersi penilaian persediaan yang dicantumkan di neraca.
6. Membuktikan asersi penyajian dan pengungkapan persediaan di neraca.

2.5 *Activity Diagram*

2.5.1 Pengertian Activity Diagram

Activity diagram adalah sebuah representasi grafik yang digunakan untuk menunjukan urutan aktifitas dalam suatu proses bisnis dengan tujuan untuk memahami proses bisnis tersebut

2.5.2 Jenis-jenis *Activity Diagram*

1. *Overview Activity Diagram*

   Overview Activity Diagram adalah diagram yang menampilkan gambaran *level* tertinggi dari proses bisnis dengan mencatat *events* kunci, urutan *events* tersebut dan aliran informasi diantara *events* itu.

2. *Detailed Activity Diagram*

   Detailed Activity Diagram adalah diagram yang menyediakan representasi yang lebih *detail* dari aktifitas-aktifitas yang ditampilkan pada *overview diagram*.