

PEMANFAATAN TEKNOLOGI INFORMASI DALAM AUDIT INVESTIGATIF

Trisna Sary Lewaru

Fakultas Ekonomi Universitas Pattimura
Jln. Ir. M. Putuhena, Kode Pos : 97233 Ambon
e-mail : eka_lewa@yahoo.com

ABSTRACT

This study purpose to description the using from information technologi in investigation audit. The results of the study showed that some tools and software audit can be supports investigation audit activity, among other : computer forensic, Generalized Audit Software (GAS), PC Software, Embedded audit routine, etc. Using of technology here is important for effectiveness and efficiency audit.

Keywords: Investigation Audit, Information Technologi, Audit Software, Computer Forensics

I. PENDAHULUAN

Perkembangan teknologi informasi (*information technology*) yang disingkat dengan IT begitu cepat dan merambah diberbagai sektor serta mempunyai dampak yang luar biasa pada seluruh aspek kegiatan dan aktifitas. Hal ini dikarenakan teknologi informasi menyediakan *contemporary management tools* yang benar-benar dapat menghasilkan nilai tambah, dan menghubungkan dengan jelas antara misi dan visi perusahaan, perencanaan strategis, programming, anggaran, dan kegiatan sehari-hari. Untuk itu implementasi teknologi informasi saat ini di banyak organisasi sudah menjadi kebutuhan.

Teknologi informasi tidak hanya berfungsi secara operasional, tetapi teknologi informasi sudah menjadi senjata bagi keunggulan bersaing. hal ini tidak terlepas dari peran komputer sebagai salah satu bentuk teknologi yang sangat membantu didalam proses bisnis. Badan Usaha Milik Negara/Daerah, Instansi Pemerintahan Pusat/Daerah, demikian pula halnya dengan masyarakat umum cenderung untuk menyandarkan diri pada sistem informasi yang berbasis komputer untuk menyatakan hasil dari pelaksanaan program/kegiatan mereka.

Teknologi auditing sistem informasi pun telah berkembang seiring perkembangan sistem komputer walau tidak seluruhnya merupakan teknologi yang digunakan untuk mengaudit. Namun, tersedia sejumlah alat dan teknik dapat dengan cepat membantu dalam pencapaian tujuan sebuah audit.

Teknologi informasi juga telah dimanfaatkan untuk melaksanakan audit investigatif yang berhubungan dengan pemeriksaan forensic dan analisis yang menggunakan teknik audit, investigasi dan pengumpulan data dan informasi (yang dapat digunakan sebagai bukti dalam pengadilan sipil dan

kriminal) untuk disajikan kepada pengambil keputusan (Sofyan dan Sianturi, 2007). Melihat begitu pentingnya teknologi informasi bagi pelaksanaan audit, maka penelitian ini bertujuan untuk mendiskripsikan mengenai pemanfaatan teknologi informasi didalam pelaksanaan audit investigasi.

II. TINJAUAN PUSTAKA

Audit Investigasi

Definisi Audit Investigasi

Audit investigasi mempunyai beberapa pengertian antara lain :

1. Menurut *Association of Certified Fraud Examiners* (ACFE): Audit investigative adalah suatu methodology untuk menyelesaikan dengan jelas, permasalahan yang berkaitan dengan adanya indikasi tindak kecurangan dari awal sampai akhir. Lebih khususnya, pemeriksaan investigative meliputi upaya untuk mendapatkan berbagai bukti-bukti dan pernyataan-pernyataan, memberikan kesaksian, penulisan laporan, dan membantu dalam pendeteksian dan pencegahan tindak kecurangan (Salman, 2007).
2. Menurut Nocha (2005), audit investigasi adalah bagian dari manajemen kontrol yang dilaksanakan dalam kegiatan internal audit, di samping audit lainnya, seperti audit keuangan dan audit kepatuhan atau compliance audit.
3. UU nomor 15 tahun 2004 (pasal 13): pemeriksa dapat melaksanakan pemeriksaan investigative guna mengungkapkan adanya indikasi kerugian negara/daerah dan/atau unsur pidana (Salman, 2007).

Dari pengertian diatas secara umum dapat dilihat bahwa Audit investigative dimaksudkan sebagai suatu audit yang dilakukan atas realisasi pelaksanaan

kegiatan dari suatu obyek audit yang telah mengindikasikan adanya penyimpangan - penyimpangan dan mengarah pada adanya kemungkinan terdapatnya kerugian negara/daerah dan/atau perekonomian negara sebagai akibat dari adanya penyimpangan - penyimpangan tersebut.

Audit investigative pada dasarnya merupakan audit yang dilaksanakan dengan menggunakan keterampilan layaknya seorang peyelidik. Oleh karena itu seseorang yang melakukan audit investigative di samping memiliki keahlian akunting dan auditing juga diharapkan memiliki pengetahuan lainnya, seperti bagaimana melakukan investigasi dan bagaimana memperoleh bukti (Suta'at, 2007).

Teknik Investigative

Audit investigative juga melibatkan suatu pendekatan dan metodologi proaktif untuk membahas penyimpangan melalui pendeteksian dengan menggunakan teknik-teknik audit yang diperlukan, yang ditunjukkan untuk mengungkapkan adanya penyimpangan secara lengkap / komprehensif dalam obyek yang diaudit. Menurut Suta'at (2007) teknik-teknik investigative dapat dilakukan dengan :

Peninjauan, Pengamatan, Wawancara, Konfirmasi, Pengujian, Analisis, Perbandingan, Audit Keabsahan, Rekonsiliasi, Penelusuran, Penghitungan Kembali dan Penelaahan Pintas.

Dalam audit investigative tata cara pemeriksaan dan sifat pemeriksaannya mengikuti kaidah atau metodologi audit internal. Akan tetapi menurut Noeha (2005), untuk mendapatkan hasil investigasi yang maksimal, seorang fraud auditor harus juga menguasai beberapa teknik investigasi, antara lain:

- Teknik penyamaran atau teknik penyadapan,
- Teknik wawancara, apabila akan menghadapi sang auditee, orang-orang yang diduga memiliki info yang dibutuhkan atau bahkan sang bosnya si auditee,
- Teknik merayu untuk mendapatkan informasi, apakah dengan memakai kesanggupan sendiri atau dengan bantuan orang lain,
- Mengerti bahasa tubuh, dalam membaca posisi si auditee, bohong atau jujur, dan
- Dapat dilakukan dengan bantuan software, seperti CAAT (*Computer Assisted Audit Tools*).

Teknologi Informasi

Teknologi informasi tidak hanya berfungsi secara operasional, tetapi teknologi informasi sudah menjadi senjata bagi keunggulan bersaing. hal ini tidak terlepas dari peran komputer sebagai salah satu bentuk teknologi yang sangat membantu didalam proses bisnis.

Kemajuan dalam teknologi komputer mempunyai dampak yang luar biasa pada seluruh aspek kegiatan usaha. Akuntansi, sudah barang tentu tidak terlepas dari dampak tersebut. Dalam sistem akuntansi manual, data sebagai masukan (*input*) diproses menjadi informasi sebagai keluaran (*output*) dengan menggunakan tangan. Hal ini berbeda dengan sistem komputer yang semuanya dikerjakan oleh/dengan komputer. Menurut Rusdiutomo dan Djajadiningrat (2007), Proses secara elektronik lebih terjamin transparan & akuntabel. Namun demikian, penerapan teknologi informasi mengandung berbagai risiko, diantaranya ketidaksesuaian antara kebutuhan bisnis dan perangkat teknologi informasi, kesalahan dalam investasi, performa yang tidak memadai dan lain-lain.

Menurut Rusdiutomo dan Djajadiningrat (2007), Pada dasarnya computer sangat membantu dalam segala hal akan tetapi computer juga dapat membantu dan mendukung segala bentuk kejahatan. Antara lain jenis jenis kejahatan computer sebagai berikut

- *Hacking/ cracking, network intrusion*
- *Computer fraud*
- *Harassment and cyberstalking*
- *Industrial espionage, insider crimes, Pirated software*

Untuk menanggulangi ancaman-ancaman kejahatan computer diatas maka diperlukan sistem keamanan yang berperan mengendalikan risiko khusus terkait dengan sistem informasi terkomputerisasi. Menurut Bodnar dan Hopwood (2006), System keamanan bisa dikembangkan dengan menerapkan pendekatan siklus hidup tradisional, seperti analisis system, desain system, implementasi sistem, serta operasi, evaluasi, dan pengendalian sistem.

Teknologi Informasi dalam Audit

Pada saat komputer pertama kali digunakan, banyak auditor mempunyai pemikiran bahwa proses audit akan banyak mengalami perubahan untuk menyesuaikan dengan penggunaan teknologi komputer.

Saat ini, penggunaan system informasi akuntansi berbasis komputer oleh organisasi bisnis dan banyak organisasi lainnya meningkat pesat. Penggunaan aplikasi akuntansi berbasis komputer juga mempunyai dampak yang cukup signifikan bagi profesi akuntan. Kompleksitas masalah-masalah dalam lingkungan proses data elektronik mendorong auditor untuk mengembangkan prosedur dan teknik untuk mengendalikan dan memeriksa system akuntansi berbasis komputer yang lebih rumit. Komputerisasi atau penggunaan system akuntansi berbasis komputer untuk menggantikan system manual, secara otomatis

akan mengurangi atau bahkan meninggalkan dokumen-dokumen konvensional (*hardcopy*) yang bersifat *verifiable evidence* dan mengarahkan ke *paperless office*. Dokumen atau *hardcopy* bukan lagi menjadi bagian utama untuk tujuan pencatatan. Dokumen-dokumen tersebut digantikan dengan sinyal kode *binary digit* dalam bahasa komputer yang *intangible*. Perubahan yang fundamental akibat kemajuan teknologi juga menyebabkan terjadinya kesalahan-kesalahan, baik tindak kecurangan maupun kelalaian, dalam bentuk yang sama sekali baru. Oleh karena itu perlu adanya upaya pencegahan terhadap segala bentuk kesalahan oleh komputer dan pengamanan terhadap system informasi berbasis komputer tersebut. Hal ini konsekuensinya, berdampak pada peningkatan kebutuhan pemeriksaan akuntan di lingkungan pemrosesan data elektronik.

Menurut budi (2007), Ada dua hal utama yang harus diperhatikan dalam audit atas pemrosesan data elektronik, yaitu :

1. Proses pengumpulan bukti (*evidence collection*)
2. Evaluasi bukti (*evidence evaluation*)

III. PEMBAHASAN

Pemanfaatan Teknologi Informasi dalam Audit Investigatif

Menurut Rusdiutomo dan Djajadiningrat (2007), pemanfaatan teknologi informasi (TI) dalam audit investigatif adalah sebagai berikut :

1. TI sebagai alat untuk melakukan audit investigasi
 - Perangkat & layanan TI sudah menjadi barang komoditas (*digicam, voice-recorder, HP, email*)
2. Audit investigasi yang dilakukan terhadap kejahatan yang dilakukan dengan bantuan IT.
 - Implementasi & penggunaan aplikasi e-??? (*e-banking, e-procurement, e-commerce*)
 - Komputer sebagai media pengolah, penyimpan, pengirim data atau informasi.

Menurut Bodnar dan Hopwood (2006), Manfaat potensial penggunaan teknologi sistem informasi dalam audit meliputi beberapa hal berikut ini:

- Kertas kerja yang dihasilkan oleh komputer umumnya lebih dapat dibaca dan konsisten. Kertas kerja seperti itu dapat juga disimpan, diakses, dan direvisi dengan mudah.
- Dapat menghemat waktu dengan mengurangi penelusuran, pengecekan silang, dan perhitungan rutin lainnya.
- Perhitungan, perbandingan, dan manipulasi data lainnya dilakukan dengan lebih akurat.

- Perhitungan kajian analisis dapat dilakukan dengan lebih efisien dan lingkungannya pun dapat diperluas.
- Informasi proyek seperti anggaran waktu dan proses pemantauan waktu aktual terhadap jumlah anggaran dapat dihasilkan dan dianalisis dengan lebih mudah.
- Korespondensi audit standar seperti kuesioner dan daftar nama, surat-surat proposal, dan bentuk laporan dapat disimpan dan dimodifikasi dengan mudah.
- Moral dan produktivitas dapat ditingkatkan dengan mengurangi waktu yang digunakan untuk tugas-tugas yang bersifat klerikal.
- Peningkatan efektivitas biaya dapat dicapai dengan menggunakan kembali dan memperluas aplikasi audit elektronik yang ada saat ini untuk audit-audit berikutnya.
- Mampu meningkatkan independensi personal sistem informasi.

Pada sistem akuntansi yang berkomputer atau yang lebih sering disebut Pemrosesan Data Elektronik (PDE), data sebagai input juga diproses menjadi informasi sebagai output. Keuntungan yang dapat dilihat secara jelas dari penggunaan komputer ini adalah kecepatan, ketepatan, dan kemudahan dalam memproses data menjadi informasi akuntansi (Budi, 2007).

Computer Forensics

Dalam audit investigasi ada yang dinamakan *computer forensics*. Menurut The SysAdmin, Audit, Network, Security (SANS) Institute, *computer forensics* adalah “ *The employment of a set of predefined procedures to thoroughly examine a computer system using software and tools to extract and preserve evidence of criminal activity*”. Sedangkan menurut ISACA (*Information System Audit and Control Association*) *computer forensics* adalah “ *The process of extracting information & data from computer storage media, and establishing its accuracy and reliability for the purpose of producing the same as evidence in a court of law*” (Rusdiutomo dan Djajadiningrat, 2007).

Bukti yang bisa ditemukan lewat teknik *computer forensics* antara lain (Rusdiutomo dan Djajadiningrat, 2007) :

- Semua data pada struktur direktori komputer
- File-file yang di/ter-hapus yang belum overwritten oleh system operasi
- Email yang di/ter-hapus.
- Dokumen yang dicetak oleh the *suspect's printer*
- Software aplikasi
- Situs yang diakses

Bukti elektronik yang bisa diperoleh antara lain (Rusdiutomo dan Djajadiningrat, 2007) :

- *Hard drives*
- *CD, DVD, Floppy disks, zip disks*
- PDA
- Handphone

Elemen kunci dari *computer forensics* antara lain (Rusdiutomo dan Djajadiningrat, 2007) :

- *Data protection*
- *Data acquisition*
- *Imaging*
- *Extraction*

Menurut Idrianita (2007), dalam pelaksanaannya, auditor TI mengumpulkan bukti-bukti yang memadai melalui berbagai teknik termasuk survei, interview, observasi dan review dokumentasi (termasuk review source-code bila diperlukan). Satu hal yang unik, bukti-bukti audit yang diambil oleh auditor biasanya mencakup pula bukti elektronis (data dalam bentuk *file softcopy*). Biasanya, auditor TI menerapkan teknik audit berbantuan komputer, disebut juga dengan CAAT (*Computer Aided Auditing Technique*). Teknik ini digunakan untuk menganalisa data, misalnya saja data transaksi penjualan, pembelian, transaksi aktivitas persediaan, aktivitas nasabah, dan lain-lain. Tentunya untuk aspek sekuriti adakalanya auditor dituntut mempunyai keahlian teknis yang cukup memadai untuk menguji keamanan sistem.

Software Edit

Kemajuan teknologi komputer sudah tidak diragukan lagi. Hal ini juga menggapai pada proses pengelolaan data akuntansi. Akibatnya auditor pun harus dapat mengantisipasinya. Auditor dapat menggunakan berbagai macam paket perangkat lunak atau software audit dalam melaksanakan audit. Satu jenis perangkat lunak dalam audit yang umum dipakai adalah *Generalized Audit Software*. Disamping itu ada beberapa software yang dapat mendukung pelaksanaan audit, baik secara langsung maupun tidak secara langsung.

a) Pengelolaan Data Elektronis (PDE)

System pemrosesan data atau pengolahan data elektronis (PDE) merupakan system pemrosesan data yang menggunakan teknologi telekomunikasi dan komputer. Ada empat komponen system PDE yaitu perangkat keras, perangkat lunak, metode pengorganisasian data dan metode pemrosesan data. System PDE walau mempunyai kelebihan daripada system manual seperti dapat memberikan konsistensi yang lebih baik dalam pemrosesan data, namun juga mempunyai kelemahan seperti menghasilkan jejak yang terbatas (Halim, 1997).

b) Generalized Audit Software

Menurut Halim (1997), *Generalized Audit Software* (GAS) merupakan penggunaan komputer untuk melaksanakan tugas atau prosedur pengujian audit secara independent terhadap record klien. *Generalized Audit Software* berisi sejumlah program komputer yang bersama-sama melaksanakan berbagai macam fungsi pengolahan data. *Generalized Audit Software* dikembangkan suatu kantor akuntan publik untuk dipakai pada berbagai audit atas klien maupun tahun audit yang berbeda. Pengembangan dan pemeliharaan *Generalized Audit Software* memerlukan biaya yang tinggi. Ada dua keuntungan penggunaan *Generalized Audit Software*. Pertama *Generalized Audit Software* dikembangkan dengan cara yang memungkinkan semua staf auditor dapat dilatih dengan cepat untuk menggunakan program umum tersebut. Kedua, program umum tunggal dapat diterapkan untuk lingkup tugas pengujian yang luas, tanpa perlu menambah biaya untuk membuat program individual. Cara kerja *Generalized Audit Software* meliputi beberapa langkah berikut :

1. Menentukan tujuan audit dan pengujian yang akan dilaksanakan. Tujuan tersebut dapat berupa penjumlahan suatu file data, pemilihan sample secara random, verifikasi perhitungan klien, membandingkan data pada dua file terpisah, dan sebagainya.
2. Menentukan kelayakan penggunaan *Generalized Audit Software* pada system PDE klien. Penentuan layak tidaknya penggunaan *Generalized Audit Software* dilaksanakan auditor atas dasar pengalaman profesionalnya.
3. Merancang aplikasi, yang meliputi logika aplikasi, penghitungan, dan format output.
4. Pembuatan kode (*coding*), hasil perancangan aplikasi kemudian dibuatkan kode (*coded*) pada kertas kerja oleh auditor pada bahasa *Generalized Audit Software* (GAS) sederhana. Kertas kerja ini merupakan instruksi yang memberi tahu GAS mengenai apa yang harus dikerjakan dengan data klien. Dengan demikian tujuan audit yang dispesifikasikan dapat tercapai.
5. Key entry. Kertas kerja berkode kemudian dimasukan program bersama dengan GAS dan file data klien.
6. Pemrosesan. Pada tahap ini GAS memproses aplikasi data file klien actual, dan menelaah hasilnya.

Generalized Audit Software dapat diterapkan pada pengujian pengendalian maupun pengujian substantif. Contohnya penggunaan *Generalized Audit Software* pada pengujian pengendalian adalah seperti perbandingan

harga jual barang dagangan antara file faktur penjualan yang terkomputerisasi, dengan master file yang berisi data harga yang terotorisasi. Perbandingan ini disusun untuk menentukan frekuensi harga yang tak terotorisasi. *Generalized Audit Software* juga dapat diterapkan pada pengujian substantif. Contoh penggunaan *Generalized Audit Software* pada pengujian substantif adalah seperti pemilihan atau seleksi dan pencetakan sample audit, menguji perhitungan dan membuat penghitungan (Halim, 1997).

c) Commercial General-Use Software

Menurut Halim (1997), *Commercial General-Use Software* merupakan penggunaan perangkat lunak yang relatif sederhana dan mudah dioperasikan. Perangkat lunak ini mudah didapatkan dengan harga ringan. Contoh perangkat lunak komersial yang banyak dipakai adalah electronic spreadsheet atau pengolah angka, dan pengolah kata atau word processors. Contoh pengolahan angka antara lain *lotus 123, quarto pro, Microsoft excel, VisiCalc, SuperCalc, dan Multiplan*. Contoh pengolahan kata yang populer antara lain *Word Star, Word Perfect, Microsoft Words, Perfect Writer*, dan sebagainya.

Selain itu masih banyak perangkat lunak yang membantu auditor dalam melaksanakan tugasnya. Ada perangkat lunak statistik yang dapat membantu perhitungan auditor yang berkaitan erat dengan statistika. Ada perangkat lunak yang membantu auditor untuk membuat *flowchart*, seperti *flowcharting, easyflow, dan ABS\C flowcharting*, ada pula perangkat lunak untuk membuat program seperti BASIC.

d) PC Software

Biaya murah PC ditambah dengan penggunaan yang makin meluas beragam paket perangkat lunak yang tersedia telah membuat PC menjadi alat penting untuk mengadministrasi sebuah audit. Paket PC *software general-purpose* seperti perangkat lunak pengolahan kata dan spreadsheet telah memiliki banyak aplikasi audit. Dan paket perangkat lunak untuk tujuan-tujuan tertentu yang berorientasi audit telah dikembangkan secara khusus untuk digunakan dalam administrasi audit.

ACL, yang dipublikasi oleh ACL software, adalah salah satu contoh perangkat lunak audit. Perangkat lunak ini memungkinkan auditor untuk menghubungkan sebuah PC dengan mainframe atau PC klien dan kemudian mengekstrak dan menganalisis data. Sebagai contoh, dengan menggunakan ACL, seorang auditor dapat secara langsung mengakses data SAP R/3. ACL Mengakses file-file dalam bentuk aslinya tanpa perlu konvermasi terlebih dahulu. ACL menyediakan sebuah rentang luas penggunaan fungsi-fungsi yang memungkinkan auditor melakukan beberapa hal seperti menghitung kembali rekening-rekening neraca untuk verifikasi, usia dan analisis piutang dagang, dan mengidentifikasi tren dan perbedaan yang muncul.

Tabel berikut ini secara ringkas menggambarkan teknik-teknik komputer yang dapat digunakan dalam audit.

Tabel 1. Teknologi *Auditing System* Informasi

TEKNIK	DESKRIPSI	CONTOH
Test data	Data pengujian adalah input yang berisi data valid dan tidak valid	Transaksi pembayaran gaji dengan nomor indentifikasi karyawan yang valid dan tidak valid
Integrated test facility (ITF)	ITF menggunakan baik data pengujian maupun penciptaan record fiktif (vendor, karyawan) pada file master sebuah sistem komputer	Transaksi pembayaran gaji untuk karyawan fiktif diproses bersamaan dengan transaksi pembayaran gaji yang valid
Parallel simulation	Pemrosesan data riil melalui program audit. Output disimulasikan dan dibandingkan dengan output regular	Penghitungan depresiasi diverifikasi dengan memproses file master bersama sebuah program audit
Audit Software	Program komputer yang memungkinkan komputer digunakan sebagai alat auditing	Seorang auditor menggunakan sebuah program komputer untuk mengekstrak record data dari sebuah file master
Generalized audit software (GAS)	GAS adalah perangkat lunak audit yang secara khusus didesain untuk	Seorang auditor menggunakan GAS untuk mencari file komputer

	memungkinkan auditor melakukan fungsi pemrosesan data audit yang terkait	untuk item yang tidak biasa
PC Software	Perangkat lunak yang memungkinkan auditor menggunakan sebuah PC untuk melakukan tugas-tugas audit	Sebuah paket spreadsheet PC digunakan untuk menyimpan kertas kerja audit dan jadwal audit
Embedded audit routine	Rutinitas auditing khusus dimasukkan dalam program komputer reguler sehingga data transaksi dapat dijadikan subjek analisis audit	Item data yang dikecualikan auditor dalam uji edit khusus dimasukkan dalam sebuah program yang ditulis untuk sebuah file audit khusus
Extended record	Modifikasi program untuk mengumpulkan dan menyimpan data-data audit yang diinginkan	Sebuah program pembayaran gaji dimodifikasi untuk mengumpulkan data-data yang terkait dengan pembayaran lembur
Snapshot	Modifikasi program untuk mendapatkan output data audit yang diinginkan	Sebuah program pembayaran gaji dimodifikasi untuk mengumpulkan data-data yang terkait dengan pembayaran lembur
Tracing	Tracing menyediakan sebuah rute audit terperinci terhadap instruksi-instruksi yang dilakukan selama operasi program	Sebuah program pembayaran gaji ditelusuri untuk menentukan apakah uji edit tertentu dilakukan dalam urutan yang benar
Reviewod system documentation	Perluasan system dokumentasi seperti flowchart program yang dikaji ulang untuk tujuan audit	Seorang auditor memeriksa pemrosesan logika sebuah program pembayaran gaji
Control flowcharting	Flowchart analitik atau teknik grafis lainnya digunakan untuk menjelaskan pengendalian pada sebuah system	Seorang auditor menyiapkan sebuah flowchart analitik untuk mengkaji ulang pengendalian pada system aplikasi pembayaran gaji
Mapping	Perangkat lunak khusus digunakan untuk memonitor eksekusi sebuah program	Eksekusi sebuah program dengan data pengujian sebagai input dipetakan untuk mengindikasikan seberapa jauh input menguji pernyataan-pernyataan program individual

Sumber: Bodnar dan Hopwood (2006)

Risiko Teknologi Informasi

Pada dasarnya setiap kegiatan pasti mengandung risiko dan pengendalian pada hakekatnya diimplementasikan untuk menghindari terjadinya risiko yang dimaksud. Hal ini tidak hanya terjadi pada operasi organisasi tetapi juga pada kehidupan manusia sehari-hari. Merupakan suatu hal yang sering terjadi, bila suatu organisasi/institusi tidak menyadari kondisi membahayakan tersebut. Hal tersebut karena kebiasaan kita untuk menyadari bahwa suatu kondisi/kejadian merupakan bahaya bila kondisi atau kejadian tersebut telah terjadi.

Seperti yang dikutip pada www.bpkp.go.id bahwa selama ini kita selalu menyandarkan diri pada apa yang dimaksudkan sebagai pengendalian (*control*), dan hampir selalu merasa yakin apabila terdapat pengendalian maka segala sesuatu akan berjalan sebagaimana mestinya. Kondisi tersebut ternyata tidak selamanya benar, sebab disamping masalah dilaksanakan atau tidaknya suatu pengendalian, akan timbul pula masalah mengenai efektivitas pengendalian yang diterapkan tersebut. Sebagai konsekuensi dari kondisi tersebut, timbul pertanyaan mengenai keterandalan (*reliability*) data/informasi yang diungkapkan sebagai laporan keuangan atau laporan

manajemen yang menyatakan hasil kegiatan yang telah dicapai suatu organisasi. Tidak mungkin suatu informasi dapat dikatakan andal atau valid bila sumber data dan pengolahannya tidak juga andal dan valid.

Menurut Budi (2007), ada beberapa hal yang perlu diperhatikan dalam menggunakan komputer sebagai alat pengolah data yaitu resiko-resiko yang khas dalam suatu lingkungan akuntansi berbasis komputer. Auditor harus menyadari resiko-resiko ini karena hal ini merupakan ancaman yang tidak ada dalam proses akuntansi manual. Resiko-resiko dalam lingkungan pemrosesan data elektronik antara lain:

1. Penggunaan teknologi yang tidak layak
2. Pengulangan kesalahan
3. Kesalahan berantai
4. Pemrosesan yang tidak logis
5. Ketidakmampuan menerjemahkan kebutuhan pemakai ke dalam persyaratan teknis.
6. Ketidakmampuan dalam mengendalikan teknologi
7. Pemasukan data yang tidak benar
8. Data yang terkonsentrasi
9. Ketidakmampuan dalam mendukung pemrosesan
10. Penyalahgunaan pemakai akhir (*end user*)
11. Kesalahan prosedur pada fasilitas EDP
12. Kesalahan-kesalahan program
13. Kesalahan sistem komunikasi

Adanya kelemahan-kelemahan seperti tersebut diatas, maka pengendalian akuntansi sangat diperlukan dalam pengolahan data elektronik (PDE). Pengendalian akuntansi mempunyai tujuan utama mengamankan harta kekayaan perusahaan dan menjamin kebenaran data serta ketepatan data akuntansi (Budi,2007).

V. PENUTUP

a.) Kesimpulan

Seiring dengan meningkatnya pemanfaatan teknologi informasi dalam mendukung proses bisnis, kebutuhan terhadap teknologi informasi pun semakin meningkat tidak terkecuali dalam bidang audit investigasi. Terdapat beberapa alat dan perangkat lunak/software audit yang dapat

membantu kegiatan audit investigasi antara lain *computer forensic, Generalized Audit Software (GAS), PC Software, Embedded audit routine*, dan lain sebagainya. Penggunaan teknologi ini menjadi penting untuk meningkatkan efektivitas dan efisiensi auditing.

b.) Saran

Untuk itu, diharapkan para auditor eksternal dan auditor internal harus memiliki kemampuan dalam mengendalikan IT.

REFERENSI

- Abdul Halim**, (1997). "Auditing 1 (Dasar-Dasar Audit Laporan Keuangan)", UPP AMP YKPN, Yogyakarta.
- Amien Rusdiutomo dan Hasan Mustafa Djajadiningrat**, (2007). "Computer Forensic: Pemanfaatan Teknologi Informasi", Workshop Audit Investigatif.
- BPKP**, (2007). "Solusi Menghadapi Resiko Teknologi Informasi", www.bpkp.go.id/index.php?idunit=21&idpage=343
- Dasriel Adnan Noeha**, (2005). "Audit Investigasi, Bukan Sekedar Audit", www.kompas.com.
- George H. Bodnar dan William S. Hopwood**, (2006), "Sistem Informasi Akuntansi", Andi Press, Yogyakarta.
- Irwan Sofyan dan Stevanus Alexander B.P Sianturi**, (2007). "Audit Investigatif/Forensik Pengenalan Metodologi", Workshop Audit Investigatif, UGM, Yogyakarta.
- Khairansyah Salman**, (2007). "Pemeriksaan Investigatif Atas Penyimpangan Pengelolaan Keuangan Negara/Daerah", Workshop Audit Investigatif, UGM, Yogyakarta.
- Sasongko Budi**, (2007). "Audit dan Komputer", www.akuntan.com.
- Suta'at**, (2007). "Teknik Audit Investigatif Atas Penyimpangan Keuangan Di Sektor Publik", Workshop Audit Investigatif, UGM, Yogyakarta.