PENGENDALIAN INTERN PADA SISTEM INFORMASI AKUNTANSI BERBASIS KOMPUTER

Oleh: **Ahmad Yani**

ABSTRACT

An Accounting Information System (AIS) is one of the subjects in a profit-oriented organization. In reality, AIS is very much influenced by the development of information technology, which result numerous computer-based AIS. The implementation of information technology in AIS does not make the system flawless (error free or corruption free). A good accounting information system (manual or computerized) must have a control. An internal control is thus needed to avoid such flaws. Furthermore, an internal control is useful for audit trail. The fact that implementing an internal control to an Accounting Information System is very important makes it a compulsory to create a high standard AIS output. This is like many other systems that are open to any errors or corruptions. The internal control covers the structure of organization, the coordinated methods, and the established measurements of a business organization to keep company's assets, accuracy and truth of the accounting data as well as the efficiency of company operational.

Sistem Informasi Akuntansi (SIA) merupakan salah satu subyek dari suatu manajemen dalam sebuah organisasi bisnis (profit oriented). Dalam kenyataanya SIA saat ini sangat dipengaruhi oleh perkembangan teknologi terutama teknologi Informasi. Karenanya sebagian besar saat ini SIA sudah berbasis komputer. Pemanfaatan teknologi informasi dalam SIA bukan berarti SIA sudah sempurna (bebas dari kesalahan, kecurangan) yang mungkin terjadi. Sistem Informasi Akuntansi yang baik (manual atau terkomputerisasi) tetap harus memiliki suatu pengendalian. Sistem pengendalian yang intern (internal control) yang diterapkan dalam Sistem Informasi Akuntansi akan sangat berguna untuk tujuan pencegahan terjadinya hal-hal yang tidak diinginkan seperti kesalahan maupun kecurangan-kecurangan. Disamping itu sistem pengendalian intern juga dapat digunakan untuk melacak kesalahan-kesalahan yang sudah terjadi (audit trail). Demikian pentingnya pengendalian intern diterapkan dalam Sistem Informasi Akuntansi sehingga hal ini merupakan suatu keharusan untuk dapat menghasilkan keluaran (output) SIA yang bernilai. Sistem Informasi Akuntansi merupakan salah satu dari sekian banyak sistem yang terbuka yang tidak bisa dijamin dari kesalahan ataupun kecurangan-kecurangan. Apabila SIA dilengkapi dengan pengendalian intern maka SIA akan berjalan dan berfungsi sebagaimana mestinya. Pengendalian intern meliputi struktur suatu organisasi dan semua metode-metode yang terkoordinir serta ukuran-ukuran yang telah ditetapkan di dalam suatu organisasi bisnis (perusahaan) untuk tujuan menjaga aset perusahaan, ketepatan dan kebenaran data akuntansi serta efesiensi operasi perusahaan.

I. PENDAHULUAN

Pemanfaatan teknologi informasi (TI) dalam Sistem Informasi Akuntansi akan sangat mempengaruhi metode dan prosedur yang ada dalam sistem. Dalam Sistem Informasi Akuntansi yang terkomputerisasi akan terjadi penggabungan prosedur dan tugas yang tidak dapat dilakukan pada Sistem Informasi Akuntansi manual. Oleh karenanya pengendalian intern pada Sistem Informasi Akuntansi yang sudah

berbasis komputer juga akan berbeda dengan yang masih manual. Dalam tulisan ini Penulis akan membahas pengendalian intern yang dilakukan dalam Sistem Informasi Akuntansi yang berbasis komputer.

Pengendalian intern pada Sistem Informasi Akuntansi yang berbasis komputer terdiri dari pengendalian umum (*General Control*) dan pengendalian khusus aplikasi (*Aplication Control*). Pengendalian umum meliputi pengendalian organisasi dan operasi, pengendalian dalam bidang pengembangan sistem, pengendalian perangkat keras (*hardware*), pengendalian perangkat lunak (*software*) serta pengendalian penggunaan komputer (fasilitas dan datanya). Sedangkan pengendalian khusus aplikasi meliputi penggunaan aplikasi-aplikasi *software* yang ada mulai dari pengendalian masukan (*input*), pengolahan (*process*) hingga keluaran yang dihasilkan (*output*). Pengendalian *intern* dalam Sistem Informasi Akuntansi yang secara garis besar meliputi struktur organisasi, semua metode-metode dan cara-cara yang terkoordinir dengan ukuran-ukuran yang telah ditetapkan mempunyai tujuan agar dapat menjaga keamanan harta kekayaan (*asset*) perusahaan, memeriksa ketepatan dan kebenaran data akuntansi, meningkatkan efesiensi operasi kegiatan serta mendorong ditaatinya kebijkan-kebijakan manajemen.

II. PEMBAHASAN

Berikut ini adalah gambaran apa saja yang dilakukan dalam pengendalian intern pada Sistem Informasi Akuntansi yang berbasis komputer. Pengendalian *intern* yang dimaksud adalah sebagai berikut:

1. Pengendalian Umum (*General Control*)

Pengendalian secara umum merupakan pengendalian akuntansi yang mempunyai tujuan keamanan dari harta kekayaan perusahaan. Pengendalian ini merupakan di luar aplikasi pengolahan data. Pengendalian secara umum terdiri dari :

a. Pengendalian organisasi dan operasi

Pengendalian organisasi dan operasi ini dirancang untuk menciptakan kerangka organisasi aktivitas pengolahan data secara elektronika (PDE). Dalam hal ini meliputi:

1). Pemisahaan Fungsi Antar Bagian

Suatu organisasi akan terdiri dari beberapa bagian (departemen) dan tiap departemen harus diorganisasikan sedemikian rupa yang mempunyai tugas dan tanggung jawab yang terpisah antara satu dengan yang lainnya. Sistem Informasi Akuntansi hanya mempunyai tanggung jawab dalam tugas-tugas tertentu seperti pengolahan data serta pembuatan laporan-laporan keuangan kepada para pemakai. Sedangkan beberapa kegiatan lain yang tidak berhubungan langsung dengan kegiatan yang ada dalam SIA harus dilakukan terpisah. Agar tidak terjadi kesimpangsiuran fungsi dalam organisasi, perlu dibuat deskripsi jabatan yang berisi tugas dan wewenang setiap departemen. Deskripsi jabatan ini perlu dibuat untuk menunjukkan nama jabatan dan berisi penjelasan-penjelasan fungsi tiap-tiap bagian.

Pemisahan tugas dan tanggung jawab antar departemen dapat berupa sebagai berikut:

a). Semua transaksi dan perubahan terhadap catatan *file* induk (*master file*) harus berasal dan diotorisasi oleh bagian lain selain PDE.
b). Bagian PDE tidak boleh menyimpan aktiva, kecuali aktiva pengolah data.
c). Bila terjadi kesalahan transaksi harus dibetulkan sendiri oleh bagian yang bersangkutan bukan oleh bagian PDE. Bagian PDE hanya boleh membetulkan kesalahan yang terjadi selama proses pengolahan.

d). Bagian yang berwenang mengotorisasi transaksi tidak boleh menyimpan aktiva hasil transaksi.

Bagian PDE bisa merupakan bagian dari fungsi akuntansi (berada di bawah *controller*) bisa juga terpisah sebagai unit yang berdiri sendiri, yaitu bagian PDE.

Bagian PDE di bawah *Controller*

Bila bagian PDE ini berada di bawah *controller*, ada beberapa keuntungan sebagai berikut:

a). Bila terjadi keinginan perubahan dari sistem akuntansi manual ke sistem yang berbasis komputer, maka tidak akan terlalu mengejutkan departemen PDE yang berada di bawah *controller* dan mudah diterima.

b). Peranan dan fungsi pengolahan akuntansi dan pelaporan keuangan terpisah dengan PDE sehingga fungsi dari akuntansi yang bertanggungjawab terhadap pengolahan transaksi dan penyedia informasi keuangan kepada manajer. Fungsi yang lainnya dan kepada pihak luar lebih efektif.

c). Karena keberhasilan aplikasi komputer di dalam kegiatan akuntansi seperti misalnya penggajian, pengendalian persediaan merupakan tanggung jawab akuntan, sedang akuntan terlibat langsung di dalamnya, maka diharapkan dalam pengembangan aplikasi tersebut akan lebih efektif.

d). Jika bagian PDE di bawah *controller*, maka seorang *controller* harus memahami dan menguasai teknologi pengolahan data dengan baik, apalagi jika data yang akan diolah juga meliputi data *non* akuntansi. Peranan *controller* harus dibekali dengan pengetahuan yang berhubungan dengan kedua jenis data tersebut.

Bagian PDE terpisah dari bagian Akuntansi.

Bagian PDE dapat juga dibuat terpisah dari bagian akuntansi, artinya bagian ini diorganisasikan menjadi unit tersendiri dan berada di bawah tanggungjawab manajer tersendiri, yakni manajer PDE. Tentu saja jika bagian PDE ini terpisah dari bagian atau fungsional akuntansi mempunyai dasar pertimbangan bahwa bagian PDE ini tidak hanya melakukan pengolahan data akuntansi akan tetapi mengolah juga data *non* akuntansi. Dengan demikian bagain PDE ini tidak hanya didominasi oleh fungsional akuntansi yang hanya melakukan fungsi pengolahan data akuntansi. Dengan melakukan pemisahan fungsi antara fungsional akuntansi dengan fungsional PDE fungsi pengolahan data akan lebih efektif.

2). Pemisahan fungsi-fungsi di dalam Bagian PDE

Bagian PDE memiliki fungsi-fungsi utama, yaitu:

Fungsi Pengembangan Sistem

Fungsi pengembangan sistem ini meliputi pembuatan program-program aplikasi yang dibutuhkan dan pengembangan sistem yang digunakan. Dengan kata lain personil yang ada pada bagian ini bertanggungjawab terhadap perubahan atau pengembangan sistem yang digunakan serta pembuatan program-program aplikasi khusus sebagai antarmuka (*interface*) antara pengguna sistem dengan sistem itu sendiri. Personil atau karyawan pada bagian pengembangan sistem departemen PDE ini terdiri dari pemrogram (*programer*) dan analis sistem (*analist system*).

Fungsi Pengolahan Data

Fungsi pengolahan data terdiri dari fungsi-fungsi sebagai berikut:

a). Penyiapan Data (*Data Preparation*)

Bagian penyiapan data adalah bagian yang mempersiapkan data (*data preparation section*) ke bentuk media yang dapat dibaca oleh peralatan masukan komputer (*input device*). Tentunya peralatan masukan yang digunakan pun harus disesuaikan dengan bentuk dan jenis data yang akan diolah komputer. Dalam fungsi ini juga verifikasi data dan validasi data harus dilakukan untuk bisa menjamin bahwa data-data yang akan diproses atau diolah benar-benar terjamin keabsahannya. Sehingga dipastikan data yang masuk adalah data-data yang bukan data sampah (*Garbage In*).

b). Operator Komputer

Operator komputer adalah bagian yang mengoperasikan komputer yang berfungsi mengolah data sampai menghasilkan keluaran (*output*) dalam bentuk laporan-laporan yang dibutuhkan. Tugas dan fungsi bagian ini dilakukan oleh personil atau karyawan sesuai dengan prosedur yang telah dibuat secara tertulis dalam bentuk manual pengoperasian.

c). Pengendalian Data (*Data Control*)

Bagian pengontrol data ini berfungsi sebagai penengah antara bagian-bagian lainnya dengan bagain PDE. Karyawan-karyawan atau personil yang bekerja dibagian ini disebut *data control group* yang akan menerima data-data dari bagian lain kemudian menggandakannya, membuat *batch control* data, mengawasi jalannya pengolahan data dan memantau koreksi yang dilakukan selama proses pengolahan data berlangsung sampai pendistribusian keluaran (*output*) kepada para pemakai yang berhak.

d). Pustakawan Data (*Data Librarian*)

Bagian pustaka data dalah bagian yang berfungsi menjaga ruangan tempat penyimpanan data yang disebut dengan perpustakaan data. Dalam perpustakaan data ini akan disimpan data dan program-program dalam bentuk media simpanan luar. Tujuan utama dari fungsi pustaka data ini adalah untuk memisahkan tugas dan tanggung jawab antara bagian yang menyimpan data dengan bagian yang akan menggunakan data untuk keperluan operasi, sehingga dapat mencegah orang yang tidak behak mengakses data.

Fungsi pengembangan sistem dan sistem pengolahan data sebaiknya dipisahkan, karena bila seseorang mengetahui program dan sistem secara detail dan dapat menggunakannya dikhawatirkan bisa terjadi perubahan atau modifikasi yang tanpa seijin dari yang berhak. Dalam kenyataannya fungsi pengembangan sistem dan fungsi pengolahan data ini tidak hanya terpisah secara organisasional, tetapi juga terpisah secara fisik. Analis sistem dan *programmer* tidak boleh mengoperasikannya untuk hal-hal yang negatif, begitu pula dengan operator komputer dan pengolah data lain tidak boleh melihat dokumentasi program.

Pada organisasi yang tidak terlalu besar, biasanya bagian PDE hanya terdiri dari sejumlah personil atau karyawan yang bertanggungjawab untuk operasional komputer saja. Sedangkan analis dan *programmer* tidak diperlukan

karena sudah menggunakan program-program (*software*) yang sudah jadi dalam bentuk paket. Sebaliknya pada organisasi yang relatif besar bagian PDE personil atau karyawannya akan lebih banyak dan variatif lagi mulai dari analis sistem, *programmer,* operator komputer, *data entry* dan lain sebagainya.

b. Pengendalian dalam Pengembangan Sistem

Pengendalian pengembangan sistem dirancang untuk memberikan keyakinan memadai bahwa sistem dikembangkan dan dipelihara dalam suatu cara yang efesien dan melalui otorisasi semestinya yang berhubungan dengan:

1). Pengkajian ulang (*review*), pengujian dan persetujuan sistem baru.
2). Pengendalian perubahan program
3). Prosedur dokumentasi

Fungsi pengembangan sistem terutama terdiri dari pemrogram dan analis sistem, yaitu orang-orang yang mengerti tentang PDE secara rinci. Agar terdapat pengendalian yang memadai terhadap pengembangan sistem, antara lain dapat diterapkan prosedur-prosedur sebagai berikut:

1). Perancangan sistem harus melibatkan wakil dari tiap-tiap bagian.
2). Pengujian sistem harus merupakan usaha bersama antara karyawan PDE dengan bagian lain.
3). Harus ada persetujuan akhir sebelum suatu sistem dilaksanakan.
4). Setiap perubahan program harus disetujui sebelum diterapkan untuk meyakinkan bahwa perubahan tersebut sudah diotorisasi, diuji dan didokumentasikan.

c. Pengendalian Dokumen

Pengendalian dokumentasi menyangkut pengendalian dokumen-dokumen dan catatan perusahan mengenai kegiatan PDE-nya. Dokumentasi yang dimaksud dapat berupa deskripsi sistem, bagan alir (*Flowchart*), daftar hasil cetakan komputer. Dokumentasi yang baik dan memadai akan sangat penting baik untuk pihak manajemen maupun *auditor*. Beberapa manfaat dokumen bagi pihak manajemen dalam hal:

1). Mengkaji ulang sistem.
2). Melatih personil atau karyawan baru.
3). Memelihara dan memperbaiki sistem dan program yang ada.

Sedangkan bagi *auditor* dokumen merupakan salah satu sumber penting yang utama mengenai aliran transaksi dalam sistem dan pengendalian akuntansi.

Dalam PDE, ada enam jenis dokumentasi, yaitu:

1). Dokumen Prosedur
Dokumen prosedur berisi posedur-prosedur yang harus dilakukan pada suatu keadaan tertentu, seperti misalnya prosedur pengetesan program, prosedur penggunaan *file*, prosedur pembuatan *backup* dan *restore* dan lain sebagainya.
2). Dokumentasi Program
Dokumentasi program menggambarkan logika dari program dalam bentuk bagan alir program (*program flowchart*), tabel keputusan (*decision table*), dan bentuk pengendalian program. Dokumentasi program ini akan sangat dibutuhkan oleh *programmer* pada saat akan melakukan modifikasi atau pengembangan program dari program yang sudah ada sebelumnya.
3). Dokumentasi Sistem
Dokumentasi sistem adalah dokumentasi yang menunjukkan tujuan dari sistem pengolahan data dan termasuk bagan alir sistem (*system flowchart*), deskripsi sistem, deskripsi masukan dan *file* yang digunakan, deskripsi keluaran yang dihasilkan, serta pesan-pesan kesalahan pengolahan (*error*

message) dan daftar pengendalian. Dokumentasi sistem sangat diperlukan oleh analis sistem, pemakai sistem dan para *auditor*.

4). Dokumentasi Operasi.
Dokumentasi operasi berisi penjelasan-penjelasan cara dan prosedur-prosedur mengoperasikan program. Dokumentasi ini sangat dibutuhkan oleh operator.

5). Dokumentasi Data.
Dokumentasi data berisi definisi-definisi dari item-item data yang ada dalam *database* yang digunakan oleh sistem informasi. Dokumentasi data ini sangat dibutuhkan oleh *database administrator* (DBA) dan *auditor*. Dokumentasi data juga berguna bagi para *programmer* sejauh berhubungan dengan *item-item* data yang diperlukan program yang dibuat.

6). Dokumentai Pemakai.
Dokumentasi pemakai menjelaskan tujuan dari sistem, pengolahan data, prosedur untuk memasukkan data, bentuk-bentuk penggunaan laporan dan keluaran lain, pesan-pesan kesalahan yang mungkin dan prosedur koreksi kesalahan. Kadang-kadang dokumentasi pemakai ini disatukan dengan dokumentasi sistem.

d. Pengendalian *Hardware*, *Software*.

Pengendalian perangkat keras (*Hardware Control*) merupakan pengendalian yang sudah dipasang di dalam komputer itu (*built in*) oleh pabrik pembuatnya (produsen). Pengendalian ini dimaksudkan untuk mendeteksi kesalahan atau tidak berfungsinya perangkat keras (*hardware malfunction*). Pengendalian perangkat keras ini dapat berupa pemeriksaan pariti (*parity check*), pemeriksaan validitas (*validity check*) dan pemeriksaan kesalahan lain-lain (*miscellaneus errors check*).

Dalam pengendalian perangkat keras yang penting adalah bagaimana menangani kesalahan yang ditemukan atau yang ditunjukkan komputer. Biasanya jika perusahaan tidak membuat ketentuan khusus untuk menangani hal ini, maka data keluaran akan tetap belum dapat diperbaiki. Kesalahan karena kerusakan perangkat keras komputer akan jarang terjadi jika perangkat keras komputer yang ada dipelihara dengan baik dan selalu diperiksa secara berkala.

Pengendalian perangkat lunak (*software control*) merupakan pengendalian yang dilakukan untuk perangkat lunak sistem operasi dan perangkat lunak yang dibuat atau dikembangkan oleh perusahaan atau pabrik komputer dan pembuat perangkat lunak.

Biasanya perusahaan pemakai komputer membeli perangkat lunak semacam itu sebagai satu paket, sehingga dapat diasumsikan bahwa pengendalian perangkat lunak melekat (*built in software control*). Seperti halnya pengendalian perangkat keras melekat (*built in hardware control*). Asumsi ini tidak berlaku jika telah dibuat perubahan atau modifikasi terhadap perangkat lunak sistem tersebut.

e. Pengendalian Penggunaan Komputer, Fasilitas dan Data

Pengendalian terhadap keamanan fisik sangat perlu dilakukan untuk menjaga keamanan terhadap perangkat keras, perangkat lunak dan manusia di dalam perusahaan. Bila pengendalian keamanan fisik tidak dilakukan secara baik dan semestinya, maka akan dapat mengakibatkan:

1) Menurunnya operasi kegiatan.
2) Membahayakan sistem.
3) Hilangnya atau menurunnya pelayanan kepada langganan.
4) Hilangnya harta kekayaan (*asset*) perusahaan.

Beberapa hal yang menyebabkan tidak amannya fisik sistem diantaranya seperti pencurian, *sabotase*, kegagalan arus listrik, kebakaran, temperatur yang

tidak sesuai (terlalu panas atau terlalu dingin), kotoran debu dan bencana alam seperti gempa bumi, angin ribut, banjir dan petir. Sebagai antisipasi dalam pengendalian fisik sistem ini diperlukan teknik-tenik pengendalian keamanan fisik. Teknik untuk pengendalian keamanan fisik dapat berupa alat-alat dan penempatan fisik yang dapat membantu melindungi harta kekayaan milik perusahaan. Teknik yang dimaksud dapat berupa:

Pengawasan terhadap Pengaksesan Fisik

Pengawasan ini merupakan proteksi yang berupa pembatasan terhadap orang-orang atau personil yang akan masuk ke bagian yang penting. Bila keleluasaan untuk dapat keluar masuk bagian yang penting selalu diawasi, maka kesempatan untuk melakukan hal-hal yang dapat merugikan perusahaan dapat dicegah atau paling tidak diminimalisir. Pengawasan ini dapat dilakukan dengan cara melakukan penempatan keamanan satpam pada bagian-bagian yang strategis dilokasi-lokasi yang penting, pengisian agenda kunjungan dimaksudkan agar dapat melacak personil atau orang-orang yang masuk, penggunaan tanda pengenal yang berbeda agar dapat dengan mudah diidentifikasi siapa saja personil yang masuk dan dari bagian mana, pemakaian kartu seperti ruangan yang dilengkapi dengan sirkuit elektronik yang dapat membukakan pintu secara otomatis bila dipergunakan kartu pengenal yang berisi kode-kode tertentu, penggunaan *Closed-Circuit television* yang dapat memonitor kegiatan yang terjadi di ruangan yang penting, penggunaan pengracik kertas untuk memusnahkan data-data penting yang ada dalam kertas sampah, serta tersedianya pintu-pintu darurat satu arah untuk mempermudah evakuasi baik personil atau pun fasilitas fisik sistem yang penting disaat terjadi keadaan darurat.

Pengaturan Lokasi Fisik

Penentuan lokasi dari ruang komputer harus dijadikan pertimbangan yang penting di dalam perencanaan sekuriti. Pengendalian terhadap lokasi fisik yang baik dari ruang komputer dapat berupa:

1). Penentuan lokasi yang tidak terganggu oleh lingkungan seperti jauh dari pangkalan udara, radar dan gelombang *microwave*, lalulintas yang padat.
2). Penentuan gedung yang terpisah hal ini dilakukan untuk mempermudah pengawasan. Kalaupun tidak terpisah, maka harus diletakan pada ruangan yang tepat dengan pertimbangan harus jauh dari jendela luar, tidak terletak pada lantai atas, tidak terletak pada lorong yang sering dilalui orang dengan bebas, tidak terletak pad ruang bawah tanah, tidak menyolok tempatnya dan tidak mengandung tanda-tanda yang jelas menunjukkan sebagai ruang komputer.
3). Tersedia fasilitas cadangan karena fasilitas cadangan mempunyai peranan yang cukup penting dalam pengolahan data. Fasilitas cadangan ini dapat berupa tenaga listrik cadangan yang digunakan bila aliran listrik utama terputus.

Penerapan Alat-alat Pengaman

Peralatan pengaman tambahan dapat digunakan untuk mengendalikan hal-hal yang dapat menyebabkan sesuatu yang fatal. Peralatan pengaman tersebut dapat berupa saluran air yang baik yang dapat mengatur dan mencegah meluapnya air yang masuk ke gedung bila terjadi banjir, alat pemadam kebakaran yang ditempatkan pada tempat-tempat yang strategis dan mudah dijangkau, UPS (*Uninteruptible Power Systems*) digunakan untuk mengatasi bila arus listrik tiba-tiba terputus, *stabilizer* untuk menstabilkan penggunaan arus listrik, *Air Conditioner*

(AC) untuk pengaturan temperatur dalam ruangan serta pendeteksi kebakaran yang dapat membunyikan alarm bila terjadi kebakaran atau bila timbul asap yang merupakan tanda-tanda mulai terjadinya kebakaran.

Pengendalian Keamanan Data

Pengendalian keamanan tidak hanya mencakup perlindungan sehari-hari terhadap komputer dan perangkat lunaknya, tetapi juga meliputi integritas data, kerahasiaan data. Menjaga integritas dan keamanan data merupakan pencegahan terhadap keamanan data yang tersimpan di simpanan luar supaya tidak hilang, rusak dan diakses oleh orang yang tidak berhak.

Pengendalian keamanan data meliputi:

1). Penggunaan Data *Log*
Agenda (*Log*) dapat digunakan pada proses pengolahan data untuk memonitor, mencatat dan mengidentifikasikan data. Kumpulan data yang dimasukkan ke departemen PDE seharusnya dicatat terlebih dahulu oleh *data control group*. *File* dan program yang dibutuhkan pada operasi pengolahan data juga harus dicatat oleh *librarian*. Dengan demikian segala sesuatu yang dapat mempengaruhi perubahan data dapat diketahui, diidentifikasi dan dilacak. Selain *data log* dapat juga digunakan *Transaction Log*, yaitu suatu *file* yang akan berisi nama-nama pemakai (*user*) komputer, tanggal, jam, tipe pengolahannya, lokasinya dan lain sebagainya yang perlu diketahui.

2). Proteksi *File*
Beberapa alat atau teknik telah dapat tersedia untuk menjaga *file* dari penggunaan yang tidak benar yang dapat menyebabkan rusak atau tergantinya data dengan nilai yang tidak benar, diantaranya adalah:
a. Cincin proteksi pita magnetik.
b. Cincin ini digunakan pada pita magnetik yang dapat memproteksi pita magnetik dari data lama jika tertimpah data yang baru (*over-written*), sehingga data sebelumnya tidak akan hilang.
c. Label *file eksternal*.
d. Label *file eksternal* (*external file label*) merupakan tempelan label kertas yang direkatkan pada simpanan luar untuk menunjukkan isi simpanan tersebut, sehingga tidak akan salah mengambil.
e. *Read-only memory*.
Merupakan simpanan luar dimana data yang tersimpan di dalamnya hanya dapat dibaca saja. Data yang telah tersimpan di dalamnya tidak dapat diubah oleh instruksi-instruksi program yang dibuat oleh pemakai.

3). Pembatasan Pengaksesan (*Access Restriction*)
Pengaksesan data oleh orang atau personil yang tidak berhak dapat mengakibatkan kerugian bagi perusahaan misalnya saja penyelewengan harta kekayaan perusahaan oleh orang yang tidak bertanggungjawab, karena itu pengaksesan data harus dibatasi hanya untuk orang-orang yang berhak saja. Pembatasan pengaksesan data dapat dilakukan dengan cara sebagai berikut:
a. Isolasi Fisik
Data yang penting dapat diisolasi dari penggunaan personil-personil yang tidak berhak. Data tersebut dapat secara terpisah dijaga oleh librarian. Bila operator membutuhkannya bisa meminta kepada *librarian* dan segera dikembalikan jika operasi telah selesai.
b. Otorisasi dan Identifikasi

Tiap-tiap personil yang berhak mengakses data dan telah diotorisasi diberi pengenal (identifikasi) tertentu berupa kode-kode untuk mengakses daa. Kode-kode ini disebut dengan *password*. Terminal akan menanyakan *password* setia kali data akan diakses. *Password* yang tidak dikenal akan ditolak oleh sistem komputer.

c. Pembatasan pemakaian
Bagi personil atau karyawan yang telah mendapatkan hak otorisasi mengakses data dengan menggunakan *password* tertentu harus dibatasi terhadap penggunaan data hanya untuk kebutuhan atau keperluannya saja. Artinya data yang lain yang tidak dibutuhkan atau diperlukan harus tidak boleh diakses.

d. Encryption.
Encryption dilakukan dengan meletakkan suatu alat pengkode pada awal jalur transmisi data, yang akan merubah data asli ke dalam bentuk teks sandi rahasia. Pada ujung akhir transmisi diletakkan *decryption device* yang akan berfungsi merubah kembali teks sandi rahasia ke data asli.

e. Pemusnahan.
Untuk data-data yang tidak lagi diperlukan atau dipakai dimusnahkan untuk pengendalian keamanan data, termasuk dalam hal ini karbon-karbon dari laporan-laporan yang dihasilkan.

4) *Data Backup* dan *recovery*
Pengendalian ini diperlukan untuk menjaga bila *file* atau *database* mengalami kerusakan, kehilangan atau kesalahan data. *Backup* adalah salinan dari *file* atau *database*, sedangkan recovery adalah *file* atau *database* yang telah dibetulkan dari kesalahan, kehilangan atau kerusakan datanya. Penyebabnya bisa karena kesalahan program (*program error*), kesalahan perangkat lunak (*system software error*), kegagalan perangkat keras (*hardware failure*), kesalahan prosedur (*procedural error*) dan kegagalan lingkungan (*environmental failure*).

Ada beberapa strategi untuk melakukan *backup* dan *recovery*, yaitu sebagai berikut:

a. Strategi Kakek-Bapak-Anak (*grandfather-father-son*)
Biasanya strategi ini digunakan untuk *file* yang disimpan di media simpanan luar pita magnetik. Strategi ini dilakukan dengan menyimpan tiga generasi *file* induk bersama-sama dengan *file* transaksinya. Ketiga *file* induk dan transaksi yang dimaksud akan disimpan secara terpisah. Bila terjadi kesalahan atau kerusakan data dalam *file* maka akan dapat dibetulkan kembali.

b. Strategi pencatatan Ganda (*dual recording*).
Strategi ini dilakukan dengan menyimpan dua buah salinan *database* yang lengkap secara terpisah dan menyesuaikan keduanya secara serentak. Jika terjadi kegagalan transaksi dalam perangkat keras dapat digunakan alat pengolah kedua yang menggantikan fungsi alat pengolah utama. Jika alat pengolah utama tidak berfungsi, secara otomatis program akan dipindah (men-*switch*) ke alat pengolah kedua dan *database* kedua menjadi *database* utama. Strategi dual *recording* ini sangat tepat untuk aplikasi-aplikasi yang *database*nya tidak boleh terganggu dan selalu siap pakai. Tetapi strategi ini memerlukan biaya yang relatif mahal karena harus menggunakan dua buah

alat pengolah dan dua buah *database*.

c. Strategi *Dumping*.
Dumping dilakukan dengan menyalin semua atau sebagian dari *database* ke media *back up* yang lain, dapat berupa pita magnetik atau ke diskette. *Recovery* pada strategi ini dapat dilakukan dengan merekam kembali (*restore*) hasil dari *dumping* ke *database* di simpanan luar utama dan melakukan proses transaksi yang teakhir yang sudah mempengaruhi *database* sejak proses *dumping* terakhir.

2. Pengendalian Khusus Atas Aplikasi (*Aplication Control*)

Dalam Sistem Informasi Akuntansi (SIA) yang berbasis komputer sudah tentu akan menggunakan program aplikasi khusus yang dibuat untuk mengatomatisasi tahapan dan proses yang ada di dalamya. Agar program-program aplikasi khusus yang akan digunakan dalam SIA haruslah benar-benar yang sudah teruji dan dipastikan tidak bermasalah. Dalam implementasinya semua kegiatan tahapan dalam SIA yang menggunakan program aplikasi perlu dilakukan pengandalian khusus, yaitu mulai dari pengendalian masukan (*input control*), pengendalian pengolahan (*process control*) dan pengendalian keluaran (*output control*).

a. Pengendalian Masukan *(input control)*

Pengendalian masukan bertujuan untuk meyakinkan bahwa data transaksi yang akan diproses adalah data-data yang valid, lengkap serta bebas dari kesalahan. Hal ini dimaksudkan agar sistem terhidar dari istilah *GIGO (Garbage In Garbage Out)* yang artinya jangan sampai ada data sampah yang diproses, karena kalau hal itu terjadi maka bisa dipastikan akan menghasilkan informasi sampah pula. Data *input* yang akan dimasukkan ke dalam komputer terdiri dari tiga tahapan, yaitu:

1). Penangkapan data (*Data Capture*)
Merupakan proses mengidentifikasikan dan mencatat kejadian nyata yang terjadi akibat transaksi yang dilakukan. Pengendalian yang dilakukan pada tahap ini dengan cara memberikan nomor urut yang tercetak pada dokumen dasar, memberikan ruang maksimum untuk masing-masing *field* di dokumen dasar, melakukan kaji ulang (*review*) serta melakukan verifikasi data (*data verification*).

2). Penyiapan data (*Data preparation*)
Merupakan proses mengubah data yang telah ditangkap ke bentuk yang dapat dibaca oleh mesin (*machine readable form*). Pengendalian yang dilakukan pada tahap ini dengan cara melakukan verifikasi visual (*visual verification*) antara hasil pengubahan data dalam bentuk *machine readable form* dengan data yang ada di dokumen dasar, kemudian melakukan verifikasi tombol kunci (*key verification*) yang dilakukan oleh dua orang operator dengan mengetikkan data yang sama.

3). Pemasukan data (*Data entry*)
Merupakan proses memasukkan data ke komputer. Pengendalian yang dilakukan pada tahap ini meliputi *Echo check* yaitu membandingkan antara data yang diketikkan dengan data yang seharusnya dimasukkan melalui layar terminal, *Existence Check* yaitu validasi dari suatu kode yang dimasukkan ke sistem komputer, *Matching Check* yaitu pengecekan yang dilakukan dengan membandingkan kode yang dimasukkan dengan *field* di *file* induk, *Field Check* yaitu *field* dari data yang dimasukkan diperiksa kebenarannya dengan mencocokkan nilai dari *field* data tersebut apakan bertipe

numerik, alphabetik ataukah tanggal, *Sign Check* yaitu pengecekan nilai suatu *field* yang bertipe numerik apakah sudah terisi dengan dengan nilai yang benar, *Relationship* atau *Logical Check* yaitu memeriksa hubungan antara *item-item* data *input* yang dimasukkan ke komputer apakah masuk akal atau tidak, Limit atau *Reasonable Check* yaitu memeriksa nilai dari *input* data apakah cukup beralasan atau tidak, *Range Check* yaitu pengecekan jangkauan nilai yang sudah ditentukan, *Self-Checking Digit Check* yaitu pengecekan untuk memeriksa kebenaran dari digit-digit data yang dimasukkan, *Sequence Check* yaitu untuk menentukan data yang harus dimasukkan dengan urutan record yang tertentu, *Label Check* yaitu memberi label internal pada pita magnetik atau pada disk magnetik untuk menghindari kesalahan penggunaan file, *Batch Control Total Check yaitu* pengecekan data pada metode *Batch processing* yang dapat berupa *financial total* (total dari nilai rupiah suatu *field*), *Hash Total* (total dari kode-kode suatu *field*), *Record Account* (total dari jumlah dokumen dasar atau *record*). Kemudian pengecekan selisih kesimbangan suatu nilai transaksi seperti debet dan kredit pada jurnal juga perlu dilakukan, pengecekan ini disebut dengan istilah *Zero-Balance Check*.

b. Pengendalian Pengolahan (*Proccessing Control*)

Tujuan dari pengendalian adalah untuk mencegah terjadinya kesalahan-kesalahan selama proses pengolahan data yang dilakukan setelah data dimasukkan ke dalam komputer. Kesalahan pengolahan data dapat terjadi karena program aplikasi yang digunakan untuk mengolah data mengandung kesalahan. Kesalahan-kesalahan yang mungkin terjadi pada saat pengolahan data umumnya disebabkan oleh kesalahan program sebagai berikut:

1). *Overflow.*
Kesalahan yang terjadi jika proses pengolahan data mengandung perhitungan yang hasilnya terlalu besar atau terlalu kecil, sehingga tidak muat untuk disimpan di memori komputer.

2). Kesalahan logika program (*Logic Error*)
Kesalahan logika dari program yang dibuat, kesalahan ini sulit dideteksi karena tidak ditunjukkan oleh komputer. Kesalahan ini hanya akan nampak dari hasil keluaran (*output*) program.

3). Logika program yang tidak lengkap.
Meskipun dalam program tidak ada kesalahan logika dan semua kondisi benar, tetapi mungkin juga ada beberapa kondisi logika yang terlewat. Bila hal ini terjadi maka bisa dipastikan hasil pengolahan data menjadi tidak benar lagi.

4). Penganganan Pembulatan yang salah.
Pengananan pembulatan yang salah bisa terjadi secara sengaja atau tidak oleh programmer. Hal ini akan menjadi masalah bila pembulatan yang terjadi tingkat ketepatan yang diinginkan tidak sesuai.

5). Kesalahan akibat kehilangan atau kerusakan *record.*
Pada *batch processing method*, *file* transaksi berisi data kumpulan dari data transaksi selama periode tertentu. Meskipun kelengkapan dan kebenaran data dari isi *file* transaksi tersebut telah dilakukan validasi pada tahap *input*, tetapi pad proses *update* data dapat terjadi beberapa *record* yang hilang atau rusak, hal ini akan

mengakibatkan data yang diproses menjadi tidak benar.

6). Kesalahan urutan data
Record pada file induk akan di-*update* oleh data transaksi. Sebelum dilakukan proses peng-*update*-an ini, bila terjadi penambahan data baru atau penghapusan data atau perubahan data terhadap *file* induk, maka proses-proses ini harus dilakukan terlebih dahulu, kalau tidak maka dapat mengakibatkan terjadinya kesalahan-kesalahan.

7). Kesalahan *file* acuan.
Banyak program yang menggunakan *file* acuan (*reference file*) untuk menyimpan data yang relatif konstan. Konsistensi kebenaran nilai dari data *file* acuan ini harus dijaga, bila tidak proses program yang akan menggunakannya juga akan salah.

8). Kesalahan proses serentak (*concurrency*)
Kesalahan yang terjadi bila sebuah *file* dalam basis data dipergunakan lebih dari seorang pemakai dalam sistem jaringan.

Untuk mendeteksi kesalahan-kesalahan yang mungkin terjadi dalam proses pengolahan data diperlukan pengendalian berupa pengecekan-pengecekan sebagai berikut:

1). *Control Total Check*
Control total check dilakukan untuk mendeteksi apakah semua data yang diolah telah lengkap dan telah benar. *Control total check* dapat dilakukan pada pengendalian masukan juga pada pengendalian pengolahan.

2). *Matching Check*
Yaitu pendeteksian pencarian data dari suatu *file* yang tidak ditemukan. *Mathcing check* pada *batch processing methode* dapat digunakan untuk mendeteksi kesalahan dari urutan data, sedangkan pada *online processing method* pengecekan ini dilakukan pada tahap *input* dan pada tahap pengolahan data dalam suatu program.

3). *Reference File Check.*
Kesalahan penggunaan data yang diambil dari *file* acuan dapat dideteksi dengan cara mencetak isi *file* acuan yang digunakan dalam proses pengolahan. Hasil cetakan isi *file* acuan kemudian diperiksa kebenarannya.

4). *Limit and Reasonable Check*
Yaitu pengecekan terhadap batas limit dan kewajaran suatu nilai yang akan diproses oleh komputer. Pada tahap *input,* pengecekan ini ditunjukan pada kewajaran dari data *input* yang dimasukkan ke komputer, sedangkan pada tahap pengolahan pengecekan ini ditujukan pada hasil pengolahannya.

5). *Crossfooting Check*
Dilakukan dengan menjumlahkan masing-masing *item* data secara kesamping (*horizontal*) dan secara tegak (*vertical*). *Crossfooting check* dilakukan dengan membandingkan antara dua hasil total dari penjumlahan kesamping dengan penjumlahan yang dilakukan tegak lurus. Pengecekan ini digunakan untuk mengecek kesalahan-kesalahan yang mungkin dihasilkan oleh logika program yang tidak benar atau kesalahan pembulatan.

6). *Record Locking*
Proses konkurensi terjadi karena *record* yang sama di dalam suatu *file* dipergunakan oleh lebih dari satu pemakai. Untuk mengatasi konkurensi dapat dilakukan dengan mengunci *record* yang sedang dipergunakan, sehingga tidak dapat dipergunakan oleh pemakai lain.

c. Pengendalian Keluaran (*output*)

Keluaran (*output*) merupakan produk dari suatu pengolahan data dapat

disajikan dalam dua bentuk utama, yaitu dalam bentuk *hard copy* dan *soft copy*. Dalam bentuk *hard copy* yang paling banyak dilakukan adalah berbentuk laporan yang dicetak menggunakan alat cetak (*printer*) dan dalam bentuk *soft copy* yang paling umum dalam bentuk tampilan di layar terminal. Berikut ini adalah beberapa pengendalian yang dilakukan pada dua bentuk keluaran utama.

Pengendalian Laporan Berbentuk *Hard Copy*

Tahapan yang dilakukan untuk bisa menghasilkan laporan yang berbentuk *hard copy* adalah sebagai berikut:

1). Tahap menyediakan media laporan.
2). Tahap memproses program yang mengasilkan laporan.
3). Tahap pembuatan laporan di *file* (*printer file*).
4). Tahap pengumpulan laporan.
5). Tahap mencetak laporan ke media kertas.
6). Tahap mengkaji ulang laporan.
7). Tahap pemilihan laporan.
8). Tahap distribusi laporan.
9). Tahap kaji ulang laporan oleh pemakai laporan.
10). Tahap pengarsipan laporan.
11). Tahap pemusnahan laporan yang sudah tidak diperlukan.

Agar kelengkapan, kebenaran data dan keamanan dari laporan yang berbentuk *hard copy* ini dapat terlaksana, maka untuk tiap-tiap tahapan tersebut perlu dilakukan pengendalian.

1). Pengendalian pada tahap penyediaan media laporan.
Pengendalian terhadap penyiapan media laporan dapat dilakukan dengan cara:
   a. Menyelenggarakan sistem penyimpanan media laporan tercetak.
   Yaitu pengaturan cara mencetakkan media laporan, bagaimana menerima dari percetakan, siapa yang berhak menyimpan, bagaimana untuk mendapatkannya dan siapa saja yang boleh mendapatkannya.
   b. Pengendalian terhadap pengaksesnya
   Yaitu menentukan hak akses untuk mendapatkan media laporan tercetak dengan maksud mereka yang tidak berhak tidak dapat menggunakannya untuk maksud-maksud yang dapat merugikan perusahaan.
   c. Pemberian nomor urut.
   Media laporan tercetak sedapat mungkin diberi nomor urut, sehingga bila ada laporan yang hilang akan segera diketahui. Penyimpanan cap pengesahan yang terpisah
   d. Yaitu penggunaan cap-cap resmi organisasi atau perusahaan dan cap tanda tangan sebaiknya disimpan di tempat yang terpisah dari ruang pengolahan data.
2). Pengendalian pada tahap pemrosesan program penghasil laporan.
Pengendalian pada proses program yang digunakan untuk mencetak laporan merupakan pengecekan-pengecekan yang sudah dipasang di dalam program. Pengendalian ini bertujuan untuk menjamin kebenaran dan kelengkapan informasi yang dicetak di dalam laporan.
3). Pengendalian pada tahap pembuatan *printer file*.
Kemungkinan suatu laporan tidak langsung dicetak ke *printer,* tetapi direkam dulu ke *file*. Hal ini disebabkan beberapa hal seperti, menunggu *printer* yang sedang digunakan oleh proses lain, bentuk dan isi laporan yang mungkin akan dimodifikasi kembali. Karena itu dibutuhkan *printer file* yang berisi laporan yang akan dicetak. Pengendalian yang bisa dilakukan terhadap *printer file* dimaksudkan

agar isi dari *printer file* tidak dapat diubah oleh orang yang tidak berhak, agar *printer file* tidak disalin oleh orang yang tidak berhak dan *printer file* hanya dicetak untuk keperluan yang sah saja dan dihapus bila tidak diperlukan lagi.

4). Pengendalian pada tahap pencetakan laporan.
Pengendalian pad tahap ini tujuannya adalah untuk meyakinkan bahwa yang dicetak hanya sejumlah tembusan yang diperlukan saja, mencegah isi dari laporan tidak terbaca oleh orang lain yang tidak berhak. Pengendalian pada tahap ini dilakukan dengan cara sebagai berikut:
   a. Laporan dapat dicetak pada *printer* yang telah diletakkan jauh dari operator komputer.
   b. Data *control group* dapat mengawasi hasil laporan sewaktu-waktu.
   c. Pada waktu pencetakan laporan *printer* tidak menggunakan pita *ribbon*, tetapi menggunakan kertas berkarbon.
   d. Digunakan kertas khusus yang lembar termuka berwarna hitam, sehingga cetakan tidak terlihat.

5). Pengendalian pada tahap pengumpulan laporan.
Setelah laporan dicetak, maka harus dikumpulkan segera oleh staf bagian pengendalian. Semua laporan dapat diletakkan terlebih dahulu di tempat yang khusus dan terkunci sbelum didistribusikan.

6). Pengendalian pada tahap kaji ulang.
Sebelum laporan didistribusikan dan digunakan oleh pemakai laporan, maka laporan-laporan tersebut harus bebas dari kesaahan-kesalahan serta harus mencerminkan informasi yang tidak menyesatkan. Oleh karena itu sebelum didistribusikan perlu dilakukan pemeriksaan kembali, pengkajian ulang terhadap kesalahan-kesalahan yang mungkin terjadi pada isi laporan.

7). Pengendalian pada tahap pemilihan laporan
Bila laporan terdiri dari beberapa halaman atau terdiri dari beberapa macam untuk beberapa pemakai yang berbeda, maka laporan-laporan tersebut perlu dipilah dan diatur kembali sesuai dengan jenis, kegunaan dan distribusinya dalam kelompok-kelompok tertentu. Pada saat hal itu dilakukan perlu dilakukan pengawasan untuk memastikan bahwa laporan tidak ada yang hilang atau di salian oleh orang yang tidak berhak.

8). Pengendalian pada tahap pendistribusian laporan.
Pegendalian pada tahap ini dilakukan untuk memastikan bahwa pendistribusian laporan kepada pemakai tidak terlambat. Pengendalian yang dapat diterapkan pada tahap ini, yaitu:
   a. Memberi tanggal pada laporan kapan dibuat laporan tersebut.
   b. Dibuat daftar distribusi siapa-siapa saja yang berhak untuk menerima laporan, sehingga distribusi tidak keliru.
   c. Untuk laporan yang penting, harus dibuat daftar penerimaan yang ditandatangani oleh penerima laporan sebagai bukti bahwa laporan telah didistribusikan dan diterima dengan benar dan lengkap.

9). Pengendalian pada tahap kaji ulang oleh pemakai.
Penerima laporan sebaiknya mengkaji ulang isi dari laporan yang diterimanya sebelum menggunakannya untuk mendeteksi kesalahan-kesalahan yang mungkin ada. Bagaimanapun juga pemakai akan lebih tahu dan mengerti isi laporan yang dibutuhkannya.

10). Pengendalian pada tahap pengarsipan laporan.

Pengarsipan laporan harus dipastikan aman, tidak mudah dijangkau oleh orang-orang yang tidak berhak. Karena kebocoran informasi penting dari laporan akan berakibat fatal.

11). Pengendalian pada tahap pemusnahan laporan.
Bila umur laporan sudah habis dan tidak lagi digunakan, maka laporan harus dimusnahkan. Pemusnahan laporan harus tidak berbekas. Pemusnahan laporan bisa dilakukan dengan cara dibakar atau menggunakan alat racikan kertas. Pada waktu pemusnahan laporan dilakukan, harus diawasi untuk meyakinkan bahwa laporan telah benar-benar dimusnahkan.

Pengendalian Laporan berbentuk *Soft Copy*

Laporan yang berbentuk *soft copy*, informasi ditampilkan pada layar terminal dan tidak menggunakan media kertas. Informasi pada media lunak tidak dapat dilepas dari alat keluarannya, sehingga tidak didistribusikan. Pengendalian yang dapat dilakukan pada laporan yang berbentuk *soft copy* ini meliputi dua hal, yaitu:

1). Pengendalian pada informasi yang ditransmisikan.
Pengendalian ini dimaksudkan agar orang tidak berhak tidak dapat menyadap di tengah jalur untuk informasi yang dikirimkan. Misalnya saja untuk transmisi jalur komunikasi, maka dapat dilakukan dengan menyandikan (*encryption*).

2). Pengendalian pada tampilan layar di layar terminal.
Pengendalian ini berguna untuk mencegah mereka yang tidak berhak dapat melihat informasi yang ditampilkan di layar terminal. Pengendalian ini dapat dilakukan dengan beberapa cara, seperti:
   a. Menempatkan masing-masing terminal di ruangan yang terpisah.
   b. Menampilkan informasi yang penting dan tidak ingin terlihat orang lain dengan tampilan intensitas rendah di layar terminal, sehingga tidak mudah terbaca dari jarak jauh.
   c. Melatakkan terminal yang menghadap ke tembok, sehingga tidak mudah terlihat bagi mereka yang lewat.

III. KESIMPULAN

Beberapa hal yang dapat penulis simpulkan dari uraian atau pembahasan pada tulisan ini adalah sebagai berikut:

a. Sistem Informasi Akuntansi (SIA) merupakan salah satu subyek dari suatu manajemen dalam sebuah organisasi bisnis (*profit oriented*).
b. Dalam kenyataanya Sistem Infomasi Akuntansi saat ini sangat dipengaruhi oleh perkembangan teknologi terutama teknologi Informasi. Karenanya sebagian besar saat ini Sistem Informasi Akuntansi sudah berbasis komputer.
c. Pemanfaatan teknologi informasi (TI) dalam Sistem Informasi Akuntansi akan sangat mempengaruhi metode dan prosedur yang ada dalam sistem. Dalam Sistem Informasi Akuntansi yang terkomputerisasi akan terjadi penggabungan prosedur dan tugas yang tidak dapat dilakukan pada Sistem Informasi Akuntansi manual. Oleh karenanya pengendalian *intern* pada Sistem Informasi Akuntansi yang sudah berbasis komputer juga akan berbeda dengan yang masih manual.
d. Pengendalian *intern* pada Sistem Informasi Akuntansi yang berbasis komputer terdiri dari pengendalian umum (*General Control*) dan pengendalian khusus aplikasi (*Aplication Control*).
e. Pengendalian umum meliputi pengendalian organisasi dan operasi, pengendalian dalam bidang

pengembangan sistem, pengendalian perangkat keras (*hardware*), pengendalian perangkat lunak (*software*) serta pengendalian penggunaan komputer (fasilitas dan datanya).

f. Pengendalian khusus aplikasi meliputi penggunaan aplikasi-aplikasi *software* yang ada mulai dari pengendalian masukan (*input*), pengolahan (*process*) hingga keluaran yang dihasilkan (*output*).

DAFTAR PUSAKA

Baridwan, Zaki. 2000. Sistem Informasi Akuntansi. BPFE. Jogyakarta.

Jogiyanto,HM. 1995. Pengenalan Komputer. Andi Offset. Yogyakarta.

_____.1995. Analisa & Desain Sistem Informasi : Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis. Andi Offset. Yogyakarta.

_____.1997. Sistem Informasi Akuntansi Berbasis komputer. BPFE. Yogyakarta.

Marshall Bromney, Paul Jhon Stainbart. 2005. Sistem Informasi Akuntansi edisi 9.Salemba Empat.Jakarta.

Mc Leod JR, Raymond. 1996. Sistem Informasi Manajemen, Jilid 1. PT.Prehallindo. jakarta.