Jurnanl Akuntansi & Investasi Vol. 1 No. 1 hal: 11-19
ISSN: 1411-6227

KONTROL TERHADAP KECURANGAN DALAM SISTEM AKUNTANSI BERBASIS KOMPUTER

Oleh :
Yesi Mutia Basri

Abstrak

Perkembangan teknologi komputerisasi yang pesat telah memberikan pengaruh yang sangat besar terhadap sistem informasi dalam suatu perusahaan. Sistem akuntansi berbasis komputer serta pemrosesan data dengan komputer merupakan bagian yang tidak dapat dipisahkan, sehingga meningkatkan perhatian terhadap area khusus akuntansi yang baru dikenal dengan "sistem informasi akuntansi".

Suatu sistem memiliki peluang terhadap kesalahan manajemen, kecurangan-kecurangan dan penyelewengan-penyelewengan umum lainnya. Kecurangan sistem komputer pada dasarnya sama dengan sistem manual. Perbedaannya terletak pada orang yang melakukan kecurangan tersebut yaitu menggunakan komputer untuk mencapai maksudnya serta jumlah rupiah yang digelapkan dengan sistem komputer jumlahnya lebih besar.

Pengendalian suatu sistem informasi akuntansi jelas merupakan suatu kebutuhan yang paling utama. Semakin kompleks teknologi yang digunakan akan mempengaruhi pengendalian yang dibutuhkan agar sistem berjalan sebagaimana mestinya. Pengendalian ini mencakup semua aspek dalam sistem informasi akuntansi itu sendiri.

Paper ini membahas pengendalian terhadap kecurangan dalam sistem informasi akuntansi dan jenis-jenis kecurangan yang ada serta membahas cara-cara yang dapat diikuti dalam upaya mengatasinya. Sebelumnya akan dibahas terlebih dahulu pengertian serta pentingnya pengendalian intern dalam suatu sistem informasi akuntansi.

Key Word: Sistem informasi akuntansi, pengendalian intern, sistem komputer,sistem manual.

Pengertian Pengendalian Intern

Suatu sistem informasi akuntansi yang baik harus mempunyai suatu pengendalian. Sistem pengendalian intern yang diterapkan pada sistem informasi akuntansi sangat berguna untuk mencegah atau menjaga terjadinya kesalahan-kesalahan atau kecurangan-kecurangan. Sistem pengendalian intern juga dapat digunakan untuk melacak kesalahan-kesalahan yang terjadi sehingga dapat dikoreksi.

Sistem pengendalian intern dapat didefinisi pertama kali tahun 1949 oleh AICPA sebagai berikut yaitu: "Pengendalian intern meliputi struktur suatu organisasi dan semua metoda-metoda yang terkoordinir serta ukuran-ukuran yang ditetapkan di dalam suatu perusahaan untuk tujuan menjaga keamanan harta kekayaan milik perusahaan, memeriksa

ketepatan dan kebenaran data akuntansi, meningkatkan efisiensi operasi kegiatan, dan mendorong ditaatinya kebijakan-kebijakan manajemen yang telah ditetapkan."

Menurut Ikatan Akuntansi Indonesia sistem pengendalian intern meliputi organisasi serta semua metoda dan ketentuan yang dikoordinasi dan dianut dalam suatu perusahaan untuk melindungi harta miliknya, memeriksa kecermatan dan kehandalan data, meningkatkan efisiensi usaha dan mendorong ditaatinya kebijakan manajemen yang telah ditetapkan.

Dari definisi tersebut dapat diartikan bahwa sistem pengendalian intern mencakup struktur organisasi, semua metoda-metoda dan cara yang terkoordinir serta ukuran-ukuran yang ditetapkan di dalam suatu organisasi. Tujuannya adalah untuk menjaga keamanan harta kekayaan milik perusahaan, memeriksa ketepatan dan kebenaran data akuntansi, meningkatkan efisiensi operasi kegiatan serta mendorong ditaatinya kebijakan-kebijakan manajemen yang telah ditetapkan.

Definisi pengendalian intern tersebut menekankan tujuan yang hendak dicapai, dan bukan pada elemen-elemen yang membentuk sistem tersebut. Dengan demikian, pengertian pengendalian intern tersebut berlaku baik dalam perusahaan yang mengelola informasinya secara manual, dengan mesin pembukuan, maupun dengan komputer.

Dalam Statement on Auditing Standar (SAS) No. 55 mengenai *Consideration of internal control structure in a financial statement audit"* dijelaskan bahwa elemen-elemen struktur pengendalian intern terdiri atas :

1. *Control Environment* yaitu suatu lingkungan dalam suatu entitas yang me-nuntut sikap, kesadaran dan tindakan yang penuh dari dewan direksi, manajemen, pemilik dan pihak-pihak terkait lainnya mengenai arti penting suatu pengendalian. Lingkungan yang dimaksud seperti filosofi dan gaya pengoperasian dari manajemen, metoda-metoda dalam pemberian hak dan tanggung jawab, dan praktek-praktek dan kebijakan personalia.
2. *Accounting System* yaitu metoda-metoda dan catatan-catatan yang dibuat dengan tujuan untuk mengidentifikasi, merangkai, menganalisis, meng-klasifikasikan catatan dan laporan atas transaksi suatu entitas, memelihara akuntabilitas aktiva dan kewajiban seperti identifikasi nilai transaksi sehingga dapat disajikan dalam laporan keuangan, penjelasan atas laporan keuangan tersebut.
3. *Control Procedure* yaitu kebijakan dan prosedur selain *control environment* dan *accounting system,* yang telah ditentukan oleh manajemen untuk memberikan jaminan yang memadai bahwa tujuan entity yang spesifik dapat dicapai, misalnya otorisasi yang lazim terhadap transaksi atau aktivitas lainnya, pemisahan tugas untuk mengurangi kesempatan dari berbagai personal untuk melakukan kecurangan atau penyimpangan dari praktik bisnis yang wajar, dan menambah keamanan baik dalam mengakses penggunaan aktiva maupun pencatatannya.

Menurut tujuannya, sistem pengendalian intern dapat dibagi menjadi dua macam yaitu "sistem pengendalian administrasi" dan "sistem pengendalian akuntansi". Sistem pengendalian administrasi meliputi struktur organisasi, metoda dan ukuran yang dikoordinasikan terutama untuk mendorong efisiensi dan dipatuhi-nya kebijakan manajemen. Sedangkan sistem pengendalian akuntansi, yang merupa-kan bagian dari sistem pengendalian intern, meliputi struktur organisasi, metoda dan ukuran yang dikoordinasikan terutama untuk menjaga kekayaan organisasi dan mengecek ketelitian dan dapat dipercaya tidaknya data akuntansi. Suatu sistem pengendalian akuntansi yang baik

akan menjamin keamanan kekayaan para invesotr dan kreditor yang ditanamkan dalam perusahaan dan akan menghasilkan laporan keuangan yang dapat dipercaya.

Pada prinsipnya, pengendalian akuntansi dan pengendalian administrasi dalam sistem akuntansi manual maupun yang sudah diotomatisasi adalah sama, tetapi pengendalian akuntansi yang digunakan untuk fungsi pemrosesan data adalah berbeda tergantung pada sistemnya, telah dikomputerisasi atau belum.

Menurut Cerrullo (1989), pengendalian akuntansi dibagi ke dalam 3 sub bagian, yaitu pengendalian umum (*general controls*), pengendalian keamanan (*security controls*), dan pengendalian aplikasi (*aplication controls*).

Pengendalian umum meliputi 6 kategori, yaitu :

1. Perencanaan organisasi
2. Operasi
3. Perencanaan dan pengembangan sistem
4. Akses
5. Dokumentasi
6. Perencanaan Kontinjensi

Pengendalian aplikasi berhubungan dengan setiap pekerjaan yang diotomatisasi meliputi program input serta pengendalian output, sedangkan pengendalian keamanan meliputi pengendalian terhadap peralatan fisik dan teknik-teknik prosedur untuk melindungi perangkat keras komputer termasuk lokasi atau tempat komputer, perangkat lunak komputer serta data dari ancaman fisik, bahaya atau rugi yang potensial karena kerusakan.

Dari berbagai kategori pengendalian yang diuraikan di atas, jelaslah bahwa sedemikian kompleksnya masalah pengendalian yang dihubungkan dengan sistem informasi akuntansi. Hal yang paling penting untuk diketahui adalah bahwa penerapan suatu sistem pengendalian intern di dalam suatu perusahaan tergantung dari situasi serta jenis dari perusahaannya. Oleh karena perusahaan yang satu berbeda dengan perusahaan lain, maka harus dipertimbangkan. Mengetahui dan memahami konsep umum dari sistem pengendalian intern yang mempunyai elemen-elemen dasar yang dapat berlaku umum hampir pada semua sistem infor-masi akuntansi adalah hal yang paling penting bagi penganalisis dan perancang sistem. Bila elemen-elemen dasar tidak ada atau kurang berfungsi, maka pengendali-an intern sistem akuntansi menjadi lemah. Elemen-elemen dasar tersebut adalah :

1. Karyawan yang jujur dan cakap
2. Adanya pemisahan tugas dan garis wewenang dan tanggung jawab yang jelas.
3. Prosedur yang tepat untuk pemberian wewenang.
4. Dokumen dan catatan yang lengkap.
5. Pengawasan fisik yang cukup terhadap aktiva dan catatan.
6. Dilakukannya pencocokan yang independen.

Kecurangan dalam Sistem Komputer

Kesalahan-kesalahan yang terjadi dalam sistem informasi akuntansi biasanya disebabkan dua hal, yaitu “kesalahan-kesalahan yang disengaja dan kesalahan-kesalahan yang tidak disengaja”. Kesalahan-kesalahn yang tidak disengaja misalnya kesalahan memasukkan kode, salah nilai dan kesalahan karena ketidaktelitian. Kesalahan-kesalahan

yang sifatnya disengaja dapat berbentuk kecurangan-kecurang-an dalam bentuk pencurian atau penyelewengan terhadap harta kekayaan milik perusahaan.

Kecurangan dalam sistem informasi akuntansi berbasis komputer antara lain disebut dengan *crime computer fraud*, atau *computer abuse*. Istilah yang lazim digunakan adalah *computer fraud* yang didefinisi yaitu suatu rencana yang disengaja atau sesuatu yang telah dipertimbangkan bahwa seseorang menggunakan komputer untuk mendapatkan keuntungan yang tidak wajar melebihi orang lain dengan cara berusaha untuk berbohong, menipu, mengejutkan, licik, curang atau hal yang tidak wajar lainnya (Wilkinson & Cerullo, 1997).

Kecurangan-kecurangan di dalam perusahaan dapat dilakukan (Jogiyanto, 1988):

1. Oleh orang lain di luar petugas yang bertanggungjawab atas keamanan harta kekayaan milik perusahaan. Kecurangan ini dapat diatasi dengan memperketat penyimpanan harta kekayaan di tempat yang aman, dan tidak sembarang orang dapat menemukannya dan dapat masuk.
2. Oleh karyawan sendiri yang dipercaya untuk menjaga keamanan harta kekayaan milik perusahaan tersebut.

Perbuatan yang dapat dikatakan kecurangan dapat diklasifikasikan sebagai berikut (Wilkinson & Cerullo, 1987) :

1. *Misrepresentation of materal fact* (Kurang menyajikan kenyataan material).
2. *Failure disclose material fact* (Kegagalan untuk mengungkapkan kenyataan material)
3. *Embezzlement* (Penggelapan)
4. *Larceny* (Pencurian)
5. *Bribery* (Penyuapan)
6. *Illegal gratuity* (persen yang tidak sah)

Jenis-jenis Kecurangan Komputer

Menurut Wilkinson & Cerullo (1997) terdapat dua tipe kecurangan yaitu:

1. *Internal fraud*, yaitu kecurangan yang dilakukan oleh manajer atau karyawan perusahaan.
2. *External fraud*, yaitu kecurangan yang dilakukan bukan oleh karyawan perusahaan.

Menurut Nash dan Roberts (1984) ada 3 bentuk utama kecurangan dalam sistem komputer yaitu :

1. *Exploitation of inavertent discoveries of control loopholes*
Kecurangan ini bisanya disebabkan oleh adanya kelemahan dalam pengendalian intern suatu sistem yang ditemukan secara tidak sengaja oleh pelakunya. Misalnya memasukkan *password* yang salah ke dalam suatu terminal komputer.

2. *Work of Pranksterns*
Kecurangan ini biasanya terjadi di sekolah dan universitas yang menawarkan kursus komputer. Para siswa melakukan akses atau memodifikasi file data ataupun mencampuri sistem komputer institusi, tidak dengan tujuan finansial, tetapi hanya untuk kepuasan diri pribadi dan untuk membanggakan diri.

3. *Intentional crime*
Bentuk kecurangan ini yang paling umum terjadi, yaitu meliputi tindakan tidak sah yang dilakukan dengan sengaja oleh orang-orang di luar organisasi, pegawai

perusahaan ataupun manajemen sendiri. Biasanya motivasi utamanya adalah keuntungan finansial.

Kecurangan dalam sistem komputer biasanya dilakukan dengan berbagai cara antara lain :

1. Memanipulasi input
2. Mengubah Program
3. Mengubah File
4. Mencuri data
5. Sabotase

Kecurangan dengan memanipulasi input hanya memerlukan sedikit keahlian teknis yaitu dengan mengubah input meliputi penambahan transaksi, pengubahan transaksi dan penghapusan transaksi. Kecurangan dengan pengubahan program dilakukan oleh pelaku dengan mengubah atau memasukkan kode yang tidak sah ke dalam program. Pengubahan file dilakukan oleh orang dalam yang dapat meng-ubah atau menghapus file dengan leluasa. Mencuri data dilakukan dengan meng-gunakan data yang tersimpan dalam komputer perusahaan tanpa izin. Sedangkan sabotase komputer dilakukan dengan merusak perangkat keras dan perangkat lunak komputer yang menimbulkan kekacauan untuk menutupi tindakan curangnya.

Mencegah, Menemukan dan Membatasi Kecurangan Komputer

Beberapa kecurangan komputer dapat dicegah atau dideteksi secepatnya untuk membatasi kerugian yang semakin timbul dengan menetapkan prosedur-prosedur pengendalian yang harus dilakukan. Dalam merancang suatu pengen-dalian sistem yang layak untuk sistem akuntansi berkomputer, pihak mana-jemen perlu menyadari bahwa konsistensi, kecepatan serta fleksibilitas komputer membutuhkan pengendalian tambahan yang memperhatikan (Paroby, 1987) :

1. Pengaruh kesalahan-kesalahan yang digabungkan. Misalnya komputer menyiapkan faktur penjualan dengan mengambil input kuantitas dan mem-perluasnya dengan harga *master file* yang dijual. Bila program tidak berfungsi, misalnya memilih harga yang salah, maka semua faktur-faktur penjualan menjadi tidak benar.
2. Reduksi terhadap keterlibatan manual dalam sistem akuntansi mungkin menimbulkan suatu pemisahan tugas yang tidak tepat.
3. *Audit trail* mungkin berkurang, dieliminir atau ada untuk jangka waktu pendek dalam bentuk *print out*.
4. Pengubahan data dan program yang dilakukan oleh individu yang kurang memahami pengendalian intern dan kebijakan akuntansi ataupun perubahan-perubahan yang dibuat tanpa pengujian yang layak atau tanpa izin mana-jemen.
5. Bertambahnya individu yang dapat mengakses data merupakan titik kritis dalam pengendalian perusahaan.

Selanjutnya ada dua sasaran utama pengendalian organisasi terhadap ling-kungan pemrosesan data komputer, yaitu untuk menjamin bahwa :

1. Pengembangan dan perubahan terhadap program yang telah disahkan, diuji serta disetujui dan telah ditempatkan dengan benar.

2. Akses terhadap file data dibatasi hanya untuk pemakai dan program yang telah disahkan.

Sasaran ini merupakan suatu sasaran pengendalian komputer yang umum, karena mempengaruhi hampir semua aktivitas akuntansi yang bersistem komputer serta mempengaruhi sejumlah rekening atau sekelompok transaksi.

Ada beberapa cara yang digunakan untuk mencegah, menemukan kecurangan komputer (Wilkinson & Cerrullo, 1997) yaitu :

1. Pembagian Tugas
2. Meningkatkan peranan *internal audit* dan komite audit
3. Kebijaksanaan dan kontrol
4. Membuka kode
5. Manajemen menunjukkan nilai etik yang kuat
6. Sertifikat profesional (seperti sertifikat *internal auditor* dan *certified fraud examinier*)
7. *Internal auditor* yang telah terlatih untuk mencegah kecurangan dan pene-muan kecurangan
8. Kontrol program
9. Penyiapan dokumen yang baik
10. Auditor terkait dalam pengembangan sistem
11. Melaksanakan pemeriksaan yang rutin
12. Pengawasan yang terbuka
13. Filosofi yang proaktif (misalnya aktif menyelidiki kecurangan, pemecatan dengan segera, melaporkan pelanggaran pada orang yang tepat).

Dalam melakukan pencegahan terjadinya kecurangan komputer ini, ada tiga alternatif tindakan yang dapat diikuti oleh auditor intern perusahaan (Sugiri, 1991), yang meliputi :

1. Auditor intern ikut aktif dalam merancang sistem komputer. Alternatif ini merupakan yang terbaik, karena auditor dapat memasukkan kendali otomatik dalam program komputer untuk mencegah seseorang mengubah program atau data.
2. Auditor intern melibatkan dirinya setelah program komputer selesai dibuat. Alternatif ini tidak sebaik alternatif pertama namun auditor dapat memainkan peranan penting dengan :
    a. Mengkaji ulang program komputer untuk mengidentifikasi dan menilai kendali-kendali yang telah dibuat.
    b. Mencoba menemukan kelemahan potensial.
    c. Merekomendasikan kendali tambahan untuk mengatasi kelemahan-kelemahan kritis tersebut.
3. Auditor intern tidak aktif kecuali setelah sistem komputer beroperasi. Alternatif ini yang paling buruk dari dua alternatif lainnya, karena tidak mudah bagi auditor untuk memberikan dampak yang signifikan pada pengendalian program komputer dan prosedur operasi.

Menurut Paroby & Barret (1987), dalam prosedur-prosedur pengendalian, ada tiga lini pertahanan terhadap kecurangan komputer yaitu:

1. **Prevention** yang membatasi akses pelaku potensial terhadap fasilitas komputer, terminal komputer, file data, program dan laporan.

2. **Dectection** untuk menemukan kecurangan di dalam peristiwa yang pelakunya lolos dari mekanisme pencegahan yang telah ada.
3. **Limitation** untuk membatasi kerugian bila terjadi kecurangan yang terencana dan terlaksana dengan baik.

Ketiga lini pertahanan ini dapat disempurnakan dengan tiga jenis prosedur pengendalian yaitu :

1. Pengendalian administrasi, merupakan kebijaksanaan pengendalian intern yang menetapkan prosedur-prosedur operasi untuk instalasi komputer.
2. Pengendalian fisik, mengatur lingkungan fisik dari fasilitas komputer sebagaimana juga input dan output fisik komputer.
3. Pengendalian teknis, melaksanakan fasilitas-fasilitas pemrosesan itu sendiri untuk membatasi akses pemakai terhadap file data dan program.

Prosedur-prosedur pengendalian yang dirancang untuk mencegah, menemukan, dan membatasi kecurangan komputer adalah sebagai berikut :

1. Pencegahan (*Prevention*)

Administrasi. Pengecekan sekuriti terhadap latar belakang personal apakah pernah berurusan dengan aktivitas kriminal sebelumnya. Pemisahan tugas yang layak untuk petugas-petugas pemrosesan data dan departemen pemakai untuk menghindari situasi kecurangan yang potensial.

Fisik. Lokasi yang tidak menarik perhatian dapat membantu mengamankan fasilitas komputer dari pengacau. Akses yang terkendali terhadap fasilitas komputer dengan menggunakan kunci atau kartu magnetik secara fisik membatasi pe-makai yang tidak sah dari terminal komputer, sehingga mengurangi kesem-patan melakukan kecurangan secara signifikan.

Teknis. Pemberian kode adalah perubahan data dari suatu sistem komunikasi ke sistem lainnya. Pelaku kecurangan harus memecahkan kode terlebih dahulu sebelum dapat memanipulasi data. Pengendalian akses perangkat lunak dan password memungkinkan pemakain mengakses ke terminal, file data, program atau utilitas stelah memasukkan *password* yang benar.

2. Penemuan (*Detection*)

Administrasi. Menggunakan log pada proses pengolahan data sehingga riview terhadap log dapat menemukan kecurangan. Pengujian program dilaksanakan setelah satu program dimodifikasi untuk menjamin tidak tersedianya kemungkinan proses kecurangan.

Fisik. Penjagaan ruang komputer sepanjang waktu atau dilaksanakan berkala terhadap fasilitas komputer agar dapat diketahui pemakai sistem yang tidak sah terutama pada waktu istirahat. Agenda masuk ruang komputer, yang harus ditandatangani individu bila masuk ruang komputer, sehingga dapat meng-identifikasikan individu yang tidak berhak.

Teknis. *Logging* transaksi memberikan laporan apakah terjadi kesalahan-kesalahan yang disengaja atau kecurangan. Total rupiah atau jumlah *filed* yang tidak dijumlahkan seperti departemen atau jumlah *part* adalah *relatif* dalam menemukan kesalahan data yang disengaja. Pembandingan kode sumber yang dikerjakan dengan program komputer dan pembandingan kode sumber versi satu program lainnya, menunjukkan apakah program cocok atau tidak diubah.

3. Pembatasan (*Limitation*)

Administratif. Rotasi tugas dalam pemrosesan data membatasi kerugian yang disebabkan oleh kecurangan, sehingga seorang individu hanya dapat melaku-kan kecurangan pada periode waktu yang terbatas. Pembatasan transaksi yang merupakan batas maksimum administrasi atas transaksi khusus dapat membatasi kerugian karena kecurangan.

Fisik. Pembatasan dokumen-dokumen cetak yang bernilai uang, misalnya cek, dapat membatasi kemungkinan rugi karena kecurangan. Pembatasan juga dilakukan terhadap *back up* data dari kerugian potensial dengan fasilitas restorasi data yang rusak.

Teknis. Pengecekan ranking untuk menjamin data yang masuk jatuh dalam rangking nilai yang diizinkan dan pembatasan kerugian yang mungkin timbul dari transaksi-transaksi yang tidak sah. Pengecekan kelayakan untuk menentukan apakah suatu input merupakan sesuatu yang normal dengan membandingkan jumlah-jumlah untuk menentukan standar.

Kesimpulan

Kecurangan komputer adalah penyalahgunaan uang atau harta orang lain dengan mengubah program komputer, file data, operasi, peralatan atau media yang menimbulkan kerugian bagi organisasi yang sistem komputernya dimanipulasi. Kecurangan ini dapat dilakukan seseorang tanpa harus mempunyai keahlian mengenai komputer atau menggunakan komputer secara langsung.

Beberapa contoh kecurangan misalnya dengan memasukkan transaksi-transaksi fiktif atau yang telah diubah ke dalam suatu sistem : menghilangkan transaksi yang sah; memodifikasi langsung atau pengrusakan file atau record komputer, mengubah program tanpa izin, pencurian atau duplikasi data secara tidak sah, serta melakukan akses yang tidak sah.

Ada dua sasaran pengendalian organisasi terhadap lingkungan pemrosesan data komputer yaitu dengan menjamin bahwa :

1. Pengembangan dan perubahan terhadap progam yang telah disahkan, diuji serta disetujui dan telah ditempatkan dengan benar.
2. Akses terhadap file data dibatasi hanya untuk pemakai dan program yang disahkan.

Dalam mencegah terjadinya kecurangan komputer, auditor intern perusahaan dapat mengikuti salah satu dari tiga alternatif yaitu : ikut aktif merancang sistem komputer, melibatkan diri setelah program komputer selesai dibuat atau auditor tidak aktif kecuali setelah sistem komputer.

Auditor intern mempunyai peranan penting dalam mencegah terjadinya kecurangan komputer. Meningkatnya potensi kecurangan komputer membutuhkan auditor yang lebih mendalami sistem komputer.

Referensi

AICPA. 1989. Codifications of Statement on Auditing Standars, New York, p. 74-75.

John F. Nash dan Martin Roberts. 1984. Accounting Information System, New York : Micmillan Publishing Company.

Josep W. Wilkinson & Michael J. Cerullo. 1997. Accounting Information System, Essential Concepts and Aplication, Third Edition, John Wiley & Sons, New York.

Michael J. Cerullo. 1989. "Evaluating EDP in Computer Environment", Journal of Accounting and EDP, Fall.

Slamet Sugiri. 1991. "Computer Fraud dan Bagaimana Mencegahnya", Majalah Akuntansi, No. 3, Maret.

Stephen M. Paroby, CPA, and William J. Barret, CPA. 1987. "Preventing Computer Fraud-A Massage For Management", The CPA Journal, November.

Yogianto, (1988), Sistem Informasi Akuntansi Berbasis Komputer. Buku I, BPFE UGM, Yogyakarta.