

1. Latar Belakang

Peradaban manusia dewasa ini telah mengalami perkembangan yang pesat, dengan semakin berkembangnya ilmu pengetahuan dan penemuan yang luar biasa. Manusia telah mengetahui bahwa penting sekali komunikasi dalam kehidupan sehari – hari. Menyadari akan pentingnya ilmu komunikasi, maka teknologi kini menjangkau penggunaan komputerisasi dalam dunia akuntansi. Kemajuan teknologi ini membantu organisasi dan dapat diandalkan. Kemampuan teknologi ini juga dapat membantu organisasi dalam mengambil keputusan yang tepat. Dengan adanya sistem, maka perusahaan juga dapat mengefisienkan peranan manusia. Maka dapat diambil suatu keputusan tepat waktu sehingga tidak menimbulkan masalah bagi perusahaan.

Di masa modern sekarang ini juga kita ketahui teknologi informasi sudah menjadi bagian yang tidak terpisahkan dalam kehidupan kita. Perkembangan ini dapat meningkatkan kinerja dan memungkinkan berbagai kegiatan dapat dilaksanakan dengan cepat, tepat, dan akurat, sehingga akhirnya akan meningkatkan produktivitas. Dimana dalam suatu perusahaan ataupun organisasi diatur dengan menggunakan sistem informasi.

Sistem Informasi merupakan asset bagi suatu perusahaan yang bila diterapkan dengan baik akan memberikan kelebihan untuk berkompetensi sekaligus meningkatkan kemungkinan bagi kesuksesan suatu usaha. Dalam mengimplementasikan sistem informasi tersebut harus adanya suatu tolok ukur untuk mencegah terjadinya hal-hal di luar rencana organisasi, dan pengoperasian sistem informasi yang dilakukan secara efektif dan efisien. Tujuan pengukuran terhadap sistem informasi tersebut adalah untuk meyakinkan manajemen bahwa apakah kinerja sistem informasi yang ada pada organisasinya sesuai dengan perencanaan dan tujuan usaha yang dimilikinya.

Pertumbuhan kemampuan teknologi informasi dan keinginan dari pelaku bisnis baik besar, menengah maupun kecil untuk mencapai *competitive advantage* yang mengarahkan peningkatan dramatis atas penggunaan teknologi informasi untuk mengorganisasi, memproses, menyimpan, dan mengkomunikasikan informasi. Saat

ini pekerja di segala level juga menggunakan teknologi informasi untuk aktivitas keseharian mereka.

Kemampuan auditor sangatlah penting bagi kelangsungan suatu perusahaan, maka tentu diharapkan dapat memudahkan auditor dalam memecahkan masalah dengan penggunaan teknologi yang diciptakan oleh manusia sendiri. Teknologi informasi telah berkembang sedemikian rupa, perusahaan melakukan operasinya dengan sistem online. Semua transaksi dan pencatatan yang terjadi telah menggunakan kemampuan komputerisasi. Pencatatan siklus suatu perusahaan ini meliputi input, proses dan output dalam melaksanakan aktivitas dan menjadi fasilitas utama yang memberikan peranan besar dalam perubahan yang mendasar pada infrastruktur dan manajemen operasi dimana pada akhirnya akan mempengaruhi pengambilan keputusan.

Namun pada kenyataannya, para auditor masih belum mampu menerapkan secara maksimal teknologi yang telah disediakan. Mereka tidak mampu memanfaatkan akses dari peranan teknologi informasi dalam mengaudit yang berbasis pada komputerisasi, baik pada saat input, proses sampai dengan output. Walaupun teknologi informasi telah meluas dalam dunia bisnis, namun masih sedikit auditor berani mengaplikasikannya. Dalam dunia pemrograman komputer, harga *software* aplikasi yang digunakan untuk mengaudit relatif tinggi sehingga hal ini juga menjadi salah satu alasan mengapa auditor mengalami kesulitan dalam penggunaan teknologi informasi.

Auditor harus mampu menggunakan kemampuannya sehingga dapat mengikuti kemajuan teknologi saat ini. Yang diinginkan oleh perusahaan adalah auditor yang memiliki kinerja baik dan mempunyai kemampuan dalam penggunaan sistem yang telah terkomputerisasi. Sehingga auditor juga dipacu untuk berusaha menguasai kemampuan dibidang teknologi.

Banyak keuntungan yang dapat diperoleh melalui audit terhadap kualitas sistem informasi. Manajer dapat melakukan perbaikan bernilai yang dapat memeriksa kualitas dan produktivitas. Lebih spesifik, audit yang terintegrasi dan inovatif

terhadap kualitas sistem secara tidak langsung akan memperbaiki kualitas teknologi. Demikian juga pemaparan *The American Society for Quality Control (ASQC)* (Willborn, 1989).

Penggunaan teknologi informasi (TI) dapat meningkatkan pengendalian internal dengan menambahkan prosedur pengendalian baru yang dilakukan komputer, dan dengan mengganti pengendalian manual yang dapat terpengaruh oleh kesalahan manusia karena manusia seringkali melakukan kesalahan-kesalahan dalam melakukan akses audit. Dengan pengendalian teknologi informasi ini pengendalian dapat dilakukan dengan suatu sistem yang lebih akurat dan terpercaya.

Walaupun teknologi informasi sangat membantu perusahaan namun terkadang hal ini juga dapat menimbulkan resiko ketergantungan, auditor harus tetap memperhatikan setiap kegiatan transaksi dan tidak boleh sepenuhnya bergantung pada sistem informasi. Karena jika terjadi kesalahan tentu akan menjadi masalah yang justru memperumit keadaan. Untuk mengurangi resiko itu auditor harus terus memantau dalam pemrosesannya.

Untuk menghadapi banyak resiko yang berkaitan dengan ketergantungan pada teknologi informasi, organisasi sering mengimplementasikan pengendalian khusus atas fungsi teknologi informasi. Standar auditing menguraikan dua kategori pengendalian atas sistem teknologi informasi yaitu pengendalian umum dan pengendalian aplikasi. Dimana pengendalian umum (*general controls*) diterapkan pada semua aspek fungsi teknologi informasi, termasuk administrasi teknologi informasi; pemisahan tugas teknologi informasi; pengembangan sistem; serta pengendalian perangkat keras. Auditor akan mengevaluasi pengendalian umum untuk perusahaan secara keseluruhan. Sedangkan pengendalian aplikasi (*application controls*) berlaku bagi pemrosesan transaksi, seperti pengendalian atas pemrosesan penjualan atau penerimaan kas. Auditor harus mengevaluasi pengendalian aplikasi untuk setiap kelas transaksi dimana auditor berencana mengurangi risiko pengendalian yang ditetapkan, karena pengendalian teknologi informasi akan berbeda

di antara kelas-kelas transaksi. Pengendalian aplikasi hanya akan efektif jika pengendalian umum efektif (Arens, Elder, dan Beasley, 2008:477).

Menurut Arens dkk (2008:485), auditor bertanggung jawab untuk memahami pengendalian internal, mereka harus mengetahui tentang pengendalian umum dan aplikasi. Pengetahuan tentang pengendalian umum akan meningkatkan kemampuan auditor dalam menilai dan mengandalkan pengendalian aplikasi yang efektif untuk mengurangi resiko pengendalian bagi tujuan audit terkait. Bagi auditor perusahaan publik yang harus menerbitkan pendapat mengenai pengendalian internal atas pelaporan keuangan, pengetahuan tentang pengendalian umum dan aplikasi sangatlah penting.

Pengendalian umum dalam lingkungan sistem informasi dapat memiliki dampak yang sangat luas atas pengolahan transaksi dalam sistem aplikasi. Jika pengendalian ini tidak efektif, maka akan terdapat resiko bahwa akan muncul kesalahan data dan informasi yang dihasilkan, dan semuanya dapat terjadi tanpa dapat terdeteksi sejak awal. Dengan demikian kelemahan dalam pengendalian umum pada lingkungan sistem informasi dapat menghalangi atau menghambat pengujian pengendalian aplikasi yang digunakan oleh perusahaan tersebut. Penggunaan pengendalian umum dan aplikasi yang efektif dapat menghasilkan efisiensi audit yang baik untuk mendukung mekanisme proses bisnisnya.

Internet merupakan media yang paling ekonomis untuk digunakan sebagai basis sistem informasi. Hubungan antar komputer di internet dilakukan dengan menghubungkan diri ke *link* terdekat, sehingga hubungan fisik biasanya bersifat lokal. Perangkat lunak untuk mengembangkan sistem informasi berbasis internet secara murah dan bahkan gratis. Dengan menggunakan internet maka jarak bukan menjadi masalah dalam melakukan aktivitas maupun komunikasi. Internet membantu memudahkan manusia dalam setiap aktivitasnya.

Melihat perkembangan internet, terdapat kesempatan dalam melakukan transaksi perdagangan dimana dilakukan secara elektronik. Dengan demikian, kegiatan – kegiatan perdagangan atau bisnis yang dilakukan via elektronik seperti

dokumentasi, pengedaran brosur, pengadaan iklan, dan sebagainya dapat digolongkan dalam *e-commerce*.

Alasan-alasan di atas menyebabkan Internet menjadi media elektronik yang populer untuk menjalankan bisnis, yang kemudian dikenal dengan istilah *electronic commerce* atau *e-commerce*. Banyak perusahaan menggunakannya untuk melakukan transaksi bisnis secara elektronik akan menghubungkan sistem akuntansi internalnya dengan sistem pihak eksternal, seperti pelanggan dan pemasok. Akibatnya risiko yang dihadapi suatu perusahaan sebagian bergantung pada seberapa baik hubungan *e-commerce* mengidentifikasi dan mengelola risiko dalam sistem teknologi informasinya. Penggunaan sistem *e-commerce* juga membuat data perusahaan yang sensitif, program, dan perangkat keras terbuka terhadap kemungkinan campur tangan atau sabotase oleh pihak luar. Untuk membatasi keterbukaan ini maka perusahaan dapat menggunakan *firewall*, teknik enkripsi, dan tanda tangan digital (Arens dkk, 2008:496).

2. Pokok Bahasan

Berdasar pada latar belakang permasalahan, maka dapat disusun pokok bahasan sebagai berikut :

1. Bagaimana peranan teknologi informasi terhadap audit komputerisasi dilihat dari prosedur audit, pengendalian internal, dan teknik komputerisasi?
2. Apa saja kemungkinan risiko yang dihadapi dalam audit sistem informasi?
3. Bagaimana mengidentifikasi masalah audit komputerisasi pada sistem *e-commerce*?

3. Tujuan Pembahasan

Untuk mengetahui bagaimana perkembangan teknologi informasi mempengaruhi proses audit dengan menggunakan sistem komputerisasi.

4. Kajian Literatur

4.1 Pengertian Teknologi informasi

Teknologi informasi lahir sekitar 1947, yang ditandai dengan ditemukannya komputer sebagai komponen utama dimana mulai populer di akhir dekade 70-an. Teknologi Informasi yang diartikan secara harfiah teknologi (Bahasa Indonesia) dan *technology* (Bahasa Inggris), berasal dari bahasa Yunani "Techne" yang berarti adalah seni. Teknologi merupakan pembuatan benda-benda yang dapat diamati secara inderawi untuk melayani kebutuhan atau gagasan manusia. Sedangkan Informasi (Bahasa Indonesia) dan *Information* (Bahasa Inggris) berasal dari "To-*Inform*" yang berarti adalah memberitahu.

Teknologi informasi adalah studi atau penggunaan peralatan elektronika, terutama komputer, untuk menyimpan, menganalisa, dan mendistribusikan informasi apa saja, termasuk kata-kata, bilangan dan gambar (Oxford, 1995; dalam Supriyati, 2006).

Teknologi informasi adalah segala bentuk teknologi yang diterapkan untuk memproses dan mengirimkan informasi dalam bentuk elektronik. Mikrokomputer, komputer *mainframe*, pembaca *barcode*, perangkat lunak pemroses transaksi, perangkat lunak lembar kerja (*spreadsheet*), dan peralatan komunikasi dan jaringan merupakan contoh teknologi informasi (Lucas, 2000; dalam Supriyati, 2006).

Teknologi informasi adalah teknologi yang menggabungkan komputasi (komputer) dengan jalur komunikasi berkecepatan tinggi yang membawa data, suara, dan video (Williams dan Sawyer, 2003; dalam Supriyati, 2006).

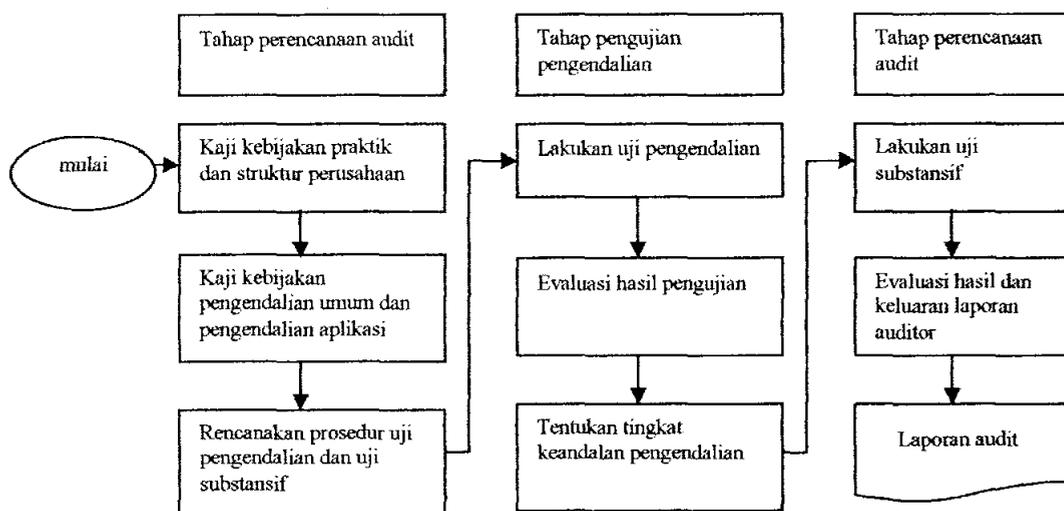
Menurut Husein dan Wibowo (2002:12), teknologi sistem informasi adalah satu alat bagi manajer untuk menyesuaikan diri dengan perubahan lingkungan usahanya. Teknologi yang dimaksud misalnya perangkat keras komputer yang digunakan untuk membantu aktivitas input, processing dan output dalam suatu sistem informasi; *software* komputer yang terdiri dari instruksi yang telah deprogram untuk mengontrol dan mengkoordinasi kerja perangkat keras komputer; teknologi penyimpanan data;

teknologi telekomunikasi yang memudahkan manajer berhubungan dari satu tempat ke tempat lain.

4.2 Pengertian audit sistem informasi

Pengertian Audit menurut Arens, dkk. (2003) Audit adalah proses pengumpulan dan pengevaluasian bukti-bukti tentang informasi ekonomi untuk menentukan tingkat kesesuaian informasi ekonomi tersebut dengan kriteria-kriteria yang telah ditetapkan, dan melaporkan hasil pemeriksaan tersebut.

Audit sistem informasi adalah audit yang berfokus pada aspek-aspek komputer dalam sebuah sistem informasi perusahaan. Audit ini meliputi kegiatan penilaian terhadap implementasi, operasi, dan pengendalian berbagai sumber daya komputer yang tepat. Menurut Hall, audit system informasi terbagi menjadi tiga tahap, yaitu tahap perencanaan, pengujian pengendalian, dan pengujian substansif (Hall, 2007).



Gambar 4.1 Tahapan dalam audit sistem informasi

Sumber: (Hall, 2007:17)

Menurut Supriyati (2006), tujuan audit sistem informasi komputerisasi akuntansi adalah untuk *mereview* dan mengevaluasi pengawasan internal yang digunakan untuk menjaga keamanan dan memeriksa tingkat kepercayaan sistem informasi serta *mereview* operasional sistem aplikasi akuntansi yang digunakan.

Menurut Abdul Halim (2004:87) audit sistem informasi adalah suatu proses mengumpulkan dan mengevaluasi bukti-bukti untuk menilai apakah sistem komputer telah menjamin keamanan aktiva, integritas data, mencapai tujuan-tujuan suatu organisasi secara efektif, dan telah menggunakan sumber daya secara efisien.

Informasi merupakan suatu power, merupakan suatu potensi yang dapat dimanfaatkan untuk menggerakkan organisasi secara efektif dan efisien. Terutama bagi perusahaan besar yang memiliki banyak cabang, masalah informasi merupakan salah satu yang sangat penting dan dibutuhkan. Unsur-unsur sistem informasi sebagai berikut:

1. Peralatan, antara lain adalah peralatan komputer dan komunikasi, maupun peralatan kantor lainnya (*hardware*);
2. Prosedur, tata kerja, ketentuan-ketentuan peraturan, termasuk sistem operasi, dan program-program komputer (*application software*);
3. Tenaga kerja pelaksana operasional (*operator*), pimpinan pada bidang tugas masing-masing, staff, termasuk teknisi komputer dan analis informasi.

Pelaksanaan audit sistem informasi ini biasanya dilakukan oleh auditor intern, dengan menerapkan pengetahuan teknis audit dan sistem informasi maupun pengalamannya, untuk mengevaluasi unit/departemen sistem informasi, pengembangan sistem aplikasi, serta mengevaluasi sistem yang sudah diimplementasikan.

Pengertian audit sistem informasi dapat dikelompokkan dalam dua tipe, yaitu audit sistem informasi akuntansi berbasis teknologi informasi yang merupakan bagian dari kegiatan audit/ pemeriksa laporan keuangan (*general functional audit*). Di lain pihak dapat pula audit sistem informasi dikategorikan sebagai jenis audit operasional, khususnya kalau pemeriksaan yang dilakukan adalah dalam rangka penilaian terhadap kinerja unit fungsional atau fungsi sistem informasi, ataupun untuk mengevaluasi sistem-sistem aplikasi yang telah diimplementasikan pada suatu organisasi.

Sistem informasi audit merupakan proses pengumpulan dan evaluasi bukti-bukti untuk menentukan apakah sistem komputer yang digunakan telah dapat melindungi

aset milik organisasi, mampu menjaga integritas data, dapat membantu pencapaian tujuan organisasi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien.

Menurut Karya (2009), Dilihat dari tipe pemroses data menjadi informasi, sistem informasi, dibagi menjadi:

1. Manual, di mana manusia sebagai *information processor*.
2. Terotomatisasi, di mana manusia sebagai operator yang menyediakan input-output, sedangkan komputer menjadi *information processor*.
3. Semi manual, di mana *information processor*, sebagian manusia dan sebagian komputer.

4.3 Peranan teknologi informasi

4.3.1 Peranan teknologi informasi terhadap audit sistem informasi komputerisasi akuntansi

Teknologi informasi mempunyai peranannya dalam sistem audit. Berkat teknologi ini, berbagai kemudahan dapat dirasakan oleh manusia seperti (Supriyati, 2006):

- a) Teknologi informasi melakukan *otomasi* terhadap suatu tugas atau proses yang menggantikan peran manusia.
- b) Teknologi informasi berperan dalam *restrukturisasi* terhadap peran manusia yang melakukan perubahan-perubahan terhadap sekumpulan tugas atau proses.
- c) Teknologi informasi memiliki kemampuan untuk mengintegrasikan berbagai bagian yang berbeda dalam organisasi dan menyediakan banyak informasi ke manajer.
- d) Teknologi informasi juga mempengaruhi antarmuka-antarmuka organisasi dengan lingkungan, seperti pelanggan dan pemasok.
- e) Teknologi informasi dapat digunakan membentuk *strategi* untuk menuju keunggulan yang kompetitif (O'Brien, 1996), antara lain:

1. Strategi biaya: meminimalisir biaya/ memberikan harga yang lebih murah terhadap pelanggan, menurunkan biaya dari pemasok.
2. Strategi diferensiasi: mengembangkan cara-cara untuk membedakan produk/jasa yang dihasilkan perusahaan terhadap pesaing sehingga pelanggan menggunakan produk/jasa karena adanya manfaat atau fitur yang unik.
3. Strategi inovasi: memperkenalkan produk/jasa yang unik, atau membuat perubahan yang radikal dalam proses bisnis yang menyebabkan perubahan-perubahan yang mendasar dalam pengelolaan bisnis.
4. Strategi pertumbuhan : mengembangkan kapasitas produksi secara signifikan, melakukan ekspansi ke dalam pemasaran global, melakukan diversifikasi produk/jasa dan, atau mengintegrasikan ke dalam produk/jasa yang terkait.
5. Strategi aliansi: membentuk hubungan dan aliansi bisnis yang baru dengan pelanggan, pemasok, pesaing, konsultan, dan lain-lain.

Namun ironisnya, pesatnya perkembangan teknologi informasi tersebut awal mulanya bertolak belakang dengan sudut pandang Auditor yang menilai bahwa hubungan bisnis yang wajar adalah jika dilaksanakan berdasarkan falsafah *arm's length transaction*-yaitu transaksi antara pihak-pihak yang bebas atau independen. Hubungan istimewa (atau dikenal dengan *related party transaction*) diyakini auditor sebagai transaksi yang dapat menimbulkan ketidakwajaran angka yang dicatat dalam catatan akuntansi. Padahal transaksi bisnis yang didasarkan atas *arm's-length transaction* dan nilai dasar ketidakpercayaan merupakan hubungan bisnis jangka pendek. Masing-masing pihak hanya mengusahakan agar pada saat transaksi bisnis terjadi, mereka yang terkait mampu bersikap *businesslike*, sehingga masing-masing pihak dapat memperoleh manfaat dari transaksi yang dilaksanakan. Apakah di kemudian hari pihak-pihak yang terkait sekarang akan melaksanakan bisnis, tergantung dari penentuan syarat-syarat independensi pada saat transaksi yang akan terjadi di masa yang akan datang tersebut sedangkan kemitraan Usaha (*Partnered Relationship*) untuk mendobrak mitos tersebut harus menitikberatkan pada *trust building dan core competency* di dalam membangun hubungan kemitraan, baik di

dalam organisasi perusahaan (antara manajer dengan karyawan dan antar fungsi dalam organisasi) maupun di antara perusahaan dengan para pemasok dan mitra bisnisnya

4.3.2 Peranan teknologi informasi terhadap audit sistem informasi komputerisasi akuntansi dilihat dari prosedur audit

Peranan teknologi informasi terhadap audit sistem informasi komputerisasi akuntansi dilihat dari prosedur audit berkaitan dengan tipe konfigurasi sistem informasi komputer yang digunakan oleh perusahaan. Tipe konfigurasi sistem informasi komputer terdiri dari:

a. Lingkungan Sistem Informasi Komputer-*Stand-alone Micro Computer*.

Komputer mikro dikenal dengan komputer pribadi (*personal computer* atau PC) yang umumnya digunakan oleh perusahaan kecil sebagai *stand-alone workstation* yang dioperasikan oleh satu atau beberapa pemakai pada waktu yang berbeda. Dalam perusahaan besar, komputer mikro umumnya digunakan sebagai *intelligent terminal* dalam *local area network* (LAN), *Wide are network* (WAN), atau dihubungkan dengan suatu komputer pusat.

Resiko pengendalian intern yang tinggi dalam lingkungan komputer mikro membuat auditor lebih memusatkan usaha audit ke pengujian substantif pada atau mendekati akhir tahun. Dengan demikian prosedur audit yang digunakan oleh auditor lebih berfokus kepada:

1. Pemeriksaan fisik dan konfirmasi aktiva.
2. Pengujian rinci.
3. Ukuran sampel yang lebih besar.
4. Penggunaan lebih banyak teknik audit berbantuan komputer (jika diperlukan).
5. Auditor dapat menempuh pendekatan lain yang berbeda dalam audit di lingkungan komputer mikro.

6. Auditor dapat meletakkan kepercayaan terhadap pengendalian intern klien setelah auditor melaksanakan pengujian pengendalian terhadap pengendalian intern tersebut.

b. Lingkungan Sistem Informasi Komputer-*On-Line Computer System*

Sistem komputer *on-line* adalah sistem komputer yang memungkinkan pemakai melakukan akses ke data dan program secara langsung melalui peralatan terminal. Sistem tersebut dapat berbasis *mainframe computers*, komputer mini, atau struktur komputer mikro dalam suatu lingkungan jejaring. Dengan sistem *on-line* pemakai dapat melaksanakan berbagai fungsi yang mencakup:

1. Melakukan entri transaksi (seperti: transaksi penjualan dalam toko pengecer, pengambilan kas di dalam suatu bank, dan pengiriman barang dalam suatu pabrik).
2. Melakukan permintaan keterangan (seperti informasi tentang *account* atau saldo terkini *customer*).
3. Meminta laporan (seperti daftar unsure sediaan yang ada di gudang, yang kuantitasnya menunjukkan angka negatif).
4. Melakukan *up-dating* terhadap *master file* (seperti pembuatan *account* bagi *customer* baru dan pengubahan kode *account* buku besar).

Sistem komputer *on-line* dapat digolongkan berdasarkan sebagai berikut:

a. *On-line/real time processing*

Dalam sistem pengolahan *on-line/real time*, transaksi secara individual dientri melalui peralatan terminal, divalidasi dan digunakan untuk *meng-update* dengan segera *file* komputer. Hasil pengolahan ini kemudian tersedia segera untuk permintaan keterangan atau laporan.

b. *On-line/batch processing*

Dalam suatu sistem dengan *on-line, input and batch processing* transaksi secara individual dientri melalui peralatan terminal, dilakukan validasi tertentu, dan ditambahkan ke *transaction file* yang berisi transaksi lain, dan kemudian dientri ke dalam sistem secara periodik. Di waktu kemudian, selama siklus pengolahan

berikutnya, *transaction file* dapat divalidasi lebih lanjut dan kemudian digunakan untuk meng-up date *master file* yang berkaitan.

c. *On-line/memo update* dan *On-line input with memo update processing*

Mengombinasikan *on-line/real time processing* dan pengolahan *on-line/batch processing*. Transaksi secara individual segera digunakan untuk meng-up date suatu *memo file* yang berisi informasi yang telah diambil dari versi terkini *master file*.

Permintaan keterangan dilakukan melalui *memo file*. Transaksi yang sama ditambahkan ke *transaction file* untuk divalidasi dan digunakan untuk *updating* berikutnya terhadap *master file* atas data *batch*. Dari sudut pemakai, sistem ini tampak tidak berbeda dengan *on-line/real time processing*.

d. *On-line/inquiry*

Membatasi pemakai pada peralatan terminal untuk melakukan permintaan keterangan dari *master file*. Dalam sistem ini, *master file* diupdate oleh sistem lain. Biasanya berdasarkan *batch* transaksi.

e. *On-line downloading/uploading processing*. *On-line downloading/ uploading processing*

Berkaitan dengan transfer data dari *master file* ke peralatan *intelligent terminal* untuk diolah lebih lanjut oleh pemakai.

4.3.3 Peranan Teknologi Informasi Terhadap Audit Sistem Informasi Komputerisasi Akuntansi Dilihat Dari Pengendalian Intern.

Kini banyak sekali komputer beredar di masyarakat, berbagai jenis dan kecanggihan telah ditawarkan dunia teknologi. Mulai kelas menengah bahkan kecil dapat menggunakan teknologi untuk membantu usahanya. Karena begitu besar peranan komputer dalam pengambilan keputusan, maka sangat perlu dilakukan kontrol.

Terkait dengan teknologi informasi, tujuan disusunnya system control atau pengendalian intern komputerisasi adalah untuk (Gondodiyoto, 2007:260):

1. Meningkatkan pengamanan aset sistem informasi (data/catatan akuntansi).

2. Meningkatkan integritas data, sehingga dengan data yang benar dan konsisten akan dapat dibuat laporan yang benar.
3. Meningkatkan efektifitas sistem.
4. Meningkatkan efisiensi sistem.

Menurut SPAP dalam SA Seksi 314.4 No. 05-09 pengendalian intern atas pengolahan komputer, yang dapat membantu pencapaian tujuan pengendalian intern secara keseluruhan, mencakup baik prosedur manual maupun prosedur yang didesain dalam program komputer. Proses pengendalian dalam lingkungan EDP terdiri atas:

Pengendalian umum:

- a. Pengendalian organisasi
- b. Pengendalian administratif
- c. Pengendalian pengembangan dan pemeliharaan sistim.
- d. Pengendalian *hardware* dan *software*.
- e. Pengendalian dokumentasi
- f. Pengendalian keamanan.

Pengendalian aplikasi:

- a. Pengendalian input
- b. Pengendalian pemrosesan
- c. Pengendalian output

4.3.4 Peranan Teknologi Informasi Terhadap Audit Sistem Informasi Komputerisasi Akuntansi Dilihat Dari Teknik-teknik audit dengan menggunakan Teknologi Informasi

Auditor harus memutuskan pendekatan mana yang akan ditempuh, maka terdapat tiga pendekatan teknik yang digunakan berkaitan dengan komputer :

1. Audit around the computer

Audit around the computer adalah audit terhadap penyelenggaraan sistem informasi berbasis komputer, tanpa menggunakan kemampuan peralatan komputer itu sendiri. Auditor mengambil kesimpulan dan merumuskan opini dengan hanya

menelaah struktur pengendalian dan melaksanakan pengujian transaksi dan prosedur verifikasi saldo. Auditor melakukan pengujian terhadap dokumen input dan laporan output. Apabila masukan dan keluarannya benar, maka prosesnya juga benar (Gondodiyoto, 2007).

Dengan teknik ini auditor menguji reliabilitas dari *computer generated information* dengan terlebih dahulu menghitung hasil yang diinginkan dari transaksi yang dimasukkan dalam sistem, dan kemudian membandingkan hasil perhitungan dengan hasil proses atau output. Jika terbukti akurat dan valid, maka diasumsikan bahwa sistem pengendalian berfungsi seperti yang seharusnya. Kondisi ini cocok jika sistem aplikasi otomasi sederhana dan ringkas. Pendekatan ini masih relevan dipakai di perusahaan yang menggunakan *software* akuntansi yang bervariasi dan melakukan proses secara periodik.

2. *Audit through the computer*

Menurut Gondodiyoto (2007:453), *Audit through the computer* yaitu pemeriksaan langsung terhadap program-program dan file komputer pada ASI berbasis teknologi informasi. Auditor menggunakan komputer (*Software Bantu*) atau dengan cek logika program dalam rangka pengujian pengendalian.

Teknik ini fokus pada pengujian tahapan pemrosesan komputerisasi, logika, program, *edit routines* dan program kontrol. Pendekatan ini mengasumsikan bahwa jika program pemrosesan dikembangkan dengan baik, dan memenuhi *edit routines* dan *programme check* yang memadai, maka *error* dan kecurangan tidak akan mudah terjadi tanpa terdeteksi (Wirapranata, 2009).

Auditor menguji dan menilai efektivitas prosedur pengendalian operasi dan program komputer serta ketepatan proses di dalam komputer. Keunggulan metode ini adalah bahwa auditor memiliki kemampuan yang besar dan efektif dalam melakukan pengujian terhadap sistem komputer, hasil kerjanya lebih dapat dipercaya dan sistem memiliki kemampuan untuk menghadapi perubahan lingkungan. Sedangkan kelemahan terletak pada biaya yang sangat besar dan tenaga ahli yang berpengalaman.

3. *Audit with the computer*

Audit with the computer adalah pendekatan audit dengan menggunakan komputer dalam berbagai bentuk, dalam pengetikan laporan, penjadwalan, penyusunan rencana kerja audit, penyusunan kertas kerja pemeriksaan (Gondodiyoto, 2007:454-455).

Dengan pendekatan ini, akuntan telah memanfaatkan komputer sebagai alat dalam melakukan pemeriksaan. Pada bentuk yang sederhana, komputer dilakukan sebagai alat untuk melakukan penulisan, perhitungan, perbandingan dan sebagainya. Bentuk yang lebih maju dalam pendekatan ini adalah digunakannya *Generalized Audit Software* yaitu program audit yang berlaku umum untuk berbagai klien.

Audit dilakukan dengan menggunakan komputer dan *software* untuk mengotomatiskan prosedur pelaksanaan audit. Metode ini lebih sulit dan kompleks serta biayanya paling besar.

TABK yaitu penggunaan teknik audit dengan menggunakan komputer. Terdapat dua macam teknik dengan menggunakan software, yaitu:

1. *Generalized Audit Software (GAS)*

GAS secara khusus adalah *software* untuk bantuan audit, yaitu untuk pengumpulan bahan bukti untuk entitas bisnis tertentu atau kegiatan tertentu. GAS adalah software yang digunakan untuk menilai kehandalan suatu sistem aplikasi.

GAS terdiri dari seperangkat program komputer yang secara bersama melaksanakan bermacam fungsi pemrosesan atau manipulasi data. Program-program yang digeneralisasi mempunyai dua manfaat penting. Yang pertama, program ini dikembangkan sedemikian rupa sehingga memudahkan pelatihan bagi staff auditor dalam menggunakan program, meskipun hanya memiliki sedikit pengetahuan tentang sistem berbasis teknologi informasi, dan tidak perlu memiliki kemampuan pemrograman. Kedua, dapat diterapkan pada lingkup yang lebih besar dan luas tanpa harus mengeluarkan biaya atau kesulitan dalam mengembangkan program (Gondodiyoto, 2007:648).

Alasan penggunaan GAS adalah praktis, efektif, efisien, ekonomis, *independent*. Sedangkan kebaikan dari GAS adalah mudah digunakan, menghemat waktu, mengakses berbagai *record*, andal dalam beberapa aspek audit, memungkinkan bagi auditor untuk mengendalikan penuh penggunaan program tersebut, serta praktis. Namun adapula alasan yang menyebabkan orang tidak menggunakan GAS adalah karena cukup sulit dalam penggunaan serta harganya yang mahal (Gondodiyoto, 2007:647).

2. *Parallel Simulation*

Dalam *parallel simulation*, auditor memroses data masukan klien dengan menggunakan program duplikat terkendali di bawah kendali auditor. Program yang digunakan dalam *parallel simulation* dapat berupa program dengan tujuan tertulis, perangkat lunak audit yang digeneralisasi, atau utilitas. *Parallel simulation* ini mempunyai keunggulan karena memungkinkan auditor untuk menguji masukan awal terhadap program terkendali, sehingga mengeliminasi kebutuhan untuk menyiapkan data pengujian (Guy, Alderman, dan Winters, 2002:318)

SA Seksi 327 *Teknik Audit Berbantuan Komputer* memberikan panduan bagi auditor dalam menghadapi sistem komputer *on-line* berikut ini:

1. Perlunya auditor memiliki keterampilan teknis dalam sistem komputer *on-line*.
2. Dampak sistem komputer *on-line* terhadap saat penerapan prosedur audit.
3. Tidak ada jejak transaksi yang dapat dilihat.
4. Prosedur yang dilaksanakan selama tahap perencanaan, mencakup:
 - a. Partisipasi individu yang memiliki keahlian teknis dalam sistem komputer *on-line* dan pengendalian berkaitan dalam tim audit.
 - b. Pertimbangan pendahuluan dalam proses penaksiran risiko tentang dampak sistem komputer *on-line* terhadap prosedur audit. Umumnya, di dalam sistem komputer *on-line* yang didesain dengan baik, auditor akan meletakkan kepercayaan lebih ke pengendalian intern sistem tersebut.
 - c. Prosedur audit yang dilaksanakan bersamaan dengan pengolahan *on-line*, mencakup pengujian kepatuhan pengendalian di dalam aplikasi *on-line*.

d. Prosedur audit yang dilaksanakan setelah pengolahan selesai dilakukan.

Menurut PSA No. 59, beberapa manfaat TABK adalah sebagai berikut:

- a. Tidak adanya dokumen masukan atau tidak adanya jejak audit (*audit trail*) dapat mengharuskan auditor menggunakan TABK dalam penerapan pengujian pengendalian dan pengujian substantif.
- b. Efektivitas dan efisiensi prosedur audit dapat meningkat dengan penggunaan TABK.

Contoh dari penerapan GAS ini adalah *Audit Command Language (ACL)*. ACL didesain sebagai metabahasa bagi auditor untuk mengakses hampir sebagian besar jenis data yang disimpan dalam peralatan elektronik dan untuk mengujinya secara komprehensif (Hall,2007:83).

Teknologi membawa dampak pada sistem audit, dimana akan menyebabkan terjadinya perubahan-perubahan pada proses audit. Dimana nantinya akan terjadi perubahan dalam pengumpulan bukti dan perubahan evaluasi bukti. Perubahan pengumpulan bukti dimana pengumpulan bukti yang dapat dipercaya pada sistem komputer lebih kompleks daripada pengumpulan bukti yang dapat dipercaya pada sistem manual. Auditor akan membandingkan perbedaan dan kompleksitas teknologi yang tidak ada pada sistem manual. Kesulitan bagi auditor untuk memahami teknologi pengendalian adalah karena *hardware* dan *software* yang kini telah berkembang dengan pesat. Kondisi ini membuat auditor mengalami kesulitan dalam pengumpulan bukti-bukti yang dapat dipercaya dari pengendalian.

Sedangkan perubahan evaluasi bukti dilihat dari sulitnya mengevaluasi kuat lemahnya sistem yang dapat dipercaya. Auditor harus terlebih dahulu memahami pengendalian secara terpercaya atau kegagalan dalam fungsi kemudian melakukan penelusuran konsekuensi dari kuat lemahnya sistem. Karena catatan konsekuensi kesalahan dalam komputer bisa menyebabkan serius dibanding secara manual (Halim, 2004:28).

4.3.5 Risiko audit berbasis komputer

Perusahaan harus melakukan penilaian risiko untuk mengidentifikasi, menganalisis, dan mengelola risiko yang berkaitan dengan pelaporan keuangan. Dalam SAS 78 mengharuskan para auditor mendapatkan pengetahuan yang cukup atas prosedur penilaian risiko perusahaan untuk memahami bagaimana cara pihak manajemen mengidentifikasi, membuat prioritas, serta mengelola berbagai risiko yang berkaitan dengan pelaporan keuangan (Hall, 2007:30).

Salah satu manfaat yang sekaligus merupakan ciri khusus komputer adalah komputer dapat mengolah data secara cepat, cermat, akurat, konsisten, dan dapat dilakukan secara terus menerus dalam waktu yang relatif tidak terbatas. Namun di sisi lain sistem berbasis komputer juga mengandung berbagai implikasi/konsekuensi/dampak yang mungkin perlu diperhatikan sungguh-sungguh. Berikut adalah beberapa resiko pada sistem komputer:

- a. Penggunaan teknologi secara tidak layak, maksudnya, ada kemungkinan desain suatu komputerisasi atau konfigurasi komputer sebetulnya kurang layak teknis namun terlampaui dipaksakan sehingga mungkin mempunyai akibat serius.
- b. Logika pengolahan yang salah, program yang salah (salah rumus, salah logika program) dapat menghasilkan keluaran pengolahan yang salah.
- c. Ketidakmampuan sistem analis/desainer dalam menterjemahkan kebutuhan calon pemakai (*user need* atau *user requirement*), sehingga sistem yang dibangun kemudian ternyata tidak sesuai dengan kebutuhan pemakai.
- d. Konsentrasi tanggungjawab pada petugas teknis komputer, terutama bila da masalah yang harus diatasi.
- e. Kerusakan sistem komunikasi dapat mengakibatkan lumpuhnya operasi perusahaan bila dari awal tidak disiapkan sistem cadangan (*back-up*).
- f. Ketidakmampuan mengendalikan teknologi, apabila teknologi yang kita adopsi sudah sedemikian canggih dan akhirnya kurang dikuasai.
- g. Praktek pengamanan sistem informasi yang tidak efektif, kurang memadai, atau bahkan mungkin tidak direncanakan dengan baik.
- h. Penyalahgunaan atau kesalahan pengoperasian atau penggunaan data.
- i. Komputer adalah mesin yang canggih, tetapi jika tidak dikelola dengan benar menjadi tidak bermakna. Oleh karena itu salah satu resiko yang dihadapi perusahaan adalah justru komputer dikelola tidak benar.
- j. Data masukan tidak dijamin validitasnya atau *diupdate* oleh yang bukan berwenang, atau *by accident* data berubah atau hilang sehingga informasi yang dihasilkan salah.

- k. Terjadinya pengingkaran akses, khususnya dalam sistem e-commerce, yaitu kegiatan perdagangan melalui interaksi secara elektronik. Hal ini sebetulnya juga berkaitan dengan mekanisme *paperless*, tanpa bukti kertas sehingga seseorang dapat tidak mengakui akses.
- l. Resiko yang umum adalah apabila karena sesuatu hal sistem komputer tidak dapat berfungsi sehingga dapat mengakibatkan operasional perusahaan menjadi terbengkalai. Sesuatu hal yang dimaksudkan di sini dapat berupa gangguan listrik, sistem jaringan, masalah yang terjadi karena tenaga teknis tertentu yang menentukan atau komputer itu sendiri.

Auditor juga harus mendapatkan informasi mengenai bagaimana sikap manajemen terhadap penilaian risiko karena penggunaan teknologi informasi. Risiko yang mungkin timbul karena penggunaan informasi yang dapat digali oleh auditor adalah jejak transaksi yang tersedia hanya dalam jangka waktu yang pendek, file dan catatan tidak dapat dibaca tanpa sebuah komputer, keterlibatan manusia yang menurun dalam pemrosesan komputer dapat mengaburkan kekeliruan yang mungkin dapat diamati dalam sistem manual, sistem informasi rentan terhadap bencana fisik, manipulasi yang tidak terotorisasi, dan kerusakan mekanis, perubahan dalam sistem lebih sulit untuk diimplementasikan dan dikendalikan (Irawan, 2009).

Namun teknologi yang berkembang ini juga memiliki suatu penyalahgunaan komputer dapat berupa:

1. Hacking yaitu kegiatan orang yang memasuki sistem komputer secara tidak sah atau tidak memiliki otorisasi dan merusak sistem ataupun data.
2. Virus yaitu program yang mampu masuk kedalam sistem tanpa diketahui dan digunakan untuk merusak sistem maupun data.
3. Akses fisik yang tidak sah yaitu seorang yang secara illegal melakukan akses secara fisik ke komputer.
4. Pelanggaran privasi yaitu melanggar privasi data perusahaan seperti membuka dokumen yang bukan haknya.
5. Gangguan operasi yaitu operasi harian dapat berhenti sesaat karena gangguan.

4.3.6 Audit *E-commerce*

Internet Commerce adalah pemakaian internet untuk melakukan pertukaran data elektronik antar partner dagang. *Electronic Commerce* memiliki konsep yang lebih luas. Pemakaian berbagai jenis jaringan, termasuk internet, untuk membantu perusahaan dalam melaksanakan tanggung jawabnya. Manfaat *e-commerce* bagi perusahaan antara lain, meningkatkan profitabilitas dan produktivitas, memperluas pangsa pasar, merampingkan operasi perusahaan, serta mengotomatisasi layanan ke konsumen.

Audit *e-commerce* merupakan *front-office system* yaitu sistem berbasis teknologi informasi yang langsung berkaitan dengan proses transaksi, atau layanan ke pihak lain atau pelanggan. Dalam *e-commerce* terjadi transaksi antara individu-individu yang tidak saling kenal, dimana mereka hanya berjumpa melalui dunia maya. Maka sangat perlu dilakukan pengawasan, serta perlindungan dan keamanan atas informasi pribadi yang dimasukkan ke dalam *website*.

Penggunaan sistem *e-commerce* juga membuat data perusahaan yang sensitif, program, dan perangkat keras terbuka terhadap kemungkinan adanya sabotase oleh pihak luar. Untuk membatasi hal ini maka perusahaan menggunakan *firewall*, teknik enkripsi, dan tanda tangan digital.

Firewall melindungi data, program, dan sumber daya yang lain pada pemakai eksternal yang tidak berhak mengakses sistem dalam suatu jaringan, seperti internet. *Firewall* adalah sistem perangkat keras dan perangkat lunak yang memantau serta mengendalikan aliran komunikasi *e-commerce* dengan menyalurkan semua koneksi jaringan dengan memverifikasi pemakai eksternal, memberikan akses pada pemakai yang berhak, menolak akses pemakai yang tidak berhak, dan mengarahkan pemakai yang sah ke program dan data yang diminta.

Teknik enkripsi (*encryption techniques*) melindungi keamanan komunikasi elektronik ketika informasi sedang dikirimkan. Enkripsi yang terkomputerisasi akan mengubah pesan standar ke dalam bentuk kode (*encrypted*), yang mengharuskan penerima pesan elektronik itu menggunakan program dekripsi untuk memecahkan

kode pesan itu. Teknik enkripsi publik digunakan untuk membuat kode pesan dan kata kunci lainnya (kunci pribadi) guna memecahkan kode pesan tersebut. Kunci public dibagikan pada pemakai yang berhak atas sistem *e-commerce* itu. Kunci pribadi dibagikan kepada pemakai internal yang memiliki otoritas untuk memecahkan kode pesan.

Untuk membuktikan keaslian validitas mitra dagang yang melaksanakan bisnis secara elektronik, perusahaan dapat menggunakan tanda tangan digital (*digital signature*). Tanda tangan tersebut berisi nama pemilik dan kunci publiknya. Pada tanda tangan itu juga berisi nama otorisasi sertifikasi dan tanggal kadaluwarsa sertifikat itu serta informasi khusus lainnya. Untuk menjamin keaslian maka setiap tanda tangan yang dilakukan secara digital ditanda tangani oleh kunci pribadi yang diselenggarakan oleh otorisasi sertifikasi.

5. Pembahasan

Teknologi yang telah berkembang pesat ini menjadi tolak ukur bagaimana perusahaan menanggapi kemajuan zaman. Dengan demikian perusahaan akan terus memperhatikan kemajuan di era masa kini dan tentunya auditor juga harus dapat mengikuti teknologi audit berbasis komputerisasi. Dalam pengembangannya, TI telah membantu manajemen dalam mengambil keputusan dengan segera, dimana keputusan yang diambil menentukan kelangsungan hidup perusahaan. Jika demikian, maka komputer juga merupakan sendi utama dalam kelangsungan proses perdagangan yang terjadi.

5.1 Peranan teknologi informasi terhadap audit komputerisasi dilihat dari prosedur, pengendalian internal, dan teknik komputerisasi

Perkembangan zaman dengan penggunaan teknologi sangat berpengaruh kuat terhadap perusahaan – perusahaan besar di sekitar kita. Teknologi ini mengubah prosedur audit yang dahulu digunakan secara manual digantikan dengan alat bantu

komputer. Sehingga perusahaan menggunakan sistem jaringan seperti LAN dengan menghubungkannya dengan komputer pusat.

Dengan teknologi ini, dapat pula menggunakan sistem *on-line*. Pemakai dapat menggunakannya untuk mengentri data transaksi seperti transaksi penjualan, dan pembelian dalam suatu perusahaan. Selain itu dapat pula digunakan untuk meminta laporan seperti data persediaan di gudang, sehingga dapat diketahui kuantitasnya. Juga dapat melakukan up-date pada *master file*, seperti membuat *account* baru bagi *customer*, dan perubahan kode *account* ke buku besar.

Perbedaan nampak jelas bahwa prosedur audit dengan peranan teknologi yang menggunakan komputer dapat digunakan untuk memudahkan setiap aktivitas perusahaan. Tidak ada lagi pencatatan secara manual untuk mencatat setiap transaksi, semua dilakukan dengan mengentri data-data. Tidak hanya itu, untuk membuat laporan keuangan yang dilaporkan juga akan menjadi mudah dengan penggunaan teknologi ini.

Sebagai contoh adalah studi kasus pada PT. Percetakan dan Penerbitan Cahaya, oleh Siti Rohajawati (2004). Perusahaan ini sudah menggunakan komputer dengan topologi jaringan pada *Local Area Network* (LAN) di bagian percetakan, terdapat lima komputer yang terhubung dengan LAN, pada staff keuangan, administrasi, pemasaran, serta dua komputer untuk desain dan tata letak. Kelima komputer tersebut dapat saling akses dan berbagi data. Namun bagi informasi yang bersifat kritikal seperti data keuangan, hanya dapat diakses dengan *ID user* dan password khusus. Pada perusahaan ini juga setiap *client* diberi hak melakukan backup data di komputer masing-masing. Administrator dituntut untuk mampu mengelola keamanan sistem dengan pengklasifikasian file-file, kebijakan, prosedur, dan standar perusahaan.

Suatu sistem pengendalian internal merupakan suatu mekanisme yang didesain untuk menjaga, mendeteksi, dan memberikan mekanisme pembetulan terhadap potensi kemungkinan terjadinya kesalahan dan penyalahgunaan. Tujuan didesainnya sistem pengendalian internal berbasis komputer adalah untuk membantu manajemen

dalam mencapai pengendalian internal menyeluruh, termasuk di dalamnya kegiatan manual, mekanis, maupun yang terkait dengan pemrosesan data dengan komputer.

Adanya penggunaan TI memungkinkan terciptanya suatu sistem pengendalian internal dimana dapat menjaga keamanan asset perusahaan, dan untuk meningkatkan integritas data. Pengendalian dengan sistem keamanan dengan menggunakan komputer. Misalnya penggunaan *password* ataupun *cryptography* yang digunakan untuk penyandian informasi, sehingga asset perusahaan dapat terus dijaga keamanannya. Serta dapat meningkatkan efektivitas dan efisiensi dari pengendalian internal secara konsisten dengan memproses sejumlah besar volume transaksi dan data dan meningkatkan ketepatan waktu dan akurasi dari informasi.

Pengendalian internal ada dua, yaitu pengendalian umum dan pengendalian aplikasi. Bagi seorang auditor dalam mengaudit sistem informasi, yang paling utama diperhatikan adalah pengendalian umum. Karena kualitas pengendalian internal dipengaruhi oleh pengendalian umumnya. Jika pengendalian umum perusahaan itu baik, maka dengan sendirinya akan memberikan dampak yang positif dalam pengendalian aplikasi suatu sistem.

Contohnya adalah studi kasus yang dilakukan oleh Siti Rohajawati (2004) pada PT. Percetakan dan Penerbitan Cahaya. Pengendalian internal pada perusahaan ini berupa adanya mekanisme dan metode yang digunakan manajer untuk mengontrol apa yang boleh diakses *user* atau staffnya. Akses kontrol dapat berupa identifikasi, otorisasi, teknik akses kontrol, dan ancaman terhadap akses kontrol, serta hanya memberikan izin bagi pengguna tertentu yang diberi otorisasi, program atau proses sistem atau akses sumber daya. Perusahaan ini juga melakukan monitoring, dengan mengawasi, membatasi, memantau, dan menjaga keutuhan dan kerahasiaan sumber daya (informasi). Setiap user diberikan hak akses yang berbeda, dimana hak tersebut diberikan sesuai dengan hak dan peranannya sehingga mereka memiliki tanggung jawabnya masing-masing.

Di sisi yang lain, auditor juga harus mempertimbangkan teknik yang menggunakan komputer sebagai alat audit. Biasanya disebut dengan TABK atau

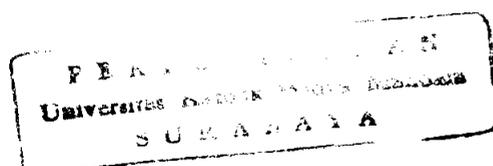
CAATs. Dengan adanya teknik, maka dapat dipilih cara yang paling tepat dalam melakukan audit suatu perusahaan. Salah satu teknik adalah GAS yaitu *software* untuk bantuan audit, dimana untuk digunakan sebagai pengumpulan bahan bukti untuk entitas bisnis tertentu atau kegiatan tertentu. Keunggulan dari GAS adalah mudah digunakan, menghemat waktu, mengakses berbagai *record*, andal dalam beberapa aspek audit, memungkinkan bagi auditor untuk mengendalikan penuh penggunaan program tersebut, serta praktis. Teknik yang berikutnya adalah *parallel simulation*, auditor memroses data masukan klien dengan menggunakan program duplikat terkendali di bawah kendali auditor.

Pemahaman mengenai pentingnya keahlian audit dengan pengetahuan sistem informasi berbasis komputer akan menghasilkan peningkatan yang sangat signifikan dalam proses audit sistem informasi. Persiapan auditor sistem informasi untuk memiliki keahlian tersebut harus dipersiapkan terlebih dahulu untuk dapat melakukan tugas sebuah audit sistem informasi. Dengan demikian maka auditor diharuskan untuk mampu menguasai *software* komputer, contohnya ACL.

Contoh perusahaan yang menggunakan ACL adalah Dominion, berkantor pusat di Richmond, Virginia. Dominion adalah salah satu penyedia layanan terkemuka US listrik, alam gas, dan layanan terkait. Dengan pendapatan tahunan lebih dari US \$ 10 miliar dan asset sebesar US \$ 35 miliar. Dengan ACL dan langsung Link, Dominion mampu untuk mengambil setiap vendor transaksi diproses antara 1998 dan 2002 dan cocok untuk menduplikasi pembayaran. ACL software Dominion memberikan kontrol lebih besar atas para vendor dan telah digunakan untuk menemukan duplikat pembayaran biaya dalam 4 tahun senilai catatan vendor dan lebih dari sejuta individu transaksi, mandiri ekstrak dan membersihkan data sensitive perusahaan, meningkatkan kontrol audit dan dibayar melalui rekening vendor master file.

5.2 Risiko yang dihadapi dalam audit sistem informasi

Dalam setiap hal selalu ada risiko yang dihadapi. Sebelum melangkah, lebih baik dipikir dengan lebih hati-hati. Karena apa yang telah ditentukan saat ini akan



menjadi pengaruh bagi akan datang. Setiap hendak memutuskan sesuatu sebaiknya kita mempertimbangkan kemungkinan terburuk yang mungkin akan dihadapi dan risiko yang kemungkinan terjadi.

Dalam audit yang telah terkomputerisasi juga demikian, secanggih-canggihnya kemajuan teknologi, tetap saja akan selalu ada cara untuk menyalahgunakannya sehingga tetap saja ada risiko. Tidak ada cara yang sempurna tanpa risiko. Maka dari itu, beberapa risiko yang mungkin akan dihadapi yakni kerusakan sistem komunikasi dapat mengakibatkan lumpuhnya operasi perusahaan bila dari awal tidak disiapkan sistem cadangan (*back-up*), praktek pengamanan sistem informasi yang tidak efektif, kurang memadai, atau bahkan mungkin tidak direncanakan dengan baik. Serta penyalahgunaan atau kesalahan pengoperasian atau penggunaan data.

Auditor harus menyadari risiko-risiko dimana merupakan ancaman dalam perusahaan, antara lain :

1. Penyalahgunaan teknologi adalah penggunaan teknologi baru sebelum adanya kepastian yang jelas mengenai kebutuhannya. Banyak organisasi memperkenalkan teknologi database tanpa menetapkan dengan jelas kebutuhan akan teknologi tersebut. Pengalaman menunjukkan bahwa para pemakai awal (*new user*) suatu teknologi baru seringkali mengkonsumsi jumlah sumberdaya yang cukup besar selama mempelajari cara penggunaan teknologi baru tersebut. Penggunaan teknologi yang tidak layak antara lain: Analisis sistem atau pemrogram tidak mempunyai keahlian yang cukup untuk menggunakan teknologi tersebut, pemakai yang awam terhadap teknologi hardware yang baru, pemakai yang awam terhadap teknologi software yang baru, perencanaan yang minim untuk instalasi teknologi hardware dan software yang baru.

2. Kesalahan berantai merupakan 'efek domino' dari kesalahan-kesalahan di segenap sistem aplikasi. Kesalahan suatu bagian program atau aplikasi akan berakibat pada kesalahan kedua yang meskipun tidak berkaitan di bagian lain aplikasi. Kesalahan kedua ini dapat berakibat kesalahan ketiga dan seterusnya. Risiko kesalahan berantai sering dikaitkan dengan pelaksanaan perubahan sistem aplikasi.

Perubahan dilaksanakan dan diuji dalam program di mana perubahan terjadi. Namun demikian, beberapa kondisi dapat berubah karena adanya perubahan yang menimbulkan kesalahan di bagian lain sistem aplikasi tersebut. Rantai kesalahan dapat terjadi di antara aplikasi-aplikasi. Risiko ini akan semakin besar sejalan dengan semakin terpadunya aplikasi.

3. Risiko yang timbul meliputi kegagalan untuk mengimplementasikan kebutuhan karena para pemakai tidak memiliki kemampuan teknis. Dampaknya adalah kebutuhan yang diimplementasikan adalah kebutuhan yang tidak layak karena personil teknis tidak memahami kebutuhan sebenarnya dari pemakai. Akibat lainnya adalah munculnya sistem manual yang semakin besar untuk menutup kelemahan-kelemahan dalam aplikasi komputer. Kondisi ketidakmampuan menerjemahkan kebutuhan pemakai ini disebabkan antara lain: para pemakai tidak memiliki keahlian teknis EDP, orang-orang teknis tidak memiliki pemahaman yang cukup mengenai permintaan pemakai, ketidakmampuan untuk merumuskan permintaan dengan cukup terinci, sistem yang digunakan oleh banyak 'user' tanpa ada 'user' yang bertanggung jawab atas sistem tersebut.

4. Ketidakmampuan dalam mengendalikan teknologi. Pengendalian memang sangat diperlukan dalam penggunaan lingkungan berteknologi. Pengendalian-pengendalian akan menjamin bahwa versi yang tepat berada digunakan pada saat yang tepat; bahwa file-file yang tepat digunakan; bahwa para operator komputer melaksanakan instruksi yang tepat; prosedur yang memadai dikembangkan untuk mencegah, mendeteksi dan memperbaiki permasalahan yang terjadi; dan bahwa data yang tepat disimpan dan kemudian diperoleh dengan mudah jika diperlukan.

Dengan adanya risiko yang demikian maka yang paling diperhatikan adalah manusia itu sendiri. Karena timbulnya risiko dan cara menghadapi risiko ini hanya manusia yang dapat mengatasinya. Teknologi diciptakan oleh manusia, sehingga

manusia juga melakukan tindakan penyalahgunaan seperti munculnya *hacker*, orang yang memasuki sistem komputer secara tidak sah atau tidak memiliki otorisasi dan merusak sistem ataupun data. Serta banyaknya tercipta virus yang dapat merusak data penting pada perusahaan.

Untuk mengantisipasi, digunakan tiga cara yaitu *firewall* untuk melindungi data, program, dan sumber daya yang lain pada pemakai eksternal yang tidak berhak mengakses sistem dalam suatu jaringan. Teknik enkripsi (*encryption techniques*) melindungi keamanan komunikasi elektronik ketika informasi sedang dikirimkan. Teknik ini mengubah pesan standar ke dalam bentuk kode (*encrypted*), yang mengharuskan penerima pesan elektronik itu menggunakan program dekripsi untuk memecahkan kode pesan itu. Dan yang paling akhir adalah penggunaan tanda tangan digital. Untuk menjamin keaslian maka setiap tanda tangan yang dilakukan secara digital ditanda tangani oleh kunci pribadi yang diselenggarakan oleh otorisasi sertifikasi.

Studi kasus pada PT. Percetakan dan Penerbitan Jaya dilakukan juga analisis risiko terhadap pengelolaan keamanan, terdapat mesin-mesin yang merupakan asset bagi perusahaan dan ancaman yang mungkin terjadi adalah kerusakan pada mesin-mesin tersebut sehingga proses percetakan menjadi terganggu. Hal ini dapat diantisipasi dengan servis mesin secara berkala serta pengoperasian mesin secara optimal.

Pada bagian ancaman yang sering muncul adalah gangguan virus karena komputer saling terhubung melalui jaringan. Dengan topologi star jika terjadi gangguan akibat virus, untuk sementara komputer yang terinfeksi diisolasi dalam jaringan sampai komputer dapat kembali berkomunikasi. Ancaman lain adalah berupa kebakaran karena bahan baku produksi umumnya dari kertas. Antisipasi selalu dilakukan dengan penyediaan pemadam kebakaran hampir di setiap ruangan dan kepatuhan dari pegawai untuk tidak merokok saat bekerja dan di ruangan terutama pada bagian gudang penyimpanan barang. Namun ancaman tersebut jarang sekali muncul karena kesadaran pegawai sudah cukup tinggi.

Hasil analisis terhadap kerawanan yang mungkin timbul adalah akibat dari kebijakan fiskal pemerintah yang dapat mengakibatkan keuangan dan produksi perusahaan terganggu. Hal tersebut dikarenakan umumnya produksi menggunakan bahan baku kertas yang diimpor dari luar negeri dengan harga pembelian dollar. Komitmen direktur dengan seluruh staf pegawai dalam menanggulangi kejadian tersebut adalah dengan bersama – sama menanggung semua kemungkinan terburuk (penurunan gaji sampai penundaan gaji). Oleh karena itu tercipta keharmonisan, rasa kekeluargaan dan saling percaya antara staf direksi dan pegawai. Namun kerawanan tersebut diidentifikasi sesekali muncul hanya jika situasi politik dan keamanan pemerintah kurang stabil.

Kerawanan lainnya yang kerap muncul adalah kesalahan proses bisnis, misalnya pencetakan telah melewati proses produksi namun hasilnya dianggap kurang memuaskan bagi pelanggan. Bagi kasus tersebut pihak manajer produksi akan diberi peringatan oleh direksi. Bila kesalahan tersebut sampai berulang tiga kali, sanksi yang harus diterima manajer produksi adalah diturunkan posisinya. Oleh karena itu manajer produksi dituntut memiliki rasa tanggung jawab, talenta dan kontrol yang baik pada staf produksi agar tidak merugikan perusahaan.

Kerawanan akibat pencurian umumnya tidak pernah terjadi karena satuan pengaman selalu ditempatkan selama 24 jam penuh dengan shif kerja pagi dan malam. Para pegawai diberikan rasa memiliki yang tinggi sehingga kekhawatiran terjadinya pencurian dari pihak dalam pun berkurang. Biasanya pegawai diberikan peringatan secara kekeluargaan untuk tidak melakukan kesalahan lagi. Para pegawai ditanamkan rasa saling memiliki dengan azas kekeluargaan dan keagamaan yang kental.

5.3 Masalah audit komputerisasi terhadap sistem *e-commerce*

Sistem *e-commerce* memang memudahkan dalam transaksi dunia perdagangan. Mereka tidak perlu harus saling tatap muka untuk melakukan transaksi. Walau terbukti sistem ini sangat efisien dan membantu, ternyata tidak mudah untuk

mengauditnya. Penggunaan sistem *e-commerce* ternyata juga membuat data perusahaan yang sensitif, program, dan perangkat keras terbuka terhadap kemungkinan adanya sabotase oleh pihak luar.

Masalah dalam *e-commerce* ini dapat berupa hilangnya jejak audit (*audit trail*) sehingga auditor mengalami kesulitan dalam melakukan audit. Untuk mengurangi kesulitan tersebut, maka auditor lebih baik memantau setiap aktivitas yang dilakukan oleh perusahaan, sehingga setiap transaksi dapat segera dideteksi. *E-commerce* telah beredar dan digunakan hampir seluruh perusahaan. Perdagangan kini sudah benar-benar bebas tanpa penghalang jarak dan waktu. Setiap transaksi dilakukan setiap saat dan untuk meminimalisasi masalah yang timbul, diperlukan suatu sistem yang tepat dalam suatu perusahaan. Proteksi sistem keamanan yang benar-benar dapat diandalkan menjadi sangat berpengaruh sekali, auditor juga akan lebih mudah dalam mengawasi setiap gerakan dari perusahaan. Auditor akan memeriksa kecocokan dengan laporan keuangan sehingga dapat memberi keputusan audit yang tepat dengan apa yang sebenarnya dialami perusahaan.

E-commerce tidak lepas dari internet dimana itu berarti akan menjadi rawan bagi perusahaan. Internet rawan akan bahaya virus, seperti trojan maupun worm. Sebaiknya untuk mengatasi hal ini setiap server perusahaan dilengkapi dengan anti virus yang selalu diupdate secara berkala, misalnya seminggu sekali. Dengan demikian maka dapat diantisipasi terjadinya kerusakan sistem dalam dunia *e-commerce*.

Selain itu untuk melengkapi keamanan dalam sistem perusahaan maka perusahaan juga harus memberikan suatu kode atau password dalam pengaksesan *e-commerce*, sehingga tidak sembarang orang dan tidak disalah gunakan oleh pihak – pihak luar yang tidak berkepentingan.

6. Kesimpulan

Pada dasarnya teknologi ini mempunyai peranan yang sangat penting dalam kehidupan sehari-hari kita. Terutama dalam kegiatan suatu perusahaan. Dimana pada akhirnya perusahaan juga akan melakukan proses audit dengan memanfaatkan kemajuan teknologi yang ada saat ini. Pengaruh teknologi informasi terhadap audit komputerisasi ini sebenarnya membantu memudahkan perusahaan supaya jauh lebih efisien dan efektif, dibandingkan dengan cara manual. Jadi sistem komputer ini telah menggeser cara manual yang sebelumnya digunakan.

Perubahan ini mempengaruhi prosedur audit dimana kini telah digunakan suatu jaringan komputer, *network* yang dapat digunakan untuk membantu melakukan aktivitas, mempermudah perusahaan karena antara satu dan yang lain saling terhubung. Selain itu dapat memudahkan setiap aktivitas perusahaan. Tidak ada lagi pencatatan secara manual untuk mencatat setiap transaksi, semua dilakukan dengan mengentri data-data. Tidak hanya itu, untuk membuat laporan keuangan yang dilaporkan juga akan menjadi mudah dengan penggunaan teknologi ini.

Di dalam pengendalian internal juga akan mengalami suatu perkembangan dengan adanya teknologi informasi yang telah berkembang. Perusahaan harus menjaga keamanan assetnya dengan melakukan pengendalian keamanan dengan dilakukan keamanan menggunakan password untuk dapat mengakses data yang diinginkan sehingga keamanan asset dapat tetap terjaga.. Serta dapat meningkatkan efektivitas dan efisiensi dari pengendalian internal secara konsisten dengan memproses sejumlah besar volume transaksi dan data dan meningkatkan ketepatan waktu dan akurasi dari informasi.

Teknologi informasi ini akan mempengaruhi teknik komputer dimana telah ada software yang digunakan perusahaan sehingga dapat menghemat waktu dalam pelaksanaan audit. Perusahaan menjadi terarah dan lebih efisien dengan menggunakan teknik komputerisasi. Hal ini akan membantu meringankan pekerjaan yang biasanya dilakukan dengan manual.

Dalam dunia teknologi yang telah berkembang ini memang dapat membantu perusahaan karena lebih cepat prosesnya dan jauh lebih efisien, tapi perlu juga diperhatikan risiko yang dihadapi nanti. Karena setiap hal pasti ada kurang dan lebihnya, demikian juga dengan sistem komputerisasi ini. Perusahaan juga mempunyai risiko – risiko yang harus diperhatikan. Untuk itu perusahaan harus dapat melakukan perkiraan apa saja yang menjadi risiko dalam perusahaannya dan bagaimana cara yang tepat untuk mengatasi permasalahan tersebut, sehingga dapat memperkecil tingkat kemungkinan terjadinya risiko.

Perdagangan di era teknologi ini menggunakan *e-commerce*, yakni perusahaan tersebut akan melakukan transaksi bisnis dengan cara *online*. Cara ini kini banyak digunakan oleh perusahaan dengan internet, sehingga jarak dan waktu bukan menjadi masalah. Apa saja dapat dilakukan dengan internet. *E-commerce* tidak lepas dari internet dimana itu berarti akan menjadi rawan bagi perusahaan. Internet rawan akan bahaya virus, seperti trojan maupun worm. Sebaiknya untuk mengatasi hal ini setiap server perusahaan dilengkapi dengan anti virus yang selalu diupdate secara berkala, misalnya seminggu sekali. Dengan demikian maka dapat diantisipasi terjadinya kerusakan sistem dalam dunia *e-commerce*.

DAFTAR PUSTAKA

- A.Hall, James dan T.Singleton, 2007, *Information Technology Auditing and Assurance*, Edisi Pertama, Jakarta: Salemba Empat.
- _____ , 2007, *Information Technology Auditing and Assurance*, Edisi Kedua, Jakarta: Salemba Empat.
- Arens, A.A., R.J.Elder, dan M.S.Beasley, 2008, *Auditing dan Jasa Assurance*, Jilid 1, Edisi Kedua Belas, Jakarta: Erlangga.
- Gondodiyoto, S., 2007, *Audit Sistem Informasi + Pendekatan CobIT*, Jakarta: Mitra Wacana Media.
- Guy, D.M., C.W.Alderman, dan A.J.Winters, 2002, *Auditing*, Jilid 1, Edisi Kelima, Jakarta : Erlangga.
- Halim, A., 2004, *Auditing dan Sistem Informasi*, Edisi Pertama, Yogyakarta: UPP AMP YKPN.
- Ikatan Akuntan Indonesia, 2001, *Standar Profesional Akuntan Publik*, Jakarta: Salemba Empat.
- Irawan, R., 2009, Pengaruh Teknologi Informasi Pada Proses Audit: Tinjauan Efektifitas Dan Efisiensi Pemeriksaan Di Masa Akan Datang, *Jurnal Akuntansi/Tahun XIII*, No. 01, Januari: 61-74.
- Karya, G., 2004, Pengembangan Model Audit Sistem Informasi Berbasis Kendali, *Integral*, Vol. 9 No. 1, Maret: 51-57.

Rohajawati, S., 2004, Proteksi dan Teknik Keamanan Sistem Informasi (Studi Kasus di PT. Percetakan dan Penerbitan Jaya), Jakarta: Program Magister Teknologi Informasi Universitas Indonesia Jakarta.

Supriyati, 2006, Peranan Teknologi Informasi Dalam Audit Sistem Informasi Komputerisasi Akuntansi, *Majalah Ilmiah Unikom*, Vol.6, hlm. 35-50.

Wirapranata, P., 2009, www.scribd.com/doc/13263189/Audit-Sistem-Informasi

www.acl.com/pdfs/success_story_utilitiestrans_dominion.pdf