BAB 2

LANDASAN TEORI

2.1 Evaluasi

2.1.1 Pengertian Evaluasi

Menurut Kamus Besar Bahasa Indonesia (2002), "Evaluasi adalah proses penilaian yang sistematis, mencakup pemberian nilai, atribut, apresiasi, pengenalan masalah dan pemberian solusi atas permasalahan yang ditemukan".

2.2. Teori Umum

2.2.1 Pengertian Sistem

Menurut Mulyadi (2001, p.2), "Sistem adalah sekelompok unsur yang erat berhubungan satu dengan yang lainnya, yang berfungsi bersama-sama untuk mencapai tujuan tertentu".

Menurut James A. Hall (2001, p.5), "Sistem adalah sekelompok dua atau lebih komponen – komponen yang saling berkaitan atau subsistem – subsistem yang saling bersatu untuk mencapai tujuan yang sama".

Menurut James A.O'Brien (2005, p.29), "Sistem adalah sekelompok komponen yang saling berhubungan, bekerja sama untuk mencapai tujuan bersama dengan menerima *input* serta menghasilkan *output* dalam proses transformasi yang teratur".

Jadi dapat disimpulkan bahwa sistem adalah kumpulan dari komponen – komponen yang saling berhubungan satu dengan yang lainnya membentuk satu kesatuan untuk mencapai tujuan tertentu.

2.2.2 Pengertian Informasi

Menurut McLeod (2001, p12), "Informasi adalah data yang diproses, atau data yang sudah memiliki arti tertentu bagi kebutuhan penggunanya".

Menurut McLeod (2004, p10), "*information is processed data that is meaningful; it usually tells the user something that she or he did not already know*". (Informasi adalah data yang diproses yang mempunyai arti; informasi biasanya memberitahukan pengguna akan sesuatu yang belum pernah di ketahui).

Menurut O'Brien (2003, p3), "*information is data that have been converted into a meaningful and useful contex for specific end users*". (Informasi adalah data yang telah diubah menjadi isi yang bermakna dan berguna untuk pengguna khusus).

Jadi dapat disimpulkan bahwa informasi adalah data yang sudah diproses atau sudah mempunyai arti dan berguna untuk pengguna khusus.

2.2.3 Karakteristik Informasi

Menurut *COBIT* (*Control Objective for Information and Related Technology*) (4.0, p11) dalam kaitan dengan tujuan bisnis organisasi, *COBIT* menetapkan ada tujuh syarat untuk kriteria informasi yang mutlak harus dimiliki

oleh setiap keluaran dari proses teknologi informasi. Ketujuh syarat informasi tersebut adalah:

1. **Efektifitas**: Relevansi informasi terhadap proses bisnis dengan pengiriman informasi yang tepat waktu, benar dan konsisten
2. **Efisiensi**: Pengadaan informasi yang memenuhi syarat dengan penggunaan sumber daya yang optimal, baik secara ekonomis maupun produktifitas.
3. **Kerahasiaan**: Perlindungan informasi sensitif terhadap akses yang tidak berwenang
4. **Integritas**: Akurasi dan keutuhan informasi saat dibutuhkan
5. **Ketersediaan**: Ketersediaan informasi saat dibutuhkan
6. **Kesesuaian/Kepatuhan**: Ketaatan pada hukum, peraturan dan perjanjian terkait dengan bisnis
7. **Kehandalan**: Pengadaan informasi yang benar bagi manajemen untuk kepentingan pelaporan.

2.2.4 Pengertian Sistem Informasi

Menurut Turban, Rainer, Potter (2003, p15) Sistem Informasi adalah mengumpulkan, memproses, menyimpan, meneliti, dan menghamburkan informasi untuk suatu tujuan spesifik yang memproses masukan dan menghasilkan keluaran yang dikirim kepada pemakai atau kepada sistem itu sendiri.

Menurut O'Brien (2003, p7), "*information systems can be any organized combination of people, hardware, software, communications networks, and data resource that collects, transforms, and disseminates information in an*

organization". (Sistem informasi dapat diorganisasikan dengan mengkombinasikan manusia, *hardware*, *software*, jaringan komunikasi dan sumber daya data dimana informasi dikumpulkan, ditransformasikan dan disebarkan dalam organisasi).

Jadi dari beberapa pendapat diatas dapat disimpulkan bahwa Sistem Informasi adalah kumpulan dari komponen – komponen yang saling terintegritas dan terpadu dalam mengolah data menjadi informasi yang dibutuhkan untuk perencanaan dan pengambilan keputusan dalam rangka usaha untuk mencapai tujuan strategis perusahaan.

2.3 Standard *COBIT*

2.3.1 Pengertian *COBIT*

COBIT adalah kerangka kerja dan seperangkat alat yang dimana dapat membantu manajemen, auditor dan pengguna dalam menjembatani *gap* antara risiko bisnis, kebutuhan *control*, dan masalah – masalah teknis IT dan mengkomunikasikannya kepada *stakeholder*.

2.3.2 Teori *COBIT*

Bilangan dari pengendalian kerangka kerja dikembangkan untuk membantu perusahaan dalam mengembangkan sistem pengendalian yang baik. Dalam bagian ini kami mendiskusikan tiga dari yang terpenting.

2.3.2.1 Kerangka kerja COBIT

The Information System Audit and Control Fondation (ISACAF) dikembangkan untuk kerangka kerja *COBIT*. *COBIT* adalah kerangka kerja yang dapat diaplikasikan secara umum untuk keamanan sistem informasi dan pengendalian yang digunakan untuk pengendalian IT. Kerangka kerja meliputi:

(1) Mengatur untuk memberikan standar keamanan dan pengendalian yang digunakan di dalam lingkungan IT.

(2) Pengguna dari layanan IT meyakinkan dimana keamanan dan pengendalian yang ada sudah memadai.

(3) Para auditor membuktikan pendapat mereka untuk pengendalian internal dan untuk memberi saran di dalam pengendalian dan keamanan IT.

Kerangka kerja mengalamatkan keluaran dari pengendalian yang dimana berasal dari 3 point dimensi – dimensi :

1. Tujuan bisnis, untuk memuaskan tunjuan bisnis, informasi harus memenuhi kriteria yang disebut keperluan-keperluan bisnis. Kriteria dibagi menjadi 7 kategori, dimana dipetakan di dalam tujuan *COSO* yaitu: efektifitas (relevan, dan tepat waktu), efesiensi, kerahasiaan, integritas, ketersedian, kesesuain atau kepatuhan terhadap peraturan dan kehandalan.
2. Sumber daya IT ini termasuk orang, aplikasi, sistem, teknologi, fasilitas dan data.
3. Proses IT, ini dibagi kedalam 4 daerah : perencanaan dan organisasi,

pengadaan dan implementasi, pengantaran dan dukungan, pengawasan dan evaluasi.

Cobit, dimana menyatukan standar dari 30 sumber yang berbeda kedalam kerangka kerja *single*, mempunyai dampak yang besar di dalam profesi sistem informasi. Dimana itu membantu para manager mempelajari bagaimana menyeimbangkan antara risiko dan pengendalian di dalam lingkungan sistem informasi. Yang menyediakan bagi para pengguna dimana meyakinkan keamanan dan pengendalian IT yang disediakan oleh bagian internal dan pihak meraka telah memadai. Itu mengarahkan auditor di dalam pemberian bukti untuk opini mereka dan ketika mereka menyediakan saran kepada managemen dalam pengendalian internal.

2.4 Audit

2.4.1 Pengertian Audit

Menurut Mulyadi (1998, p7) "*Auditing* 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 tersebut dengan kriteria yang telah ditetapkan, serta penyampaian hasil-hasilnya kepada pemakai yang berkepentingan".

Menurut James A. Hall (2001, p42), "*Auditing* adalah salah satu bentuk pengujian *independen* yang dilakukan oleh seorang auditor yang menunjukkan pendapatnya, tentang kejujuran laporan keuangan".

Jadi dapat disimpulkan bahwa pengertian audit adalah kegiatan memperoleh dan mengevaluasi bukti audit oleh auditor berdasarkan standar atau kinerja yang telah ditetapkan untuk menghasilkan laporan keuangan yang jujur.

2.4.2 Jenis – jenis Audit

Menurut Amir Abadi Jusuf (2003, p4), jenis – jenis audit antara lain :

1. Audit Laporan Keuangan

   Bertujuan menentukan apakah laporan keuangan secara keseluruhan merupakan informasi terukur yang akan diverifikasikan, telah disajikan sesuai dengan kriteria tertentu.

2. Audit Operasional

   Merupakan penelahaan atas bagian maupun dari prosedur dan metode operasi suatu organisasi untuk menilai efisiensi dan efektifitasnya.

3. Audit Ketaatan

   Bertujuan mempertimbangkan apakah *auditee* atau klien telah mengikuti prosedur atau aturan tertentu yang telah ditetapkan pihak yang memiliki otoritas yang lebih tinggi.

2.4.3 Standard Audit

Menurut Mulyadi (1998, p15), Jenis – jenis standard audit adalah :

1) Standard Umum

   - Audit harus dilaksanakan oleh seorang atau lebih yang memiliki keahlian dan pelatihan teknis yang cukup sebagai auditor.
   - Dalam semua hal yang berhubungan dengan penugasan, independensi

dalam sikap mental harus dipertahankan oleh auditor.

- Dalam pelaksanaan audit dan penyusunan laporannya, auditor wajib menggunakan kemahiran profesionalnya dengan cermat dan seksama.

2) Standard Pekerjaan Lapangan

- Pekerjaan harus direncanakan sebaik-baiknya dan jika digunakan asisten harus disupervisi dengan semestinya.
- Pemahaman yang memadai atas struktur pengendalian *intern* harus diperoleh untuk merencanakan audit dan menentukan sifat, waktu dan lingkup pengujian yang akan dilakukan.
- Bahan bukti kompeten yang cukup harus diperoleh melalui inspeksi, pengamatan, pengajuan pertanyaan, dan konfirmasi sebagai dasar yang memadai untuk menyatakan pendapat atas laporan keuangan yang diaudit.

3) Standard Pelaporan

- Laporan audit harus menyatakan apakah laporan keuangan telah disusun sesuai dengan prinsip akuntansi diterima secara umum.
- Laporan audit harus menunjukkan keadaan yang di dalamya prinsip akuntansi tidak secara konsisten diterapkan dalam penyusunan laporan keuangan periode berjalan dalam hubungannya dengan prinsip akuntansi yang diterapkan dalam periode sebelumnya.
- Pengungkapan informatif dalam laporan keuangan harus dipandang memadai, kecuali dinyatakan lain dalam laporan audit.

- Laporan audit harus memuat suatu pernyataan pendapat mengenai laporan keuangan secara keseluruhan tidak dapat diberikan, maka alasannya harus dinyatakan.

2.4.4 Instrumen Audit

Menurut Weber, R (1999, p789-801), instrumen audit yang digunakan untuk mengumpulkan data :

a. Wawancara

Dalam audit, auditor menggunakan teknik *interview* atau wawancara dengan beberapa alasan:

- Sistem analisa dan programmer yang mendesain dan mengimplementasikan sistem aplikasi dapat di wawancara sehingga audior lebih mengerti akan fungsi dan kontrol sistem.
- *User* juga dapat di wawancara untuk menjelaskan seberapa besar kualitas dari sistem yang mereka gunakan.
- Pengendalian organisasi dapat di wawancara untuk mengidentifikasikan sistem yang kritis yang terdapat di dalam organisasi.

b. *Check List*

Adalah membuat daftar pertanyaan yang ditujukan kepada pihak yang terkait di perusahaan, khususnya bagian penjualan untuk mengetahui kondisi yang sebenarnya.

c. Observasi

Adalah cara memeriksa dengan mengunakan panca indera terutama mata, yang dilakukan secara berulang - ulang selama kurun waktu tertentu untuk membuktikan sesuatu keadaan atau masalah.

2.5 Audit Sistem Informasi

2.5.1 Pengertian Audit Sistem Informasi

Menurut Weber, R. (1999, p10), *"Information systems auditing is the process of collecting and evaluating evidence to determine wheter a computer system safeguards assets, maintains data integrity, allows organizational goals to be achieved effectively, and users resources efficienty"*. (Audit Sistem Informasi adalah proses pengumpulan dan pengevaluasian bukti – bukti untuk menentukan apakah sistem aplikasi komputerisasi telah menetapkan dan menerapkan sistem pengendalian intern yang memadai, semua aktiva dilindungi dengan baik untuk menjamin integritas data, keandalan serta efektifitas dan efisiensi penyelenggaraan sistem informasi berbasis komputer tersebut).

2.5.2 Tujuan Audit Sistem Informasi

Menurut Weber, R. (1999, p11-13), tujuan Audit Sistem Informasi adalah:

1) Meningkatkan objektifitas keamanan *asset* perusahaan

   Asset perusahaan seperti perangkat keras (*hardware*), perangkat lunak (*software*), sumber daya manusia, dan *file* data harus mempunyai sistem pengendalian *intern* yang baik agar tidak terjadi penyalahgunaan *asset* perusahaan.

2) Meningkatkan objektifitas integritas data

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

3) Meningkatkan objektifitas efektifitas sistem

   Efektifitas sistem informasi perusahaan memiliki peranan dalam pengambilan keputusan. Suatu sistem informasi dapat dikatakan efektif apabila suatu sistem sudah sesuai dengan kebutuhan *user*.

4) Meningkatkan efisiensi sistem

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

2.5.3 Dasar Audit Sistem Informasi

Menurut Weber, R (1999, p18), "Audit Sistem Informasi bukan hanya suatu eksistensi yang sederhana dari audit tradisional, pengenalan akan kebutuhan untuk fungsi audit sistem informasi datang dari 2 arah. Pertama, auditor menyadari bahwa komputer telah mempengaruhi kemampuannya untuk menampilkan fungsi atestasi. Kedua, baik perusahaan dan manajemen sistem informasi mengetahui bahwa komputer adalah sumber daya yang berharga yang perlu diatur seperti sumber daya kunci lainnya dalam organisasi".

2.5.4 Jenis Audit Sistem Informasi

Menurut Weber, R (1999, p106-107), jenis – jenis Audit Sistem Informasi adalah sebagai berikut:

1) Audit secara bersamaan (*Concurrent Audit*)

   Auditor merupakan anggota dari tim pengembangan sistem, mereka membantu tim dalam meningkatkan kualitas dari pengembangan untuk sistem spesifik yang mereka bangun dan akan diimplementasikan.

2) Audit setelah impelementasi (*Post Implementation* Audit)

   Auditor membantu organisasi untuk belajar dari pengalaman pengembangan dari sistem aplikasi. Mereka mengevaluasi apakah sistem perlu dihentikan, dilanjutkan atau di modifikasi.

3) Audit Umum (*General Audit*)

   Auditor mengevaluasi kontrol pengembangan sistem secara keseluruhan, memberi *opini* audit tentang pernyataan keuangan ataupun tentang keefektifan dan keefisienan sistem.

2.5.5 Metode Audit Sistem Informasi

Menurut Weber, R (1999, p56-57), metode Audit Sistem Informasi meliputi:

1) *Audit Around the Computer*

   Auditing around the computer terlibat dengan penerimaan pendapat audit selama memeriksa dan mengevaluasi *control* manajemen kemudian *input* dan *output* hanya untuk sistem aplikasi. Berdasarkan kualitas pemrosesan dan sistem aplikasi, pemrosesan sistem aplikasi tidak diperiksa secara langsung. Selain itu, auditor memandang komputer sebagai *black box*. Auditor hanya dapat melakukan metode itu untuk mendapatkan biaya termurah untuk melakukan audit. Keadaan dapat dipulihkan kembali jika sistem aplikasi mempunyai tiga karakteristik berikut :

1. Sistem harus sederhana dan berorientasi pada sistem *batch*. Pada umumnya, sistem *batch* komputer merupakan suatu pengembangan langsung dari sistem *manual*. Sistem *batch* itu harus mempunyai kriteria sebagai berikut :
   a. Risiko yang ada harus rendah. Risiko itu tidak dapat dikelompokan dengan subjek kesalahan material akibat ketidakberesan dan ketidakefisienan dalam beroperasi.
   b. Logika sistem harus tepat sasaran. Tidak ada *rutinitas* (kegiatan) yang dikembangkan untuk mengizinkan komputer untuk memproses data.
   c. Transaksi *input* dilakukan dengan sistem *batch* dan kontrol dipelihara dengan metode tradisional.
   d. Proses utama terdiri dari penyelesaian *input* data dan memperbaruhi *file master* secara terus-menerus.
   e. Adanya jejak audit yang jelas. Laporan terperinci dipersiapkan pada kunci pokok dalam sistem
   f. Jadwal pekerjaan relatif sangat stabil dan sistem jarang dimodifikasikan.
2. Sering kali keefisienan biaya dalam metode *audit around the computer* pada saat aplikasi yang digunakan untuk keseragaman kemasan dalam program *software.*
3. Auditor harus menggunakan metode *audit around the computer* pada pengguna lebih tinggi daripada sistem kontrol komputer untuk menjaga perawatan keintegrasian data dan mencapai tujuan keefektifan dan keefisienan sistem. Biasanya, metode *auditing around the computer*

adalah pendekatan yang sederhana yang berhubungan dengan audit dan dapat dipraktekan oleh auditor yang mempunyai pengetahuan teknik yang sedikit tentang komputer.

2) *Audit Through the Computer*

Untuk banyak bagian, auditor terlibat dalam metode *audit through the computer* harus digunakan pada kasus proses logis dan adanya kontrol dalam sistem.

3) *Audit With the Computer*

Audit With the Computer adalah pendekatan audit dengan menggunakan bantuan dalam berbagai bentuk, misalnya : pengetikan laporan, penjadwalan, penyusunan rencana kerja audit, penyusunan kertas kerja pemeriksaan, dan lainnya.

2.5.6 Tahapan Audit Sistem Informasi

Menurut Weber, R (1999, p47-55) audit terdiri dari 5 tahap sebagai berikut :

1. *Planning the audit*

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

2. *Test of Control*

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

3. *Test of Transaction*

Auditor menggunakan *test of transaction* untuk mengevaluasi apakah kesalahan atau proses yang tidak sesuai dengan ketentuan telah mengarah pada kesalahan material informasi keuangan. Biasanya *Test Of Transaction* meliputi menelusuri jurnal masukkan sampai pada dokumen sumber, memeriksa daftar harga, dan pengujian kekuratan perhitungan.

4. *Test Of Balances or Overall Result*

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

5. *Completion of The Audit*

   Pada tahap audit, auditor kemudian harus merumuskan *opini* tentang kehilangan material dan keabsahan pernyataan laporan muncul dan membuat sebuah laporan. Standar laporan yang berlaku dibeberapa Negara terdiri dari 4 jenis *opini* sebagai berikut:

   a. *Disclamer of Opinion*

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

   b. *Adverse Opinion*

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

   c. *Qualified Material*

Auditor menyimpulkan bahwa kehilanhan telah muncul / kesalahan laporan secara material telah ada tetapi tidak besar / material.

d. *Unqualified Opinion*

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

2.6 Sistem Pengendalian *Internal*

2.6.1 Pengertian Sistem Pengendalian *Internal*

Menurut Weber, R (1999, p35), Pengendalian adalah suatu sistem untuk mencegah, mendeteksi dan mengkoreksi kejadian yang timbul saat transaksi dari serangkaian pemrosesan yang tidak terotorisasi secara sah, tidak akurat, tidak lengkap, mengandung redudansi, tidak efisien dan efektif. Dengan demikian, tujuan dari pengendalian adalah untuk mengurangi risiko atau mengurangi pengaruh yang sifatnya merugikan akibat suatu kejadian (penyebab).

Berdasarkan pengertian diatas maka pengendalian dapat dikelompokan menjadi tiga bagian :

1) *Preventive Control*

Pengendalian ini digunakan untuk mencegah masalah sebelum masalah itu muncul.

2) *Detective Control*

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

3) *Corrective Control*

Pengendalian ini digunakan untuk memperbaiki masalah yang ditemukan pada pengendalian *detective*. Pengendalian ini mencakup prosedur untuk menentukan penyebab masalah yang timbul, memodifikasikan sistem proses. Dengan demikian bias mencegah kejadian yang sama dimasa mendatang.

Menurut Mulyadi, Puradiredja (1998, p171), pengendalian *internal* adalah suatu proses yang dijalankan oleh dewan komisaris, manajemen, dan personil lain, yang didesain untuk memberikan keyakinan memadai tentang pencapaian tiga golongan tujuan, yaitu keandalan pelaporan keuangan, kepatuhan terhadap hukum dan peraturan yang berlaku, dan efektivitas dan efisiensi operasi.

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

Menurut Arrens (2005, p270), *"Internal control is that related to the realibility of financial reporting, is important to the auditr's purpose"*. (Pengendalian *internal* adalah berhubungan dengan kehandalan laporan keuangan, yang penting bagi tujuan auditor).

Jadi pengendalian *internal* secara normal meliputi prosedur pengendalian yang dirancang untuk menyediakan manajemen dengan tingkat

jaminan bahwa informasi yang disajikan oleh sistem informasi dapat dipercaya dan dapat disajikan tepat waktu.

2.6.2 Komponen Sistem Pengendalian *Internal*

Menurut Weber, R (1999, p49), sistem pengendalian *internal* terdiri dari 5 komponen yang berhubungan sebagai berikut:

1) Lingkungan Pengendalian

   Elemen ini memperlihatkan bahwa hal yang tergantung pada pengendalian terutama pada sistem akuntansi pada prosedur harus dijalankan.

2) Penilaian Risiko

   Elemen ini mengidentifikasi dan menganalisa risiko yang dihadapi organisasi dengan cara risiko tersebut dikelolah.

3) Aktivitas Pengendalian

   Elemen ini memastikan bahwa setiap transaksi telah diotorisasi oleh yang berwenang, telah ada pemisahan fungsi, dokumentasi dan pencatatan yang memadai, harta dan catatan telah diamankan dan pengecekan oleh pihak *independent* telah dilakukan serta penilaian terhadap pencatatan telah dilaksanakan.

4) Informasi dan Komunikasi

   Pada elemen ini informasi diidentifikasikan, diambil dan diubah sepanjang waktu dan menyediakan formulir untuk memperbolehkan karyawan mengubah tanggung jawabnya.

5) Pengawasan

Elemen yang berfungsi untuk memastikan bahwa pengendalian *internal* telah berjalan dengan baik.

Dalam setiap pemeriksaan auditor harus memperoleh pemahaman yang memadai atas masing-masing dari ke lima unsur tersebut diatas untuk merencanakan audit dengan cara melaksanakan prosedur untuk memahami rancangan kebijakan dan prosedur yang relevan dengan perencanaan audit dan untuk menentukan apakah rancangan tersebut dilaksanakan.

Hal tersebut sesuai dengan standar pekerja lapangan yang ke dua yaitu:

- Otorisasi yang benar atas transaksi dan aktivitas

  Karyawan melakukan tugas dan membuat keputusan yang mempengaruhi *asset - asset* perusahaan karena manajemen tidak mempunyai waktu dan sumber daya untuk mengawasi setiap kegiatan dan keputusan yang dibuat. Mereka mempunyai kebijakan bagi karyawan untuk mengikuti dan memaksa mereka untuk melakukan pekerjaan yang sesuai dan teratur. Pemaksaan ini disebut sebagai otorisasi. Otorisasi sering didokumentasikan dengan menandatangani, memulai, atau memasukkan kode otorisasi pada dokumen transaksi *record*.

- Pemisahan atau pembagian tugas

  Pengendalian *internal* yang baik mengharuskan seorang karyawan tidak diberikan telalu banyak tanggung jawab.

- Rancangan dan pemakaian dokumen yang baik dan benar

Penggunaan dan perancangan dokumen dan *record* yang benar membantu untuk memastikan keakuratan dan kelengkapan *record* dari semua data transaksi yang relevan.

- Perlindungan atas *asset* dan *record* yang baik

  prosedur berikut ini melindungi *asset* dari pencurian, penggunaan dari pihak yang tidak berwenang, perusakan, selain itu juga:

  - Mengawasi karyawan dan pemisahaan tugas
  - Memelihara ketepatan *record* dari *asset*, termasuk informasi
  - Membatasi akses fisik pada *asset*
  - Memproteksi *record* dan dokumen-dokumen
  - Mengendalikan lingkungan
  - Membatasi akses ke ruang komputer, *file* komputer dan informasi

- Pemeriksaan *independent* atas kinerja

  Pemeriksaan *internal* untuk memastikan transaksi diproses secara akurat merupakan elemen pengendalian yang penting. Pemeriksaan ini seharusnya dilakukan secara *independent* karena biasanya lebih efektif bila dilakukan oleh orang yang bertanggung jawab pada bagian opersional tersebut.

2.6.3 Jenis-jenis Pengendalian *Internal*

2.6.3.1 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 data

yang dicatat, diolah, dan dilaporkan secara akurat, tepat waktu dan sesuai dengan kebutuhan manajemen.

Pengendalian aplikasi meliputi:

1. Pengendalian *Boundary*

   Weber, R (1999, p370-405), menyebutkan bahwa subsistem *boundary* membangun hubungan antara yang akan menjadi pengguna sitem komputer dan sistem komputer itu sendiri. Pengendalian dalam subsistem *boundary* mempunyai tiga tujuan:

   1. Untuk memastikan bahwa pemakai komputer adalah orang yang mempunyai wewenang.
   2. Untuk memastikan bahwa identitas yang diberikan oleh pemakai adalah benar.
   3. Untuk membatasi tindakan yang dapat dilakuakan pemakai untuk menggunakan komputer ketika melakukan tindakan otorisasi.

   Tipe pengendalian yang berhubungan dengan pengendalian subsistem *boundary*:

   a. *Cryptographic Control*

      Kontrol *cryptographic* dirancang untuk mengamankan data pribadi dan untuk menjaga modifikasi oleh orang yang tidak berwenang, cara ini dilakukan dengan cara mengecek data sehingga tidak memiliki arti bagi orang yang tidak dapat menguraikan data tersebut.

   b. *Acces Control*

      Jenis kontrol yang digunakan pada subsistem *boundary* adalah control

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

c. *Personel Indetification Numbers*

PIN adalah teknik yang digunakan secara luas untuk mengidentifikasikan orang, sebuah *PIN* merupakan *password* yang sederhana, itu biasa merupakan nomor rahasia seseorang yang berhubungan dengan orang tersebut, melayani memverifikasi keontetikan orang. *PIN* digunakan oleh intitusi keuangan seperti untuk kartu *ATM*, kartu *debit*. Secara umum cara kerjanya adalah pemakai menggesekan kartunya pada sebuah alat dan mengisi *PIN* pada *PIN key pad.*

d. *Digital Signatures*

Jika berita atau kontrak dibuat dalam bentuk formulir elektronik maka tanda tangan yang biasa dilakukan pada kontrak biasa tidak dapat dilakukan untuk mengantisipasi hal tersebut dibuatlah tanda tangan *digital*. *Digital signature* ini terdiri dari rangkaian 0 dan 1 yang terdapat pada halaman.

e. *Plastic card*

Bila *PIN* dan *Digital signature* digunakan untuk keperluan pembuktian keaslian, kartu plastik digunakan untuk keperluan identifikasi. Pengendalian disekitar kartu plastik, bagaimanapun unsur penting dari

keseluruhan latihan pengendalian *boundary* dalam beberapa tipe dari sistem.

f. *Audit Trail Control*

Diketahui ada dua jenis jejak audit yang harus ada pada subsistem yaitu:

1. Jejak audit akuntansi untuk menjaga catatan setiap kejadian pada subsistem.
2. Jejak audit operasional untuk menjaga catatan pemakaian sumber daya yang berhubungan dengan setiap kejadian pada subsistem.

g. *Exsistence Control*

Jika subsistem pada *boundary* tidak berhasil, kemungkinan pemakaian sistem komputer tidak dapat mengadakan hubungan dengan sistem. Kegagalan dapat terjadi pada setiap komponen subsistem sebagai contoh: sirkuit terminal bias rusak, *sotfware* akses kontrol bisa rusak, dan lain-lain.

2. Pengendalian *Input*

Menurut Weber, R (1999, p420-456), komponen dalam subsistem *input* bertanggung jawab untuk membawa data dan instruksi kedalam sistem informasi. Data dapat di *input* kedalam sistem informasi dengan berbagai cara. Tipe metode *input* data yang digunakan dalam sistem informasi mempengaruhi keamanan data, integritas data, efektifitas sistem, dan tujuan efesiensi sistem.

Tipe pengendalian yang berhubungan dengan pengendalian *input*:

a. *Data input Methods*

Mengingat bahwa cara yang dilakukan auditor untuk mengevaluasi *control* terhadap sistem aplikasi adalah dengan menelusui jenis-jenis transaksi pada sistem, maka untuk dapat melakukan tugas itu dengan baik mereka harus mengerti bagaimana cara sistem tersebut bekerja terutama pada proses *input* data. Dengan cara memahami metode *input* data yang digunakan pada aplikasi maka auditor dapat mengembangkan cara pengendalian terhadap kekuatan maupun kelemahan dari *input* subsistem tersebut.

b. *Source Document design*

Beberapa dokumen data menggunakan dokumen sumber untuk mencatat data yang akan dimasukkan pada komputer. Sumber daya dokumen digunakan bila terdapat interval waktu antara waktu terjadinya data dengan waktu *input* berbeda. Proses desain sumber data dimulai setelah analisis terhadap sumber daya yang telah dilakukan, apa saja data yang akan direkam pada sumber data tersebut, bagimana cara data tersebut direkam, siapa yang akan merekam data, bagaimana data tersebut disiapkan dan dimasukkan dalam komputer dan bagaimana data tersebut ditangani, disimpan dan diarsip

c. *Data entry screen disgn*

Jika data dimasukkan ke dalam monitor, maka diperlukan desain yang berkualitas terhadap layar tampilan masukkan data agar mengurangi kemungkinan terjadinya kesalahan dan agar tercapaianya efesiensi dan efektifitas masukkan data pada subsistem *input.*

d. *Data code control*

Data kode memiliki dua tujuan, yaitu:

1. Sebagai identitas yang unik,

2. Untuk keperluan identifikasi

e. *Check Digits*

Pada beberapa kasus kesalahan pengetikan data dapat berdampak serius. Pengendalian data yang digunakan untuk menjaga terjadinya kesalahan adalah dengan melakukan *check digit. Check digit* ini biasanya digunakan pada berbagai aplikasi untuk mendeteksi kesalahan, seperti pada proses kartu kredit, proses rekening bank dan lain-lain.

f. *Batch Controls*

Cara kontrol yang mudah dan efektif untuk melakukan pengendalian terhadap masukkan data adalah *batch control. Batching* adalah proses pembentukkan suatu transaksi yang memiliki hubungan satu sama lainnya.

g. *Validation of data input*

Data yang dimasukkan pada aplikasi harus segera divalidasikan setelah di*input*.

h. *Instruction input*

Memastikan bahwa kualitas dari instruksi *input* pada aplikasi sistem merupakan tujuan yang sulit untuk dicapai dari pada hanya memastikan kualitas dari data *input*. Data masukkan cenderung untuk mengikuti pola yang telah tersandarisasi.

i. *Validation of Instruction input*

Seperti pada *input* data, *input* transaksi juga harus divalidasi. Auditor harus memberikan perhatian kepada validasi *input* transaksi, ketika:

1. Instruksi itu merupakan bagian dari paket *software* yang digunakan secara luas.
2. Instruksi itu diintepretasikan melalui bahasa pemograman tingkat tinggi.

j. *Audit trial Control*

Jejak audit pada subsistem *input* memelihara kronologis kejadian data dari waktu ke waktu dan instruksi yang diterima serta yang dimasukkan pada sistem aplikasi sampai pada waktu penentuan data tersebut *valid* dan dapat dikirim kepada subsistem yang lain, yang terdapat pada aplikasi.

k. *Existence Control*

Pengendalian yang ada terhadap proses data *input* subsistem yang merupakan hal yang kritis. Jika *file master* aplikasi sistem rusak atau dikorupsi, proses pemulihan harus dilakukan dengan menggunakan versi sebelumnya dari *master file* dan proses *input* harus dilakukan lagi terhadap data yang hilang.

3. Pengendalian *output*

Menurut Weber, R (1999, p615-646), subsistem *output* menyediakan fungsi-fungsi yang menentukan isi dari data yang akan disediakan bagi pengguna, cara di mana data dapat diformat dan dipersembahkan bagi

pengguna, dan cara dimana data dapat diperbaiki untuk dan dikeluarkan oleh pengguna.

Tipe pengendalian yang berhubungan dengan pengendalian *Output:*

a. *Inference Controls*

   Pengendalian model akses memperbolehkan atau menolak akses pada *item* data berdasarkan nama dari *item*, isi dari data *item*, atau beberapa dari karakteristik dari serangkaian data yang terdapat pada data *item*, agar data yang tidak boleh diakses dapat di blok maka timbullah apa yang disebut *database statistikal*.

b. *Batch Output Production dan Distribution controls*

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

c. *Batch Report Disgn Control*

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

d. *Online Output Production and Distribution Control*

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

e. *Audit Trail Control*

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

f. *Exsitance Controls*

Output dapat hilang atau rusak karena berbagai alasan seperti, *invoice* hilang, *online output* terkirim pada alamat yang salah, *output* terbakar karena kebakaran. pada beberapa kasus pemulihan kembali *output* mudah dilakukan tetapi pada kasus lain hal tersebut sulit bahkan mustahil dilakukan. *Recovery* terhadap subsistem *output* secara akurat, lengkap dan tepat merupakan hal yang sangat membantu kelangsungan hidup banyak organisasi.

2.6.3.2 Pengendalian Manajemen Keamanan

Weber, R. (1999, p244-274) berpendapat bahwa *Adiministrator Security Information System* bertanggungjawab untuk memastikan bahwa *asset* sistem informasi aman. *Asset* aman bila kemungkinan kehilangan yang dapat timbul berada pada *level* yang dapat diterima.

Yang dimaksud dengan *asset* disini adalah:

- *Asset* fisik yaitu: personil, *hardware*, *f*asilitas, dokumentasi dan *supplier.*
- *Asset* logika yaitu: data atau informasi dan *software* (sistem dan aplikasi).

Program keamanan adalah serangkaian aktivitas yang terus menerus, teratur, ditelah secara berkala untuk memastikan bahwa harta yang berhubungan dengan fungsi sistem informasi cukup aman. Langkah – langkah yang harus dijalankan dalam memimpin program keamanan sistem informasi yaitu:

1. Menyiapkan rencana proyek

Rencana Proyek	Penjelasan
Tujuan *Review*	Tujuan *Review* biasanya luas atau sempit, misalnya *review* bertujuan untuk meningkatkan keamanan fisik s*erver* atau untuk meningkatkan pengendalian terhadap ancaman keamanan logika.
Bidang *Review*	Menentukan bidang yang akan di*review*
Tugas yang harus dikerjakan	Walaupun secara keseluruhan tugas yang harus dilakukan sudah diketahui, tetapi tugas yang khusus harus ditentukan.
Organisasi Tim Proyek	Tergantung kepada besarnya dan kompleksitas materi yang akan di*review*
Anggaran Kebutuhan Sumber Daya	Anggaran yang diperlukan sangat tergantung kepada besarnya dan kompleksitas materi yang akan di*review.* Harus diperinci jam kerja, bahan dan dana yang diperlukan untuk menyelesaikan *review.*
Jadwal Penyelesaian Tugas	Memperlihatkan tanggal penyelesaian tugas bila di*review* dilakukan berbasis waktu.

Tabel 2.1 Rencana Proyek

2. Melakukan Identifikasi Harta

   Keamanan yang berhubungan dengan harta dibidang sistem informasi, tugas ini menjadi sulit karena 2 alasan, yaitu:

a. Beberapa perusahaan memiliki banyak harta dibidang sistem informasi,seperti ratusan komputer, *network* yang luas, ribuan *file* dan program.

b. Harta dibidang sistem informasi ditempatkan pada banyak tempat pada perusahaan, seperti *hardware* ditempatkan pada banyak departemen sesuai dengan tempat *user*nya.

3. Menilai harta

   Langkah ketiga untuk melakukan *review* keamanan adalah melakukan penilaian terhadap harta, harta itu juga sulit dilakukan karena penilaian ini sangat tergantung kepada orang yang melakukan penilaian, cara hilangnya harta, periode terjadinya kehilangan dan unsur harta tersebut.

4. Melakukan identifikasi ancaman

   Salah satu cara yang dapat digunakan untuk mengidentifikasikan ancaman adalah dengan mengetahui sumber dari ancaman tersebut dan tipe ancaman yang timbul. Ada dua sumber ancaman yaitu yang berasal dari luar perusahaan dan yang berasal dari dalam perusahaan.

5. Penilaian terhadap ancaman

   Tahap selanjutnya adalah melakukan taksiran kemungkinan terjadinya setiap ancaman selama suatu periode, pada beberapa kasus, data statistik tersedia, sebagai contoh perusahaan asuransi mungkin memiliki informasi tentang kemungkinan terjadinya kebakaran untuk suatu periode tertentu. Jika data yang diperlukan tidak ada, administrator keamanan dapat menganalisis kemungkinan terjadinya ancaman dari perusahaan lain yang sejenis.

6. Menganalisa ancaman

   Analisa ancaman terdiri dari 4 fase tugas yaitu:

   - Mengidentifikasikan kontrol ditempat.
   - Menilai kehandalan kontrol ditempat

     Evaluasi terhadap kemungkinan ancaman dapat diatasi dengan cara memberikan seperangkat alat kontrol ditempat
   - Menilai kerugian yang akan timbul bila tidak dapat mengelak timbulnya ancaman.

7. Menyesuaikan kontrol

   Setelah periode analisa *eksoposure* selesai, administrator keamanan harus melakukan evaluasi apakah setiap *level eksposure* dapat diterima, secara umum evaluasi ini dimaksudkan untuk melakukan penelitian apakah setelah sewaktu – waktu kontrol dapat didesain, diimplementasikan, dijalankan dimana biaya untuk kontrol tersebut kurang dari penurunan yang diharapkan dan kehilangan yang terjadi.

8. Menyiapkan laporan keamanan

   Fase terakhir dari *review* keamanan ini adalah membuat laporan kepada *management*. Laporan ini berisi hal – hal yang harus diperoleh dari *review* dan beberapa rekomendasi yang diusulkan, yang harus diimplementasikan dan beberapa pengamanan sekarang yang harus dibuang atau di modifikasi. Laporan ini juga harus meliputi rencana untuk melakukan implementasi terhadap rekomendasi dibidang keamanan yang diusulkan.

Bila bencana terjadi masih terdapat kemungkinan untuk mengurangi kerugian dan me-*recover* operasional dengan melakukan:

1. *Disaster recovery plan* (Perencanaan *recovery* jika terjadi bencana)
    a. *Emergency plan* : bencana *emergency* ini merupakan tindakan khusus yang akan dilakukan segera setelah terjadinya bencana.
    b. *Back up plan* : rencana *back up* berisi jangka waktu *back up* dilakukan, prosedur untuk melakukan *back up*, letak perlengkapan *back up*, karyawan yang bertanggung jawab untuk melakukan kegiatan *back up* ini.
    c. *Recovery plan* : Rencana *recovery* merupakan kelanjutan dari rencana *back up* karena *recovery* adalah kegiatan yang dilakukan agar sistem informasi dapat berjalan seperti biasa.
    d. *Test plan* : Komponen terakhir adalah *test plan* yang berfungsi untuk memastikan bahwa ketiga rencana diatas berjalan dengan baik.
    e. Asuransi

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

2.7 Sistem Informasi Akuntansi

2.7.1 Pengertian Sistem Informasi Akuntansi

Menurut Jones dan Rama (2003, p5), Sistem Informasi Akuntansi adalah subsistem dari MIS (*Management Information System*) yang menyediakan

informasi akuntansi dan keuangan, sebaik infomasi lainnya yang didapat dalam proses rutin dari transaksi akuntansi.

2.7.2 Komponen Sistem Informasi Akuntansi

Menurut Romney (2003, p2), Sistem Informasi Akuntansi memiliki beberapa komponen yang terdiri dari :

a. *People* (manusia)

   Adalah yang mengoperasikan sistem dan melakukan bagian fungsi.

b. *Procedures* (prosedur)

   Adalah baik yang *manual* dan otomatis, terlibat di dalam mengumpulkan, memproses, dan menyimpan data mengenai aktivitas organisasi.

c. Data

   Adalah mengenai proses bisnis organisasi.

d. *Software* (perangkat lunak)

   Adalah yang digunakan untuk memproses data – data organisasi.

e. *Information Technology Infrastructure* (infrastruktur teknologi informasi)

   Adalah termasuk komputer - komputer, alat – alat disekelilingnya dan alat - alat jaringan komunikasi.

2.8 Sistem Informasi Penjualan

2.8.1 Pengertian Sistem Informasi Penjualan

Menurut http://id.wikipedia.org/wiki./SistemInformasi yang dikutip pada tanggal 29 September 2006, sistem informasi penjualan adalah suatu sistem informasi yang mengorganisasikan serangkaian prosedur dan metode yang

dirancang untuk menghasilkan, menganalisa, menyebarkan, dan memperoleh informasi juga mendukung pengambilan keputusan mengenai penjualan.

2.8.2 Jenis – jenis Penjualan

Menurut Mulyadi (2001, p202), 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 dan perusahaan melalui sistem penjualan kredit.

2. Kegiatan Penjualan Tunai

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

2.8.3 Fungsi Yang Terkait Dalam Sistem Informasi Penjualan

Fungsi yang terkait dalam Sistem Informasi Penjualan tunai menurut Mulyadi (2001, p462) adalah :

1. Fungsi Penjualan

   Dalam transaksi penerimaan kas dari penjualan tunai, fungsi ini bertanggung jawab untuk merima *order* dari pembeli, mengisi faktur penjualan tunai, dan menyerahkan faktur tersebut kepada pembeli untuk kepentingan pembayaran

harga barang ke fungsi kas. Fungsi ini berada ditangan bagian *order* penjualan.

2. Fungsi Kas

   Dalam transaksi penerimaan kas dari penjualan tunai, fungsi ini bertanggung jawab untuk menyediakan barang yang dipesan oleh pembeli. Fungsi ini berada ditangan bagian kasa.

3. Fungsi Gudang

   Dalam transaksi penerimaan kas dari penjualan tunai, fungsi ini bertanggung jawab untuk menyiapkan barang yang dipesan oleh pembeli, serta menyerahkan barang tersebut ke fungsi pengiriman. Fungsi ini berada ditangan bagian gudang.

4. Fungsi Pengiriman

   Dalam transaksi penerimaan kas dari penjualan tunai, fungsi ini bertanggug jawab untuk membungkus barang dan meyerahkan barang yang sudah dibayar harganya kepada pembeli. Fungsi ini berada ditangan bagian pengiriman.

5. Fungsi Akuntansi

   Dalam transaksi penerimaan kas dari penjualan tunai, fungsi ini bertanggung jawab sebagai pencatat transaksi penjualan dan penerimaan kas dan pembuat laporan penjualan, fungsi ini berada ditangan bagian jurnal.

2.8.4 Jaringan Prosedur Sistem Informasi Penjualan

Menurut Mulyadi (2001, p469), Jaringan prosedur yang membentuk sistem penerimaan kas dari penjualan tunai adalah :

1. Prosedur *order* penjualan
2. Prosedur penerimaan kas
3. Prosedur penyerahan barang
4. Prosedur pencatatan penjualan tunai
5. Prosedur penyetoran kas ke bank
6. Prosedur pencatatan penerimaan kas
7. Prosedur pencatatan harga pokok penjualan

2.8.5 Prosedur Pencatatan Penjualan

Menurut Mulyadi (2001, p470), prosedur pencatatan penjualan tunai adalah fungsi akuntansi melakukan pencatatan transaksi penjualan tunai dalam jurnal penjualan dan jurnal penerimaan kas. Disamping itu fungsi akuntansi juga mencatat berkurangnya persediaan barang yang dijual dalam kartu persediaan.

2.8.6 Risiko dan Pengendalian

Menurut Peltier (2001, p1),berisiko didefinisikan sebagai seseorang atau sesuatu yang menyebabkan ancaman.

Menurut Peltier (2001, p74), risiko dibagi menjadi tiga tingkatan yaitu:

1. *High Vulnerability*

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

2. *Medium Vulnerability*

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

3. *Low Vulnerability*

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

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

1. *Servere Impact* (*High*)

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

2. *Significant Impact* (*Medium*)

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

3. *Minor Impact* (*Low*)

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

2.8.7 Laporan Yang Digunakan

Menurut Mulyadi (2001, p462), laporan yang digunakan dalam sistem informasi penjualan tunai adalah :

1) Laporan *Order* Penjualan

Laporan ini digunakan oleh bagian penjualan untuk memberikan kontribusi kepada fungsi terkait lainnya untuk melayani *order* dari pembeli.

2) Laporan Pengiriman Barang

Laporan ini digunakan oleh bagian gudang untuk menyiapkan barang dan kemudian bagian pengiriman melakukan pengiriman sesuai dengan informasi yang tercantum.

3) Laporan Pencatatan Penjualan

Laporan ini digunakan fungsi akuntansi untuk mencatat transaksi kedalam jurnal penjualan.

2.9 Data Flow Diagram (DFD)

2.9.1 Simbol – simbol *Data Flow Diagram* (DFD)

Menurut Mulyadi (2001, p57-58), “Bagan alir data adalah suatu model yang menggambarkan aliran data dan proses untuk mengolah data dalam suatu sistem”.

Menurut Hall (2001, p69), “Diagram arus data menggunakan simbol – simbol untuk mencerminkan proses, sumber – sumber data, cari data dan entitas dalam sebuah sistem”.

Dalam aliran data terdapat tingkatan – tingkatan dimana masing – masing tingkatan menggambarkan isi dari sistem, yaitu:

1) Diagram Hubungan / Diagram Konteks

Diagram konteks merupakan proses tunggal, diagram ini menggambarkan hubungan sistem data *flow dan eksternal entity*.

2) Diagram Nol

Diagram nol menggambarkan subsistem dari diagram hubungan yang diperoleh dengan memecahkan proses pada diagram hubungan atau kontek.

3) Diagram Rinci

Diagram rinci merupakan uraian dari diagram nol yang berisi proses – proses yang menggambarkan bagian dari subsitem pada diagram nol.