JURNAL AKUNTANSI DAN KEUANGAN
Volume 3, No. 1, April 2004
Halaman 38 - 50

PENGENDALIAN INTERN DALAM SISTEM INFORMASI AKUNTANSI BERBASIS KOMPUTER

Agus Endro Suwarno
Universitas Muhammadiyah Surakarta

Growth of computer give many advantage in the form of on schedule, decreasing of it handling of other benefit and document. But at the same time with growth of accounting information system base on computer emerge the problem of internal control. Computer skilled earn is easily misused if internal control don't be developed to make balance to accounting information system base on the computer.

This article study how applying of internal control in accounting information system of base on computer? Result of its solution is accounting control in accounting system base on computer cover General controls; Security controls and Application controls. Implementation internal control in an existing system, hence complexity a computer system can lessen insincerity and mistake which don't detect.

Keywords: *internal control, general controls, security controls, application controls*

LATAR BELAKANG MASALAH

Sistem informasi akuntansi yang canggih merupakan produk dua disiplin yaitu akuntansi dan komputer. Komputer memiliki keahlian yang luar biasa untuk memproses data akuntansi menjadi informasi. Jika suatu transaksi dimasukkan untuk diproses, maka komputer akan membawa transaksi tersebut keseluruh komponen sistem yang berhubungan secara otomatis. Komputer dapat mem-*posting* informasi yang cepat sehingga setiap rekening akan sealu diperbaharui. Informasi dapat disediakan secepatnya sesuai dengan kebutuhan pemakai.

Suatu sistem memiliki peluang terhadap kesalahan manajemen, kerusakan atau kemacetan, dan penyalahgunaan. Komputer dan kemampuan manusia merupakan peralatan yang dapat mendukung untuk

mencapai prestasi tinggi, namun keduanya juga tetap mempunyai kapasitas untuk melakukan kesalahan. Jika kesalahan terjadi dalam sistem informasi berbasis komputer, maka perlu adanya suatu sistem pengendalian yang diimplementasikan dan dipelihara.

Kehadiran komputer sebagai pendukung sistem informasi adalah netral. Dengan demikian kecurangan (*fraud*) yang mungkin terjadi lebih disebabkan faktor manusianya. Hal ini logis, karena manusia adalah salah satu elemen penting dalam sistem pengendalian pencegahan. (Barry E Cushing:1982).

Perkembangan komputer memberikan banyak keuntungan berupa tepat waktu, berkurangnya penanganan dokumen dan manfaat lainnya. Tetapi bersamaan dengan perkembangan sistem informasi akuntansi berbasis komputer muncul masalah pengendalian intern. Keahlian komputer dapat dengan mudah disalahgunakan jika pengendalian intern tidak dikembangkan untuk mengimbangi sistem informasi akuntansi berbasis komputer tersebut.

PERUMUSAN MASALAH

Berdasarkan latar belakang tersebut masalah yang akan dibahas adalah bagaimana penerapan pengendalian intern dalam sistem informasi akuntansi berbasis komputer?

PEMBAHASAN

1. Pengertian Internal Kontrol (Boockhold,1999)

Internal kontrol merupakan suatu proses, dipengaruhi oleh anggota direktur suatu entitas, manajemen dan personal yang lain, dirancang untuk menyediakan kepastian yang masuk akal yang memerlukan pencapaian suatu tujuan dalam kategori di bawah ini:

- Efektivitas dan efisiensi dari suatu operasi
- Reliabilitas dari pelaporan keuangan
- Ketaatan akan peraturan dan hukum yang diterapkan

Internal kontrol bukan merupakan proses tunggal tetapi merupakan kombinasi dari banyak proses yang terjadi sebagai bagian dari aktivitas organisasi. Internal kontrol dikatakan efektif bila dapat mencapai tujuannya, tidak efektif ketika mereka tidak dapat mencapai tujuannya.

Orang mengimplementasikan proses suatu organisasi mereka membuat kerja internal kontrol. Manajemen menetapkan bagaimana kerjanya dengan menyetujui perancangan sistem organisasional.

Karena anggota direktur mempunyai otoritas kelalaian dan menyetujui kebijakan dan transaksi yang pasti, juga merupakan elemen penting dalam internal kontrol.

Setiap organisasi mempunyai suatu misi dan manajemen mengidentifikasi tujuan organisasional yang konsisten dengan misi itu, tujuan untuk organisasi sebagai keseluruhan dan aktivitas yang spesifik di dalamnya.

Internal kontrol tidak dapat menjamin tujuan manajemen. Mereka hanya dapat menyediakan *reasonable assurance* untuk memenuhinya. Suatu internal kontrol organisasi mempunyai keterbatasan yang membuat suatu kepastian yang absolut tidak mungkin.

2. Keterbatasan Internal Kontrol

Menurut Boockhold,1999 ada tiga keterbatasan internal kontrol:

- Kesalahan (*errors*)
- Kolusi (*collusions*)
- Penolakan manajemen (*management override*)

Kesalahan timbul ketika pekerja melakukan penilaian yang buruk atau mempunyai gangguan perhatian terhadap pekerjaan mereka. Penilaian yang buruk menghasilkan keputusan yang jelek dan gangguan perhatian timbul dari kecerobohan yang disebabkan lelah, gangguan dari luar atau kerja lembur. Meskipun dilatih dengan baik dan kehati-hatian pekerja menyebabkan sedikit kesalahan. Kebanyakan manajer menyadari meskipun pekerja terbaik, suatu waktu akan membuat suatu kesalahan. Meskipun untuk menerapkan kebijakan dan prosedur yang mendeteksi pencurian dimana kolusi terjadi, kebanyakan manajer sadar bahwa usaha tersebut. Tidak masuk akal dan malahan mencoba untuk menggaji pekerja yang jujur dan menjaga mereka puas akan pekerjaan mereka. Ini untuk meminimkan keinginan untuk mencuri dan membuat kolusi yang tidak disukai.

Kolusi terjadi ketika dua orang atau lebih bersekongkol/ berkonspirasi untuk melakukan pencurian dari pekerjaan mereka. Contohnya: pegawai penjualan dan supervisor penjualan mungkin setuju untuk mencuri kas dari register kas dan untuk menutupi pencurian adalah dengan memalsukan rekonsiliasi untuk register tersebut.

Manajer dalam suatu organisasi mempunyai otoritas lebih dari personal produksi atau pegawai administrasi, proses kontrol akan

efektif pada level bawah dalam suatu organisasi menjadi tidak efektif pada level tingkat atas.

Management override, seperti kolusi tidak dapat dicegah dengan cara yang masuk akal (*means reasonable*). Malahan organisasi mencoba untuk memperkerjakan manajer yang jujur dan mengganti kerugian mereka yang cukup untuk mendapatkan *performance* yang bagus. Kemungkinan penolakan manajemen merupakan keterbatasan dari macam kebijakan dan prosedur internal kontrol yang dirancang dengan baik. Ini tidak masuk akal untuk mencoba memilih kontrol yang pasti efektif dalam pendeteksian kesalahan dari kecerobohan atau dalam pencegahan kolusi antara pekerja.

3. Pentingnya Pengendalian Intern

Jonathan B Schiff and Claire B May 1990, menulis artikel yang berjudul *What is Internal Control? Who owns It?* artikel ini mengungkapkan secara jelas bahwa pengendalian intern di dalam suatu perusahaan adalah penting untuk menghindari kesalahan-kesalahan dan kecurangan-kecurangan informasi keuangan, sehingga perlu diketahui apa itu pengendalian intern dan siapa yang bertanggungjawab atas pengendalian intern dalam suatu perusahaan.

Dalam sistem akuntansi berbasis komputer otomatisasi banyak digunakan dalam komponen sistem. Sekali data dimasukkan untuk diproses maka akan lenyap dari daya jangkauan manusia. Hal ini menunjukkan pentingnya perancangan pengendalian intern yang baik pada awal perancangan suatu sistem. Pengendalian pada umumnya akan lebih efektif jika dibangun di dalam suatu sistem dari pada jika ditambahkan setelah suatu sistem itu diimplementasi-kan. Oleh karena itu dapat dikatakan bahwa mengembangkan sistem akuntansi berbasis komputer berarti juga mengembangkan pengendalian intern di dalam sistem tersebut. Dalam pemrosesan data secara elektronik (EDP), penangannan dokumen semakin berkurang dan keterlibatan manusia dalam permrosesan data semakin berkurang. Hal ini menuntut metode-metode pengendalian intern untuk mendukung kebenaran informasi tersebut.

Kompleksitas suatu lingkungan komputer seperti pemrosesan *on-line*, sistem komunikasi, pemrosesan data tersebar, sistem manajemen basis data (*data base management systems*) dapat menimbulkan kesalahan dan kecurangan yang tidak terdeteksi. Untuk mengatasi hal ini perlu dikembangkan pengendalian intern yang memadai pada sistem akuntansi berbasis komputer.

Michael J. Cerullo, 1989 berpendapat bahwa pengendalian intern yang cukup harus diimplementasikan dan dipelihara dengan alasan antara lain:

1) Untuk mencegah suatu kejadian jangan sampai terjadi, misalnya pengendalian diperlukan untuk mencegah kesalahan, kelupaan, kecurangan, *invension of privacy, key punch, an input errors* dan kesalahan proses.
2) Untuk mendeteksi sesuatu sesudah hal itu terjadi, misalnya ukuran pengendalian dan keamanan diperlukan untuk mendeteksi kebakaran, kesalahan, pecahnya mesin atau kegagalan fungsi tertentu.
3) Untuk melakukan tindakan koreksi yang cocok segera sesudah sesuatu terjadi, misalnya suatu organisasi harus membuat *back up, recovery plans and contingency plans* untuk memperkecil konsekuensi kekacauan dan untuk mengejar kembali kapasitas kegiatan yang penuh.
4) Untuk memperkecil kerugian *financial* dari kehilangan komputer atau kerusakan fisik kekayaan.
5) Untuk memperkecil terhentinya kegiatan karena sistem yang kacau, keusangan atau bencana.
6) Untuk mengurangi tuntutan sah yang potensial karena perkara hukum akibat penanganan rekening, data atau laporan keuangan yang tidak tepat.
7) Untuk memenuhi persyaratan dari *forigen corrupt practices act of 1977.*
8) Untuk memenuhi rekomendasi yang dibuat tahun 1987 oleh *national commission on fraudellent financial reporting.*

4. Elemen Pengendalian Intern

Lima komponen internal kontrol suatu organisasi (Bookhold 1999) adalah kontrol lingkungan, penaksiran resiko, kontrol aktivitas, informasi dan komunikasi dan pengawasan.

a. Kontrol Lingkungan (the control environment)

Ini menciptakan sifat dari suatu organisasi. Menyediakan disiplin dan struktur, ini merupakan dasar untuk komponen internal kontrol yang lain. Ini dipengaruhi oleh sejarah organisasi dan budaya dan mempunyai dampak yang mempengaruhi pada bagaimana organisasi mencapai tujuan. Kontrol lingkungan terdiri dari:

- Integritas dan nilai etika (*integrity and ethical values*)

- Komitmen ke kemampuan (*commitment to competence*)
- Partisipasi anggota direktur dan komite audit (*board of directors and audit committee participantion*)
- Filosofi manajemen dan gaya operasi (*management philosophy and operating style*)
- Struktur organisasional (*organizational structure*)
- Penugasan otoritas dan tanggungjawab (*assigment authority and responsibility*)
- Kebijakan dan praktek sumber daya manusia (*human resources polities and practices*)

b. *Penaksiran resiko (risk assessment)*

Penaksiran resiko merupakan proses mengidentifikasi dan menganalisis suatu resiko oleh manajemen yang mungkin menjaga organisasi dari pencapaian tujuannya. Resiko timbul dari faktor eksternal maupun faktor internal. Resiko yang timbul dari faktor eksternal mempengaruhi organisasi secara keseluruhan. Ini termasuk resiko yang berasal dari persaingan, perubahan ekonomik, atau tehnologi, peraturan pemerintah dan bencana alam yang terjadi secara alami. Sedangkan resiko yang berasal dari faktor internal berkaitan dengan aktivitas yang spesifik suatu organisasi. Ini termasuk di antaranya adalah gangguan sistem informasi, kesalahan yang disebabkan kurangnya pelatihan dan tidak termotivasinya para pegawai atau merubah tanggungjawab manajemen dan hasil dari tidak efektifnya anggota direktur atau komite audit.

c. *Pengendalian aktivitas (control activity)*

Pengendalian aktivitas merupakan kebijakan dan prosedur yang dipakai manajemen untuk menyediakan kepastian yang masuk akal sesuai dengan petunjuk yang diingini oleh manajemen. Akuntan mengetahui banyak tipe pengendalian aktivitas yaitu:

1) Prosedur pengotorisasian transaksi (*authorizing transaction*)
2) Keamanan untuk asset dan catatan (*security for asset and record*)
3) Pemisahan tugas (*segregation datics*)
4) Catatan dan dokumen yang cukup (*adequate documents and record*)

d. Informasi dan Komunikasi

Informasi komunikasi diperlukan pada seluruh level organisasi untuk membuat keputusan operasional, untuk pelaporan keuangan dan untuk kepatuhan diidentifikasi, dipahami, diproses, dan dilaporkan oleh sistem informasi. Komunikasi melekat dalam sistem informasi. Bagaimanapun juga komunikasi menyampaikan melalui pemrosesan data keuangan yang meliputi formulir eksternal maupun internal. Komunikasi memakai formulir seperti kebijakan manual, akuntansi manual dan memorandum. Ini juga dibuat secara lisan dan melalui tindakan manajemen.

Sistem informasi mengkomunikasikan informasi, baik eksternal maupun internal. Secara tradisional akuntan mengetahui sistem informasi sebagai salah satu bentuk komunikasi internal. Sistem akuntansi modern menerapkan metode akuntansi *double entry*. Ini meliputi beberapa figur yang mencegah dan mendeteksi kesalahan dan ketidakberesan, analisa debet kredit, chart rekening, voucher, jurnal standar, trial balance dan pengendalian rekening.

e. Pengawasan

Pengawasan merupakan suatu proses untuk mengukur kualitas dari kinerja internal kontrol sepanjang waktu. Pengawasan membantu manajemen menetapkan modifikasi apa untuk sistem yang dibutuhkan ketika perubahan kondisi.

Pengawasan aktivitas yang sedang berjalan (*on going monitoring activities*). Banyak aktivitas yang harus mengawasi efektivitas dari internal kontrol dalam kegiatan operasi yang umum. Ini meliputi clerical check, perbandingan asset yang ada dengan catatan akuntansi, pengawasan prosedur yang dipakai program komputer, review yang dilakukan manajemen terhadap ringkasan perubahan account balance dan review oleh pemakai pelaporan komputer.

Evaluasi yang terpisah (*separated evaluation*). Dari waktu ke waktu manajemen mungkin memutuskan untuk melaksanakan evaluasi yang terpisah dari efektivitas sistem internal kontrol suatu organisasi. Evaluasi ini mungkin berdasarkan lingkupnya atau frekuensinya, tergantung dari resiko yang dikendalikan dan pentingnya pengendalian dievaluasi. Evaluasi mungkin berupa *self-assesment* yang dilaksanakan oleh manajer melalui pengendalian dalam area tanggungjawab mereka.

5. Pengendalian Akuntansi dalam Sistem Akuntansi Berbasis Komputer

Pengendalian akuntansi terdiri dari rencana organisasi dan semua metode-metode yang digunakan oleh organisasi untuk menjaga atau mengamankan kekayaan organisasi dan dapat dipercayainya informasi keuangan. Pengendalian ini sering disebut *preventive controls* sebab bertujuan untuk mencegah terjadi hal-hal yang tidak diinginkan. Dalam suatu sistem secara elektronik, pengendalian akuntansi dibagi menjadi

(Michael J Cerullo 1989):

a) General controls
b) Security controls
c) Application controls

a. General controls

Pengendalian umum merupakan pengendalian sistem informasi yang mempengaruhi semua aplikasi komputer dalam suatu organisasi. Menurut (Boockhold,1999) ada empat kategori pengendalian umum yaitu

1) *Data center operations controls*
2) *Systems software acquisitions and maintenance controls*
3) *Acces security controls*
4) *Applications system development and maintenance controls.*

1). *Pengendalian Operasi Pusat Data (Data center operations controls)*

Pusat data merupakan segmen dari suatu organisasi yang menyediakan pelayanan komputer untuk segmen lainnya. Dalam perusahaan yang besar, pusat data mungkin adalah cabang atau divisi yang dikepalai oleh wakil presiden. Dalam perusahaan yang berukuran menengah, sering merupakan departemen yang terpisah yang dikepalai oleh manajer MIS melaporkan ke kontroler. Dalam perusahaan yang kecil, mungkin beberapa pegawai yang mengoperasikan komputer pribadi sebagai tambahan untuk melaksanakan tugas akuntansi yang lain.

Pengendalian pusat data meliputi prosedur data pendukung, kontijensi rencana, dan pemisahan tugas. Prosedur data pendukung (*data backup procedure*). Sistem informasi memroses banyak data yang dikumpulkan setiap hari. Kadang-

kadang suatu kejadian terjadi merusak satu atau lebih data, prosedur data pendukung dapat mencegah kehilangan data.

Kontijensi Rencana (*contingency plans*) merupakan dokumen formal yang menjelaskan bencana yang terjadi dalam prosedur yang akan digunakan dalam ousat data. Bencana seperti kebakaran, banjir dan lain-lain. Yang dapat merusak fasilitas secara lengkap. Jika catatan akuntansi rusak seperti fasilitas tersebut, ini akan sulit untuk mengumpulkan piutang dan menetapkan seberapa banyak organisasi berhutang kepada vendor dan pegawai.

Pemisahan tugas (*segregation duties*). Pemisahan tugas yang baik bahwa fungsi kritikal dilaksanakan pada pusat data yang terpisah. Fungsi ini adalah sistem analisis dan pemrograman, operasi mesin, dan pemeliharaan data.

Tanggungjawab untuk penerimaan perangkat lunak sistem dan pemeliharaan meliputi administrasi jaringan, pendukung tehnik personal komputer (PC), administrasi *database* dan administrasi *web*. Administasi jaringan merupakan seseorang yang bertanggung jawab untuk memelihara perangkat lunak yang mengendalikan jaringan komputer.

2). *Pengendalian Sistem Perangkat Lunak dan Pemeliharaan (Systems software acquisitions and maintenance controls)*

Pengendalian Sistem Perangkat Lunak dan Pemeliharaan mempengaruhi semua aplikasi dan merupakan pengendalian umum. Aktivitas ini memerlukan pengetahuan yang khusus yang tinggi, dan biasanya orang ditetapkan pada pusat data melaksanakannya. Manajemen seharusnya menetapkan tanggungjawab untuk penerimaan perangkat lunak. Sistem dan pemeliharaan, seharusnya melaksanakan kebijakan dan prosedur yang tepat melalui aktivitas ini.

3). *Pengendalian Melalui Akses Keamanan (Acces security controls)*

Pengendalian akses membatasi kemampuan seseorang untuk mendapatkan kembali atau memodifikasi data dan untuk keuntungan yang tidak dibenarkan menggunakan perlengkapan komputer. Manajemen melakukan pengendalian akses dengan penetapan pemisahan tugas, dengan permintaan prosedur identitas dan pembuktian keaslian dan dengan menyediakan keamanan secara fisik untuk perlengkapan komputer.

Dengan penetapan tugas yang baik dalam pusat data, manajemen meminimalisasi kesempatan untuk menutupi pencurian suatu asset. Ini memerlukan pemisahan tugas antara pengembangan sistem, operasi mesin dan pemeliharaan data.

Perangkat lunak sistem melaksanakan identifikasi dan prosedur pembuktian keaslian. Perangkat lunak sistem ini mungkin mengoperasikan perangkat lunak sistem atau mungkin paket perangkat lunak keamanan komputer yang digunakan bersama dengan pengoperasian suatu sistem.

Beberapa sistem yang mengijinkan akses *dial-up* dengan telepon menggunakan prosedur pemenggilan kembali otomatis. Pengguna memanggil nomer telepon dari *switchboard* komputer otomatis. Komputer menjawab panggilan, menerima *password* dari pemakai dan kemudian memutus sambungan. Komputer mencari dalam file nomor telepon pemakai yang terdaftar untuk *password* dan memanggil kembali pemakai pada nomor tersebut.

Otorisasi file mengidentifikasi tidak hanya sistem *password* tetapi juga *password* untuk file yang disimpan. Ini menunjukkan semua file pemakai dibenarkan untuk diakses, *password* untuk tiap file dan *file permission*. *File permission menunjukkan* macam dari akses yang diperbolehkan untuk pemakai.

4). Pengembangan Sistem Aplikasi dan Pengendalian Pemeliharaan (Applications system development and maintenance controls.)

Prosedur yang cukup untuk perubahan sistem dan program adalah *preventive control* (pengendalian preventif). Ini meminimalkan kesalahan dan ketidakberesan yang diperkenalkan oleh sistem baru atau perubahan dari sistem yang telah ada. Suatu organisasi seharusnya mempunyai prosedur yang memerlukan *formal review* dan *authorization* untuk suatu sistem yang baru sebelum mengimplementasikannya. Ini mencegah implementasi banyak sistem yang tidak efisien, tidak efektif dan tidak dapat untuk dipertemukan dengan kebutuhan organisasi.

Semua manual dan terkomputerisasi prosedur seharusnya mempunyai *adequate documentation* yang memudahkan programmer dan analis untuk memahami prosedur yang tersedia sebelum merubahnya. Ini mencegah perubahan yang mempunyai pengaruh yang tidak terduga atau mungkin

menghasilkan data tidak akurat dan tidak dipercaya.

Organisasi seharusnya mempunyai prosedur yang diperlukan untuk mencatat dan mendokumentasikan perubahan pemilihan program dan sistem yang sudah ada. Banyak perusahaan memerlukan pemasukan program yang merubah catatan dalam paket dokumentasi untuk program komputer. Ketika programmer membuat perubahan produksi versi suatu program (versi yang digunakan selama pemrosesan rutin), kepala petugas informasi memerlukan programmer untuk mendaftar perubahan dalam catatan perubahan program.

b. Security controls

Pengendalian keamanan merupakan alat fisik dan tehnik prosedural yang bertujuan untuk melindungi perangkat keras komputer, termasuk tempat komputer, perangkat lunak dan ancaman fisik data, bahaya resiko atau kerugian dan kerusakan potensial lainnya (Michael J Cerullo,1989). Alat-alat keamanan fisik misalnya: alarm, penjagaan dan lain-lain. Tehnik-tehnik keamanan yang prosedural antara lain: tatanan rekontruksi file, jaminan asuransi, *fidelity bond*, dan *off-premis storage of data*, juga termasuk dalam hal ini adalah cincin pelindung file, pelindung catatan, tempat anti api, AC, alat pengendali untuk mencegah akses ke fasilitas komputer tanpa izin/otorisasi (Fratis Francis Gultom dalam Abdul Halim, 1994).

Struktur pengendalian intern dipilih untuk mengendalikan kebijakan, praktek dan prosedur untuk suatu sistem akuntansinya untuk menyediakan kepastian yang masuk akal untuk mencegah atau mendeteksi kesalahan dan ketidakberesan. Pengendalian tentang kebijakan, praktek dan prosedur yang memastikan data yang akurat dan dapat dipercaya menyediakan kebutuhan data (*data integrity*). Karena komputer terdiri atas catatan dan transaksi suatu asset yang diperlukan telah diotorisasi, pengendaliannya untuk menjaga keamanan file komputer dan juga menjaga keamanan asset, Pengendalian ini menyediakan keamanan data (*data security*)

c. Application controls

Pengendalian aplikasi mempengaruhi aplikasi individual, seperti catatan permintaan penjualan, penerimaan kas, atau aplikasi penggajian. Tim kerja mengembangkannya selama perancangan dan implementasi sistem aplikasi. Secara tradisional akuntan mengidentifikasi ada tiga cara pengendalian aplikasi dalam

mencegah dan mendeteksi kesalahan dan ketidakberesan (Boockhold,1999)

yaitu:

1) Pengendalian input
2) Pengendalian pemrosesan
3) Pengendalian output

Pengendalian input bertujuan untuk menjamin bahwa data yang diterima untuk diproses telah diotorisasi, lengkap, bebas dari kesalahan, diidentifikasi menjadi data yang dapat dibaca oleh mesin (komputer). Pengendalian input menyangkut perubahan data menjadi bentuk yang mudah dibaca oleh komputer dan dengan pencegahan atau pendeteksian kesalahan sementara memasukkan data (Fratis Francis Gultom dalam Abdul Halim,1994). Menurut Boockhold, 1999 pengendalian input terdiri dari *check digit dan validitas data*. *Check digit* merupakan digit yang ditambahkan ke nomor rekening. Algoritma menetapkan bagaimana untuk menghitung nilai yang benar dari *check digit* dari digit yang lain dalam nomor rekening. Program komputer menggunakan algoritma untuk memeriksa nomor rekening transaksi. Validitas data terdiri atas prosedur untuk mendeteksi kesalahan data sebagaimana ini memasukkan sistem aplikasi dan mencegah sistem dari salah memasukkan data. Ada dua macam pendekatan dalam data validitas yaitu: data validitas dalam pemrosesan *batch* dan data validitas dalam sistem *on-line real-time*. Pengendalian input terdiri dari pengendalian tahap penangkapan/perolehan data; pengendalian tahap penyiapan data; pengendalian tahap pemasukkan data (Fratis Francis Gultom dalam Abdul Halim,1994). Pengendalian pemrosesan bertujuan untuk mencegah kesalahan yang terjadi selama pemrosesan data yang dimasukkan dalam komputer. Kesalahan pemprosesan dapat terjadi karena program aplikasi yang digunakan dalam memproses data (Fratis Francis Gultom dalam Abdul Halim, 1994). Kesalahan yang terjadi dalam pemrosesan data dapat dideteksi dengan adanya pengendalian-pengendalian yang dibuat oleh programmer.

Pengendalian output bertujuan untuk menjamin ketelitian dalam memproses hasil dan menjamin bahwa fihak yang berhak saja yang menerima output. Output dapat berupa *printout*, disk, CD, tampilan di monitor dan lain-lain. Pengendalian output bervariasi tetapi untuk tujuan penggolongan menjadi dua bentuk *hard copy* dan *soft copy* (Fratis Francis Gultom dalam Abdul Halim, 1994).

Pengendalian *hard copy* meliputi antara lain pengendalian pada tahap penyediaan media keluaran, pengendalian pada tahap pemrosesan pengeluaran dan pengendalian pada tahap pendistribusian laporan. Pengendalian keluaran berbentuk *soft copy* meliputi pengendalian pada informasi yang ditransmisikan dan pengendalian pada tampilan di layar terminal.

KESIMPULAN

Dari pembahasan di atas dapat disimpulkan sebagai berikut:

1. Pengendalian akuntansi dalam sistem akuntansi berbasis komputer meliputi pengendalian umum (*general controls)*; pengendalian keamanan (*security controls*) dan pengendalian aplikasi (*application controls)*. Pengendalian akuntansi mencakup pengendalian terhadap *hardware*, *software*, masukan, pemrosesan dan keluaran. Pengendalian intern dalam masukan dapat menjamin bahwa data yang diterima untuk diproses telah diotorisasi, lengkap dan bebas dari kesalahan. Pengendalian dalam pemrosesan dapat mendeteksi kesalahaninput, kecurangan, kesalahan program aplikasi dan lain-lain.
2. Pengimplementasian pengendalian intern dalam suatu sistem yang ada, maka kompleksitas suatu sistem komputer dapat mencegah kesalahan dan kecurangan yang tidak terdeteksi.

DAFTAR PUSTAKA

Abdul Halim, 1995. *Sistem Informasi Akuntansi*, Yogyakarta: BPFE UGM.

Barry E. Cushing, 1982. *Accounting Information Systems and Business Organizations*, Third Edition. Massachusetts: Addiso-Wesley Publishing Company.

Boockhold, 1999. *Accounting Information System*, Transaction Processing and Control, 4 th Edition,

Jonathan B Schiff and Claire B May, 1990. What is Internal Control? Who Owns It? *Management Accounting*. November.

James A Hall, 2001. *Sistem Informasi Akuntansi*, Jakarta: Penerbit Salemba Empat.

Michael J Cerullo, 1989. Evaluating EDP in Computer Environment, *Journal of Accounting and Full*.