BAB 2

LANDASAN TEORI

2.1 Sistem Informasi Akuntansi

2.1.1 Pengertian Sistem Informasi Akuntansi

Menurut Jones dan Rama (2003, p5), sistem informasi akuntansi adalah subsistem atau bagian dari MIS (*Management Information System*) yang menyediakan informasi akuntansi dan keuangan, serta informasi lain yang diperoleh dari proses transaksi akuntansi secara rutin.

Menurut Sutabri (2004), sistem informasi akuntansi adalah kumpulan sumber daya, seperti manusia dan peralatan, yang diatur untuk mengubah data menjadi informasi. Informasi ini dikomunikasikan kepada beragam pengambilan keputusan.

Maka dapat disimpulkan bahwa sistem informasi akuntansi adalah salah satu subsistem dari sistem informasi manajemen yang mengarah pada *input*, proses hingga *output* laporan keuangan.

2.1.2 Tujuan / Kegunaan Sistem Informasi Akuntansi

Menurut Hall (2001, p17), pada dasarnya tujuan dari sistem akuntansi adalah :

- Untuk mendukung fungsi pertanggungjawaban kepengurusan suatu organisasi atau perusahaan, karena manajemen bertanggung jawab untuk menginformasikan peraturan dan penggunaan sumber daya organisasi dalam rangka pencapaian tujuan organisasi tersebut.

- Untuk mendukung pengambilan keputusan manajemen, karena sistem informasi memberikan informasi yang diperlukan oleh pihak manajemen untuk melakukan tanggung jawab pengambilan keputusan.
- Untuk mendukung kegiatan operasi perusahaan.

2.1.3 Siklus Proses Transaksi Sistem Informasi Akuntansi

Menurut George H. Bodnar dan William S. Hopwood yang diterjemahkan Jusuf, A.A pada buku 1 (2000, p136), bahwa arus transaksi operasional dapat dikelompokan sesuai dengan empat siklus aktivitas bisnis, yaitu:

- Siklus pendapatan

  Yaitu : siklus proses data transaksi terkait dengan distribusi barang / jasa ke pihak lain dan penagihan pembayarannya.

- Siklus pengeluaran

  Yaitu : siklus proses yang berkaitan dengan perolehan barang / jasa dari pihak lain dan penetapan kewajiban yang berkaitan.

- Siklus produksi

  Yaitu : pemrosesan data yang berkaitan dengan pengubahan sumber daya menjadi barang / jasa.

- Siklus keuangan

  Yaitu : pemrosesan data yang berkaitan dengan perolehan dan manajemen dana modal, termasuk kas.

2.1.4 Siklus Yang Dibahas Dalam Skripsi

Siklus yang akan dibahas dalam skripsi ini adalah siklus pendapatan. Menurut Romney (2003, p359), siklus pendapatan adalah seperangkat atau kumpulan bisnis dan operasi proses informasi terkait yang diasosiasikan dengan penyediaan barang dan jasa kepada pelanggan dan pengumpulan kas dalam pembayaran terhadap transaksi penjualan.

Tujuan utama siklus pendapatan adalah untuk menyediakan produk yang tepat pada tempat, waktu, dan harga yang tepat pula. Terdapat empat dasar aktivitas bisnis yang dilakukan dalam siklus pendapatan :

- *Entry order* penjualan
- Pengiriman
- Penagihan dan piutang dagang
- Penerimaan kas

2.2 Sistem Pengendalian *Intern*

2.2.1 Pengertian sistem pengendalian *intern*

Menurut Weber (1999, p35), pengendalian *internal* adalah suatu sistem untuk mencegah, mendeteksi, mengkoreksi kejadian yang timbul saat transaksi serangkaian pemrosesan tidak terotorisasi secara sah, tidak akurat, tidak lengkap, mengandung redundansi, tidak efektif dan tidak efesien.

2.2.2 Tujuan / kegunaan Sistem Pengendalian *Internal*

Menurut Weber (1999, p35), tujuan dari pengendalian adalah untuk mengurangi resiko / mengurangi pengaruh yang sifatnya merugikan akibat suatu kejadian.

Berdasarkan pengertian diatas, maka pengendalian dikelompokan menjadi 3 bagian :

- *Preventive Control*

  Digunakan untuk mencegah masalah sebelum masalah tersebut muncul.

- *Detective Control*

  Digunakan untuk menemukan masalah yang berhubungan dengan pengendalian segera masalah tersebut muncul.

- *Corective Control*

  Digunakan untuk memperbaiki masalah yang ditemukan pada pengendalian *Detectiv*e. Pengendalian ini mencakup prosedur untuk menentukan penyebab masalah yang timbul, memperbaiki kesalahan / kesulitan yang timbul, memodifikasi sistem proses. Dengan demikian dapat mencegah kejadian yang sama.

2.2.3 Komponen Pengendalian *Intern*

Komponen pengendalian *internal* menurut Webber (1999, p49), Pengendalian Internal terdiri dari lima komponen yang saling berinteraksi, antara lain :

- Pengendalian lingkungan

  Komponen ini diwujudkan dengan cara pengoperasian serta pembagian tugas, wewenang dan tanggung jawab dalam suatu organisasi yang digunakan untuk memonitor dan mengontrol suatu kinerja yang ada.

- Penilaian Resiko

  Penilaian yang dilakukan untuk mengidentifikasikan dan menganalisa resiko – resiko yang dihadapi oleh perusahaan dan cara – cara menghadapi resiko – resiko tersebut.

- Pengendalian Kegiatan

  Pengendalian yang bertujuan untuk memastikan transaksi telah terotorisasi dan pemeliharaan dalam dokumen.

- Informasi & Komputer

  Pengendalian atas informasi dan komputer yang bertujuan untuk menjaga aset perusahaan.

- Pengawasan

  Pengendalian ini dilakukan untuk menjaga keamanan atas data dan aset perusahaan.

2.2.4 Sistem Pengendalian *Intern* Pada Sistem Berbasis Komputer

Menurut Gondodiyoto (2006, p203), dengan diterapkannya sistem terkomputerisasi, maka sistem pengendalian *internal* juga mengalami perubahan. Salah satu penyebabnya adalah karena data tidak lagi ditulis pada lembar kertas maka daya saji sudah tidak dapat dilihat lagi secara visual. Selain itu juga proses terkomputerisasi dan komunikasi menyebabkan resiko yang dihadapi semakin besar dan makin kompleks.

Hal ini juga dapat dilihat dalam menangani keamanan *hardware, software*, media yang digunakan, proses data yang juga sangat tergantung pada ruang / tempat penyimpanan, *power* listrik, tempratur dan lain – lain.

2.3. Audit Sistem Informasi

2.3.1 Pengertian Audit Sistem Informasi

Menurut Weber (1999, p10), audit sistem informasi adalah proses pengumpulan dan pengevaluasian bukti untuk menentukan apakan sistem komputer dapat melindungi aset kekayaan, memelihara integritas data, memungkinkan tujuan organisasi untuk dicapai secara efektif dan menggunakan sumbar daya efesien.

Menurut Karya (2004, p52), audit sistem informasi didefinisikan sebagai proses pengumpulan dan evaluasi fakta / *evidence* untuk menentukan apakah suatu sistem informasi telah melindungi aset, menjaga integritas data, dan memungkinkan tujuan organisasi tercapai secara efektif dengan menggunakan sumber daya efesien.

Dapat disimpulkan bahwa pengertian audit sistem informasi adalah proses pengumpulan dan pengevaluasian bukti oleh orang yang kompeten dan independen untuk menentukan apakah sistem yang dijalankan sesuai dengan kriteria yang ditentukan.

2.3.2 Tujuan Audit Sistem Informasi

Menurut Weber (1999, p11), tujuan audit sistem informasi dapat dibagi menjadi empat, yaitu :

- Meningkatkan keamanan aset perusahaan
- Meningkatkan integritas data
- Meningkatkan efektifitas sistem
- Meningkatkan efesiensi

2.3.3 Prosedur Audit

Menurut Weber (1999, p47-55), tahapan audit sistem informasi adalah :

a. Perencanaan audit

Perencanaan audit yaitu :

- Mengetahui apakah pekerjaan mengaudit dapat diterima
- Menempatkan *staff* audit
- Menghasilkan informasi latar belakang klien
- Mengerti tentang masalah hukum klien
- Melakukan analisa terhadap prosedur yang ada
- Mengidentifikasi resiko audit

b. Pengujian Pengendalian

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

c. Pengujian transaksi

Pengujian transaksi dilakukan untuk mengevaluasi transaksi atau kejadian yang tidak sesuai dengan ketentuan ketentuan.

d. Pengujian saldo atau hasil keseluruhan

Dalam audit keuangan terhadap sistem akuntansi berbasis komputer, pengujian subtantif atas saldo misalnya dilakukan dengan memeriksa apakah saldo suatu rekening telah sesuai, misalnya piutang.

e. Penyelesaian audit

Di tahapan akhir audit, auditor *eksternal* membuat kesimpulan dan rekomendasi untuk dikomunikasikan pada manajemen.

2.3.4 Standar Audit

Standar audit merupakan pedoman bagi seorang auditor dalam menjalankan tanggung jawab profesionalnya.

Menurut www.iasii.or.id standar audit sistem informasi adalah :

S-1 Penugasan Audit

S-1.1 Tanggung Jawab, Wewenang dan Akuntabilitas

Tanggung jawab, wewenang dan akuntabilitas dari auditor sistem informasi harus dinyatakan dengan jelas secara formal dan tertulis dalam piagam atau surat tugas audit sistem informasi serta disetujui secara bersamaan oleh auditor sistem informasi dan pemberi tugas.

S-2 Independensi dan Objektifitas

S-2.1 Independensi

Dalam berbagai hal yang berkaitan dengan audit sistem informasi, auditor harus menjaga independensinya baik secara factual maupun penampilan.

S-2.2 Objektifitas

Auditor sistem informasi harus menjaga objektifitasnya dalam merencanakan, melaksanakan, dan melaporkan audit sistem informasi.

S-3 Profesionalisme dan Kompetensi

S-3.1 Profesionalisme

Auditor sistem informasi harus memenuhi berbagai standar audit yang berlaku serta menerapkan kecermatan, dan keterampilan profesionalnya.

S-3.2 Kompetensi

Auditor sistem informasi secara kolektif harus memiliki atau memperoleh pengetahuan dan keahlian yang diperlukan untuk melaksanakan audit sistem informasi.

S-3.3 Pendidikan Profesi Berkelanjutan

Auditor sistem informasi harus meningkatkan pengetahuan dan keahlian yang diperlukan untuk melaksanakan sudit sistem informasi melalui pendidikan profesi berkelanjutan.

S-4 Perencanaan

S-4.1 Perencanaan Audit

Auditor sistem informasi harus merencanakan audit sistem informasi dengan baik agar dapat mencapai tujuan audit serta memenuhi standar audit yang berlaku.

S-5 Pelaksanaan

S-5.1 Pengawasan

Staff audit sistem informasi harus disupervisi dengan baik untuik memberikan keyakinan yang memadai bahwa tujuan audit sistem informasi dapat tercapai dan standar audit yang berlaku dapat dipenuhi.

S-5.2 Bukti – bukti Audit

Dalam melaksanakan audit sistem informasi, auditor sistem informasi harus memperoleh bukti – bukti audit yang cukup, dapat diandalkan dan bermanfaat untuk mencapai tujuan audit sistem informasi secara efektif.

S-5.3 Kertas Kerja Audit

Dalam melaksanakan audit sistem informasi, auditor harus mendokumentasikan secara sistematis seluruh bukti – bukti audit yang diperoleh.

S-6 Pelaporan

S-6.1 Laporan Audit

Setelah menyelesaikan pelaksanaan audit sistem informasi, auditor sistem informasi harus memberikan suatu laporan audit dalam bentuk yang memadai kepada pihak – pihak yang berhak menerima.

S-7 Tindak Lanjut

S-7.1 Pemantauan Tindak Lanjut

Auditor sistem informasi harus meminta dan mengevaluasi informasi yang dipandang perlu sehubungan dengan temuan, kesimpulan dan rekomendasi audit yang terkait dari audit sebelumnya untuk menentukan apakah tindak lanjut yang layak telah dilaksanakan dengan tepat waktu.

2.3.5 Metode Audit Sistem Informasi

Menurut Weber (1999, p55-57), metode audit meliputi :

- *Auditing Around the Computer*

  Auditing Around the Computer adalah suatu pendekatan audit dengan memperlakukan komputer sebagai *black box*. Maksudnya metode ini tidak menguji langkah – langkah proses secara langsung, tetapi hanya berfokus pada *input* dan *output* dari sistem komputer.

  Auditor yang melakukan *auditing around the computer* merupakan cara yang paling efektif karena dengan pendekatan biaya (paling murah). Auditor juga dapat menggunakan *auditing around the computer* ketika kepercayaan kepada user lebih tinggi dibandingkan dengan kontrol komputer untuk mengamankan harta kekayaan, memelihara data *integrity* dan pencapaian efektifitas dan efesiensi sistem. Pada saat melakukan pengetesan fokus diberikan kepada keandalan kontrol oleh *user* daripada keandalan kontrol komputer.

  Pendekatan ini menggunakan dua *limitation*, yaitu :

  a. Jenis aplikasi yang dapat digunakan dengan baik sangat terbatas. Hal itu tidak dapat digunakan bila semestinya rumit, sehingga auditor mungkin gagal untuk memahami beberapa aspek dari sistem tersebut yang memiliki efek yang cukup berpengaruh pada pendekatan audit.

b. Pendekatan ini tidak memberikan informasi tentang kemampuan sistem untuk mengatasi perubahan. Sistem dapat didesain dan ditulis oleh programer dengan banyak cara untuk mengurangi keterbatasan mereka melakukan perubahan sesuai dengan keinginan pemakai.

- *Auditing Through the Computer*

  Auditor yang menggunakan cara ini menggunakan

  komputer untuk menguji logika proses dan kontrol yang ada saat ini pada sistem dan produksi *record* oleh sistem.

  Keuntungan dari pendekatan ini adalah auditor dapat meningkatkan kemampuan untuk melakukan pengetesan terhadap sistem lebih efektif.

  Dua kelemahan pendekatan ini adalah :

  a. Pemakaian pendekatan ini mengakibatkan membengkaknya biaya, terutama tambahan waktu tenaga kerja untuk memahami cara kerja *internal* dari aplikasi sistem tersebut.
  b. Pada beberapa diperlukan tambahan kemampuan teknis jika ingin dimengerti cara kerja sistem.

2.3.6 Instrumen Audit yang Dipakai

Menurut Karya (2004, p55), instrumen audit terdiri dari :

- Wawancara, terutama untuk mendapatkan informasi gambaran umum sistem informasi dan pointer ke fakta – fakta yang akan dikumpulkan lebih lanjut.
- Inspeksi, terutama untuk memeriksa bukti – bukti dokumen dan aktifitas untuk meyakinkan bahwa suatu kriteria telah dipenuhi.
- Kuesioner, terutama untuk mengumpulkan informasi dari beberapa sumber sekaligus beberapa pendapat / penilaian dari masing – masing sumber yang hasilnya akan diolah secara statistik.
- Tes program, terutama digunakan untuk malakukan pemeriksaan terhadap perangkat lunak aplikasi.
- Tes data, untuk meyakinkan akan integritas data, kebenaran data dan konsistensi antara dokumen masukan dengan adata yang akan diproses.

2.3.7 Penetapan Resiko

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

Resiko dibagi menjadi 3 tingkatan, yaitu :

a. *High Vulnerability*

   Kelemahan yang sangat besar yang berada didalam sistem atau rutinitas operasi dan dimana dampak potensial pada bisnis adalah penting. Untuk itu, harus ada pengendalian yang ditingkatkan.

b. *Medium Vulnerability*

   Beberapa kelemahan yang ada pada sistem dan dimana dampak potensial pada bisnis adalah penting. Untuk itu, harus ada pengendalian yang ditingkatkan.

c. *Low Vulnerability*

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

d. *Severe Impact (High)*

   Dapat menyebabkan perusahaan mengalami kebangkrutan dalam bidang usahanya, memberikan dampak yang sangat besar dalam bisnisnya.

e. *Significant Impact (Medium)*

   Dapat menyebabkan kerugian yang cukup berpengaruh dan biaya yang cukup besar, tetapi perusahaan tetap dapat bertahan.

f. Minor Impact (Low)

Dapat memberikan dampak yang biasa terjadi dalam kegiatan bisnis sehari-hari.

2.4 Pengendalian Umum

Menurut Weber (1999, p32), menyebutkan auditor sistem informasi berkonsentrasi pada evaluasi terhadap tingkat kepercayaan data atau efektifitas .

Menurut Gondodiyoto (2006, p252), pengendalian umum adalah sistem pengendalian *internal* komputer yang berlaku umum meliputi seluruh kegiatan komputerisasi sebuah organisasi secara menyeluruh.

Pengendalian umum terdiri dari :

A. Pengendalian *top* manajemen

Top Manajemen terdiri dari direktur utama dan para direktur lainnya. Direksi bertanggung jawab terhadap seluruh organisasi perusahaan, termasuk bidang TI yang merupakan salah satu pendukung keberhasilan perusahaan.

Pengendalian *top* manajemen adalah sistem pengendalian *intern* yang ada pada suatu organisasi yang mendorong keterlibatan, kepedulian dan tanggung jawab pucuk pimpinan organisasi terhadap kegiatan TI pada organisasi tersebut.

B. Pengendalian manajemen pengembangan sistem

Pengendalian pengembangan dan pemeliharaan sistem diperlukan untuk mencegah dan mendeteksi kesalahan pada waktu pengembangan dan pemeliharaan sistem, serta untuk memperoleh

keyakinan memadai bahwa sistem berbasis teknologi informasi dikembangkan dan dipelihara dengan cara yang efesien dan melalui proses otorisasi.

C. Pengendalian manajemen sumber data

Dalam suatu sistem berbasis teknologi informasi, pengendalian sumber data yang baik adalah :

- *User* harus dapat berbagi dengan data.
- Data harus tersedia untuk digunakan kapan saja, dimanapun, dan dalam bentuk apapun.
- Sistem manajemen data harus menjamin adanya sistem penyimpanan yang efesien, tidak terjadi *redundancy* data, adanya data *security*, *integrity*.
- Data harus dapat dimodifikasi dengan mudah oleh yang berwenang sesuai dengan kebutuhan *user*.

D. Pengendalian manajemen jaminan kualitas

Pengendalian manajemen kualitas berkonsentrasi untuk memastikan bahwa :

- Sistem informasi yang dihasilkan oleh fungsi sistem informasi mencapai suatu standart kualitas yang dapat diterima.
- Pengembangan, pengimplementasian, operasional, dan *maintenance* terhadap sistem informasi.

E. Pengendalian manajemen operasi

Pengendalian manajemen operasi merupakan jenis pengendalian *intern* yang didesain untuk menciptakan kerangka kerja organisasi

pendayaan sumber daya informasi, pembagian tugas yang baik bagi suatu organisasi yang menggunakan sistem berbasis teknologi informasi.

F. Pengendalian manajemen keamanan

Pengendalian *intern* terhadap manajemen keamanan dimaksudkan untuk menjamin agar aset sistem informasi tetap aman. Aset sumber daya informasi mencakup fisik serta aset tak berwujud.

2.5.1 Pengendalian Manajemen Operasional

Menurut Gondodiyoto (2006, p290), pengendalian manajemen operasional merupakan jenis pengendalian *intern* yang didesain untuk menciptakan kerangka kerja organisasi.

Pengendalian manajemen operasi dapat diterapkandengan menggunakan metode – metode :

- Memisahkan fungsi yang mengelola teknologi informasi
- Memisahkan fungsi pekerjaan
- Pengendalian personil
- Perencanaan, penganggaran, dan sistem pembebanan biaya kepada *user*.
- Adanya komisi pengarah TI yang berfungsi untuk menetapkan kebijakan TI.

Dengan demikian, secara garis besar manajemen operasi bertanggung jawab terhadap hal – hal sebagai berikut :

- Pengoperasian komputer

  Tipe pengendalian yang harus dilakukan adalah :

  1. Menentukan fungsi – fungsi yang harus dilakukan operator komputer maupun fasilitas operasi otomatis.
  2. Menentukan penjadwalan kerja pada pemakaian *hardware / software.*
  3. Menentukan perawatan terhadap *hardware / software* agar dapat berjalan baik.
  4. Pengendalian perangkat keras berupa *hardware controls.*

- Pengendalian jaringan

  Pengendalian yang dilakukan adalah seperti memonitor dan memelihara jaringan dan pencegahan terhadap akses oleh pihak yang tidak berwenang.

- Persiapan dan pengentrian data

  Fasilitas – fasilitas yang ada harus dirancang untuk memiliki kecepatan dan keakuratan data serta telah dilakikan pelatihan terhadap pengentri data.

- Pengendalian produksi

  Fungsi yang harus dilakukan untuk pengendalian produksi adalah :

  1. Penerimaan dan pengiriman *input* dan *output.*
  2. Penjadwalan kerja
  3. Manajemen pelayanan

2.5.2 Pengendalian Manajemen Keamanan

Menurut Gondodiyoto (2006, p303), pengendalian manajemen keamanan dimaksudkan untuk menjamin agar aset sistem informasi tetap aman. Aset sumber daya sistem informasi mencakup fisik mesin dan fasilitas penunjangnya, serta aset tak berwujud fisik, misalnya data atau informasi dan program aplikasi komputer.

Ancaman utama terhadap keamanan dapat bersifat karena alam, manusia yang bersifat kelalaian atau kesengajaan, antara lain :

- Ancaman kebakaran

  Beberapa pelaksanaan keamanan untuk ancaman kebakaran :

  1. Memiliki alat pemadam kebakaran otomatis dan tabung pemadam kebakaran.
  2. Memiliki pintu / tangga darurat.
  3. Melakukan pengawasan rutin dan pengujian terhadap sistem perlindungan kebakaran untuk dapat memastikan bahwa segala sesuatunya telah dirawat dengan baik.

- Ancaman banjir

  Beberapa pelaksanaan pengamanan untuk ancaman banjir adalah :

  1. Usahakan bahan untuk atap, dinding, dan lantai yang tahan air.
  2. Semua material aset sistem informasi ditaruh di tempat yang tinggi.

- Perubahan tegangan sumber energi

  Pelaksanaan pengamanan untuk mengantisipasi perubahan tegangan sumber energi listrik, misalnya menggunakan *stabilizer* atau *power supply* (UPS).

- Kerusakan struktural

  Pelaksanaan pengamanan untuk mengantisipasi kerusakan struktural misalnya : memilih lokasi perusahaan yang jarang terjadi gempa, angin ribut, banjir.

- Penyusup

  Pelaksanaan keamanan untuk mengantisipasi penyusup adalah penempatan penjaga dan penggunaan alarm, atau kamera pengawas.

- Virus

  Pelaksanaan keamanan untuk mengantisipasi virus adalah :

  1. *Preventif*, seperti menginstal anti virus dan melakukan *update* secara rutin.
  2. *Detektif*, misalnya melakukan *scan file* sebelum digunakan
  3. *Korektif*, misalnya memastikan *back up* data bebas virus, pemakaian anti virus terhadap *file* yang terinfeksi.

- *Hacking*

  Beberapa pelaksanaan pengamanan untuk mengantisipasi *hacking* :

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

2.5 Pengendalian aplikasi

Menurut Gondodiyoto (2007, p328), pengendalian aplikasi adalah sistem pengendalian *intern* pada sistem informasi berbasis teknologi yang berkaitan dengan pekerjaan / kegiatan / aplikasi tertentu.

Pengendalian aplikasi terdiri dari :

A. Pengendalian *Boundary*

   Weber (1000, p329), menyebutkan bahwa pengendalian akses membatasi penggunaan *resource* sistem komputer hanya kepada *user* yang mendapatkan otorisasi dalam mendapatkan sumber ini dan menjamin bahwa *user* hanya mendapatkan sumber yang otentik.

B. Pengendalian *input*

   Gondodiyoto (2006, p 332) , menyebutkan bahwa pengendalian *input* dirancang dengan tujuan untuk mendapat keyakinan bahwa data transaksi *input* adalah *valid*, lengkap, serta bebas dari kesalahan dan penyalahgunaan.

C. Pengendalian komunikasi

   Menurut Weber (1999, p469), menyebutkan subsistem komunikasi bertanggung jawab untuk mengirim data ke seluruh subsistem yang lain dalam sebuah sistem dan untuk mengirim dan menerima data dari sistem yang lain.

D. Pengendalian Proses

   Menurut Gondodiyoto (2006, p353), pengendalian proses ialah pengendalian *internal* untuk mendeteksi jaringan sampai data menjadi *error* karena adanya kesalahan proses.

E. Pengendalian Database

Menurut Gondodiyoto (2006, p374), menyebutkan dalam suatu instalasi sistem database yang sudah komprehensif dan terpadu, kebijakan manajemen sumber data telah memenuhi hampir seluruh kenutuhan pengendalian, termasuk kebutuhan spesifikasi aplikasi.

F. Pengendalian *Output*

Menurut Gondodiyoto (2006, p363), pengendalian keluaran merupakan pengendalian yang dilakukan untuk menjaga keluaran sistem tetap akurat, lengkap dan digunakan sebagaimana mestinya.

2.5.1 Pengendalian *Input*

Menurut Gondodiyoto (2007, p332), pengendalian *input* dirancang dengan tujuan untuk mendapat keyakinan bahwa data transaksi *input* adalah *valid*, lengkap, serta bebas dari kesalahan dan penyalahgunaan.

Menurut George H. Bodnar dan Willian S. Hopwood yang diterjemahkan oleh Jusuf,A.A. (2000, p208), pengendalian *input* dirancang untuk tindakan *preventif / detektif* terhadap kesalahan – kesalahan dalam tahap *input* pengolahan data.

Jadi, dapat disimpulkan bahwa pengendalian *input* memiliki kaitan dengan audit karena pengendalian *input* merupakan area yang rawan terjadinya *error*, dan jika terjadi kesalahan akibatnya akan sangat fatal dan banyak dampaknya.

Pengendalian input dalam batch dilakukan dalam beberapa tahap :

- *Data Capturing*

  Dilakukan pada pengisian dokumen *input*, misalnya dengan desain formulir / dokumen yang baik.

- *Batch data preparation*

  Dilakukannya *editing code* atau isian – isian nomor – nomor tertentu. Misalnya jumlah uang.

- *Data entry & validation*

  Data yang di *entry* biasanya langsung dicek secara terprogram sederhana oleh mesin *data entry*.

Dari sudut pandang auditor, *input control* merupakan hal yang penting karena 3 alasan :

- Pada sistem informasi kontrol yang besar jumlahnya adalah pada subsistem input, sehingga auditor harus memberikan perhatian yang lebih pada kehandalan *input* kontrol yang ada.
- Kegiatan subsistem *input* melibatkan jumlah kegiatan yang besar dan rutin dan merupakan kegiatan yang dapat menyebabkan terjadinya kesalahan.
- Subsistem *input* seringkali merupakan target dari *fraud*, banyak kegiatan yang tidak seharusnya dilakukan, seperti penambahan, penghapusan.

2.5.2 Pengendalian *Output*

Menurut Gondodiyoto (2006, p363), pengendalian keluaran merupakan pengendalian yang dilakukan untuk menjaga *output* sistem tetap akurat, lengkap, dan digunakan sebagaimana mestinya.

Menurut Weber (1999, p612), pengendalian *output* ialah pengendalian yang menyediakan fungsi – fungsi yang dikelompokan dalam isi dari data yang akan disediakan, alur data yang akan diperbaiki dan disajikan *user*. Komponen utama dari pengendalian *output* adalah *software*.

Jadi, dapat disimpulkan bahwa pengendalian *output* dirancang dengan tujuan untuk menjamin hasil *output* informasi dapat sesuai dengan *input* data yang dilakukan serta memenuhi syarat *output* yang baik. Pengendalian data *output* yang dapat dilakukan dapat berupa :

- Mencocokan data *output*
- Mereview data *output* untuk melihat format yang tepat, format tersebut terdiri dari :
    A. Judul laporan
    B. Tanggal dan waktu pencetakan
    C. Banyaknya *copy* laporan
    D. Periode laporan
    E. Nama program
    F. Nama personil yang bertanggung jawab atas dikeluarkanya laporan tersebut.
    G. Masa berlaku laporan
    H. Nomor halaman

I. Tanda akhir halaman

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

2.5.3 Pengendalian *Boundary*

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

- Identifikasi dan otentikasi (Identification and Authentication)

  User mengidentifikasi dirinya pada mekanisme pengendalian akses dengan memberi informasi seperti nama atau nomor rekening. Informasi tersebut memungkinkan mekanisme untuk menentukan bahwa data yang masuk sesuai dengan informasi pada file otentikasi.

  Terdapat tiga bagian yang dapat diisi oleh user untuk informasi otentikasi

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

- Sumber Daya Objek

  Sumber daya yang digunakan oleh user berdasarkan sistem informasi berbasis computer dapat dibagi menjadi tiga jenis, yaitu:

  a. *Hardware*, contohnya: terminal, printer, *processor*.

b. *Software*, contohnya: program sistem aplikasi, *software* umum.
c. Komoditi, contohnya: *processor time, storage device*.

Menurut Weber (1999, p329), menyebutkan bahwa pengendalian akses membatasi penggunaan *resource* sistem komputer hanya kepada *user* yang mendapatkan otorisasi, membatasi *user* yang mendapat otorisasi dalam mendapatkan sumber ini dan menjamin bahwa *user* hanya mendapatkan sumber daya yang otentik.

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

Kontrol terhadap subsistem terhadap sistem *boundary* memiliki tiga tujuan, yaitu :

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

2.6 Sistem Informasi Penjualan

2.6.1 Pengertian Sistem Informasi Penjualan

Menurut Mulyadi (2001, p202), kegiatan penjualan terdiri dari transaksi penjualan barang atau jasa, baik secara kredit maupun tunai.

Dalam transaksi penjualan kredit, jika order dari pelanggan telah dipenuhi dengan penerimaan barang atau penyerahan jasa, untuk jangka waktu tertentu perusahaan memiliki piutang kepada pelanggannya.

Dalam transaksi penjualan tunai, barang atau jasa baru diserahkan oleh perusahaan kepada pembeli jika perusahaan telah menerima kas dari pembeli.

2.6.2 Jaringan Prosedur Sistem Penjualan

Menurut mulyadi (2001, p219), jaringan prosedur yang membentuk sistem penjualan adalah:

- Prosedur *order* penjualan

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

- Prosedur persetujuan kredit

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

- Prosedur pengriman

  Dalam prosedur ini, fungsi pengiriman mengirim barang kepada pelanggan sesuai dengan informasi yang tercantum dalam surat *order* pengiriman yang diterima dari fungsi pengiriman.

- Prosedur penagihan

  Dalam prosedur ini fungsi pengiriman mngirimkan barang kepada pelanggan sesuai dengan informasi yang tercantum dalam surat *order* pengiriman yang diterima dari fungsi pengiriman.

- Prosedur pencatatan piutang

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

- Prosedur distribusi penjualan

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

- Prosedur pencatatan harga pokok penjualan

  Dalam Prosedur ini fungsi akuntansi secara periodik total harga pokok produk yang dijual dalam periode akuntansi tertentu.

Informasi yang umumnya diperlukan oleh manajemen dari kegiatan penjualan kredit adalah :

- Jumlah pendapatan penjualan menurut jenis produk selama jangka waktu tertentu.
- Jumlah piutang kepada setiap debitur dari transaksi penjualan kredit.
- Jumlah harga pokok produk yang dijual selama jangka waktu tertentu.
- Nama dan alamat pembeli.
- Kuantitas produk yang dijual.
- Nama wiraniaga yang melakukan penjualan.
- Otorisasi yang berwenang.