Jurnal Pendidikan Akuntansi Indonesia, Vol. IX. No. 1 – Tahun 2011, Hlm. 24 - 42

AUDIT LINGKUNGAN TI: PERSPEKTIF DAN DAMPAK PADA PROSES AUDITING SECARA KOMPREHENSIF

Oleh
Mahendra Adhi Nugroho[1]

ABSTRAK

Perkembangan tekhnologi pada beberapa dasawarsa terakhir mempengaruhi hampir seluruh aspek kehidupan. Perkembagan tersebut juga mempengaruhi proses bisnis. Perusahaan pada perkembangannya mempunyai kecenderungan untuk mengadopsi Tekhnologi Informasi (TI) untuk menjalankan bisnisnya. Pengadopsian tersebut mengakibatkan perubahan peran, prosedur dan model audit yang perlu dijalankan pada linkungan perusahan yang mengadopsi TI pada proses bisnisnya. Tulisan ini menyajikan beberapa aspek dampak TI terhadap proses auditing secara komprehensif. Pertama, tulisan ini membahas peran TI terhadap auditing yang membahas perubahan peran auditor dan bentuk bukti yang akan dihadapi, kedua, membahas risiko dan keamanan audit, ketiga, mengulas peran auditor dalam tata kelola TI, keempat, proses audit TI dan diakhiri dengan teknik audit TI.

Kata kunci: Dampak TI terhadap proses audit, Peran auditor, Proses audit TI, Teknik audit TI

A. PENDAHULUAN

Perkembangan tekhnologi dalam beberapa dasawarsa terakhir sangat berdampak pada berbagai aspek kehidupan, tanpa kecuali pada proses bisnis yang dilakukan oleh perusahaan. Perusahaan atau organisasi cenderung memanfaatkan tekhnologi untuk meningkatkan efisiensi yang bertujuan untuk mendongkrak pendapatan dan memperbaiki kinerja. Pemanfaatan tekhnologi baik secara langsung maupun tidak langsung sudah menjadi menu utama dalam proses bisnis. Fenomena tersebut secara langsung maupun tidak akan mempengaruhi perilaku dan kebutuhan semua pihak yang berhubungan dengan perusahaan baik secara langsung maupun tidak langsung, termasuk auditor baik auditor internal yang masuk dalam struktur organisasi maupun auditor eksternal yang bekerja berdasarkan surat perikatan.

Salah satu dampak yang sangat berpengaruh pada proses auditing adalah adanya pergeseran audit tradisional yang berbasis tugas menuju audit TI berbasis risiko. Secara logika sederhana, pergeseran sudut pandang proses audit tersebut akan berpengaruh secara luas pada proses audit secara keseluruhan. Fungsi kontrol audit yang berbasis pada penditeksian risiko akan berfokus pada awal terjadinya suatu kejadian ekonomi dengan pencegahan terjadinya fraud melalui kelayakan pengendalian internal. Hal tersebut dilakukan karena dampak TI yang cenderung menghilangkan bukti transaksi yang berupa dokumen kertas. Dengan logika pengendalian yang baik akan menghasilkan outcome yang baik pula maka evaluasi efektivitas pengendalian dapat digunakan sebagai proxy pengganti pengujian subtantif yang lebih sulit dilakukan dalam lingkungan TI.

Tantangan yang dihadapi auditor pada kondisi tersebut adalah bagaimana auditor dapat melakukan audit dengan efektif dan tepat sehingga tidak mempengaruhi pendapat auditor yang merupakan produk utama dalam kegiatan audit tersebut. Untuk menjawab tantangan tersebut auditor perlu menyusun strategi baru dalam kaitan audit dalam lingkungan TI. Selanjutnya seorang auditor juga harus memiliki pengertian yang cukup mengenai teknik

[1] Dosen Jurusan Pendidikan Akuntansi – Universitas Negeri Yogyakarta

audit dan tools yang dapat digunakan untuk menunjang kegiatan audit. Dengan demikian seorang auditor dapat berperan dengan porsi yang tepat dan tidak menjadi usang.

B. TI DAN AUDITING

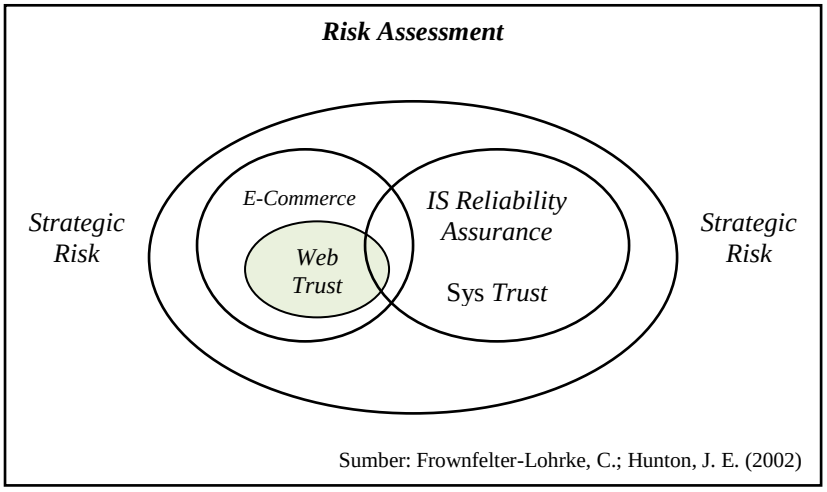
Tekhnologi Informasi (TI) akan melanjutkan dampak dramatis secara virtual pada setiap fase audit, dari program audit yang dihasilkan audit sampai software audit yang mampu untuk menguji keseluruhan data klien, tekhnologi sangat esensial untuk akuntan dalam memahami proses bisnis klien dan dihubungkan dengan lingkungan audit yang paperless (Bierstaker, J. L; Burnaby, P.; Thibodeau, J.;2001).

Menurut Glover and Romney (1997) dalam Rezaee, Z.; Reinstein, A. (1998) dampak utama auditing tekhnologi dalam beberapa dekade ini termasuk:

- Lebih sering menggunakan program word processing dan spreadsheet.
- Tekhnologi mengurangi kebutuhan sumber daya manusia.
- Meningkatnya kemampuan komunikasi elektronik.
- Melibatkan peran internal auditor untuk memberikan jasa yang bernilai tambah.
- Memungkinkan monitoring secara kontinyu
- Kertas kerja elektronik lebih merata.
- Meningkatkan prosedur sampling karena teknik EDP yang lebih kuat.

Tekhnologi Informasi (TI) hampir tidak dapat dipisahkan dengan kegiatan auditing dalam beberapa dekade terakhir. Idelanya, TI akan membantu auditor dalam menyelesaikan tugas dan memberi penjaminan dalam menjawab tantangan baru di dunia bisnis. Secara teknis TI akan membantu penilaian risiko dan penentuan strategi risiko dalam penjaminan yang dilakukan seorang auditor. Peran TI dalam membantu jasa penjaminan oleh seorang auditor sudah tidak diragukan lagi mengingat kegiatan bisnis dewasa ini cenderung menuju ke arah penggunaan TI. Rerangka kerja hubungan TI dan jasa penjaminan dapat dilihat pada gambar 1.

Gambar 1
Rerangka Kerja Hubungan TI dan Jasa Penjaminan



Sumber: Frownfelter-Lohrke, C.; Hunton, J. E. (2002)

Gambar 1 menjelaskan dua jasa penjaminan yang saling berkaitan satu dengan yang lain dalam lingkungan jasa penjaminan Web Trust dan Sys Trust (kedua jasa ini merupakan jasa yang dikembangkan oleh AICPA). Dalam gambar menunjukan bahwa Sys Trust tidak independen dan berhubungan dengan jasa penjaminan lain yaitu, penjaminan penilaian risiko, penjaminan e- commerce dan Web Trust.

Satu pergeseran yang cukup signifikan dalam lingkungan auditing yang diakibatkan oleh TI adalah pergeseran bentuk dan nilai bukti yang diperoleh auditor. Kecenderungan perusahaan ke arah TI mengakibatkan bukti fisik yang pada kegiatan auditing tradisional merupakan pusat perhatian dan digunakan untuk melaksanakan kegiatan auditing hampir tidak ada. Sebagai ganti bukti yang berupa kertas, kejadian ekonomi perusahaan terekam dalam bentuk bukti elektronik Dengan memberikan beberapa atribut Rezaee, Z.; Reinstein, A. (1998) membandingkan kedua bukti tradisional dan elektronik yang disajikan dalam tabel 1.

Tabel 1 menunjukan bukti kertas dan elektronik berbeda secara signifikan satu dengan yang lain, auditor harus memperhatikan isu evaluatif yaitu:

- *Informasi elektronik sebagai bukti yang kompeten.* Untuk memverifikasi kompetensi bukti auditor harus memperhatikan validitas, kelengkapan dan atribut lain dari bukti tersebut.
- *Penyajian bukti elektronik*: informasi elektronik yang sama dapat disajikan dalam bentuk yang sama, oleh karena itu auditor harus konsisten dalam menyajikan.
- *Kompetensi alat yang digunakan untuk memperoleh bukti elektronik*: alat yang digunakan untuk memperoleh bukti harus diuji dan dicek dengan baik untuk logical error.
- *Definisi error*: bukti elektronik memungkinkan perubahan yang tidak terditeksi yang meningkatkan risiko audit.
- *Kinerja pengendalian yang melekat*: error yang tidak terditeksi pada perubahan yang tidak diinginkan terjadi ketika pengendalian internal ditujukan pada perubahan yang diinginkan.

Tabel 1
Perbandingan Bukti Tradisional dan Elektronik.

Evidence		
Attributes	***Traditional***	***Electronic***
Difficulty of alteration	*Paper evidence is difficult to alter and there is a reasonable likelihood to detect such alteration in the normal course of audit*	*Electronic evidence is much easier to alter and much harder to detect and, accordingly, an effective internal control plays an important role in detecting certain changes to electronic evidence.*
Prima facie credibility	*Paper documents have a high degree of credibility*	*Electronic evidence's credibility depends highly on the effectiveness of internal control structure*
Completeness of documents	*Paper evidence typically includes all essential terms of a transaction*	*Electronic processing may mask the evidence with codes or by cross reference to other data fields*
Evidence of approvals	*Paper evidence approvals are prominent on the face of original documents*	*Electronic approvals may not be viable and can be done by pressing one key on the key board*

Ease of use	*Paper evidence does not require special tools to use in evaluating and understanding the evidence*	*Electronic evidence may require knowledge of data extraction techniques to evaluate and understand the evidence*
Clarity	*Paper evidence is usually clear and leads to the same conclusions by different authors*	*Electronic evidence is not as clear and may lead to different conclusions by auditors depending on the procedures used and controls implemented*

Sumber:Rezaee, Z.; Reinstein, A. (1998)

Beberapa pergeseran yang diakibatkan TI memaksa auditor untuk mencari bentuk baru auditing. bentuk baru tersebut akibat dari hilangnya bukti kertas yang dapat diuji secara subtantif. Oleh karena itu, kecenderungan yang ada akan menuju ke arah penilaian risiko pengendalian suatu sistem. Untuk itu pemahaman risiko secara komprehensif wajib dimiliki seorang auditor dalam bertugas terutama dalam lingkungan TI.

C. RISIKO DAN KEAMANAN

Risiko dan pengendalian merupakan dua sisi mata uang yang tidak dapat dipisahkan. Semakin baik pengendalian semakin kecil risiko yang harus dihadapi sebuah sistem. Seorang auditor harus memahami risiko suatu sistem dengan baik. Semakin kecil risiko semakin baik pula suatu sistem. Baik buruknya suatu sistem sangat mempengaruhi bukti yang dihasilkan dari sistem tersebut. Untuk mengetahuinya, dapat dilihat dengan pengendalian internal yang dilakukan sistem tersebut. Semakin baik suatu pengendalian internal, sistem dan bukti yang dihasilkan sistem tersebut akan semakin dapat dipercaya.

Pengendalian internal secara umum membantu memastikan operasi yang efektif dan efisien penyelesaian tujuan manajemen Gallegos, F., (2003) lebih lanjut, pengendalian internal yang baik biasanya berisi:

- *Review independen manajemen*: organisasi memberikan jaminan kebijakan dan prosedur yang dilakukan bekerja seperti yang diharapkan
- *Review struktur organisasional*: untuk memastikan pemisahan hak dan tanggung jawab
- *Pembangunan point pengendalian ke dalam siklus hidup pengembangan sistem*: proses untuk memastikan bahwa kebutuhan user dipenuhi.

Pertanyaan berikutnya adalah mengapa pengendalian internal digunakan? Beberapa alasan yang diajukan oleh Bakshi, S. (2004) untuk menggunakan pengendalian internal yaitu:
Perubahan proses bisnis

- Perubahan fokus pada TI – organisasi (khususnya yang bergerak di bidang jasa) semakin tergantung pada tekhnologi.
- Investasi pengendalian – untuk memelihara kesuksesan organisasi, pemahaman mengenai risiko dan pengendalian implementasi tekhnologi baru, dan petunjuk yang sesuai mengenai pengendalian dan batasan TI.
- Kompetisi – persaingan global memaksa organisasi untuk menggunakan TI.
- Nature of bisnis – struktur dan bentuk usaha yang mengharuskan menggunakan TI
- Adanya SOA – pemberlakuan SOA (khususnya di AS) memaksa organisasi bisnis untuk mengimplentasi pengendalian dengan lebih baik.

- Control self assessment – auditor ketika diminta melakukan audit tidak dapat bekerja di setiap cabang perusahaan yang tersebar, pengendalian internal yang baik memungkinkan auditor memberikan pendapat dengan tepat.

Setelah pengendalian internal dilakukan dan digunakan bukan berarti audit dalam lingkungan TI bebas dari risiko. Risiko audit bagaimanapun juga tidak dapat dihilangkan seratus persen. Hal tersebut karena terdapat risiko yang melekat dalam audit itu sendiri. Risiko audit akan meningkat bila auditor tidak memiliki kemampuan yang cukup memadai dalam melaksanakan audit di lingkungan TI. Kekurangan itu baik akibat kurang cakapnya auditor atau karena faktor lain yang memaksa auditor untuk mengadopsi ahli atau pihak ketiga dalam melakukan penilaian. Isu risiko akibat pihak ketiga diangkat oleh (ISACA Standards Board; 2002) sebagai konsekuensi penggunaan jasa pihak ketiga. Lebih lanjut, risiko lain dapat terjadi disekitar:

- Pengendalian di tempat pihak ketiga
- Proses tatakelola pihak ketiga
- Pengendalian dalam organisasi
- Proses tatakelola organisasi melalui pihak ketiga.

Isu risiko dan pengendalian yang lain muncul pada perkembangan tekhnologi yang meniru kinerja suatu organisme dalam menangkap respon yang disebut Biometric. Tekhnologi biometric modern mengklaim memberikan penyelesaian masalah authentifikasi pada sistem yang berbasis password dan token. Penyebaran arsitektur keamanan dalam tekhnologi biometric menyembunyikan banyak lubang, menambah kewajiban auditor sistem informasi untuk lebih memperhatikan risiko yang berhubungan dengan tekhnologi seperti itu.

Mengkombinasikan pemahaman metodologi dan alat dengan pedoman spesifik pada sistem biometric dan database dari risiko spesifik biometric dan pengendalian yang berhubungan dapat memastikan keamanan dengan level yang tinggi yang menuntun auditor sistem informasi menuju sukses (Dimitriadis, C.K; Polemi, D.; 2004). Secara ringkas, risiko dan pengendalian biometric dapat dilihat pada tabel 2. di dalam tabel 2 jelas terlihat beberapa risiko yang mungkin dihadapi dalam tekhnologi biometric dan pengendalian yang dapat dilakukan.

Tabel 2
Risiko dan Pengendalian Biometric

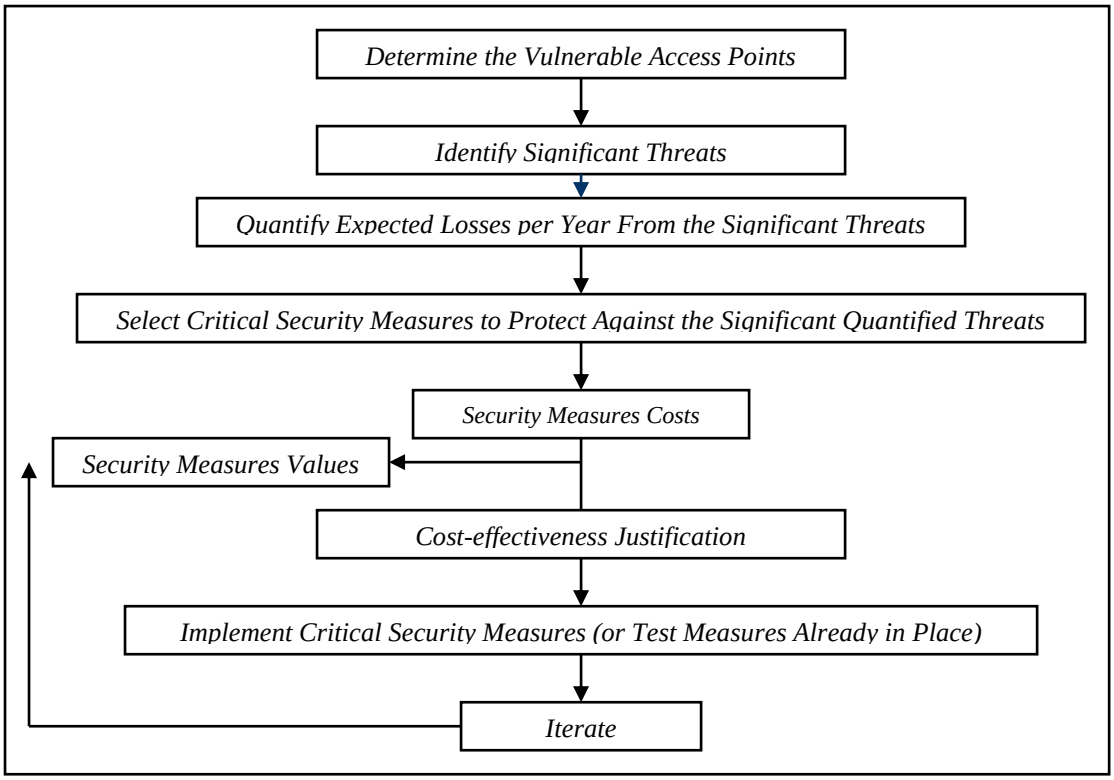
Risk	***Controls***
Spoofing—Mimicry	*Vitality detection, multimodal biometrics, interactive authentication*
Server side—Fake template risks	*Well-implemented security policy incorporating encryption technologies and intrusion prevention, detection and response controls; storage of the template in a secure smart card*
Communication links risks—Replay and bypass attacks risks	*System integration into one hardware security module, interactive authentication, rejection of identical signals*
Cross-system risk	*Custom biometric-encoding algorithms, deployment of hash functions*

Component alteration risks	*System integration into one hardware security module, well-implemented security policy*
Enrollment, administration and system use risks	*Well-designed and implemented security policy and procedures*
Noise and power loss risks	*Well-implemented security policy*
Power and timing low power analysis risks	*Noise generators, low power consumption chips in the biometric device*
Residual characteristic interactive risk	*Technology assessment, authentication*
Similar template—Similar characteristics risk	*Technology assessment and calibration review*
Brute force attack risk	*Traditional controls, account lock after a number of attempts*

Sumber: Dimitriadis, C.K; Polemi, D. (2004).

Setelah mengerti risiko yang berkaitan dengan TI seorang auditor juga harus mengerti bagaimana menilai suatu risiko. Penilaian risiko akan menentukan langkah yang harus dilakukan seorang auditor. jika menilik isu risiko suatu sistem maka secara simultan isu mengenai keamanan suatu sistem akan mengikuti. Keamanan suatu sistem akan mempengaruhi risiko sistem, dan risiko sistem dapat ditekan dengan peningkatan keamanan sistem. Oleh karena itu, penilaian risiko akan selalu berkaitan dengan isu keamanan sistem itu sendiri. Gambar 2 memberikan beberapa langkah dalam penilaian risiko keamanan. Sedangkan langkah awal dalam gambar 2 melibatkan penilaian risiko sedangkan sisanya merupakan justifikasi pengukuran keamanan.

Gambar 2
Analisis Risiko dan Justifikasi Ukuran Keamanan



Sumber: Cerullo, M. J.; Cerullo, V. (2005)

Dari gambar 2 nampak bahwa penilaian risiko akan diawali dengan pengidentifikasian tempat akses yang lemah atau dengan kata lain mengidentifikasi kelemahan sistem. Setelah mengidentifikasi diteruskan dengan mengidentifikasi ancaman yang mungkin dan memperkirakan kerugian yang ditimbulkan. Selanjutnya diperlukan suatu ukuran keamanan yang digunakan untuk menghadapi ancaman. Dilain pihak, setengah akhir dari gambar 2 menunjukan bagaimana suatu keamanan sistem dibatasi oleh biaya keamanan itu sendiri. Untuk memutuskan suatu perangkat keamanan sistem diperlukan suatu analisis yang komprehensif dalam menentukan titik kritis keamanan

Isu keamanan lain merujuk pada keamanan aplikasi yang didefinisikan sebagai satu set mekanisme keamanan disekitar suatu aplikasi yang melindungi kerahasiaan, integritas dan ketersediaan. Survey yang dilakukan Greene, F. (2002), memberikan perbandingan beberapa standar dan dokumentasi yaitu: ISO 17799, ISO 15408, COBIT, SP800-14, SP800-27 dan SAS94. Kelima standar dan dokumentasi tersebut dibandingkan. Hasil perbandingan berdasarkan tujuan dan komponen kuncinya. Hasil perbandingan disajikan dalam tabel 3. Tabel 3 menunjukan komponen kunci dari masing-masing keamanan aplikasi. Setiap standar mempunyai dampak pada stakeholder, fungsi bisnis, pendekatan dan tujuan yang berbeda.

Selanjutnya, keamanan suatu sistem tidak berhenti pada pemahaman dan pencegahan suatu risiko. Untuk dapat melaksanakan proses pengauditan dengan baik, auditor juga harus mengetahui seluruh segi keamanan. Satu bagian yang tidak kalah penting adalah pemahaman mengenai tujuan pengamanan itu sendiri. Tujuan pengamanan harus dipenuhi, bukan hanya untuk menyelamatkan data dan mengidentifikasi risiko tetapi terlebih untuk menekan risiko yang mungkin terjadi.

Stanley, R. A. (2004) mengindikasikan tujuan pengamanan berfokus pada empat segi yang meliputi confidentiality (kerahasiaan), Authenticity (keaslian), integrity (integritas), dan Availability (ketersediaan). Kerahasiaan mengacu pada kerahasiaan suatu aktivitas yang kritis

untuk kelangsungan perusahaan. Di dalam kasus ini auditor harus memperhatikan kepastian suatu transaksi yang bersifat privat berjalan sebagaimana mestinya tanpa intervensi atau bahkan suatu usaha untuk melakukan fraud. Keaslian mengacu pada penjaminan pada pesan atau transaksi yang dikirim benar-benar asli dan diterima oleh orang yang tepat. Integrity memberikan jaminan bahwa pesan yang diterima sama dengan pesan yang dikirim tanpa perubahan apapun.

Ketersediaan memberikan jaminan bahwa data yang akan digunakan kembali tidak hilang dan rusak. Dalam isu keamanan ini, auditor harus memastikan bahwa suatu sistem telah berjalan sebagaimana mestinya dan tujuan keamanan tercapai. Jika tujuan tersebut tercapai auditor dapat memperoleh sedikit keyakinan bahwa sistem tersebut dapat berjalan dengan baik atau paling tidak terjadi intervensi dari pihak ekternal maupun internal.

Setelah keamanan dan penekanan risiko suatu sistem tercapai, seorang auditor harus memahami posisi auditor di lingkungan TI yang terus berkembang dan mengalami perubahan secara kontinyu. Bukan hanya memeriksa kelayakan suatu sistem, auditor juga dituntut untuk dapat berperan aktif dalam pengelolaan TI itu sendiri, dengan mengetahui peran auditor, seorang auditor dapat mejaga independensi dan objektivitas dalam melaksanakan audit khususnya pada audit yang berkelanjutan. Pada bagian berikutnya akan dibahas mengenai peran auditor dalam tatakelola TI.

Tabel 3
Perbandingan Berbagai Standar dan Dokumentasi

	ISO 17799: Code of Practice for information Security Management	***IS0 15408: Evaluation Criteria for IT Security***	***CoBiT: Control Objectives for Information and related Technology***	***SP800-14 + 27: Generally Accepted Principles and Practices for Securing Information Technology Systems***	***SAS 94: The Effect of Information Technology on the Auditors Consideration of Internal Control in a Financial Audit***
Approach to application security	*To p.-event loss. modification or misuse of user data. input. process. output controls. cryptographic and application development controls*	*To prevent unauthorized disclosure. modification or loss of use; security guidelines for developers and assurance for users*	*Security and controls around IT processes of planning. acquiring. developing. supporting and motoring applications*	*Practices and controls on each of the life cycle phases; operational! controls*	*Focused on security around applications that process financial transactions and accounting journal entries*

Objectives	*Set of controls comprising best practices in information security*	*Standard for measuring the security and assurance associated with an IT product*	*IT governance within a framework of business requirements. IT processes and IT resources*	*Security principles and practices for the use. protection and design of government information and data systems*	*Integrity of all information that affects financial statements and audits*
Key components	*Ten domain convening all aspects of IT security*	*Security "functional" and "assurance" requirements used to evaluate IT products: evaluation assurance levels (EAL)*	*Domains planning and organization. acquisition and implementation, delivery and support, and monitoring*	*Eight principles and 14 practices (SP800-14): 33 principles on security in the life cycle phases (SP800-27)*	*Control environment. risk assessment. control activities. information and communication. monitoring*
Business function	*Information technology*	*Application and IT product development*	*Information technology*	*Information technology*	*financial reporting*
Intended audience	*Management, uses*	*Consumers. Developers. evaluators*	*Management. users. auditors*	*Management. users. auditors, developers*	*External auditors*

Sumber: Greene, F. (2002),

D. AUDITOR DALAM TATAKELOLA TI

Pengelolaan TI yang sudah diimplementasikan dalam suatu perusahaan melibatkan berbagai pihak termasuk auditor. seluruh pihak yang terlibat mempunyai peran dan kontribusi masing-masing. Untuk mensingkronkan berbagai macam kepentingan dari berbagai pihak diperlukan suatu tatakelola TI yang baik dan tepat. Pemahaman peran auditor mengenai tatakelola juga dapat digunakan untuk menyusun strategi audit dan teknik yang akan dilakukan.

Hamaker, S; Hutton, A. (2004), memberikan prinsip-prinsip dasar yang merupakan *best practice* umum dalam semua bentuk dari tatakelola. Prinsip-prinsip minimal tersebut harus dipenuhi dalam melakukan tatakelola yang baik dari sebuah sistem. Secara ringkas disajikan pada tabel 4. Dalam tabel nampak bahwa review independen diperlukan dalam sebuah tatakelola yang baik.

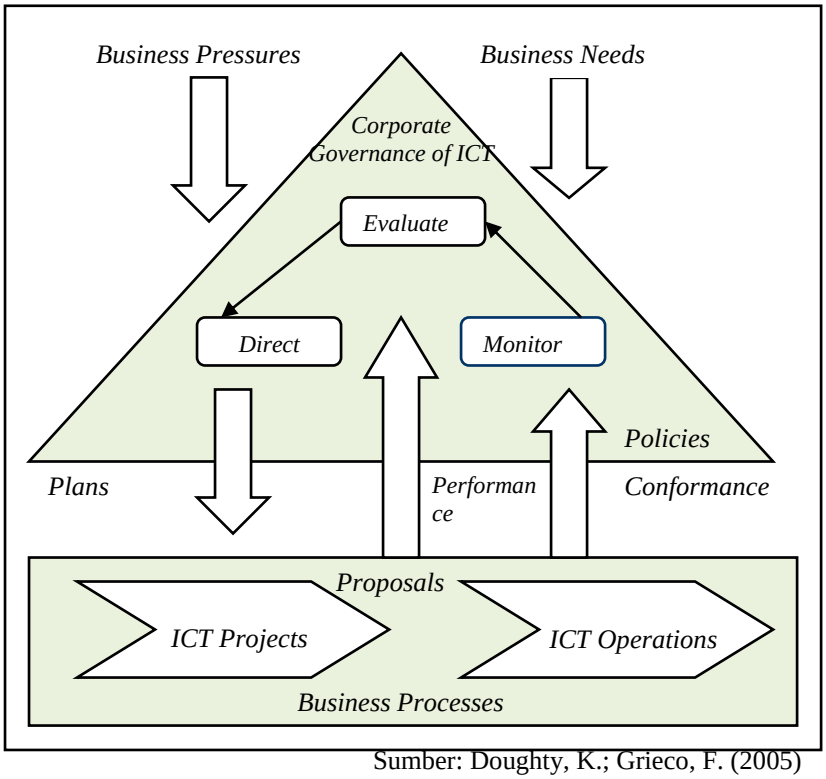
Tabel 4
Prinsip Tatakelola TI

• ***Clear expectations***	• ***Responsible and clear handling of business operations***
– Clear values	*– Competent organizational structure*
– Explicit policies and standards	*– Orderly processes*
– Strong communication	*– Effective use of technology*
– Clear strategy	*– Responsible asset management*
• ***Independent review and continuous improvement***	• ***Timely and accurate disclosures***
• ***Proactive change management***	

Sumber: Hamaker, S; Hutton, A. (2004)

Secara keseluruhan tujuan dari tatakelola TI adalah untuk memfasilitasi dan meningkatkan kemampuan organisasi untuk memberikan informasi yang baik mengenai keputusan yang berkaitan dengan TI ke dalam operasi, program, dan pelayanan jangka pendek dan jangka panjang. TI harus meningkatkan kemampuan akses, komprehensif dan kecepatan informasi yang mendukung pembuatan keputusan dalam organisasi. Rerangka kerja tatakelola TI dapat dilihat dalam gambar 3.

Gambar 3
***Scorecard* Perspektif Tatakelola TI dan Hubungan Sebab Akibat**



Sumber: Doughty, K.; Grieco, F. (2005)

Dalam memberikan keterangan gambar yang diberikan Doughty, K.; Grieco, F. (2005), rerangka kerja yang disajikan dalam gambar 3 harus terstruktur dan melibatkan: Perencanaan, kebijakan, petunjuk dan standar yang memberi penuntun, struktur dan tanggung jawab, dan proses. Seluruh elemen dalam tatakelola harus berfungsi dengan semestinya. Kegagalan

dalam satu elemen menyebabkan kegagalan tatakelola tersebut. Lebih lanjut, dalam tatakelola TI akan melibatkan berbagai macam pihak. Stakeholder kunci dalam proses tersebut meliputi: IT steering committee, Board audit committee, IT management, Project sponsor, Project director/manager, Business unit managers. Semua stake holder memegang peran yang sama besar dalam tatakelola TI.

Di dalam proses tatakelola TI seorang auditor memegang peran dan tanggung jawab yang cukup signifikan. Peran yang dipegang seorang auditor tidak sekedar memberikan evaluasi sistem., auditor juga harus mejaga hubungan dengan stakeholder kunci lainnya. Review independen dari manajer senior dana komite audit dapat sangat membantu dalam memastikan pengeluaran TI dan aktivitas dapat diarahkan dengan tujuan dan strategi organisasi. Selanjutnya, sistem pelaporan harus memberikan informasi yang relevan, akurat dan tepat waktu. Fungsi audit biasanya berada pada posisi unik untuk memberikan opini yang independen dan objektif yang berkaitan dengan inisiatif dan proses TI. Secara umum proses audit berfungsi untuk memberikan:

- Analisis dan opini independen pada kelayakan pengendalian termasuk alur dan akurasi informasi.
- Saran ahli untuk mengembangkan pengendalian atau memperbaiki kekurangan yang ada.

Kefektivan peran tersebut tergantung pada hubungan dengan stakeholder kunci. Hubungan baik dengan stakeholder dapat membuat auditor berperan dengan baik. Dalam prosesnya seorang auditor harus memperingatkan manajer mengenai perbaikan kelemahan sistem pengendalian, jika manajer menolak, auditor harus mengangkat lagi isu tersebut, jika diterima, tingkatan isu ke arah level manajemen yang lebih tinggi.

E. PROSES AUDIT TI

Tidak ada satupun definisi umum dari audit sistem informasi, Ron Weber dalam Sayana, S. A. (2002), mendefinisikan sebagai proses dari pengumpulan dan evaluasi bukti untuk mendeterminasikan apakah sistem komputer (sistem informasi) keamanan (safeguard) aset, pemeliharaan integritas data, mencapai tujuan organisasi secara efektif dan penggunaan sumber daya secara efisien. Luas pemrosesan komputer yang digunakan dalam aplikasi akuntansi signifikan, seperti kompleksitas pemrosesan tersebut, akan berpengaruh terhadap sifat, waktu, dan luas prosedur audit. (Wilkinson J.W.; Cerullo M.J.; Raval V; Wong-on-wing B.; 2003). Penyebab utama pengaruh tersebut dikarenakan bergesernya bukti audit menjadi bukti elektronik. Di samping itu, TI memungkinkan transaksi *real time* yang mempengaruhi perilaku bukti menjadi terus berubah. Dalam kasus tersebut peran audit berkelanjutan sangat dibutuhkan.

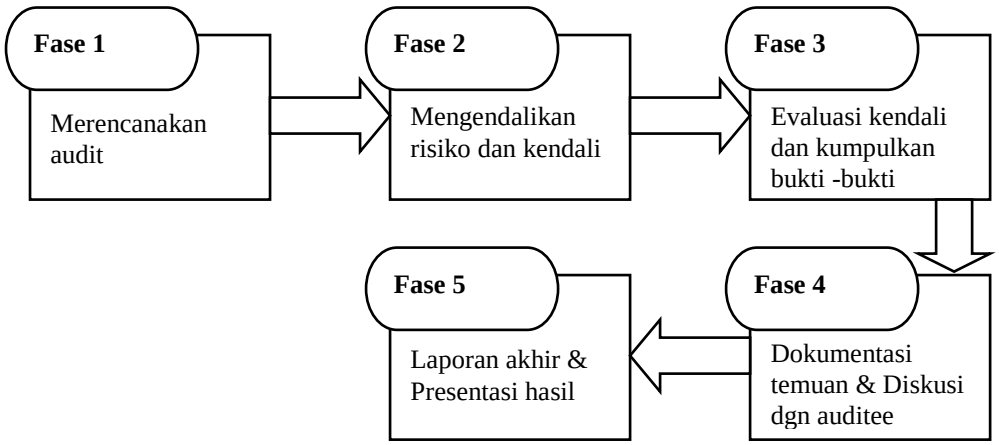
Cakupan audit TI sedikitnya enam komponen yang sangat esensial. Antara lain: pendefinisian tujuan perusahaan; penentuan isu, tujuan dan perspektif bisnis antara penanggung jawab bagian dengan bagian TI; review terhadap pengorganisasian bagian TI yang meliputi perencanaan proyek, status dan prioritasnya, staffing levels, belanja TI dan IT change process management; assessment infrastruktur tekhnologi, assessment aplikasi bisnis; serta temuan-temuan, dan laporan rekomendasi. Subyek **audit TI** lebih terfokus pada keamanan, keandalan, kinerja dan *manageability* (eBizzAsia, Volume II No 17 - Mei - Juni 2004)

Sistem informasi dan TI merupakan dua hal yang tidak dapat dipisahkan. Pendekatan yang digunakan dalam audit SI dapat dipastikan selalu mencakup peran dan pengaruh TI terhadap sistem. Di dalam audit sistem review terhadap TI mutlak diperlukan. Sayana, S. A. (2002) memberikan tujuan audit TI yaitu untuk mereview dan memberikan *feedback*, jaminan dan saran. Hal tersebut dapat dikelompokan dalam tiga kelompok yaitu; *Availability, Confidentiality, dan Integrity*. Lebih lanjut Sayana, S. A. (2002), dalam mengaudit sistem

informasi tidak hanya pada audit komputer tetapi juga harus melibatkan elemen: review lingkungan dan fisik, review administrasi sistem, review software aplikasi, review keamanan jaringan, review kelangsungan bisnis, dan review integritas data.

Sesuai dengan standar auditing ISACA (*Information Systems* Audit *and Control Association),* selain melakukan pekerjaan lapangan, auditor juga harus menyusun laporan yang mencakup tujuan pemeriksaan, sifat dan kedalaman pemeriksaan yang dilakukan. Laporan ini juga harus menyebutkan organisasi yang diperiksa, pihak pengguna laporan yang dituju dan batasan-batasan distribusi laporan. Laporan juga harus memasukan temuan, kesimpulan, rekomendasi sebagaimana layaknya laporan audit pada umumnya. Metodologi secara umum yang dapat dilakukan oleh auditor digambarkan pada gambar 4.

Gambar 4
Metodologi Audit TI



Sumber: eBizzAsia, Volume II No 17 - Mei - Juni 2004

Secara prinsip dasar proses audit TI mirip dengan proses audit manual yang tidak berbasis TI. Perbedaan hanya pada audit berbasis TI penekanannya pada penilaian risiko dilakukan lebih banyak. Pada proses auditor berbasis TI diperlukan pendekatan berbeda dengan dibantu dengan software audit. Peran software tersebut membantu tugas auditor untuk mereview bukti audit elektronik. Software akan sangat membantu terutama dalam kecepatan dan keakuratan penilaian mengingat bukti transaksi yang berbentuk elektronik bisa mencapai ribuan.

Meskipun demikian, penggunaan software audit tidak dapat secara otomatis digunakan begitu saja. Ada beberapa persyaratan yang harus dipenuhi sebagai berikut (Sayana, S. A.; 2003):

- *Connectivity and Access to Data*. Auditor harus memperoleh akses pada data secara *"live".*
- *Knowledge of the Application and Data.* Setelah data diperoleh, auditor harus mempunyai pengetahuan mengenai file atau tabel dimana data berada yang juga dibutuhkan. Auditor juga memerlukan deskripsi data dan file dan kode file yang digunakan. Disamping itu kemampuan teknis mengenai software yang digunakan juga harus dimiliki.
- *Audit Skills and Identifying the Concerns*. Setelah data di-*download* auditor harus mempunyai kemampuan teknis dalam menggunakan software. Atau bahkan kemampuan me-*download* data itu sendiri.

Dengan kemajuan TI dan penggunaan software, memberikan manajemen dan auditor kemampuan untuk melakukan audit dan monitoring berkelanjutan. Perkembangan tersebut memungkinkan pengitegrasian tekhnologi dengan audit berkelanjutan. Meskipun demikian, dua hambatan terbesar berasal dari sisi teknis klien dan pelatihan staff (Sarva, S.; 2006).

Klien cenderung tidak suka pada monitoring secara berkelanjutan, sedangkan audit memerlukan seluruh akses informasi dalam perusahaan. Untuk melakukan audit berkelanjutan, auditor mengembangkan program yang secara rutin bekerja pada proses bisnis normal setiap hari.

Metodologi audit secara berkelanjutan dapat dibagi menjadi tiga area level data, yang mana merupakan area dasar dari pemeriksaan data (Sarva, S.; 2006):

- *Keystroke level*. Untuk keberhasilan kebijakan auditing berkelanjutan analisis statistis dari setiap *keystroke* utuk operasi utilitas data base adalah kegiatan yang esensial.
- *Transaction level*. Secara umum transaksi divalidasi pada saat dimasukan pada software aplikasi.
- *Transaction pattern level*. Memonitor *keystroke* secara dinamika dan menjalankan CAAT adalah perangkat audit yang kuat pada transaksi *real time*. Pada level in, memonitor data melampaui perioda waktu menggunakan *expert system* dan kriteria berbasis aturan. Level ini juga memfasilitasi auditor untuk membuktikan dan melaporkan penilaian pengendalian internal manajemen.

Proses audit yang baru dan berbasis TI akan memerlukan strategi baru untuk menghadapinya. Pada sesi berikutnya akan dibahas strategi untuk menghadapinya.

F. STRATEGI AUDIT TI

Perubahan risiko, proses bisnis dan peran auditor dalam lingkungan baru yang berbasis TI memaksa auditor untuk menggunakan strategi baru dalam melaksanakan tugas auditing yang diterimanya. Strategi yang digunakan dan diterapkan harus secara komprehensif dapat menampung seluruh kebutuhan audit baru. Kebutuhan baru tersebut berbentuk karena pengaruh TI terhadap seluruh aspek auditing, mulai dari standar, fokus auditing, risiko yang dihadapi sampai teknis pelaksanaan auditing yang mungkin dilakukan.

Berkaitan dengan standar, peraturan, dan struktur organisasi Milus, S., (2004), memberikan suatu strategi audit secara komprehensif. Komponen auditing tersebut adalah:

Dukungan organisasional yang tinggi. Menurut definisi, strategi auditing komprehensif mengartikanya dapat melihat seluruhnya dan dipalikasikan pada setiap orang. Dan ketika setiap rang sepakat untuk bekerja sama, untuk lebih efisien dan efektif maka akan muncul berbagai macam sudut pandang dan cara pikir. Untuk mejaga proses berjalan sesuai jalur diperlukan satu pengambil keputusan.

Kebijakan keamanan informasi perusahaan. Kebijakan menjadi konstitusi yang digunakan perusahaan sebagai dasar pengambilan keputusan masa yang akan datang dan menentukan batasan pemenuhan. Konstruksi dari kebijakan harus berdasarkan standar yang *god practice* (misal; terdapat pada tabel 3). Standar tersebut tidak hanya memberikan penghematan waktu tetapi juga mengijinkan organisasi membangun fondasi yang sudah diakui.

Satu badan pengendalian. Pusat dari strategi audit komprehensif terletak pada rerangka kerja pengendalian – satu set aturan yang mana dapat dibangun melalui audit dan penilaian. Seperti pada lingkungan yang didukungnya, satu set aturan yang mengadopsi tekhnologi baru atau menemukan kelemahan baru. Hal tersebut digunakan untuk mendeterminasikan apa yang diaudit dan memastikan bahwa seluruh area yang membutuhkan inspeksi telah diispeksi. Dengan kata lain, hal tersebut mengkoordinasi dan mengintegrasi aktivitas auditing yang banyak.

Selain pendekatan audit komprehensif, Gallegos, F.; Smith, M. L., (2006), dalam artikelnya menggunakan pendekatan red teams dalam penjaminan informasi. Taktik *red team* muncul dari dunia keamanan jaringan yang sering diganggu *Black-hat hackers*. Banyak organisasi melakukan perjanjian dengan *White-hat hackers* selama penilaian keamanan atau audit yang bekerja sama dengan *red team*. *Red team* terdiri dari individu-individu yang

mempunyai kemampuan untuk melakukan *hacking* yang etis, menemukan kelemahan dari sistem keamanan perusahaan dan melaporkan kembali pada organisasi untuk diperbaiki. Konsep red team muncul dapat membantu perancang strategi dalam menyusun strategi dengan cara:

- Memberikan pengganti saran dengan kemampuan yang lebih tajam dalam mendeteksi kelemahan yang mungkin dapat dihindari dari lawan yang mungkin muncul dan meningkatkan pemahaman dari respon yang tersedia untuk lawan dan competitor.
- Memainkan "*devil advocate*". Red team dapat menawarkan alternatif yang berbeda pada perencanaan, operasi, proses, dan asumsi yang sedang berjalan.
- Menawarkan judgment ekternal pada organisasi dan bertindak seperti "*sounding board*" untuk ide baru yang mungkin muncul dari perjanjian dengan red team.

Auditor sistem informasi dapat menggunakan metoda red team untuk memperoleh pemahaman yang lebih baik ancaman keamanan yang muncul dan baru, dan membuat pembuktian yang dapat dilakukan untuk membuat kasus untuk perubahan fundamental dalam praktik keamanan organisasi. Auditor yang menggunakan red team dapat memberikan opini ekternal dalam membangun praktik keamanan organisasi. Dalam penilaian risiko, auditor harus menggunakan kategori *best practice* untuk mengkategorikan risiko dengan tegas.

Di dalam lingkungan bisnis *E-commerce* yang berhubungan langsung dengan dunia maya, seorang auditor dapat menggunakan strategi yang berbeda, mengingat setiap proses bisnis mempunyai karakter yang unik. Di dalam dunia maya, organisasi dan proses transaksi terjadi secara abstrak dan imajiner. Pertanyaan berikutnya, apa peran auditor dalam kondisi seperti itu?

Auditor harus tetap melaksanakan peran audit untuk mengidentifikasi risiko dan mengugkapkan secara relatif pada *e-commerce*, memastikan pengendalian tersedia untuk mengurangi risiko dan mengevaluasi kefektivan pengendalian tersebut. Lebih lanjut, strategi audit harus diperluas untuk memasukan peningkatan level kepedulian manajer dan dewan direksi pada (Paliotta, A. R.; 2001):

- Signifikansi proteksi dan keamanan informasi relatif pada rencana E-commerce dan keberadaan risiko yang dapat membahayakan rencana tersebut.
- Rasionalisasi bahwa masyarakat umum tidak siap untuk menerima argumen bahwa pemecahan tekhnologi saat ini yang berkaitan dengan keamanan informasi adalah memuaskan.
- Simpulanya, hasilnya, keamanan informasi harus ditunjukan sebagai strategi dasar isu bisnis, dan tidak hanya isu audit atau tekhnologi.

G. TEKNIK AUDIT TI

Setelah strategi tersusun, pertanyaan selanjutnya adalah, bagaimana secara teknis audit lingkungan TI dapat dilakukan? Penggunaan pendekatan audit yang terstruktur merupakan persyaratan utama untuk melaksanakan audit dalam lingkungan apapun. Secara garis besar teknik audit yang berkaitan dengan pemrosesan data elektronik yang berbasis komputer dapat dibagi menjadi (Wilkinson J.W.; Cerullo M. J.; Raval V; Wong-on-wing B.; 2003):

1. Auditing around the computer → pendekatan ini memperlakukan komputer sebagai **black box.** Pada intinya pendekatan ini berfokus pada input dan outputnya.
2. Auditing through the computer → pendekatan ini membuka **black box** dan secara langsung berfokus pada langkah pemrosesan dan edit check dan check yang terprogram. Pendekatan ini menangani aplikasi pemrosesan real time dan periodic secara langsung dimana audit trail terpengaruh.
3. Auditing with the computer → pendekatan ini menggunakan baik mainframe atau microcomputer untuk membantu di dalam melakukan langkah-langkah pada program

audit terperinci. Prosesnya menggunakan tekhnologi informasi pada auditan. Pendekatan ini terbagi dua :

- Microcomputer Audit-Assist Software → melakukan audit dengan bantuan microcomputer atau laptop dengan paket software yang tersedia, misalnya excel
- Audit Software → menggunakan software audit selama menguji subtantif atas file record perusahaan. Contohnya; GAS (Generalized audit Software)

Penggunaan software audit mempunyai beberapa persyaratan dan keuntungan (telah diuraikan pada sub bab proses audit TI). Disamping itu, pendekatan lain yang dapat dilakukan dengan pendekatan red team seperti dalam strategi audit. Pendekatan ini berfokus pada risiko dan siklus pengamanan yang dapat dilakukan.

Meskipun demikian, pertanyaan selanjutnya adalah apakah teknik yang telah disebutkan tersebut dapat 100% mencakup kebutuhan audit di lingkungan TI yang terus berkembang? Dalam mengadopsi prinsip *best practice* dalam menterjemahkan risiko seorang auditor harus memonitor apa yang terjadi di dalam lingkungan organisasi secara kontinyu. Paul E.; Lindow; Race, J. D.(2002), memberikan perbandingan keterlibatan peran auditor (internal) pada pendekatan tradisional dan progresif (*best practice*). Pendekatan tradisional mengambil satu titik (*snapshot*) untuk di audit sedang pendekatan progresif mengikuti setiap proses yang berjalan . perbandingan tersebut dapat dilihat pada tabel 5.

Tabel 5
Pendekatan Tradisional VS Progresive

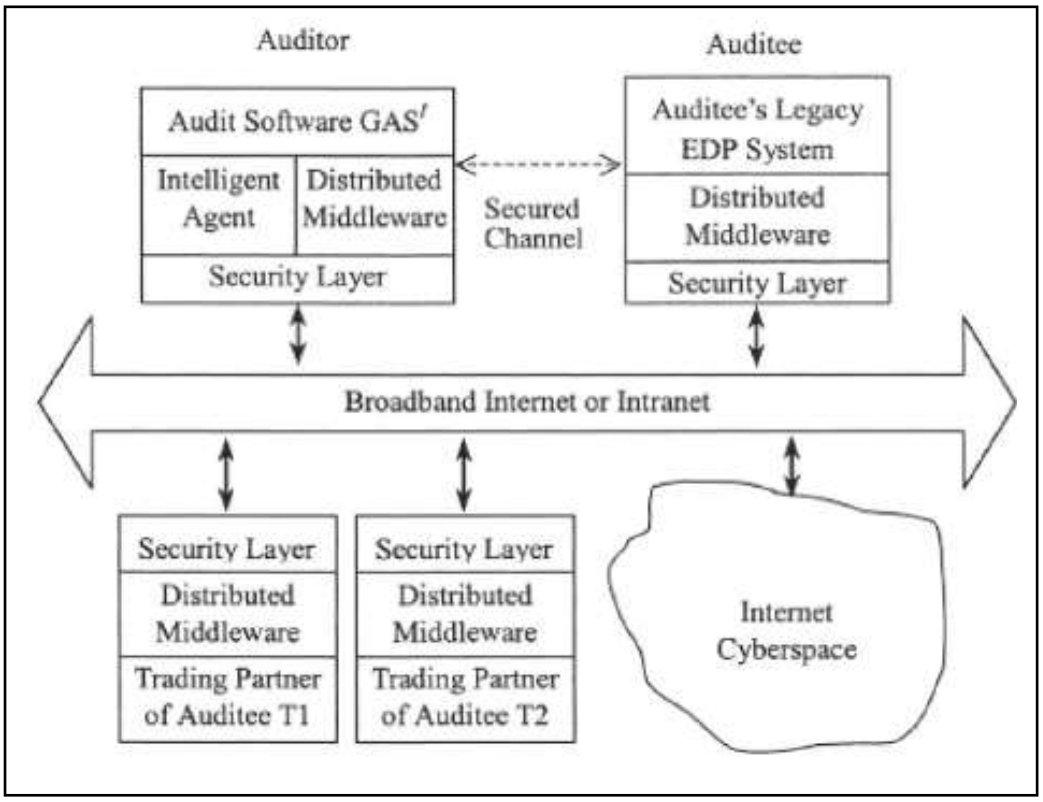
Traditional	***Progressive (best practices)***
Audit focus	*Business focus*
Transaction-based	*Process-based*
Financial account focus	*Customer focus*
Compliance objective	*Risk identification, process improvement objective*
Policies and procedures focus	*Risk management focus*
Multiyear audit coverage	*Continual-risk-reassessment coverage*
Policy adherence	*Change facilitator*
Budgeted cost center	*Accountability for performance improvement results*
Career auditors	*Opportunities for other management positions*
Methodology: Focus on policies, transactions and compliance	*Methodology: Focus on goals, strategies and risk management processes*

Sumber: Paul E.; Lindow; Race, J. D.(2002).

Lebih lanjut, untuk melaksanakan audit di lingkungan internet dan intranet pendekatan audit diatas tidak dapat memenuhi kebutuhan audit. Pada lingkungan internet, audit harus dilakukan secara kontinyu dan komprehensif dengan mempertimbangkan faktor keamanan dari proses audit tersebut karena di lingkungan internet dan intranet, sangat terbuka dan dapat lubang keamanan yang dapat disusupi lebih banyak dan sensitive.

Pendekatan audit yang digunakan harus komprehensif dan melibatkan semua pihak dalam organisasi dan harus terintegrasi dengan sangat baik. Rerangka kerja yang dapat digunakan dapat dilihat pada gambar 5.

Gambar 5
Rerangka Kerja Audit Elektronik



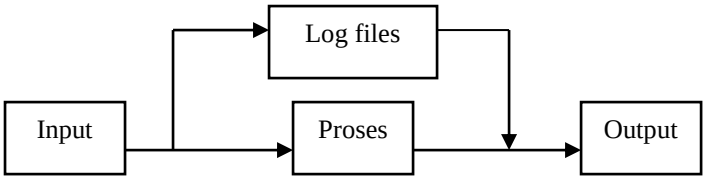
Sumber: Shaikh, J. M., (2005)

Dari gambar dapat dilihat bahwa dilihat bahwa seluruh aktivitas auditing, auditee dan partner perdagangan auditee terhubung dalam satu broadband yang terhubung dengan langsung dengan internet. Pada posisi tersebut peran security layer untuk mengamankan seluruh kegiatan ekonomi perusahaan dengan partner dan kegiatan auditor dari pencurian data oleh pihak lain. Pada kondisi tersebut, hubungan baik antara auditor dengan auditee sangat diperlukan.

Rerangka kerja yang digambarkan pada gambar 5 dapat digunakan auditor sebagai panduan dalam melakukan audit di lingkungan internet. Teknik yang digunakan dapat berfokus pada kefektivan security layer dalam mejaga keamanan data sebagai jaminan kualitas data disamping teknik lain yang mungkin dilakukan.

Suatu teknik yang lazim dilakukan oleh auditor untuk mejaga audit trail khususnya pada lingkungan terkomputerisasi baik yang *online* maupun *off line* adalah dengan menempelkan software pada komputer klien. Alles, M.; Kogan, A.; Vasarhelyi, M., (2003), menyarankan satu teknik yang disebut Black Box logging (BB log). Konsep BB log adalah menempelkan software yang mencatat seluruh kegiatan yang terjadi dalam organisasi dalam suatu file log yang tidak dapat dihapus maupun di edit. Konsep BB log ini juga dapat digunakan untuk lingkungan bisnis yang menggunakan aplikasi ERP, SAP, EDI dan lain-lain. Mekanisme dapat dilihat pada gambar 6.

Gambar 6
Mekanisme BB log



Pada gambar 6 terlihat bahwa log file akan terbentuk secara bersamaan ketika proses berlangsung. Log files akan merekam seluruh kegiatan dalam proses dari input sampai output yang dihasilkan. Teknik audit ini dapat digunakan untuk mengatasi keterbatasan waktu auditor dalam mengikuti seluruh aktivitas perusahaan. Dengan BB log dapat mengatasi permasalahan perolehan jejak audit pada transaksi *real time* akibat penggunaan TI dalam oprasional perusahaan.

H. SIMPULAN

Perkembangan TI dewasa ini sudah tidak dapat dihindari lagi. Pada kondisi tersebut seorang auditor dituntut mempunyai ketrampilan dan pengetahuan lebih akibat pergeseran perspektif proses bisnis. Pergeseran bukti audit dari bukti yang berbasis kertas menjadi bukti elektronik merupakan tantangan baru bagi auditor. perubahan tersebut berdampak pada seluruh segi audit. Perspektif audit yang pada mulanya beorientasi pada tugas mulai bergeser ke arah orientasi risiko. Pada kondisi tersebut, penilaian risiko dan keamanan TI menjadi isu yang sangat penting. Untuk dapat memberikan penilaian risiko dan keamanan dengan tepat, seorang auditor harus mengerti posisinya dalam tatakelola TI di dalam perusahaan sehingga auditor tidak salah kaprah dalam memberikan pendapat dan berperan dalam perusahaan yang menuju ke arah penggunaan TI. Pergeseran tersebut juga berdampak pada strategi dan teknik yang digunakan dalam audit TI. Strategi harus dikembangkan agar dapat mencakup seluruh aspek akibat otomatisasi proses bisnis baik secara langsung maupun tidak langsung. Akibat perubahan strategi yang berbasis TI, teknik audit secara simultan berubah pula. Perubahan dilakukan untuk mengatasi perubahan strategi dan lingkungan bisnis.

Ringkasnya, dalam menghadapi perubahan lingkungan bisnis seorang auditor harus dapat menyesuaikan diri dengan kecepatan paling tidak sama dengan perubahan lingkungan. Penyesuaian itu tidak hanya pada satu sisi saja tetapi harus secara menyeluruh mencakup seluruh sendi audit. Yang menjadi pertanyaan berikutnya adalah apakah auditor mampu menjawab tantangan itu atau akan kalah dan tersingkir?

DAFTAR PUSTAKA

Alles, M.; Kogan, A.; Vasarhelyi, M., (2003), Black Box Logging and Tertiary Monitoring of Continuous Assurance Systems, *Information Systems Control Journal*, Volume 1.

Bakshi, S. (2004) Control Self-assessment for Information and Related Technology, ? *Information System Control Journal,* Volume 1.

Bierstaker, J. L; Burnaby, P.; Thibodeau, J. (2001). The Impact Of Information Technology On The Audit Process: An Assessment Of The State Of The Art And Implications For The Future, *Managerial Auditing Journal*,16/3 pp. 159-164.

Cerullo, M. J.; Cerullo, V. (2005),Threat Assessment and Security Measures Justification for Advanced IT Networks, *Information System Control Journal,* Volume 1.

Dimitriadis, C.K; Polemi, D. (2004), Biometrics—Risks and Controls, *Information System Control Journal*, Volume 4.

Doughty, K.; Grieco, F. (2005), IT Governance: Pass or Fail?, *Journal Online*, www.isaca.org.

eBizzAsia, (2004) Bagaimana Audit TI Dilakukan?, *eBizzAsia*, Volume II No 17 - Mei - Juni 2004. http://www.ebizzasia.com/0217-2004/focus,0217,04.htm 16 Mar 2007

Frownfelter-Lohrke, C.; Hunton, J. E. (2002). New Opportunities for Information Systems Auditors: Linking SysTrust to COBIT, *Information Systems Control Journal*, Volume 3

Gallegos, F., (2003), IT Audit Independence: What Does It Mean? *Information System Control Journal*, Volume 5.

Gallegos, F.; Smith, M. L., (2006), Red Teams: An Audit Tool, Technique and Methodology for Information Assurance, *Journal Online*, www.isaca.org.

Greene, F. (2002), A Survey of Application Security in Current International Standards, *Information Systems Control Journal*, Volume 6.

Hamaker, S; Hutton, A. (2004), Principles of IT Governance, *Information Systems Control Journal*, Volume 3.

ISACA Standards Board, (2002). Effect of Third Parties on an Organization's IT Controls, *Information System Control Journal*, Volume 4.

Milus, S., (2004), The Institutional Need for Comprehensive Auditing Strategies, *Information Systems Control Journal*, Volume 6.

Paliotta, A. R., (2001), Cybersecurity and the Future of E-commerce: The Role of the Audit Community, *Information Systems Control Journal*, Volume 2.

Paul E.; Lindow; Race, J. D.(2002), Beyond Traditional Audit Techniques, *Journal Of Accountancy*, July, pp. 28-33.

Rezaee, Z.; Reinstein, A. (1998) The Impact Of Emerging Information Technology On Auditing, *Managerial Auditing Journal*,13/8 pp. 465–471.

Sarva, S., (2006), Continuous Auditing Through Leveraging Technology, *Journal Online*, www.isaca.org.

Sayana, S. A. (2002), IT Audit Basics The IS Audit Process, *Information Systems Control Journal*, Volume 1.

Sayana, S. A., (2003), Using CAATs to Support IS Audit, *Information Systems Control Journal*, Volume 1.

Shaikh, J. M., (2005), E-Commerce Impact: Emerging Technology – Electronic Auditing, *Managerial Auditing Journal*, Vol. 20 No. 4, pp. 408-421.

Stanley, R. A. (2004). Security, Audit and Control Issues for Managing Risk in the Wireless LAN Environment, *Information Systems Control Journal*, Volume 3.

Wilkinson J.W.; Cerullo M. J.; Raval V; Wong-on-wing B., (2003). *Accounting Information Systems: Essential concepts and Applications.* 4th ed. Wiley.