Karya Ilmiah

SISTEM INFORMASI AKUNTANSI DENGAN MENGGUNAKAN ELECTRONIC COMMERCE SYSTEMS

UNIVERSITAS MEDAN AREA PERPUSTAKAAN PUSAT

Oleh :

Drs. Halomoan Situmorang, Ak.

UNIVERSITAS MEDAN AREA FAKULTAS EKONOMI

UNIVERSITAS MEDAN AREA
MEDAN
2009

Karya Ilmiah

SISTEM INFORMASI AKUNTANSI DENGAN MENGGUNAKAN ELECTRONIC COMMERCE SYSTEMS

UNIVERSITAS MEDAN AREA PERPUSTAKAAN PUSAT

Oleh :

Drs. Halomoan Situmorang, Ak.

UNIVERSITAS MEDAN AREA PERPUSTAKAAN PUSAT

UNIVERSITAS MEDAN AREA
MEDAN
2009

338

KATA PENGANTAR

Dengan Rahmat Tuhan Yang Maha Esa yang senantiasa melimpahkan karuniaNya sehingga penulis dapat menyelesaikan Karya Ilmiah ini dengan baik sesuai dengan bidang yang digeluti penulis adapun judul Karya Ilmiah ini adalah **"Sistem Informasi Akuntansi Dengan Menggunakan Electronik Commerce System".**

Tujuan dari penulisan Karya Ilmiah ini adalah merupakan salah satu persyaratan penilaian kepangkatan dosen. Penulis menyadari bahwa penyajian dan isi dari Karya Ilmiah ini masih membutuhkan penambahan dan perbaikan isi seiring dengan perkembangan zaman.

Untuk itu penulis berharap adanya saran dan kritik yang membangun sehingga Karya Ilmiah ini dapat lebih sempurna dan memberikan manfaat bagi pembaca yang membutuhkannya.

Medan, **Juni 2009**
Penulis,

Drs. Halomoan Situmorang, Ak.

DAFTAR ISI

			Halaman
KATA PENGANTAR			i
DAFTAR ISI			ii
BAB	I	PENDAHULUAN	1
	1.1.	Latar Belakang	1
	1.2.	Tujuan Penulisan	5
BAB	II	URAIAN TEORITIS	6
	2.1.	Isu Baru diseputar Pengendalian Internal	6
	2.2.	Keamanan Harta Perusahaan	21
	2.3.	Implikasi e-Commerce terhadap Internal Kontrol	24
	2.4.	Peluang yang Dimiliki oleh Akuntan	30
BAB	III	PEMBAHASAN	32
BAB	IV	PENUTUP	40
DAFTAR PUSTAKA			44

BAB I

PENDAHULUAN

1.1. Latar Belakang

Internet adalah salah satu infrastruktur dalam bisnis sebagai salah satu pemampu munculnya e-commerce yang tidak dimiliki oleh siapapun dan juga sekaligus dimiliki oleh siapapun. Ditinjau dari aspek biaya dan legalitas, potensi pemanfaatan prasarana internet untuk bisnis sangat luas terbuka. Disamping itu luasnya daya jangkau penyebaran informasi oleh internet menyebabkan pemanfaatan infrastruktur ini dapat dikategorikan sebagai infrastruktur yang cost effective. Pemberdayaan internet untuk mendukung bisnis komersial semakin marak dengan ditemukannya world wide web yang memampukan pemakai untuk berpindah dari satu situs ke situs lain secara mudah dan cepat meskipun masing masing dibangun atas platform yang berbeda.

Perusahaan dapat memanfaatkan kemampuan ini untuk berinteraksi dengan potential customer dan trading partner nya diseluruh dunia tanpa khawatir terjadi masalah incompatibility

sistem pada kedua belah pihak. Ternyata hal ini membawa dampak yang cukup signifikan dalam pengelolaan bisnis. Bahkan memaksa beberapa bisnis tradisional harus memikirkan ulang (fundamental rethinking) cara bisnis mereka.

Sebagai contoh, munculnya perusahaan amazon.com yang sukses memanfaatkan webbased strategy, yang menyediakan situs di internet yang menawarkan berbagai macam barang dan sekaligus menyediakan sistem akuntansi ordering cycle, shipping system, inventory cycle and payment cycle dalam website nya yang dapat diakses di seluruh dunia.

Cara bisnis ini tentunya sangat berbeda jika dibandingkan dengan bisnis tradisional dimana sistem informasi akuntansi merupakan sistem internal perusahaan yang tertutup dan tidak memberi kesempatan customer untuk melakukan akses pada sebagian sistem akuntansi tersebut. Oleh karena itu sistem informasi yang dihasilkan perusahaan haruslah merupakan sistem informasi yang andal.

Sistem informasi akuntansi yang andal mensyaratkan bahwa database dan sistem pemrosesan data internal perusahaan beserta dengan sistem jaringannya dapat menghasilkan dan

mendistribusikan informasi yang akurat, relevan, lengkap, tepat waktu dan aman.

Accessibilitas sebagian sistem informasi akuntansi oleh pihak luar, baik customer maupun rekanan bisnis ini tentunya memberikan dampak yang cukup besar bagi seorang akuntan dalam melakukan pekerjaannya. Sistem akuntansi seolah-olah kehilangan sebagian unsur pengendaliannya karena siapapun dapat berpura-pura untuk menjadi customer potensial yang dapat melakukan modifikasi data order yang mungkin dalam kenyataan sebenarnya bertujuan membobol sistem atau merugikan perusahaan.

Selain mengubah cara bisnis, teknologi juga telah mengubah cara perusahaan mempublikasikan laporan keuangan mereka. Sampai saat ini sebagian besar perusahaan yang telah memanfaatkan internet akan menggunakan format HTML untuk mempublikasikan laporan keuangannya di internet. Format HTML ini harus didownload dan ditransfer dalam spreadsheet dan program aplikasi lainnya terlebih dahulu seandainya akan dilakukan manipulasi atau pengolahan data selanjutnya.

Format pelaporan dengan menggunakan HTML akhir-akhir ini telah mengalami perkembangan yang cukup pesat dengan dikembangkannya XBRL atau eXtensible Business Reporting Language.

Menurut hasil survei yang dilakukan oleh Boston Consulting Group, pengeluaran orang Indonesia untuk belanja di Internet masih tergolong rendah yaitu 0.01 cent perkapita pada tahun 1999. Walaupun demikian jumlah transaksi elektronik pada tahun yang sama mencapai US$ 2 juta. Diperkirakan pada tahun 2000 diperkirakan akan tumbuh 200% seiring dengan perbaikan infrastruktur telekomunikasi (Pinnarwan 2001). Internet dan www yang merupakan pemampu keberadaan e-commerce mulai dikembangkan dari bidang teknologi informasi, sehingga banyak pemahaman dan istilah atau kosa kata baru yang harus dimiliki akuntan pada saat akuntan menjalankan penugasannya, khususnya dalam mengantisipasi dampak terbaginya distribusi pengolahan data pada berbagai pihak diluar perusahaan, termasuk pihak yang kemungkinan dapat merugikan perusahaan serta dalam mengantisipasi pelaporan keuangan dalam lingkungan e-commerce.

1.2. Tujuan Penulisan

Untuk mengetahui sistem informasi akuntansi dengan menggunakan Electronic Commerce Systems.

BAB II

URAIAN TEORITIS

2.1. Isu Baru diseputar Pengendalian Internal

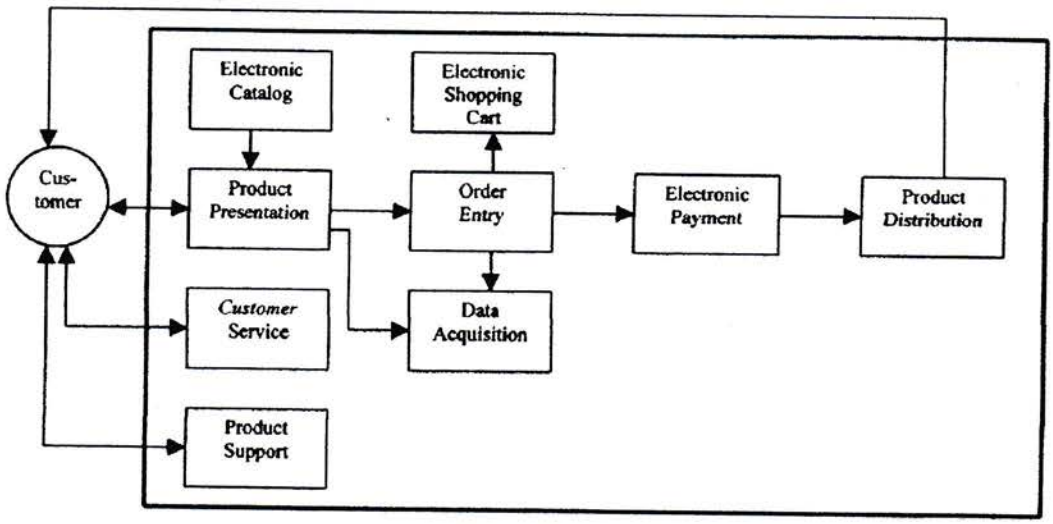
Telah dipaparkan diatas bahwa internet dan e-commerce menyebabkan sebagian sistem akuntansi perusahaan dapat diakses oleh pihak diluar perusahaan. Nickerson (2001) mengemukakan hal ini dengan cara menjelaskan fungsi e-commerce.

Dari gambar tersebut dapat diketahui bahwa fungsi e-commerce, customer berhadapan langsung atau dapat mengakses langsung electronic catalog, product presentation, customer service, product support, shopping cart, order entry, electronicpayment dan product distribution. Semua modul tersebut biasanya sudah terdapat dalam website perusahaan yang telah menjalankan e-commerce. Sisi positif yang ditimbulkan antara lain adalah bahwa sebagian tanggung jawab fungsi pemrosesan data digeserkan kepada konsumen. Pada kasus amazon.com, customer lah yang bertanggungjawab untuk melakukan siklus order entry system dengan cara memasukkan

sendiri data yang terkait dengan pemesanan di internet.

Seandainya terjadi kesalahan, maka kemungkinan besar adalah tanggungjawab customer yang memasukkan sendiri data pesanannya. Oleh karena itu, keterlibatan dan tanggungjawab karyawan amazon.com dalam siklus ini jadi sangat minimal.

Gambar 1.
Functions of Electronic Commerce Systems



(Sumber: Nickerson 2001)

Namun disisi lain, hal tersebut berarti menimbulkan masalah pengendalian internal baru yang muncul dalam lingkungan e-commerce ini. Beberapa masalah pengendalian internal tersebut diantaranya adalah: (Romney dan Steinbart 2000: 237)

1. Validitas transaksi: istilah teknis dalam perdagangan elektronik adalah authentication dan data integrity atas transaksi
2. Otorisasi transaksi: istilah teknis dalam perdagangan elektronik adalah tidak adanya repudiation atau penyangkalan atas informasi yang telah terkirim dari pihak-pihak yang bertransaksi
3. Keamanan harta perusahaan

Pada saat melakukan audit laporan keuangan, akuntan publik berkepentingan untuk mendapatkan pembuktian yang cukup atas asersi existence/occurrence, yaitu bahwa semua harta dan modal pada neraca benar-benar ada dan bahwa semua transaksi yang tercermin dalam laporan rugi laba sesungguhnya telah terjadi dalam perusahaan (Konrath 1999: 3). Pembuktian yang cukup berasal dari data-data akuntansi dan semua informasi pendukungnya yang harus juga merupakan pembuktian yang kompeten, artinya relevan dan valid. Relevan berarti sesuai dengan tujuan audit, sedangkan valid berarti pembuktian yang dapat dipercaya dan meyakinkan. Dalam kaitannya dengan hal ini, maka internal kontrol yang baik

menghendaki agar sistem akuntansi perusahaan hanya mencatat transaksi yang valid saja, yaitu transaksi yang benar-benar terjadi. Sehingga hanya transaksi yang benarbenar terjadi saja yang nampak dalam laporan keuangan.

Pada sistem perdagangan tradisional, perusahaan dengan yakin dapat mengenali customernya. Keyakinan mengenai keaslian dan keabsahan atau validitas customer dapat dilihat dari adanya surat-menyurat secara resmi, tanda tangan, tatap muka dan sebagainya. Pada sistem perdagangan elektronik, dengan mudah orang dapat menyamar dan berlaku seolah-olah dia adalah pihak customer yang sebenarnya, karena pada sistem ini tidak terjadi surat-menyurat secara resmi dan tidak ada juga tatap muka. Semua dilakukan secara elektronik. Customer yang sesungguhnya tidak dapat dikenal dengan lebih baik, karena customer hanya memasukkan identitasnya saja sebagai pengenal seperti nama, alamat, nomor kartu kredit, sementara identitas ini dapat dengan mudah dipalsukan atau dicuri. Pemalsuan atau pencurian identitas ini menyebabkan pengenalan perusahan akan customer yang sesungguhnya (legitimate customer) akan salah. Kesalahan dalam menentukan keaslian customer ini

mengakibatkan tidak validnya transaksi yang terjadi karena customer yang tidak legitimate. Jadi dalam lingkungan perdagangan elektronis, validitas transaksi berarti bahwa transaksi yang benar-benar terjadi harus terjadi diantara pihak-pihak yang sebenarnya dan sesungguhnya melakukan aktifitas transaksi.

Disamping isu mengenai legitimate customer, isu legitimate company yang terjun dalam bisnis perdagangan elektronik (memiliki website) juga menjadi masalah yang perlu diperhatikan. Jika customer membeli barang lewat website, tentunya customer harus merasa yakin dengan pihak mana dia bertransaksi. Harus ada keyakinan customer bahwa website tersebut memang merupakan website milik perusahaan yang dimaksud. Sehingga setelah data untuk kepentingan pembayaran dimasukkan, customer merasa yakin dan aman melakukan transaksi tersebut.

Website palsu kadang dibangun untuk mengumpulkan dan mencuri data yang penting seperti user ID, password ataupun informasi kartu kredit customer. Jadi perdagangan yang terjadi diantara customer dan supplier yang salah satu atau keduanya

tidak legitimate dapat dikatakan bahwa transaksi tersebut tidak valid dan tidak dapat dicatat dalam sistem akuntansi masing-masing perusahaan. Secara teknis isu ini disebut sebagai isu authentication. Istilah ini berarti proses untuk menentukan bahwa partner bisnis adalah pihak yang sesungguhnya melakukan bisnis dan mengajukan klaim atas transaksi tertentu.

Secara teknis juga sangat dimungkinkan bahwa website palsu ditujukan untuk mengambil data yang ada di hard disk perusahaan yang bertindak sebagai customer, terutama customer yang berada dalam lingkungan B2B atau Business to Business ECommerce.

UNIVERSITAS MEDAN AREA PERPUSTAKAAN PUSAT

Pada saat melakukan akses sebuah website (palsu), maka program JavaScript dapat dikirimkan untuk memeriksa seluruh hard disk atas komputer yang dipakai untuk akses website tersebut. Melalui teknik file sharing, file-file tertentu dapat di upload atau dikirim ke website tersebut (Greenstein dan Feinman 2000:137).

Seandainya file tersebut adalah file yang berisi data akuntansi, keuangan, data pelanggan ataupun data lain yang bersifat rahasia, maka berarti data tersebut telah bocor ditangan

pihak ketiga. Pemahaman ini sangat diperlukan, sehingga dapat dikeluarkan kebijakan manajemen bahwa komputer yang digunakan untuk mengelola sistem akuntansi dan keuangan serta sistem bisnis lain yang penting tidak dihubungkan dengan internet.

Beberapa solusi teknis yang dapat dipakai untuk mengatasi masalah authentication adalah penggunaan digital signature, password dan biometric devices. Authentication berhubungan dengan verifikasi atas identitas dari mana transaksi tertentu berasal.

Pada transaksi perdagangan tradisional yang menggunakan kartu kredit misalnya, untuk memastikan bahwa customer adalah pemilik kartu kredit yang sesungguhnya, maka dilakukan three-factor authentication (Greenstein dan Feinman 2000: 230).

Dalam skema ini, untuk memastikan pemilik kartu kredit, maka pada saat terjadi transaksi, kartu kredit harus ditunjukkan pada penjual (first factor: something you have: credit card), faktor kedua yang harus dipenuhi adalah pembeli harus memasukkan nomor PIN (second factor: something you know: PIN), dan sebagai faktor verifikasi ketiga adalah adanya foto

dan/atau tandatangan pada kartu kredit (third factor: something you are: tanda tangan). Namun demikian, dalam perdagangan elektronik, three-factor authentication ini tidak dapat sepenuhnya dilakukan, mengingat penjual hanya bisa mengandalkan salah satu faktor saja, yaitu faktor PIN (something you know) dan ternyata PIN ini mudah sekali diketahui atau dicuri orang lain apabila seseorang telah melakukan transaksi yang menggunakan kartu kredit dengan website palsu. Jadi dilihat dari aspek pengendalian internal, maka three-factor authentication memiliki aspek pengendalian internal lebih kuat jika dibanding one or two-factor authentication.

Untuk meningkatkan pengendalian internal, sehingga transaksi pada perdagangan elektronik dapat mengandalkan pada two factor authentication, maka selain menggunakan PIN, faktor kedua perlu dipikirkan. Faktor something you have, dalam hal ini menunjukkan kartu kredit yang digunakan saat bertransaksi tidak mungkin dilakukan karena customer hanya berhadapan dengan komputer saat bertransaksi.

Oleh karena itu, faktor yang memungkinkan adalah faktor something you are. Faktor ini menghendaki adanya tandatangan

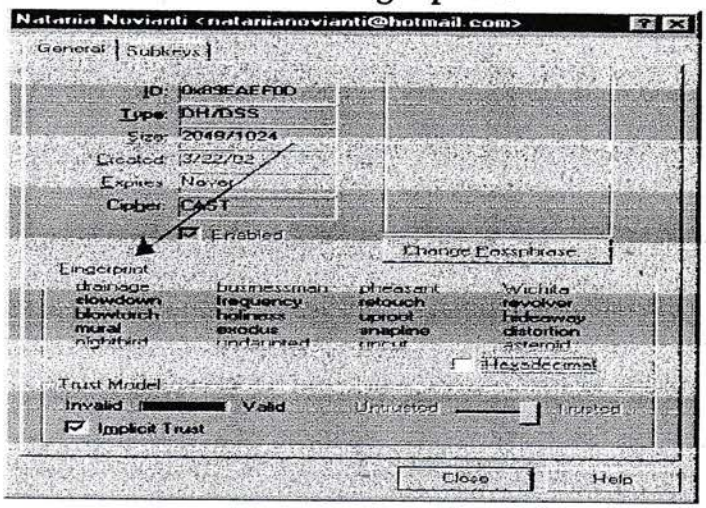
pada kartu kredit sebagai salah satu sarana untuk memverifikasi keaslian customer pemegang kartu kredit. Dalam perdagangan elektronik, tandatangan ini diubah bentuknya menjadi tandatangan digital atau digital signature (fingerprint). Contoh fingerprint dapat pada gambar 2 dan gambar 3.

Pada dasarnya fingerprint tersebut secara teknis tercipta saat kita memasukkan identitas kita dan semua isian yang disyaratkan melalui website sebelum transaksi dilakukan. Daftar isian tersebut kadang tertulis dalam beberapa halaman atau beberapa kali kita tekan tombol send. Informasi yang kita masukkan kemudian pada dasarnya adalah jejak kita saat melakukan penciptaan asal informasi yang sangat unik yang dimana halaman tersebut secara khusus hanya diperuntukkan bagi orang yang mengisi informasi tersebut. Dengan teknik tertentu jejak pengisian informasi ini akan menghasilkan fingerprint yang selalu berbeda untuk setiap orang. Berarti bahwa unsur verifikasi pelaku transaksi dapat diidentifikasi secara langsung. Hal ini dapat dipakai sebagai faktor lain yang melengkapi one-factor authentication.

Verifikasi keaslian pelaku transaksi juga dapat dicapai dengan menggunakan skema one-time password untuk melindungi pencurian password. Password akan terus berubah dalam jangka waktu yang sangat pendek. Host komputer akan menerbitkan password baru yang akan disinkronkan dengan password yang dipegang pemegang smart card Disamping itu password ini juga dienkripsi atau disandikan.

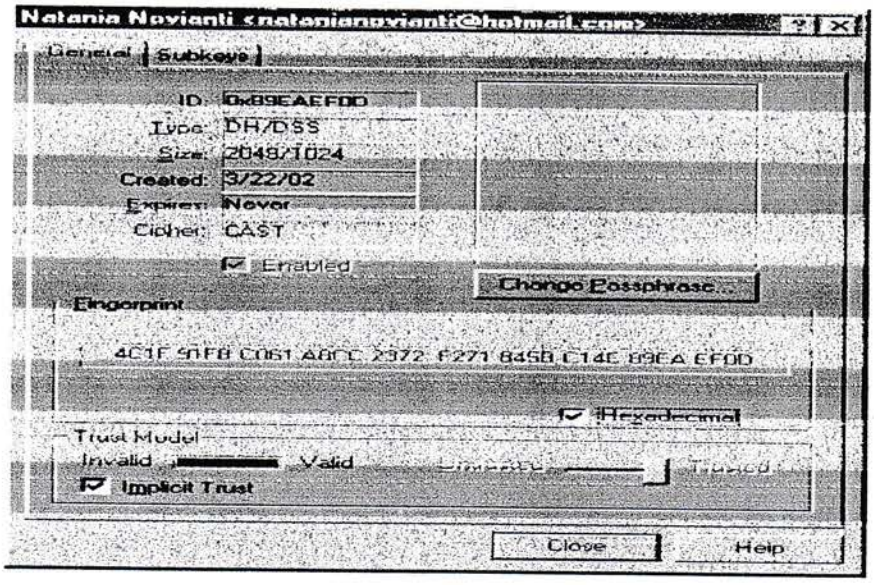
Sehingga dengan demikian, kemungkinan untuk terbobolnya sistem karena tercurinya password jadi makin kecil. Authentication juga bisa dicapai dengan menggunakan biometric identification seperti sidik jari, telapak tangan, pola wajah dan retina.

Gambar 2.
Contoh fingerprint



(Sumber: Tampilan layar PGP Software)

Gambar 3.
Contoh fingerprint dalam Bentuk Hexadecimal



(Sumber: Tampilan layar PGP Software)

Dalam pengertian transaksi yang valid termasuk juga adanya pemahaman tentang informasi yang tepat sama antara informasi yang disampaikan customer dan yangditerima supplier dan sebaliknya. Jadi selama informasi tersebut dikirim danditransmisikan melalui jaringan teknologi informasi dan komunikasi, informasi tersebut tidak mengalami perubahan, penambahan, duplikasi maupun pengurangan.

Secara teknis hal ini dikenal dengan istilah data integrity. Pada saat ditransmisikan kemungkinan ada pihak lain yang dapat melihat informasi pembeli-penjual ini, dan mengubah

informasinya. Sehingga harus ada cara untuk meyakinkan bahwa informasi yang dikirimkan, misalnya informasi mengenai perintah pembelian saham perusahaan tertentu dalam jumlah dan harga tertentu harus sama persis dengan informasi yang nantinya diterima. Untuk memastikan integritas data/informasi ini maka dalam perdagangan elektronik digunakan konsep encryption. Konsep ini menghendaki agar data-data disandikan atau dikodekan, tentunya termasuk didalamnya data akuntansi dan keuangan. Sehingga seandainya ada masalah dalam transmisi data dan adanya pihak lain yang seharusnya tidak berhak menerima informasi tetapi ternyata dapat menerima informasi tersebut, maka pihak tersebut tidak bisa membaca dan mengubah informasinya.

Untuk menjamin efektifitas metode encryption atau cryptography dalam menyakinkan terjadinya data integrity, maka dilakukan cara hashing. Dengan cara ini maka pesan yang dikirimkan dijumlah dengan menggunakan algoritma dan isi pesan.

Kemudian jumlah yang dihasilkan oleh perhitungan ini disertakan dalam pengiriman pesan. Jadi seperti penggunaan

check-sum digit dalam sistem informasi akuntansi. Pada saat pesan ini diterima maka penerima pesan juga akan melakukan hashing dengan cara yang sama. Apabila jumlah yang dihasilkan sama dengan jumlah hash yang diterima, maka berarti data integrity terjadi, bahwa pesan yang dikirimkan sama persis dengan pesan yang diterima. Hashing bukan enkripsi, tapi dapat digunakan secara bersamaan dengan enkripsi. Teknologi untuk melakukan enkripsi ini juga telah menyediakan software enkripsi. Dalam software enkripsi biasanya juga dapat dilacak authentication atau pelaku yang sesungguhnya karena nantinya ada tandatangan digital (digital signature) yang dapat dilihat yang esensinya sama dengan tandatangan tradisional biasa untuk memverifikasi keaslian pelaku bisnis.

Manajemen dapat mendayagunakan atau melakukan empowerment pada karyawan sehingga masing-masing karyawan dapat menjalankan tugas dan kewajibannya dan melakukan pengambilan keputusan dalam batas-batas yang sudah ditentukan tanpa perlu dilakukan supervisi yang berlebihan oleh manajemen level lebih atas kepadakaryawan tersebut. Empowerment ini disebut juga authorization atau otorisasi.

Otorisasi ini diwujudkan dalam bentuk tandatangan, terpicunya dokumen baru atau pemasukan kode otorisasi pada dokumen transaksi atau catatan Dengan adanya otorisasi diharapkan maka transaksi yang terjadi sudah disetujui dan dicek kebenarannya. Namun demikian dalam kenyataannya, tidak jarang juga terjadi penyangkalan atas transaksi yang sudah terjadi, meskipun sudah diotorisasi, sudah disetujui dan integritas data sudah baik. Artinya, terjadi penyangkalan atau repudiation dari pembeli atau penjual bahwa transaksi sudah dilakukan dengan baik.

Sebagai contoh, pada kasus transaksi sesorang yang melakukan jual beli lewat perantara dengan cara elektronik. Perantara diperintahkan untuk membeli saham dalam jumlah tertentu. Ketika harga baik, maka perantara tersebut diperintahkan untuk menjual kembali, tapi ternyata perantara melakukan penyangkalan bahwa perantara pernah diperintah untuk melakukan pembelian saham dalam jumlah tertentu.

Penyangkalan ini disebut sebagai proof of origin. Dapat pula terjadi kasus dimana justru yang memerintahkan pembelian saham pada perantara menyatakan menolak bahwa dia telah

memberi perintah pembelian saham setelah melihat bahwa memegang saham tersebut merugikan. Jika kasus ini terjadi, berarti penyangkalan ini disebut sebagai proof of receipt. Sedangkan bila semua pihak mengakui bahwa transaksi tersebut telah terjadi, tetapi yang dipermasalahkan adalah jumlah lembar saham yang berbeda atau tidak disepakati, maka penyangkalan ini disebut sebagai proof of content. Ketiga skenario repudiation ini membutuhkan kekuatan hukum untuk penyelesaiannya.

UNIVERSITAS PERPUSTAKAAN PUSAT MEDAN AREA

Dalam sistem perdagangan tradisional, penyangkalan ini relatif lebih mudah untuk dibuktikan kebenarannya. Sistem perdagangan tradisional menggunakan dokumendokumen atau kontrak yang ditandatangani sehingga dapat dipakai sebagai referensi yang dapat diacu sewaktu dibutuhkan. Dalam sistem perdagangan elektronis, hal seperti ini tentunya akan mengalami perubahan, karena dalam perdagangan elektronik dimungkinkan terjadinya sistem paperless sehingga yang dipentingkan bukanlah kertas sebagai medium penyimpanan informasi. Yang menjadi fokus perhatian adalah adanya informasi yang tidak berubah setelah ditransmisikan dari pembeli kepadapenjual. Jadi e-commerce harus memberikan keyakinan kepada pihak-pihak

yang bertransaksi bahwa tidak terjadi repudiation. Untuk kepentingan itu, maka secara teknis dapat dilakukan kombinasi hashing atas pesan atau perintah yang diberikan oleh kedua belah pihak yang bertransaksi disertai dengan pemakaian digital signature. Jadi masalah ini dapat diselesaikan dengan menyakinkan terjadinya data integrity dan authentication.

2.2. Keamanan Harta Perusahaan

Yang dimaksud dengan harta perusahaan adalah data, informasi, dokumen, laporan dan harta fisik perusahaan. Pada perusahaan yang telah menggunakan e-commerce semua jenis harta tersebut juga harus dijaga keamanannya. Karena semua data dan informasi sudah menggunakan teknologi informasi dan komunikasi yang saling terhubung dalam network atau jaringan sistem informasi, maka data dan informasi menjadi rentan terhadap masalah kerahasiaan atau confidentiality.

Masalah kerahasiaan atau privacy ini juga semakin berpotensi untuk terjadi ketika e-commerce memanfaatkan prasarana internet yang memang sangat lemah unsurpengendaliannya. Hal ini disebabkan, dalam teknis ilmu

komunikasi data, pengiriman data tidak melewati jalur yang selalu sama dan telah ditentukan sebelumnya. Jalur pengiriman data dibagi dalam potongan-potongan data yang masing-masing potongan yang dikirim tergantung pada saluran komunikasi tercepat dapat mengirimkan data.

Dengan demikian data akan mudah untuk disadap sehingga kerahasiaan data tidak dapat dipertahankan. Untuk menghindarkan hal ini maka biasanya perusahaan memanfaatkan software enkripsi untuk keperluan menjaga kerahasiaan data. Jadi sebelum dikirim data atau informasi dienkripsi atau disandikan terlebih dahulu. Seandainya sistem transmisi data bocor dan data dapat disadap, maka data yang bocor adalah data yang berada dalam bentuk sandi atau kode yang tidak dapat dibaca oleh pihak yang berhak. Pihak yang berhak dapat mentranslasikan data dalam bentuk sandi tersebut menjadi data yang sesungguhnya karena pihak yang berhak menerima transmisi data tersebut akan memiliki kunci sandi untuk mengartikannya. Selain itu, untuk menjaga keamanan data perusahaan dari akses atas pihak yang tidak memiliki otorisasi untuk melihat atau mengambil data perusahaan dapat dilakukan

dengan menentukan siapa saja yang berhak memiliki akses masuk dalam system. Untuk itu dalam sistem jaringan komputer biasanya digunakan firewall. Firewall adalah software dan hardware yang yang dibangun untuk melindungi sistem informasi internal perusahaan sehingga hanya pihak-pihak tertentu yang mendapatkan otorisasi untuk akses sistem bisnis perusahaan saja yang dapat menembus firewall dan dapat melihat, mengambil ataupun memodifikasi data internal perusahaan. Dengan demikian accessibilitas data atau sebagian dari sistem bisnis perusahaan hanya ada pada pihak-pihak tertentu saja (Nickerson 2001: 191).

BAB III

PEMBAHASAN

3.1. Implikasi E-Commerce terhadap Internal Kontrol

Seiring dengan makin kompleksnya transaksi bisnis dan semakin banyaknya pihakpihak yang berkepentingan terhadap bisnis, maka definisi internal kontrol semakin mengalami perluasan. Internal kontrol yang semula berarti rencana dan metode organisasi, kemudian berkembang menjadi struktur pengendalian internal yang tidak lagi mengartikan internal kontrol sebagai rencana dan metode tapi mengartikannya sebagai kebijakan dan prosedur. Sebagai sebuah rencana, internal kontrol menjadi sesuatu yang terpisah terhadap pelaksanaan atau fungsi operasional. Sebagai sebuah kebijakan dan prosedur, berarti internal kontrol secara langsung sudah dilaksanakan pada tahap operasional, dimana pada tahap operasional biasanya terdapat berbagai macam prosedur seperti prosedur penjualan, prosedur pembelian dan sebagainya, termasuk prosedur pengendalian. Disamping itu, pada tahap operasional juga terdapat banyak kebijakan, seperti kebijakan pemberian kredit, kebijakan

penghapusan piutang dan sebagainya. Oleh karena itu, didalam kebijakan operasional dapat disisipkan kebijakan pengendalian.

Dengan demikian, sebagai sebuah prosedur dan kebijakan, maka internal kontrol diharapkan dapat diterapkan secara langsung dalam proses operasional bisnis sehari-hari. Namun demikian kenyataannya, prosedur dan kebijakan dapat terjadi tidak ditaati sehingga kemudian dirasa perlu untuk mengembangkan definisi internal kontrol.

COSO telah mendefinisikan internal kontrol sebagai proses yang dijalankan oleh dewan direksi, manajemen dan semua pihak yang berada dalam arahan mereka untuk memberikan keyakinan yang memadai bahwa tujuan pengendalian tercapai. Adapun tujuan pengendalian tersebut adalah (1) efektifitas dan efisien operasi (2) reliabilitas pelaporan keuangan (3) ketaatan dengan hukum dan peraturan yang berlaku (Romney dan Steinbart 2000: 256). Definisi internal kontrol sebagai proses berarti bahwa mau tidak mau dalam pelaksanaan proses atau aktifitas bisnis, internal kontrol telah menjadi bagian yang tak terpisahkan dari aktifitas bisnis itu sendiri. Dengan demikian sepanjang bisnis melakukan kegiatan operasionalnya, sejauh itu juga proses

pengendalian internal dilakukan. Ada lima komponen yang saling terkait dengan internal kontrol yang didefinisikan dalam COSO Report atau Internal Control - Integrated Framework, yaitu (1) Control Environment (2) Control Activities (3) Risk Assessment (4) Information and communication (5) Monitoring (Romney dan Steinbart 2000: 256).

Komponen pertama, yaitu lingkungan pengendalian mencerminkan dan mempengaruhi budaya organisasi dan merupakan dasar dari empat komponen pengendalian yang lain. Dalam lingkungan bisnis berbasis sistem elektronik, tentunya lingkungan pengendalian juga akan mengalami perubahan. Misalnya saja, kebijakan mengenai jumlah karyawan yang mempunyai kompetensi yang cukup dibidang teknologi dan keamanan sistem komputer untuk menjalankan misi perusahaan, adanya petunjuk atau pengarahan detail mengenai sistem informasi atau rencanarancana keamanan yang dikomunikasikan dengan baik, letak departemen sistem informasi, EDP serta internal auditor dalam struktur organisasi perusahaan, bagaimana melakukan proteksi sistem informasi ada data-data

utama perusahaan terhadap mantan karyawan yang masih memiliki password untuk masuk dalam sistem, dan sebagainya.

Komponen kedua, yaitu aktifitas pengendalian juga mengalami perluasan. Pengendalian umum akan meliputi pengendalian atas pengendalian atas pusat data, pengendalian atas pengembangan sistem, pengendalian atas pemeliharaan sistem, pengendalian atas akses dan sebagainya. Sedangkan pengendalian aplikasi adalah pengendalian terhadap input, proses, output, dan storage. Dengan diaplikasikannya sistem-sistem bisnis seperti penjualan, pembelian, pengeluaran dan penerimaan kas dan sebagainya dalam komputer maka pemahaman atas cara penggunaan dan pengendalian software lebih banyak dibutuhkan. Seperti misalnya jurnal dan buku besar dalam sistem akuntansi manual akan berubah bentuk menjadi transaction file dan master file dalam sistem berbasis komputer.

Dengan demikian tentunya akuntan harus memahami bagaimana file itu dibuat dalam sebuah database dan bagaimana melakukan pengendaliannya. Risk assessment atau pemrakiraan resiko dilevel enterprise dan level aktifitas bisnis dalam tingkat yang lebih detail. Resiko dilevel enterprise dapat merupakan faktor resiko yang berasal dari luar, seperti perkembangan

teknologi yang terbaru dan faktor internal berupa gangguan operasi pemrosesan transaksi, masalah keamanan aplikasi teknologi yang digunakan seperti yang telah dibicarakan diatas yang terkait dengan isu confidentiality, authentication, non-repudiation, data integrity dan sebagainya.

Oleh karena itu risk assessment dalam lingkungan perdagangan elektronik mensyaratkan akuntan agar memiliki pengetahuan dan wawasan yang lebih baik akan isu-isu teknologi tersebut. Tentunya akan lebih baik lagi jika akuntan dapat memahami dan memiliki sedikit skill yang terkait dengan hal tersebut tanpa harus menjadi counterproductive atas kompetensinya dalam melakukan penugasan.

Hal ini merupakan tantangan tersendiri bagi profesi akuntan untuk tetap dapat memiliki bahkan meningkatkan perannya dalam lingkungan perdagangan elektronik, apalagi dalam lingkungan perdagangan yang sudah sepenuhnya paperless. Sifat proaktif harus senantiasa menjadi jiwa seorang akuntan, bukannya sifat defensive.

Akuntan harus mencari cara untuk melakukan pekerjaan akuntansi dan auditing yang tidak lagi didukung oleh bukti fisik yang kasat mata seperti adanya dokumen sumber dan dokumen

pendukung, catatan-catatan dalam bentuk jurnal, buku besar dan sebagainya. Akuntan harus mulai sadar bahwa journalizing transaksi tertentu sudah berubah bentuknya menjadi entry data saja dalam sistem pengolahan data elektronik dan posting telah berubah menjadi updating.

Komponen berikutnya yaitu informasi dan komunikasi. Pada komponen pengendalian ini ditekankan bahwa sistem informasi akuntansi harus dapat melakukan identifikasi dan pencatatan semua transaksi yang telah valid. Disamping itu sistem informasi akuntansi harus dapat melakukan klasifikasi yang tepat atas transaksi tertentu pada golongan rekening tertentu dalam jumlah yang tepat juga dan pada periode akuntansi yang benar. Sistem informasi akuntansi juga harus dapat memaparkan adanya disclosure dan mengkomunikasikan-nya. Sistem informasi akuntansi yang dapat memenuhi semua tujuan, tersebut pasti akan dapat memberikan audit trail yang cukup. Dalam sistem perdagangan elektronikpun sistem informasi akuntansinya juga harus dapat menyediakan jejak audit secara layak meskipun dengan adanya sistem paperless jejak audit juga semakin tidak terlihat atau tidak kasat mata.

Komponen terakhir dalam COSO Report adalah monitoring, dimana unsur yang diutamakan adalah adanya supervisi yang efektif dan penerapan internal audit. Agar pengendalian berjalan efektif, maka monitoring harus dilakukan secara berkesinambungan.

Jadi internal kontrol dalam perdagangan elektronik melampaui internal kontrol yang terjadi dalam lingkungan bisnis tradisional. Esensi pengendalian itu sendiri tetap sama, tetapi terjadi perubahan bentuk dan cara pengendalian karena cara dan lingkungan bisnis juga berubah dalam perdagangan elektronik

3.2. Peluang yang Dimiliki oleh Akuntan

Setiap tantangan pasti akan menimbulkan peluang yang baru. Seperti juga dalam lingkungan perdagangan elektronik, kompetensi akuntan telah ditantang dengan adanya berbagai macam pemahaman baru yang bukan berasal dari disiplin ilmu akuntansi. Tantangan ini mestinya dijawab dengan terus mengembangkan diri agar kompetensi akuntan tetap dapat mengikuti perubahan lingkungan bisnis akibat pemanfaatan teknologi informasi. Pasar baru atau peluang ini selain

disebabkan oleh perubahan lingkungan bisnis adalah juga disebabkan oleh adanya teknologi yang terus berkembang serta kebutuhan akuntan publik untuk terus dapat mencari lahan dan kesempatan jenis pekerjaan baru baginya.

Kesempatan diversifikasi jenis pekerjaan ini semakin besar jika diingat bahwa dalam menjalankan penugasannya akuntan publik harus selalu ingat perannya, yaitu sebagai pihak ketiga yang independen. Akuntan harus tetap memberikan keyakinan pada pihak-pihak yang melakukan transaksi bahwa dengan adanya pemanfaatan teknologi, maka keamanan transaksi tidak perlu menjadi satu masalah yang perlu dikhawatirkan. Akuntan bersama -sama dengan praktisi lain dibidang teknologi informasi, misalnya programmer dapat memberikan jasa penyusunan sistem akuntansi berbasis komputer dan desain pengendalian internalnya, membangun database akuntansi dan keuangan yang terintegrasi, merancang program-program yang dapat membantu pengambilan keputusan manajerial secara cepat dan akurat dan sebagainya.

Beberapa waktu belakangan ini AICPA sedang dan terus bekerja untuk mengembangkan XBRL atau eXtensible Business

Reporting Language specification untuk menggantikan penggunaan format HTML. Before XBRL, there was no generally accepeted format for business reporting data [online aicpa].

Dengan XBRL akan tersusun pelaporan keuangan dalam format standar yang memungkinkan terjadinya translasi dan sharing informasi atas pelaporan keuangan yang dihasilkan tersebut. XBRL uses accepted financial reporting standards and practices to exchange financial statements across all software and technologies, including the Internet [Reuters 2000].

Keberadaan XBRL yang dapat digunakan untuk menyiapkan laporan keuangan dalam format yang bisa dioperasikan dalam berbagai aplikasi berarti mengurangi kebutuhan untuk menyiapkan laporan keuangan dalam format yang berbeda. Oleh karenanya akan terjadi penghematan waktu, biaya dan kesalahan data tertentu pada berbagai dokumen. Meskipun masih banyak pro kontra dikalangan profesi akuntan di AS, namun demikian beberapa perusahaan besar seperti Microsoft, Deutsche Bank dan The Australia Prudential Regulatory Authority (APRA) telah mengadopsi penggunaan XBRL untuk penyusunan pelaporan keuangan perusahaan

mereka. Sebagian akuntan yang pesimis dengan adopsi teknologi menyatakan bahwa sudah selayaknya akuntan kembali pada panggilan awalnya (back to basic) dengan mengingat pelajaran yang didapat dari kasus bangkrutnya perusahaan besar Enron [online].

Dokumen elektronik dan real time accounting systems ini menyebabkan perubahan peran akuntan publik pada pekerjaan yang terkait dengan proses pelaporan laporan keuangan, termasuk didalamnya adalah permrakiraan resiko audit dan exposure yang mungkin timbul. Untuk dapat melakukan penugasan dalam lingkungan sistem informasi akuntansi yang sudah online real time, akuntan publik harus dapat terus mengembangkan teknologi audit untuk kepentingan continuous audit techniques (Rezaee et al. 2002).

Pada audit tradisional, bukti yang dikumpulkan adalah bukti historis, sedangkan dalam continuous audit rentang waktu yang diperlukan antara terjadinya transaksi, proses pemerolehan bukti audit sampai terbitnya laporan audit sangatlah singkat. Dengan demikian dalam continuous audit, waktu untuk menjalankan penugasan sangat terbatas, sehingga jika akuntan

publik tidak dapat memanfaatkan waktu yang singkat tersebut, maka laporan audit akan kehilangan relevansinya. Untuk itu, akuntan publik harus memastikan terlebih dahulu bahwa sistem informasi akuntansi perusahaan adalah sistem yang andal sehingga laporan atau output yang dihasilkan andal dan tidak mengandung salah saji secara material (Pinnarwan 2001) Akuntan publik harus dapat memahami pengendalian internal dalam lingkungan e-commerce baik yang bersifat preventif maupun detektif. Dalam proses continuous audit akuntan publik harus dapat menggunakan software audit yang akan lebih bermanfaat apabila dapat terintegrasi dengan sistem informasi perusahaan klien sehingga memungkinkan audit dilakukan bersamaan waktunya dengan perusahaan klien yang sedang melakukan pemrosesan transaksi (embedded audit module).

Oleh karena itu, continuous audit mensyaratkan agar akuntan memiliki kompetensi dalam aspek penguasaan teknologi informasi, meskipun sesungguhnya kompetensi ini dulunya bukan kompentensi inti disiplin ilmu akuntansi Peluang lain yang sangat luas terbuka bagi akuntan adalah peluang dibidang assurance services. Elliot Committee atau The AICPA's Special

Committee on Assurance Services mendefinisikan assurance services sebagai independent professional services that improve the quality of information, or is context for decision makers [online]. Komite ini juga mendefinisikan bahwa assurance services adalah jenis pekerjaan baru akuntan yang lebih luas lingkupnya daripada audit atas laporan keuangan yang merupakan jasa tradisional yang dapat diberikan oleh akuntan publik.

Seperti tercantum dalam SAS 78, e-commerce memberikan pengaruh pada luas dan metode atas penugasan traditional assurance services dalam hal internal kontrol, pemrakiraan resiko audit dan prosedur perencanaan audit (Greenstein dan Feinman 2000).

Informasi yang menjadi bahan oleh dalam assurance services bukan hanya informasi keuangan, tetapi juga meliputi informasi non keuangan. Tujuan dari assurance services adalah perbaikan informasi dan bukan pada tersusunnya laporan, meskipun mungkin bisa juga dalam bentuk tersusunnya laporan.

Contohnya adalah terjadinya perbaikan informasi tentang proses atau sistem tertentu seperti internal kontrol atau model

pengambilan keputusan. Contoh lain adalah informasi tentang sebuah produk atau pernyataan pihak lain atas atribut produk tertentu, dimana semua perbaikan informasi tersebut dapat berguna untuk pengambilan keputusan baik pengambilan keputusan yang dilakukan oleh pihak internal maupun oleh pihak eksternal. Dengan demikian audit atas laporan keuangan hanyalah merupakan salah satu bagian dari assurance services (Alles et al. 2002)

Lebih jauh mengenai perkembangan dan perbedaan assurance services pada masa dahulu dan masa yang akan datang dapat dilihat pada gambar 4 dibawah ini. Tampak bahwa dalam lingkungan bisnis elektronik akan menyebabkan akuntan tidak hanya akan menghasilkan opini atau pendapat audit tapi lebih pada memberikan assurance atau pernyataan mengenai keyakinan bahwa informasi yang dihasilkan atau disajikan oleh pihak tertentu adalah informasi yang berkualitas dan dapat dipercaya sehingga menimbulkan kepercayaan dalam bertransaksi. Sedangkan waktu pelaksanaan pekerjaan tersebut bukan hanya tahunan tapi berkesinambungan untuk mengimbangi sistem bisnis yang semakin menuju kearah online real time.

Gambar 4.
Perbandingan antara Historical dan Future Assurance Services

Historical Service	*Future Service*
Annual	*Continuous*
Opinion	*Assurance*
On financial statement	*On user-chosen information*
For investors and creditors	*For decision makers*
Error focus	*Fraud focus*
Auditee pays	*User pays ?*
Independence	*Independence ?*

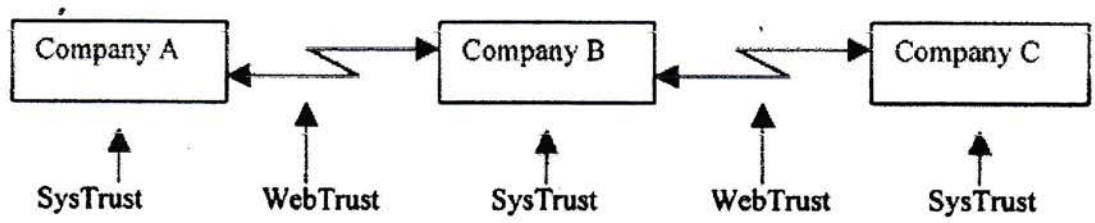
(Sumber: Elliott 2002: 140)

Contoh tipe assurance services yang dapat dilakukan oleh akuntan adalah a web assurance services., yaitu SysTrust dan WebTrust. Keduanya dikembangkan secara bersama-sama oleh AICPA dan CICA (organisasi akuntan publik Kanada). SysTrust berhubungan dengan masalah security, integrity, availability, dan maintainability dari sebuah sistem informasi bisnis. Sedangkan WebTrust diterapkan untuk ecommerce dalam kaitannya dengan masalah security, availability, business practices dan transaction integrity. Jika web assurance services, yaitu, SysTrust dan WebTrust diterapkan semuanya pada perusahaan maka berarti transaksi yang terjadi dengan bisnis tersebut adalah transaksi yang dapat dipercaya. Perusahaan yang sudah diverifikasi sistem informasinya oleh AICPA ini akan dapat menggunakan stempel atau logo WebTrust. Logo pada

website ini berarti bahwa website telah dinilai oleh akuntan publik dan pendapat yang diberikan adalah wajar tanpa perkecualian atau unqualified opinion atas penerapan standar, prinsip dan kriteria suatu website yang sesuai dengan standar (Franky 2001). Masyarakat dapat mengklik ikon logo WebTrust untuk melihat laporan akuntan yang ada.

Akuntan publik harus senantiasa melakukan penilaian kembali atas website tersebut minimal 6 bulan sekali dan setiap kali perusahaan melakukan perubahan isi website yang akan memiliki dampak terhadap kriteria WebTrust maka perusahaan harus melaporkan kepada akuntan publik untuk dinilai kembali. Inilah peranan akuntan sebagai pihak ketiga yang independen. Perbedaan SysTrust dan WebTrust dapat dilihat pada gambar dibawah ini.

Gambar 5.
A Web of Assurance



(Sumber: Elliott 2002: 142)

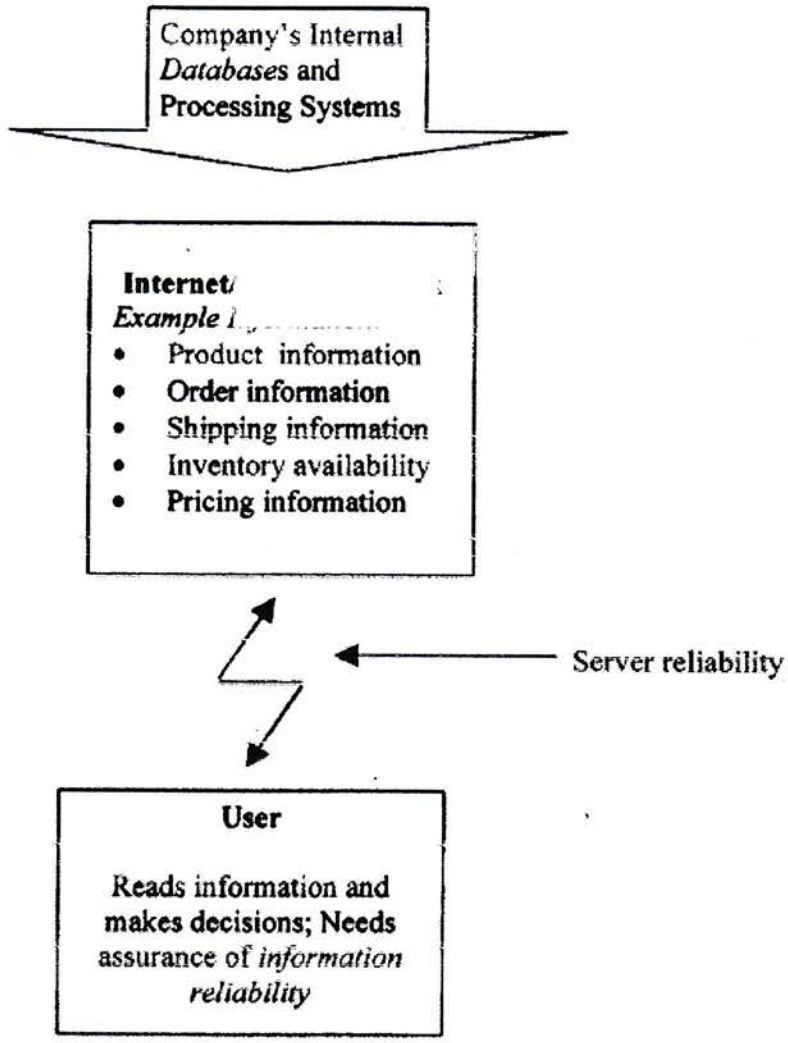
Pada intinya jasa yang diberikan untuk pekerjaan diatas adalah jasa E-commerce Integrity and Security Assurance. Integrity assurance system akan meyakinkan bahwa elemen data yang ditangkap dalam transaksi elektronik adalah transaksi yang sudah disepakati dan bahwa prosedur pemrosesan data transaksi dan penyimpanannya telah mempertimbangkan unsur integrity atas elemen data dan meyakinkan bahwa data transaksi tidak berubah selama ditransmisikan.

Sedangkan security assurance system meyakinkan bahwa telah authentication atas pihak-pihak yang bertransaksi telah diverifikasi dan bahwa data elektronik telah dilindungi dari pengungkapan informasi yang tidak atau belum diotorisasi.

Jenis assurance services yang lain adalah E-commerce System Reliability Assurance. Gambar 6 penjelaskan tentang kebutuhan informasi yang berkualitas dari trading partnernya. Untuk memenuhi kebutuhan ini, maka keandalan server dan informasi menjadi syarat utama. Keandalan server atau server reliability menjamin pemakai yang sudah memiliki otorisasi untuk dapat mengakses informasi pada saat yang dibutuhkan. Jadi pada saat user mengambil informasi dari website, dengan

segera server harus dapat memberikan responnya. Informasi yang dikirimkan oleh server adalah informasi yang akurat dan informasi yang terkini yang berguna untuk pengambilan keputusan.

Gambar 6.
Reliable Information Systems



(Sumber: Greenstein and Feinman 2000: 36)

Assurance services juga dapat berupa risk assessment assurance. Risk assessment adalah proses untuk melakukan identifikasi, analisis, dan pengelolaan resiko yang dapat mempengaruhi pencapaian tujuan manajemen. Sesungguhnya akuntan telah biasa melakukan pekerjaan risk assessment pada waktu melakukan audit keuangan, yaitu pada saat menentukan efektifitas pengendalian internal perusahaan atau menentukan control risk. Jadi hanya merupakan perluasan ruang lingkup pekerjaan risk assessment yang sebelumnya telah ada.

BAB IV

PENUTUP

Fungsi sisten e-commerce yang antara lain meliputi online order entry dan electronic payment menyebabkan sistem informasi perusahaan tidak lagi tertutup untuk pihak luar karena customer dan trading partner dapat secara langsung melakukan akses ke dalamnya dan hal ini akan menyebabkan pengendalian internal perusahaan jadi semakin lemah. Beberapa isu pengendalian internal yang muncul antara lain adalah authentication, data integrity, non-repudiation, confidentiality dan privacy yang dalam sistem] :rdagangan tradisional dikenal dengan isu validitas, otorisasi dan keamanan harta perusahaan. Esensi pengendalian internal dalam perdagangan tradisional dan elektronik adalah sama, hanya terjadi perubahan bentuk dan cara pengendalian karena cara dan lingkungan bisnis yang berubah atau berbeda.

Hal ini menimbulkan tantangan baru terhadap kompetensi akuntan yang dalam pekerjaan sehari-harinya sangat terkait dengan pengendalian internal. Akuntan harus terbuka dan

memperkaya wawasan terhadap perkembangan disiplin ilmu lain, khususnya disiplin teknologi informasi tanpa menjadi counterproductive terhadap detail teknis teknologi itu sendiri. Namun demikian banyak pula peluang baru yang ditawarkan akibat kemunculan e-commerce ini.

Beberapa diantaranya adalah pemberian jasa assurance services, penyusunan laporan keuangan dalam format standar XBRL, jasa-jasa lain yang terkait dangan real-time accounting systems dan continuous audit techniques.

DAFTAR PUSTAKA

Alles, Michael G. et al. (March 2002), "Feasibility and Economics of Continuous Assurance", Auditing: A Journal of Practice and Theory, Vol. 21, No. 1

Elloitt, Robert K. (March 2002), "Twenty-First Century Assurance", Auditing: A Journal of Practice and Theory, Vol. 21, No. 1

Franky (September 2001), "Saatnya Akuntan Melirik Bisnis E-commerce", Media Akuntansi, edisi 20?sept/Tahun VIII/2001, hal 40-43.

Greenstein, Marilyn and Todd M. Feinman (2000), Electronic Commerce: Security, Risk Management and Control, Boston: Irwin McGraw-Hill.

Konrath, Larry F. (1999), Auditing Concepts and Applications: A Risk Analysis Approach, Fourth Edition, Cincinnati: South-Western College Publishing.

Nickerson, Robert C. (2001), Business and Information Systems, Second Edition, New Jersey: Prentice-Hall, Inc.

Pinnarwan, Djohan (Juni 2001), "Real Time Reporting dan Continous Auditing", Media Akuntansi, edisi 18/Juni/Tahun VIII/2001.

Rezaee, Zabihollah et al. (March 2002), "Continuous Auditing: Building Automated Auditing Capability", Auditing: A Journal of Practice and Theory, Vol. 21, No. 1.

Romney, Marshall B. and Paul John Steinbart (2000), Accounting Information Systems, Eight Edition, New Jersey: Prentice-Hall, Inc.

http://www.pgpi.org/ pgp software

Reuters (Wire), http:www.aicpa.org/news/2000/040600c.htm, accessed June 21, 200.

_____,(April 20, 2000), "Electronic Accountant: XBRL Elicits Mixed Reaction from CPAs" http://www.aicpa.org/news/2000/042000a.htm, accessed June 21, 200.

http://www.aicpa.org/trustservices/ecommentnewsletterpa402.htm, accessed June 21, 200.

http://www.aicpa.org/assurance/systrust/what.htm, access 14 mei 2002.