Bab II

Tinjauan Pustaka

2.1. Pengantar

Dalam suatu organisasi yang kompleks, sebuah sistem diperlukan untuk membantu aktivitas operasional, sehingga aktivitasnya menjadi lebih efisien dan efektif. Apabila sistem telah dirancang dan dilaksanakan, maka kebutuhan di dalam organisasi dapat berkembang. Seiring dengan perkembangan kebutuhan tersebut, maka pengembangan sistem perlu dilakukan untuk diseimbangkan dengan kebutuhan pemakai sistem yang semakin berkembang.

Pengembangan sistem dapat berarti menyusun suatu sistem yang baru untuk menggantikan sistem yang lama secara keseluruhan atau memperbaiki sistem yang telah ada (Jogiyanto dalam Widyastuti, 2009). Salah satu pengembangan sistem yang sering digunakan para pengembang sistem yaitu, *Systems Development Life Cycle* (SDLC). Siklus hidup dari pengembangan sistem ini memiliki beberapa tahapan (Sutedjo dalam Widyastuti, 2009), yaitu perencanaan sistem, analisis sistem, perancangan sistem, penerapan sistem, evaluasi sistem, dan pemeliharaan sistem.

Setelah pengembangan sistem dilakukan, tahapan penting yang kadang terlupakan yaitu evaluasi dan pemeliharaan sistem di tingkat operasional. Jika tahapan tersebut terlewati, maka kinerja sistem akan semakin menurun dan menghambat kinerja sistem secara keseluruhan. Oleh sebab itu, sistem yang sudah berjalan pada suatu organisasi memerlukan analisis lebih lanjut untuk mengetahui penyebab kelemahan dari sistem yang telah digunakan tersebut. Analisis lebih

lanjut tersebut disebut dengan audit operasional sistem, sehingga kelemahan sistem yang ditemukan ketika analisis maupun pengumpulan informasi temuan-temuan dapat didiskusikan kembali dalam organisasi untuk diperbaiki supaya kinerja sistem yang sedang berjalan menjadi lebih baik.

2.2. Audit

Audit adalah suatu proses pengumpulan dan pengevaluasian bahan bukti tentang informasi yang dapat diukur mengenai suatu entitas ekonomi yang dilakukan seorang yang kompeten dan independen untuk dapat menentukan dan melaporkan kesesuaian informasi dengan kriteria-kriteria yang telah ditetapkan (Arens dan Loebbecke dalam Salsabila, 2011).

Berdasarkan definisi tersebut dapat dilihat bahwa audit harus dilakukan oleh orang yang independen dan kompeten. Auditor harus memiliki kemampuan dalam memahami kriteria yang digunakan dan harus kompeten untuk mengetahui jenis serta jumlah bukti yang akan dikumpulkan supaya pemeriksaan yang dilakukan hingga pemberian opininya tepat, akurat, dan dapat dipercaya publik. Kompetensi orang-orang yang melaksanakan audit akan tidak ada nilainya, jika mereka tidak independen dalam mengumpulkan dan mengevaluasi bukti (Arens dkk. dalam Tjun, 2012).

2.2.1 Jenis-Jenis Audit

Terdapat beberapa jenis audit yang dikategorikan berdasarkan bidang yang diaudit. Menurut Herawati (2008), jenis-jenis audit berdasarkan bidang auditnya masing-masing adalah :

1. Audit Keuangan (*Financial Audit*), bertujuan untuk menentukan apakah laporan keuangan secara keseluruhan telah dinyatakan sesuai dengan kriteria tertentu.
2. Audit Operasional (*Operational Audit*), bertujuan untuk pemeriksaan efektifitas, efisiensi, dan ekonomis atau tidaknya bidang kegiatan tertentu.
3. Audit Ketaatan (*Compliance Audit*), bertujuan untuk memeriksa apakah klien atau nasabah telah mengikuti prosedur atau peraturan tertentu yang telah ditetapkan oleh yang berwenang.
4. Audit *E-commerce*, bidang audit terhadap *e-commerce* merupakan kegiatan jasa yang ditekankan pada beberapa hal, yaitu pengungkapan praktik bisnis, keyakinan atas keandalan transaksi, dan perlindungan atas informasi.
5. Audit Kecurangan (*Fraud Audit*), *fraud management* menurut Roberston dalam Herawati (2008), mengacu pada kejahatan organisasional yaitu perbuatan para manajer untuk membuat laporan keuangan secara curang, memalsukan, dan membesar-besarkan atau mengecil-kecilkan aset atau laba dengan tujuan untuk menipu pihak-pihak di luar organisasi.
6. Audit Sistem Informasi (*Information System Audit*), menurut Weber dalam Herawati (2008), adalah proses pengumpulan dan evaluasi bukti-bukti untuk menentukan apakah sistem komputer yang digunakan telah dapat melindungi aset milik organisasi, mampu menjaga integritas data, dapat membantu pencapaian tujuan organsasi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien.

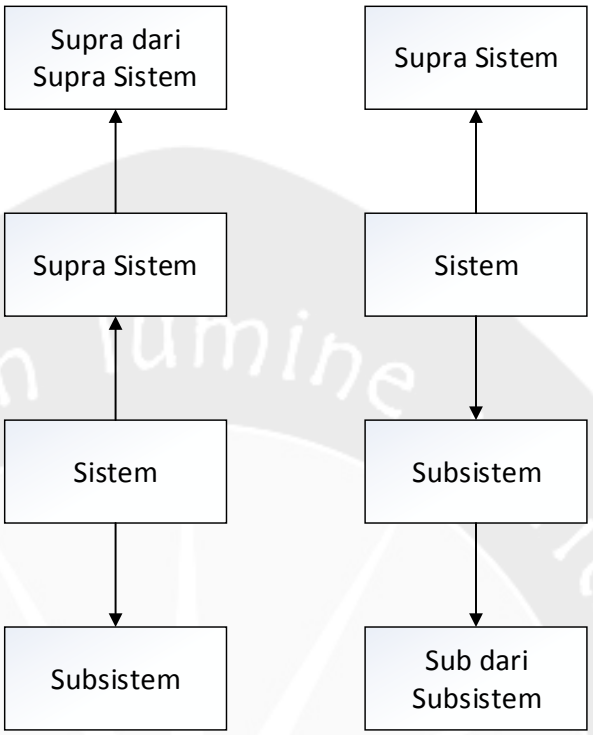
2.3. Sistem

Menurut Mulyadi dalam Purnomo (2013), sistem merupakan sekelompok unsur yang erat hubungan satu dengan yang lainnya yang berfungsi bersama-sama untuk mencapai tujuan tertentu. Kumpulan unsur-unsur yang membentuk suatu sistem ini akan bekerja secara berkesinambungan untuk mencapai tujuan yang diharapkan. Apabila terdapat masalah pada salah satu unsurya, maka sistem tersebut akan mengalami masalah juga. Oleh karena itu, hubungan antarunsur menjadi komponen yang sangat penting supaya sistem dapat berjalan dengan lancar, sehingga dapat mencapai tujuan organisasi.

Dalam suatu sistem, terdapat beberapa karakteristik yang dapat mengidentifikasikan suatu sistem. Karakteristik suatu sistem terdapat beberapa macam (Jogiyanto dalam Purnomo, 2013), yaitu:

1. Komponen Sistem

   Suatu sistem terdiri dari sejumlah komponen yang saling berinteraksi, yang artinya saling bekerjasama membentuk suatu kesatuan. Setiap sistem tidak peduli betapapun kecilnya, selalu mengandung komponen-komponen atau subsistem-subsistem. Setiap subsistem mempunyai sifat-sifat dari sistem yang menjalankan suatu fungsi tertentu dan mempengaruhi proses sistem secara keseluruhan.



Gambar 2.1 Subsistem, Sistem, Supra Sistem

(sumber: Jogiyanto dalam Purnomo, 2013)

Suatu sistem dapat mempunyai suatu sistem yang lebih besar yang disebut dengan *supra system*. Apabila masih ada sistem yang lebih besar lagi diatas *supra system* maka disebut dengan *supra* dari *supra system* dan sebaliknya.

2. Batas Sistem

Batas sistem merupakan daerah yang membatasi antara suatu sistem dengan sistem yang lainnya atau dengan lingkungan luarnya. Batas sistem ini memungkinkan suatu sistem dipandang sebagai suatu kesatuan. Batas suatu sistem menunjukkan ruang lingkup (*scope*) dari sistem tersebut.

3. Lingkungan Luar Sistem

Lingkungan luar dari suatu sistem adalah apapun di luar batas dari sistem yang mempengaruhi operasi sistem, dapat bersifat menguntungkan maupun

merugikan sistem tersebut. Lingkungan luar yang menguntungkan merupakan energi dari sistem dan dengan demikian harus tetap dijaga dan dipelihara, sedangkan lingkungan luar yang merugikan harus ditahan dan dikendalikan, kalau tidak maka akan mengganggu kelangsungan hidup dari sistem.

4. Penghubung Sistem

Penghubung merupakan media penghubung antara suatu subsistem dengan subsistem yang lainnya. Keluaran (*output*) dari satu subsistem akan menjadi masukan (*input*) untuk subsistem yang lainnya dengan melalui penghubung. Dengan penghubung, satu subsistem dapat berintegrasi dengan subsistem lainnya membentuk suatu kesatuan.

5. Masukan Sistem

Masukan sistem adalah energi yang dimasukkan ke dalam sistem. Masukan dapat berupa masukan perawatan (*maintenance input*) dan masukan sinyal (*signal input*). *Maintenance input* adalah energi yang dimasukkan supaya sistem tersebut dapat beroperasi. *Signal input* adalah energi yang diproses untuk menghasilkan keluaran.

6. Keluaran Sistem

Keluaran sistem adalah hasil dari energi yang diolah dan diklasifikasikan menjadi keluaran yang berguna dan sisa pembuangan. Keluaran dapat merupakan masukan untuk subsistem yang lain atau kepada supra sistem (sistem yang lebih kompleks).

7. Pengolahan Sistem

Suatu sistem dapat mempunyai suatu bagian pengolah atau sistem itu sendiri sebagai pengolahnya. Pengolah yang akan merubah masukan menjadi keluaran. Sistem akuntansi akan mengolah data-data transaksi menjadi laporan-laporan keuangan dan laporan-laporan lain yang dibutuhkan manajemen.

8. Sasaran Sistem

Suatu sistem pasti mempunyai tujuan (*goal*) atau sasaran (*objective*). Kalau suatu sistem tidak mempunyai sasaran, maka operasi sistem tidak akan ada gunanya. Sasaran dari sistem sangat menentukan sekali masukan yang dibutuhkan sistem dan keluaran yang dihasilkan sistem. Suatu sistem dikatakan berhasil bila mencapai sasaran atau tujuan.

2.4. Informasi

Informasi merupakan suatu olahan data ke dalam bentuk yang dapat memberikan arti bagi penerima dan dapat menjadikan sebagai dasar pertimbangan keputusan saat ini atau mendatang (Jogiyanto, 1991). Berdasarkan informasi, bagi penerima yaitu manajer akan melakukan suatu pertimbangan untuk mengambil keputusan. Oleh sebab itu, diperlukan informasi yang benar dan akurat supaya keputusan yang akan diambil oleh manajer menjadi lebih tepat.

2.4.1 Kualitas Informasi

Informasi merupakan hasil keluaran dari sistem, kemudian akan digunakan oleh manajer untuk membuat keputusan. Maka diperlukan suatu informasi yang berkualitas supaya manajer dapat memutuskan keputusannya dengan tepat.

Menurut Jogiyanto dalam Purnomo (2013), terdapat beberapa kategori kualitas informasi, yaitu:

1. Akurat

   Informasi harus bebas dari kesalahan-kesalahan, tidak bias atau menyesatkan, informasi harus jelas mencerminkan maksudnya. Informasi harus akurat karena dari sumber informasi sampai ke penerima informasi kemungkinan terjadi gangguan (*noise*) yang dapat merusak atau mengubah informasi tersebut.

2. Tepat pada waktunya

   Informasi yang datang pada penerima tidak boleh terlambat karena informasi yang telah usang tidak akan mempunyai nilai lagi. Informasi merupakan landasan di dalam pengambilan keputusan, bila keputusan terlambat maka dapat berakibat fatal bagi organisasi.

3. Relevan

   Informasi tersebut mempunyai manfaat untuk pemakainya. Dengan pemakai yang berbeda-beda, relevansi informasi untuk orang yang satu dengan yang lainnya juga akan berbeda.

2.5 Sistem Informasi

Definisi sistem informasi menurut Leitch dan Davis dalam Jogiyanto (1991) adalah suatu sistem di dalam organisasi yang mempertemukan kebutuhan pengolahan transaksi harian, mendukung operasi, bersifat manajerial, dan kegiatan strategi dari suatu organisasi dan menyediakan pihak luar tertentu dengan

laporan-laporan yang dibutuhkan. Oleh karena itu, sistem informasi merupakan komponen yang sangat penting dalam proses pengambilan keputusan para manajer atau pihak tertentu yang membutuhkan hasil dari sistem informasi.

2.6 Sistem Informasi Akuntansi

Sistem Informasi Akuntansi (SIA) adalah sebuah sistem yang memproses data dan transaksi guna menghasilkan informasi yang bermanfaat untuk merencanakan, mengendalikan, dan mengoperasikan bisnis (Krismaji dalam Andreas, 2006). Dalam SIA, data dan transaksi yang digunakan adalah semua yang berkaitan dengan akuntansi dalam suatu kegiatan operasional bisnis, sehingga hasil yang diharapkan adalah informasi data yang akurat untuk membuat keputusan bisnis.

2.7 Sistem Informasi Akuntansi Persediaan

2.7.1 Persediaan

Persediaan adalah pos harta yang ditahan untuk dijual dalam kegiatan usaha yang biasa atau barang yang akan digunakan atau dikonsumsi dalam produksi barang yang akan dijual (Kieso & Weygandt dalam Hartono, 2010). Berdasarkan pengertian tersebut, aktivitas yang dilakukan terhadap persediaan dapat dipisahkan menjadi barang yang tersedia untuk dijual langsung tanpa diolah dan barang yang dipakai untuk diproduksi dan akan dijual setelah selesai diolah.

Sistem persediaan menjadi sangat penting karena umumnya persediaan merupakan salah satu komponen aset lancar yang jumlahnya cukup material

(Herawati, 2008). Jumlahnya yang banyak menjadi aset terbesar dalam perusahaan. Pengelolaan yang baik atas persediaan perusahaan sangat diperlukan supaya risiko dalam persediaan dapat diminimalkan.

2.7.2 Metode Penataan Persediaan Obat

Menurut Febriawati (2013), terdapat tiga metode yang dapat digunakan untuk menata persediaan obat, yaitu:

1. *First In First Out* (FIFO) adalah sistem penataan obat atau perbekalan farmasi dengan meletakkan barang baru (datang terakhir) di belakang barang yang datang sebelumnya.
2. *Last In First Out* (LIFO) adalah sistem penataan obat atau perbekalan farmasi dengan meletakkan barang baru (datang terakhir) di depan barang yang datang sebelumnya.
3. *First Expired First Out* (FEFO) adalah sistem penataan obat atau perbekalan farmasi dengan meletakkan obat yang mempunyai tanggal kadaluarsa lebih dahulu di depan obat yang mempunyai tanggal kadaluarsa lebih akhir.

2.7.3 Bagian-Bagian yang Terlibat dalam Sistem Akuntansi Persediaan

Terdapat beberapa bagian yang terlibat dalam sistem akuntansi persediaan (Suhendar, 2006), yaitu:

1. Bagian Pembelian

   Bagian pembelian bertugas melakukan pembelian semua barang dan jasa yang dibutuhkan perusahaan. Untuk dapat melakukan fungsi ini, bagian pembelian harus melakukan langkah-langkah bahwa pembelian dilakukan dengan harga yang paling menguntungkan dan barang-barang yang dibeli akan dapat diterima tepat pada waktunya.

   Bagian pembelian perlu mengirimkan surat permintaan penawaran pada penyalur, agar pembelian dapat dilakukan dengan harga yang paling menguntungkan. Untuk menentukan penyalur yang akan diberi surat penawaran harga, perlu dipertimbangkan keadaan penyalur tersebut, seperti cukup terpercaya atau tidak, penyerahan barang tepat waktu atau tidak, dan syarat-syarat dari pernyalur tersebut.

   Apabila pembelian dilakukan dalam jumlah besar dan pembayaran bertahap, maka bagian pembelian harus membuat kontrak pembelian dan mengikuti setiap pengiriman barang dari penyalur. Bila diterima faktur pembelian, maka bagian pembelian bertugas untuk memeriksa faktur ini mengenai kebenaran barang yang dipesan, kuantitas barang, dan jumlah uang.

2. Bagian Penerimaan Barang

   Bagian ini bertugas untuk menerima semua barang yang dibeli. Pada waktu menerima barang, bagian ini harus melakukan perhitungan fisik atas

barang yang diterima baik dengan cara menghitung, menimbang, atau cara yang lainnya. Selain itu, bagian penerimaan barang harus mengadakan pemeriksaan kualitas dari barang yang diterima. Apabila barang-barang yang diterima itu sudah disetujui kualitas dan kuantitas fisiknya, maka bagian penerimaan barang akan membuat laporan penerimaan barang atau menandatangani tembusan pesanan pembelian yang berfungsi sebagai laporan penerimaan barang.

Jika terdapat barang-barang yang ditolak karena cacat atau tidak sesuai dengan pesanan pembelian, maka bagian penerimaan barang akan membuat berita acara penolakan barang yang diserahkan pada bagian pengiriman barang. Kemudian, barang tersebut akan diserahkan kembali kepada penyalur.

3. Bagian Gudang

Bagian ini bertugas untuk menyimpan barang-barang milik perusahaan. Tugas bagian gudang adalah mencocokkan terlebih dahulu jenis dan kuantitas barang yang datang dan keluar dengan data yang tercantum dalam laporan penerimaan barang, kemudian melakukan pencatatan pada kartu gudang dan kartu persediaan. Bagian gudang bertanggung jawab atas penyimpanan fisik persediaan di gudang.

4. Bagian Akuntansi

Bagian ini terdiri dari tiga subbagian yaitu subbagian jurnal, subbagian kartu persediaan, dan subbagian utang. Bagian akuntansi yang terkait dalam transaksi pembelian adalah fungsi pencatatan utang dan fungsi pencatatan persediaan. Bagian pencatatan utang bertanggung jawab untuk mencatat

transaksi pembelian ke dalam register bukti kas keluar untuk menyelenggarakan arsip dokumen sumber (bukti kas keluar) yang berfungsi sebagai catatan utang atau menyelenggarakan kartu utang sebagai buku pembantu utang. Bagian pencatatan persediaan bertanggung jawab untuk mencatat harga pokok persediaan barang yang dibeli ke dalam kartu persediaan.

5. Bagian Penjualan

Bagian ini bertanggung jawab melayani kebutuhan barang pelanggan dengan mengisi faktur penjualan dan untuk meminta barang dari bagian gudang,

2.8 Sistem Pengendalian Internal

Sistem pengendalian internal adalah kebijakan, prosedur, latihan, dan struktur organisasi yang didesain untuk memberikan jaminan yang layak pada upaya pencapaian tujuan bisnis yang akan dicapai dan memastikan kejadian-kejadian yang tidak diinginkan akan dicegah atau dideteksi dan dikoreksi (Cangemi dan Singleton dalam Herawati, 2008). Pengendalian internal dilaksanakan oleh manusia, tetapi tidak hanya berfokus sebagai pedoman kebijakan, melainkan perlu berfokus pada manusia sebagai pihak yang terlibat dalam berbagai tingkatan organisasi (Boynton *et al.*, 2002)

Dalam memahami pengendalian internal, diperlukan beberapa pertimbangan pengendalian yang berhubungan dengan tujuan organisasi. Pemahaman tersebut dilakukan dengan mengidentifikasi komponen pengendalian

internal. Menurut Boynton *et al.*(2002), terdapat lima komponen pengendalian internal yang termasuk dalam kerangka COSO (*Committee of Sponsoring Organizatons*), yaitu:

1. Lingkungan Pengendalian (*Control Environment*)

Menetapkan suasana dari suatu organisasi yang mempengaruhi kesadaran akan pengendalian dari orang-orangnya. Lingkungan pengendalian merupakan pondasi dari semua komponen pengendalian internal lainnya yang menyediakan disiplin dan struktur. Faktor pembentuk lingkungan pengendalian yaitu integritas dan nilai etika, komitmen terhadap kompetensi, dewan direksi dan komite audit, filosofi dan gaya operasi manajemen, struktur organisasi, penetapan wewenang dan tanggung jawab, serta kebijakan dan praktik sumber daya manusia.

2. Penilaian Risiko (*Risk Assessment*)

Dalam tujuan pelaporan keuangan, maka dilakukan identifikasi, analisis, dan pengelolaan risiko suatu organisasi yang relevan dengan penyusunan laporan keuangan yang disajikan secara wajar sesuai dengan prinsip-prinsip akuntansi yang berlaku umum. Kemudian, manajemen juga perlu mempertimbangkan beberapa hal mengenai risiko yang akan muncul atau perubahan kondisi, seperti perubahan dalam lingkungan operasi, personel (staf) baru, sistem informasi yang baru atau dimodifikasi, pertumbuhan yang cepat, teknologi baru, produk atau aktivitas baru, restrukturisasi organisasi, operasi di luar negeri, pernyataan akuntansi.

3. Informasi dan Komunikasi (*Information and Communication*)

Terdiri dari metode-metode dan catatan-catatan yang diciptakan untuk mengidentifikasi, mengumpulkan, menganalisis, mengklasifikasi, mencatat, dan melaporkan transaksi-transaksi atau kejadian-kejadian organisasi dan untuk memelihara akuntabilitas dari aset dan kewajiban yang berhubungan. Komunikasi melibatkan penyediaan suatu pemahaman yang jelas mengenai peran dan tanggung jawab individu berkenaan dengan pengendalian internal atas pelaporan keuangan.

4. Aktivitas Pengendalian (*Control Activities*)

Aktivitas pengendalian atau kebijakan dan prosedur yang membantu memastikan bahwa perintah manajemen telah dilaksanakan atau tindakan yang diperlukan berkenaan dengan risiko telah diambil untuk pencapaian tujuan organisasi. Dalam audit operasional, aktivitas pengendaliannya adalah pemisahan tugas, pengolahan pengendalian informasi (pengendalian umum dan aplikasi), pengendalian fisik, dan *review* kinerja.

Pada aktivitas pengendalian umum, terdapat lima jenis, yaitu pengendalian organisasi dan operasi, pengendalian pengembangan sistem dan dokumentasi, pengendalian perangkat keras dan sistem perangkat lunak, pengendalian akses, serta pengendalian data dan prosedur. Kemudian untuk pengendalian aplikasi terbagi menjadi tiga jenis, yaitu pengendalian masukan, proses, dan keluaran.

5. Pemantauan (*Monitoring*)

Suatu proses yang menilai kualitas kinerja pengendalian internal pada suatu waktu. Pemantauan melibatkan penilaian rancangan dan pengoperasian

pengendalian dengan dasar waktu dan mengambil tindakan perbaikan yang diperlukan. Aktivitas pemantauan dapat dilaksanakan melalui aktivitas yang berkelanjutan, contohnya masalah pengendalian internal yang menarik perhatian manajemen melalui keluhan dari pelanggan tentang kekeliruan tagihan. Kemudian, aktivitas pemantauan dengan pengevaluasian periodik secara terpisah, contohnya auditor internal secara umum menilai bagian yang berbeda dari pengendalian internal organisasi pada berbagai interval dan melaporkan kelemahan kepada manajemen dan komite audit dengan memberikan rekomendasi perbaikan yang sesuai. Dengan demikian, manajemen dapat menerima informasi mengenai kelemahan dan perbaikan yang direkomendasikan.

Penetapan sistem pengendalian internal oleh manajemen organisasi dapat mendorong tercapainya tujuan audit operasional sistem informasi. Menurut Weber (1999), terdapat beberapa komponen utama sistem pengendalian internal, yaitu:

1. Pemisahan tugas
2. Delegasi wewenang dan tanggung jawab
3. Staf yang kompeten dan terpercaya
4. Sistem otorisasi
5. Dokumen dan arsip yang memadai
6. Pengendalian fisik atas aset dan arsip
7. Pemantauan manajemen yang memadai
8. Pengawas independen atas kinerja
9. Perbandingan arsip yang dapat dipertanggungjawabkan dengan aset

Menurut Hadibroto dalam Lubis (2003), terdapat masalah dalam pengendalian persediaan. Masalah pengendalian persediaan tersebut yaitu:

1. Pengendalian fisik

   Hal ini merupakan pengendalian terhadap fisik barang yang disimpan agar tidak terjadi pencurian atau kerusakan pada barang tersebut. Perusahaan harus membuat gudang yang baik, mempekerjakan orang-orang tertentu untuk menjaga, dan apabila perlu persediaan juga diasuransikan terhadap pencurian, kebakaran, dan lain-lain.

2. Pengendalian akuntansi

   Hal ini merupakan pengendalian melalui prosedur-prosedur pembukuan yang baik. Pengendalian ini timbul karena adanya pencatatan jumlah-jumlah persediaan dalam kartu-kartu persediaan yang langsung diambil dari salinan laporan penerimaan dan permintaan pemakaian, sehingga semua yang terjadi di gudang akan terlihat dalam kartu persediaan. Pengendalian yang lebih efektif memerlukan pemisahan tugas antara orang yang bertanggung jawab terhadap gudang dan orang yang mencatat kartu persediaan, sehingga mereka dapat saling mengawasi. Selain itu, sistem otorisasi dan pemeriksaan fisik ke gudang juga merupakan bagian dari pengendalian akuntansi.

3. Pengendalian jumlah yang dibutuhkan

   Hal ini merupakan pengendalian yang bertujuan agar persediaan selalu ada dan cukup tersedia dalam memenuhi permintaan langganan atau untuk produksi. Keterangan persediaan akan menimbulkan kerugian tidak dipenuhinya permintaan langganan atau terganggunya proses produksi, tetapi

persediaan yang terlalu banyak menimbulkan kerugian karena membutuhkan biaya, bunga, biaya penyimpanan, dan lain-lain yang relatif besar. Jumlah persediaan yang optimal dalam perusahaan harus selalu diawasi sesuai dengan kebutuhan agar tidak menimbulkan kerugian.

2.9 Jenis Pengendalian Sistem Informasi

Menurut Weber (1999), terdapat dua jenis pengendalian sistem informasi yang menjadi dasar pelaksanaan audit sistem informasi, yaitu sistem manajemen (*management systems*) dan sistem aplikasi (*application systems*). Jika sistem manajemen akan menyediakan infrastruktur yang stabil sehingga sistem informasi dapat dibangun dan dioperasikan secara harian, sedangkan sistem aplikasi akan melakukan pengolahan transaksi dasar, pelaporan manajemen, dan dukungan keputusan. Sistem manajemen dan aplikasi tersebut merupakan suatu jenis pengendalian dalam sistem informasi.

Dalam pengendalian manajemen terdapat subsistem-subsistem (Weber, 1999), yaitu:

1. *Top management*: harus memastikan fungsi sistem informasi diatur dengan baik, bertanggung jawab terutama atas keputusan kebijakan jangka panjang sehingga sistem informasi akan digunakan dalam organisasi.
2. *Information systems management*: pertanggungjawaban atas perencanaan dan pengendalian semua aktivitas sistem informasi, penyediakan saran untuk *top management* dalam hubungannya dengan pembuatan keputusan

kebijakan jangka panjang, dan menerjemahkan kebijakan tersebut menjadi tujuan yang lebih singkat.

3. *Systems development management*: bertanggung jawab atas desain, implementasi, dan pemeliharaan sistem aplikasi.
4. *Programming management*: bertanggung jawab atas pemprograman sistem baru, pemeliharaan sistem lama, dan penyediaan *software* pendukung sistem umum.
5. *Data administration*: bertanggung jawab atas penyebutan perencanaan dan pengendalian masalah yang berhubungan dengan penggunaan data organisasi.
6. *Quality assurance management*: bertanggung jawab atas kepastian pengembangan sistem informasi, implementasi, pelaksanaan, dan pemeliharaan sesuai dengan standar kualitas.
7. *Security administration*: bertanggung jawab atas pengendalian akses dan keamanan fisik atas fungsi sistem informasi.
8. *Operations management*: bertanggung jawab atas perencanaan dan pengendalian operasional sistem informasi harian.

Dalam pengendalian aplikasi terdapat subsistem-subsistem (Weber, 1999), yaitu:

1. *Boundary*: terdiri atas komponen-komponen yang membentuk hubungan antara pengguna dengan sistem.
2. *Input*: terdiri atas komponen-komponen yang mengambil, menyiapkan, dan memasukan perintah dan data ke sistem.

3. *Communication*: terdiri atas komponen-komponen yang mengirimkan data diantara subsistem dan sistem.
4. *Processing*: terdiri atas komponen-komponen yang melakukan pengambilan keputusan, penghitungan, pengklasifikasian, pemesanan, dan peringkasan data dalam sistem.
5. *Database*: terdiri atas komponen-komponen yang menegaskan, menambah, mengakses, mengubah, dan menghapus data dalam sistem.
6. *Output*: terdiri atas komponen-komponen yang menerima kembali dan memberi data kepada pengguna sistem.

Kumpulan subsistem yang terintegrasi dari masing-masing pengendalian akan membentuk suatu pengendalian sistem informasi yang kokoh.

2.9.1. Pengendalian Manajemen Pengamanan (*Security Management Controls*)

Menurut Weber (1999), terdapat dua macam pengamanan sistem informasi, yaitu:

1. *Physical Security*, melindungi aset sistem informasi fisik dalam organisasi, seperti personil (staf), *hardware*, fasilitas, *supplies*, dan dokumentasi.
2. *Logical Security*, melindungi data atau informasi dan *software*.

Dalam usaha pengamanan aset sistem informasi organisasi, terdapat masalah atau ancaman yang akan muncul pada kegiatan operasionalnya. Sembilan ancaman aset sistem informasi, menurut Weber (1999), yaitu : *Fire Damage* (kebakaran), *Water Damage* (banjir), *Energy Variations* (Perubahan Energi),

Structural Damage (Kerusakan Struktural), *Pollution* (Polusi), *Unauthorized Intrusion* (Gangguan dari Pihak yang Tidak Berwenang), *Viruses and Worm*, *Missuse of Software, Data, and Services* (Penyalahgunaan *Software*, Data, dan Jasa), dan *Hacking*.

Terdapat berbagai macam ancaman yang dapat menyerang aset sistem informasi. Apabila ancaman keamanan sudah tidak dapat dicegah, maka diperlukan pengendalian terakhir (*control of last resort*) untuk meminimalkan kerugian dan memastikan kegiatan operasional organisasi tetap berjalan. Menurut Weber (1999), terdapat dua macam pengendalian terakhir yaitu *Disaster Recovery Plan* dan *Insurance*.

A. *Disaster Recovery Plan* (Rencana Pemulihan Bencana)

Rencana pemulihan bencana meliputi empat bagian (Cerullo dalam Weber, 1999), yaitu:

1. *Emergency Plan*: menentukan tindakan yang harus dilakukan segera setelah terjadi bencana. Pada semua kasus, semua karyawan bertanggung jawab atas tindakan yang harus dilakukan dan mengikuti semua protokol yang ditentukan dengan jelas.
2. *Backup Plan*: menetapkan jenis cadangan yang akan disimpan, frekuensi cadangan yang akan dibuat, prosedur untuk menbuat cadangan, lokasi sumber daya cadangan, tempat sumber daya dapat dipasang dan operasi dimulai kembali, personil (staf) yang bertanggung jawab atas kumpulan sumber daya cadangan dan mengulangi operasi, prioritas yang ditugaskan untuk memperbaiki berbagai sistem, dan batasan waktu dalam

memperbaiki setiap sistem yang terpengaruh. Sumber daya yang perlu dipertimbangan dalam membuat cadangannya adalah personil (staf), *hardware*, fasilitas, dokumentasi, persediaan, data, informasi, *application software*, dan *systems software*.

3. *Recovery Plan*: sebagai prosedur perlengkapan untuk memulihkan kemampuan sistem informasi secara penuh.
4. *Test Plan*: bertujuan untuk mengidentifikasi kekurangan pada *emergency, backup,* atau *recovery plans* atau pada persiapan organisasi dan personil saat kejadian bencana. Secara periodik, *test plan* harus dilakukan, contohnya bencana yang harus disimulasikan dan personil sistem informasi yang dibutuhkan untuk memahami prosedur *backup* dan *recovery.*

B. *Insurance* (Asuransi)

Terkadang asuransi dapat digunakan untuk mengurangi kerugian yang timbul ketika bencana terjadi. Polis asuransi biasanya dapat menutupi kerugian sumber daya perlengkapan, fasilitas (aset sistem informasi), media penyimpanan, *business interruption*, beban tambahan, kertas dan arsip yang bernilai, piutang dagang, media transportasi, malpraktik, kesalahan, dan kelalaian.

Asuransi sistem informasi merupakan suatu asuransi yang baru, sehingga masih ada kemungkinan beberapa bencana yang belum dapat diatasi seperti serangan virus komputer. Dalam perjanjian dengan perusahaan asuransi,

administrator keamanan harus memastikan bahwa organisasinya telah memenuhi kewajiban atas kebijakan (polis) yang telah disepakati.

2.9.2. Pengendalian Manajemen Operasi (*Operations Management Controls*)

Pengendalian manajemen operasi memiliki hubungan yang erat dengan aktivitas operasional suatu organisasi. Manajemen sebagai pengelola organisasi memiliki tanggung jawab yang besar untuk mengendalikan semua aktivitas yang terjadi. Manajemen operasional yang mengelola aktivitas harian organisasi bertanggung jawab untuk menjalankan kegiatan operasional harian *hardware* dan *software*, sehingga sistem aplikasi produksi dapat menyelesaikan tugasnya dan staf pengembangan dapat merancang, melaksanakan, dan memelihara sistem aplikasi (Weber, 1999).

2.9.3. Pengendalian Batasan (*Boundary Controls*)

Boundary subsystem (subsistem batasan) menentukan hubungan antara pengguna sistem komputer dengan sistem komputer itu sendiri. Hubungan ini melibatkan beberapa komponen yang saling terintegrasi untuk menjaga keamanan aset, memelihara integritas data, dan mencapai tujuannya yaitu efektif dan efisien. Fungsi utama pengendalian batasan adalah untuk mengidentifikasi dan memastikan kebenaran pengguna, serta memberikannya hak istimewa (Weber, 1999).

Pengendalian dalam *bounday subsistem* memiliki tiga kegunaan utama (Weber, 1999), yaitu:

1. Menentukan identitas dan kebenaran pengguna sistem komputer.

   (Sistem harus memastikan bahwa penggunanya adalah pengguna yang sebenarnya)
2. Menentukan identitas dan kebenaran sumber daya bahwa keinginan pengguna untuk mempergunakannya.

   (Pengguna harus memastikan bahwa mereka diberikan sumber daya yang sebenarnya)
3. Membatasi tindakan akibat pengguna yang memperoleh sumber daya komputer supaya tindakannya benar.

   (Pengguna diijinkan untuk menggunakan sumber daya hanya dalam batasan tertentu)

Subsistem batasan memiliki beberapa komponen pengendalian yang memperkokoh sistem pengendaliannya. Menurut Weber (1999), terdapat beberapa macam pengendalian yang digunakan dalam *boundary subsystem*, yaitu:

1. *Cryptographic Controls*

Berfungsi untuk melindungi kerahasiaan data dan mencegah modifikasi data yang tidak benar. Pencapaian tujuan organisasi dengan penyebaran data sehingga data rahasia tersebut menjadi tidak berarti bagi orang lain yang tidak mempunyai cara untuk menyatukannya kembali menjadi data utuh yang bernilai. Pengendalian ini meningkat menjadi suatu hal yang sangat penting karena saat ini menjadi lebih sulit mencegah terjadinya akses data secara tidak benar.

Berdasarkan prespektif audit, aspek terpenting dari *cryptosystems* adalah pedoman *cryptographic* yang telah diatur. Pengaturan *cryptographic* ini disebut

sebagai *cryptographic key management*. Fungsinya yaitu untuk mengatur bagaimana pedoman akan dihasilkan, didistribusikan kepada pengguna, dan diinstal pada alat atau fasilitas yang disediakan untuk *cryptographic*.

2. *Access Controls*

Pengendalian ini membatasi penggunaan sumber daya sistem komputer kepada pengguna yang sebenarnya, membatasi tindakan pengguna dapat dilakukan sehubungan dengan sumber daya, dan memastikan pengguna hanya memperoleh sumber daya yang benar. Tahapan yang dilakukan dalam pengendalian akses adalah membuktikan pengguna yang benar-benar terlibat dalam sistem (sistem mengenali pengguna), membuktikan sumber daya yang diminta oleh pengguna, dan membatasi tindakan pengguna kepada orang-orang yang berwenang.

Pengguna dapat menetapkan tiga golongan informasi pembuktian dalam mekanisme pengendalian akses yaitu informasi yang diingat (*password*), memasukkan benda atau barang (*plastic cards*), dan karakteristik personal (*fingerprints*). Berdasarkan masing-masing golongan, pengendalian yang paling lemah adalah menggunakan *password* karena ada kemungkinan pengguna lupa dengan *password* yang dihafalnya, sedangkan pengendalian yang paling kuat adalah dengan *fingerprint* (sidik jari) karena masing-masing individu memiliki karakteristik yang berbeda-beda.

Kemudian, pengguna memakai empat macam sumber daya dalam sistem komputer yaitu *hardware, software,* barang-barang (pengolah waktu), dan data.

Berdasarkan sumber daya yang digunakan, sumber daya yang paling sulit dikendalikan adalah sumber data.

Dalam mekanisme pengendalian akses, terdapat dua kebijakan yang memperkuat pengendalian internal, yaitu kebijakan *discretionary access controls* dan *mandatory access controls*. Jika menggunakan kebijakan *discretionary access controls,* maka pengguna akan dapat memilih arsip-arsip yang akan mereka bagikan dengan pengguna lain atau membatasi akses arsip-arsipnya, sedangkan jika menggunakan kebijakan *mandatory access controls*, maka pengguna dan sumber daya ditugaskan memperbaiki keamanan atribut atau perlengkapan yang dapat menentukan pengguna dengan kewenangan akses sumber daya tertentu.

3. *Audit Trail Controls*

Audit trail (jejak audit) harus merekam semua peristiwa penting yang terjadi dalam subsistem batasan (*boundary*). Terdapat dua macam jejak audit yang harus ada dalam setiap subsistem, yaitu:

a. *Accounting Audit Trail*

Semua aplikasi material berdasarkan peristiwa yang terjadi dalam subsistem batasan (*boundary*) harus dicatat atau direkam dalam jejak audit akuntansi (*accounting audit trail*). Beberapa data yang berhubungan dengan peristiwa tertentu yang harus disimpan yaitu identitas pengguna sistem, kebenaran informasi yang disalurkan, sumber daya yang diminta, *terminal identifier*, waktu memulai dan mengakhiri, nomor saat mencoba masuk sistem, sumber daya yang disediakan atau ditolak, dan hak atas tindakan yang diizinkan atau tidak diizinkan. Data-data tersebut mengizinkan manajemen atau para auditor

untuk menggambarkan kembali urutan peristiwa ketika pengguna mencoba untuk dapat mengakses dan menggunakan sumber daya sistem.

b. *Operations Audit Trail*

Data-data yang terkumpul dalam *accounting audit trail* juga menyajikan *operations audit trail.* Contohnya, mencatat waktu awal dan akhir, mencatat sumber daya yang diminta, dan memudahkan analisis penggunaan sumber daya dalam subsistem. Seperti *accounting audit trail*, beberapa macam pemakaian sumber daya juga akan menjadi dasar pendeteksian aktivitas yang tidak sesuai dengan hak atau wewenang.

Pengendalian-pengendalian dalam subsitem batasan (*boundary*) memiliki alat untuk memastikan kebenaran informasi dari pengguna sistem komputer yang terotorisasi. Konsep pengendalian ini akan membuktian keaslian orang (*authenticating people*) dengan menggunakan *personal identification numbers* dan *digital signatures* dan mengidentifikasi orang (*identifying people*) dengan menggunakan *plastic cards*. *Personal identification numbers* (PINs) adalah bentuk informasi yang diingat, digunakan untuk membuktikan kebenaran pengguna sistem. *Digital signatures* digunakan untuk mencegah pemalsuan dan pengingkaran pesan elektronik, kemudian cara menggunakannya sama seperti *analog signature* yang dilakukan untuk menandatangani dokumen. *Plastic cards* bermaksud untuk mengidentifikasi individu yang ingin menggunakan sistem komputer.

2.9.4. Pengendalian Masukan (*Input Controls*)

Komponen subsistem *input* bertanggung jawab untuk membawa data dan perintah ke dalam sistem aplikasi. Kedua jenis *input* (data dan perintah) harus divalidasi atau disahkan dan dideteksi kesalahannya agar *input*-nya akurat, lengkap, unik, dan tepat waktu. Untuk melakukan *input* data ke dalam sistem aplikasi, auditor harus mengetahui beberapa macam cara yang digunakan yaitu *direct entry* (memasukan langsung) dan *recording medium* (direkam dahulu dalam perantara). *Direct entry* melalui *keyboard, touch screen, mouse,* dan lain-lain, sedangkan *recording medium* melalui dokumen sumber, *optical scanner, point-of-sale device, automatic teller machine,* dan lain-lain (Webber, 1999).

Perancangan dokumen sumber dan tampilan *data-entry* yang baik dapat mengurangi kesalahan memasukan data dan data yang masuk ke sistem aplikasi menjadi lebih efisien dan efektif. Faktor pengaruh yang terpenting dalam perancangan tampilan *data-entry* adalah tampilan yang digunakan untuk *direct-entry* input data atau tampilan yang digunakan untuk petunjuk data dari dokumen sumber. Pada kasus akhir-akhir ini, tampilan seharusnya mencerminkan dokumen sumber pada data adalah ditangkap dan direkam pertama kali (Weber, 1999).

Menurut Weber (1999), cara termudah dan pengendalian terefektif dalam aktivitas menangkap dan memasukan semua data adalah dengan *batch control*. *Batching* adalah proses mengelompokkan transaksi yang memuat beberapa macam hubungan satu sama lain. Terdapat dua macam pengelompokan yang dapat digunakan adalah *physical batches* dan *logical batches*. *Physical batches* adalah kelompok transaksi yang terdapat pada unit fisik, misalnya sekumpulan

dokumen sumber, sedangkan *logical batches* adalah kelompok transaksi yang terikat bersama-sama pada dasar logis, tetapi tidak berdekatan secara fisik, misalnya transaksi dimasukan secara langsung ke dalam sambungan atau terminal selama beberapa periode waktu. Pengendalian dapat dilakukan dengan pengelompokkan untuk mengidentifikasi suatu hal yang tidak berwenang, tidak akurat, dan data yang tidak lengkap.

Data yang dimasukan sebagai *input* sistem aplikasi seharusnya telah divalidasi segera setelah data ditangkap dan serupa dengan sumbernya (Weber, 1999). Jika terjadi kesalahan memasukan data, maka dapat segera dikoreksi supaya sistemnya dapat berjalan dengan lancar.

Menurut Weber (1999), jejak audit dalam subsistem input mengelola kronologi peristiwa dari data dan perintah waktu yang ditangkap dan dimasukan ke dalam sistem aplikasi sampai dianggap *valid* (sah) dan melewati subsistem lain dalam sistem aplikasi. Kemudian, jejak audit akuntansinya harus mencatat sumber, isi, dan pemilihan waktu dari data dan perintah dimasukan ke dalam sistem aplikasi.

2.9.5. Pengendalian Keluaran (*Output Controls*)

Subsistem *output* memberikan konten atau isi data yang akan diberikan kepada pengguna, data akan disusun dan diberikan kepada pengguna, dan data akan disiapkan dan diteruskan ke pengguna. Komponen utama pada subsistem *output* adalah *software* dan personil yang akan menentukan konten atau isi, susunan, dan ketepatan waktu dari data untuk diberikan kepada pengguna.

Beberapa perangkat *hardware* juga dibutuhkan untuk menyusun data *output*, misalnya *printers*, *terminals*, dan *voice synthesizers* (Weber, 1999).

Sistem keluaran memiliki beberapa komponen yang saling melengkapi dan memperkokoh sistem. Menurut Weber (1999), terdapat beberapa macam pengendalian yang digunakan dalam *output subsistem*, yaitu:

1. *Inference Controls*

Pengendalian ini digunakan untuk mencegah terjadinya sesuatu yang membahayakan *database* statistik dengan cara mempertimbangkan kewenangan akses data. Oleh karena itu, *inference controls* digunakan untuk menyaring *output* yang diizinkan untuk dilihat oleh pengguna. Bentuk *database* yang didapatkan pengguna hanya dapat memperoleh statistik jumlah dari nilai suatu data individu, sedangkan *database* statistik berisi data yang sensitif dan rahasia, seperti kumpulan data riwayat medis.

2. *Batch Output Production and Distribution Controls*

Batch output adalah keluaran yang dihasilkan dari beberapa operasi dan kemudian dibagi-bagikan kepada pengguna *output*. *Batch output production and distribution controls* digunakan untuk memastikan *batch output* tidak hilang, rusak, atau kerahasiaan data tidak dilanggar selama persiapan dan perjalanan ke pengguna. Pengendalian perlu dibentuk dalam produksi dan distribusi *batch output* untuk memastikan bahwa keakuratan, kelengkapan, dan ketepatan waktu *output* disediakan hanya untuk pengguna yang berwenang.

Pengendalian ini dapat dilakukan melalui bermacam-macam tahapan dalam produksi dan distribusi *output batch*, contohnya mengamankan tempat

penyimpanan surat-surat khusus yang digunakan untuk membuat *output batch*, memastikan hanya pengguna yang berhak diperbolehkan mengeksekusi program *batch report*, memastikan konten *file* yang dicetak tidak dapat diubah, mencegah pihak ketiga yang tidak berhak untuk melihat konten laporan rahasia yang sudah dicetak, mengumpulkan laporan dengan segera untuk mencegah kehilangan laporan, memiliki staf *client service* untuk meninjau *batch output* yang sebelumnya salah didistribusikan ke pengguna, memiliki pengguna akhir *output* yang meninjau kesalahan dan ketidakbenaran, menyimpan *batch output* secara aman, menentukan periode penyimpanan yang tepat untuk *batch output*, dan menyobek hasil *batch output* jika tidak dibutuhkan lagi.

3. *Batch Report Design Controls*

Laporan *batch output* dirancang untuk melakukan pengendalian yang efisien dan efektif, contohnya pada halaman judul laporan seharusnya menampilkan daftar distribusi dari laporan dan orang yang dapat dihubungi jika masalah operasional ditemui pada pembuatan laporan dan pada halaman rincian seharusnya berisi nomor halaman dari laporan yang dideteksi.

4. *Online Output Production and Distribution Controls*

Online output adalah keluaran yang dikirimkan secara elektronis ke terminal yang dipakai pengguna untuk mendapatkan akses ke sistem. Pengendalian perlu dibentuk dalam produksi dan distribusi *batch output* untuk memastikan bahwa keakuratan, kelengkapan, dan ketepatan waktu *output* disediakan hanya untuk pengguna yang berwenang.

Pengendalian ini dapat dilakukan melalui beberapa tahapan dalam produksi dan distribusi *online output*, contohnya memastikan bahwa *output* yang diakses *online* sudah disahkan atau divalidasi, akurat dan lengkap, memastikan bahwa *online output* didistribusikan ke alamat jaringan yang benar, menjaga integritas dan rahasia *online output* yang dikirimkan melalui saluran komunikasi, mengecek data yang diterima dari pengguna bermaksud tertentu, menentukan periode penyimpanan yang tepat untuk *online output*, dan menghapus *online output* secara lengkap jika sudah tidak dibutuhkan lagi.

5. *Audit Trail Controls*

Pada pengendalian ini, subsistem *output* menyimpan kronologi peristiwa yang terjadi dari waktu konten *output* yang disatukan sampai waktu pengguna melengkapi penyelesaian *output* karena tidak harus disimpan lagi. Jejak audit akuntansi dalam subsistem *output* menunjukkan *output* yang disatukan untuk diberikan kepada pengguna mengenai *output* yang disajikan, orang yang akan menerima *output*, kapan *output* diterima, dan tindakan apa yang selanjutnya dilakukan setelah menerima *output*. Kemudian, untuk jejak operasional audit, pencatatan penggunaan sumber daya oleh komponen dalam subsistem *output* menyatukan, menghasilkan, mendistribusikan, menggunakan, menyimpan, dan menyelesaikan berbagai macam *output*.

2.10. Audit Sistem Informasi

Audit sistem informasi merupakan proses pengumpulan dan pengevaluasian bukti untuk menentukan apakah sistem komputer dapat

melindungi aset, memelihara integritas data, mencapai tujuan organisasi secara efektif, dan menggunakan sumber daya secara efisien (Weber, 1999). Berdasarkan pengertian tersebut, audit sistem informasi menganalisis segala aspek yang dimiliki organisasi dan mendukung tujuan audit tradisional. Audit sistem informasi dilakukan untuk mengevaluasi sistem informasi dan menyarankan tindakan untuk meningkatkan nilai bagi bisnisnya.

Menurut Weber (1999), terdapat empat tujuan audit sistem informasi, yaitu:

1. Perlindungan Aset (*Safeguarding Asset*)

   Aset sistem informasi organisasi yang dimaksud adalah *hardware, software*, fasilitas, orang-orang (pengetahuan), arsip data, dokumentasi sistem, dan persediaan.

2. Integritas Data (*Data Integrity*)

   Suatu data harus memiliki atribut kelengkapan (*completeness*), kekuatan (*soundness*), kemurnian (*purity*), dan ketelitian *(veracity*).

3. Efektifitas Sistem (*System Effectiveness*)

   Evaluasi efektifitas berdampak pada pengetahuan atas kebutuhan pengguna seperti karakteristik pengguna dan lingkungan pengambilan keputusan, sehingga digunakan untuk mengevaluasi apakah informasi laporan sistem dapat memfasilitasi pembuatan keputusan oleh pengguna.

4. Keefisienan Sistem (*System Efficiency*)

   Sistem informasi yang efisien menggunakan sumber daya yang minimal untuk mencapai tujuannya. Manajemen harus menentukan apakah efisiensi

dapat meningkat dengan sumberdaya yang ada atau membeli sumber daya tambahan.

Dalam melakukan audit sistem informasi, auditor yang akan melakukan pengujian pengendalian harus memutuskan untuk menguji pengendalian dengan pendekatan tertentu. Ada dua pendekatan yang dapat digunakan (Weber, 1999), yaitu:

1. *Audit Around the Computer*

   Pendekatan ini melibatkan suatu opini audit melalui pengujian dan pengevaluasian pengendalian manajemen, kemudian hanya *input* dan *output* pada sistem aplikasi (*application systems*). Apabila kualitas *input* dan *output* dalam sistem sudah berkualitas, maka dapat dipastikan bahwa proses yang berlangsung juga berkualitas.

   Audit Around the Computer lebih cocok dilakukan jika sistem aplikasinya sederhana (*simple*), *input* data dengan sistem *batch*, risiko bawaannya rendah, dan keandalan pengolahan internal sistem dapat dengan mudah ditaksir atau diduga. Pendekatan ini berfokus pada keandalan pengendalian pengguna daripada keandalan pengendalian komputer.

2. *Audit Through the Computer*

   Pendekatan ini menggunakan komputer untuk menguji pengolahan logika dan pengendalian sistem yang ada, serta arsip yang dihasilkan oleh sistem. Pengujian yang dilakukan dalam pendekatan ini lebih berfokus pada aplikasi komputer yang digunakan dalam sistem aplikasi, sehingga jangkauan dan

kapasitas pengujian dapat diperluas, serta meningkatkan keandalan pengumpulan dan pengevaluasian bukti.

Audit Through the Computer lebih cocok dilakukan jika risiko bawaan aplikasinya tinggi dan sulit untuk menaksir atau menduga pengolahan internal yang dijalankan oleh sistem. Apabila suatu audit menggunakan pendekatan ini, maka kadang kala membutuhkan biaya yang banyak dan keahlian teknis yang luas.

2.11. Audit Operasional Sistem Informasi

Menurut Romney dan Steinbart (2006), teknik dan prosedur yang digunakan dalam audit operasional mirip dengan audit sistem informasi dan laporan keuangan, tetapi memiliki perbedaan pada ruang lingkupnya. Jika audit sistem informasi pada lingkup pengendalian internal, sedangkan laporan keuangan hanya pada *output* sistemnya. Kemudian, untuk operasional audit ini lingkupnya lebih luas yaitu semua aspek manajemen sistem informasi yang bertujuan untuk mengevaluasi keefektifan, keefisienan, dan pencapaian tujuan organisasi.

Beberapa aktivitas yang dilakukan selama audit operasional dalam pengumpulan bukti (Romney dan Steinbart, 2006) adalah meninjau pelaksanaan kebijakan dan dokumentasi, mengkonfirmasi prosedur manajemen dengan personil operasional, mengamati aktivitas dan fungsi operasional, menguji laporan dan perencanaan operasional dan keuangan, menguji akurasi informasi opersional, dan menguji pengendalian.