BIOMETRIC SECURITY: ALTERNATIF PENGENDALIAN DALAM SISTEM INFORMASI AKUNTANSI TERKOMPUTERISASI

Josua Tarigan
Staf Pengajar Fakultas Ekonomi - Universitas Kristen Petra
E-mail: josuat@peter.petra.ac.id

Abstrak: Adanya keinginan setiap organisasi untuk mencari metode pengamanan *authentication* yang lebih untuk akses *user*, dijawab dengan adanya teknologi *biometric security* yang mendapat perhatian yang cukup besar bagi organisasi. Implementasi teknologi *biometric security* cukup luas dalam sistem informasi akuntansi yaitu sebagai pengendalian pada *physical access, virtual access, e-commerce applications* dan *covert surveillance.* Dalam mengimplementasikan teknologi *biometric,* ada tiga tahapan yang harus dilakukan organisasi, yakni *strategic planning and budgeting, developing a system reliability plan* dan *documentation.* Tantangan yang akan dihadapi dalam mengembangkan teknologi *biometric* sebagai pengendalian dalam sistem informasi akuntansi yakni standarisasi, aplikasi teknologi *hybrid* dan manajemen siklus hidup pada *biometric security*.

Kata kunci: *authentication,* akses *user* dan *biometric security*.

Abstract: *As organization search more secure authentication method for user access, biometric security technology is gaining more and more attention. The implementation of biometric security technology in accounting information systems was physical access, virtual access, e-commerce applications and covert suveillance. There are three phase when an organization implementation biometric technology: strategic planning and budgeting, developing a system reliability plan and documentation. The challenges will face when develop biometric technology as control in accounting information system are standardization, hybrid technology uses, life cycle management.*

Keywords*: authentication, user access and biometric security.*

Sistem informasi akuntansi tentu saja bukan merupakan wacana yang baru lagi ketika berbicara mengenai *business process*, namun yang menjadi pertanyaaan adalah bagaimana pengendalian yang ada dalam sistem informasi akuntansi tersebut, sehingga sistem informasi akuntansi yang ada pada organisasi dapat diandalkan. Sistem informasi akuntansi yang dapat diandalkan adalah sistem yang mempunyai pengendalian memadai sehingga informasi yang dihasilkan oleh sistem tersebut dapat diandalkan untuk digunakan dalam pengambilan keputusan, dalam hal ini pengendalian merupakan elemen yang tidak dapat dipisahkan dari sistem informasi akuntansi yang ada (Romney and Steinbart 2003: 195). Menurut SysTrust dalam (Romney and Steinbart 2003: 226), ada 4 elemen

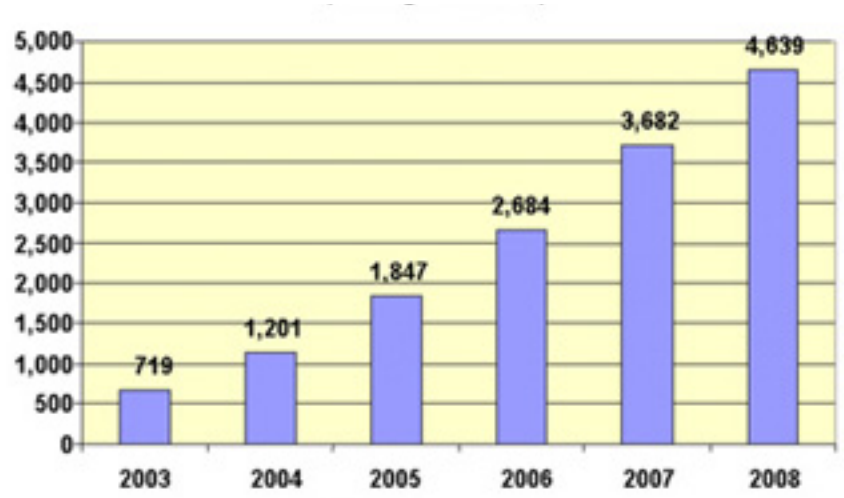
yang harus dimiliki oleh sebuah sistem yang dapat diandalkan: (1) *Availability*. Indikator ini menunjukkan bahwa sistem tersebut tersedia dan siap digunakan (2) *Security*. Sistem di lindungi dari akses yang diluar otorisasi (3) *Maintainability*. *Update* dan modifikasi yang dilakukan pada sistem tidak akan mempengaruhi *availability, security* dan *integrity* dari sistem yang ada (4) *Integrity*. Konsep ini berbicara mengenai proses yang dilakukan sistem akurat, lengkap dan tepat waktu.

Ernst & Young sebagai salah satu konsultan terkemuka, memberikan *awaraness* kepada organisasi-organisasi yang ada di dunia agar mempunyai kesadaran dalam hal pengendalian. Hal ini diungkapkan oleh Ernst & Young berdasarkan penelitian yang dilakukan pada tahun 2002. Penelitian yang melibatkan 450 CIO *(Chief Information Officer)* dan direktur di bidang teknologi informasi dari 16 negara ini menyimpulkan perlunya perusahaan-perusahaan di dunia memiliki *awareness* terhadap ancaman dan resiko yang muncul dalam lingkungan organisasi. Pengendalian yang tidak memadai akan menyebabkan kerugian berupa kehilangan atau kerusakan aset organisasi, misalnya kehilangan data yang berharga bagi organisasi (Ross 2003:9). Menurut data yang dikemukan oleh Presiden Information System Security Association, Carl Jackson bahwa permasalahan yang berhubungan dengan keamanan disebabkan oleh kesalahan manusia sebanyak 65% sedangkan 20% disebabkan oleh bencana alam dan 15% disebabkan oleh *fraud* (Romney & Steinbart 2003:192). Melalui data diatas kita dapat melihat bahwa 80% permasalahan yang disebabkan oleh manusia, baik *error* maupun *fraud* dapat dikurangi dengan mengembangkan pengendalian yang memadai, walaupun memang beberapa organisasi mencoba mengembangkan pengendalian untuk mengatasi bencana alam yang sebesar 20%. Isu mengenai pengendalian dalam sistem informasi memang sedang menjadi suatu wacana yang hangat dibicarakan publik, termasuk di Indonesia khususnya ketika sistem informasi KPU (Komisi Pemilihan Umum) ditembus oleh seorang mahasiswa teknologi informasi dari salah satu universitas di Yogyakarta (Donny: 2005).

Kegiatan akuntansi sebenarnya bukanlah kegiatan yang sangat rumit, meskipun juga tidak sederhana, namun seiring dengan perkembangan perusahaan, seringkali yang menjadi masalah adalah banyaknya data transaksi. Permasalahan akan muncul ketika banyaknya data transaksi yang harus diolah, sehingga kondisi akan membuat proses akuntansi yang semula sederhana menjadi rumit jika mengandalkan kemampuan manusia. Berbagai kelemahan manusia dapat menyebabkan terhambatnya kegiatan akuntansi, dimana pada saat mengalami kelelahan, ketelitian manusia akan mengalami penurunan, sehingga kesalahan dalam melakukan pemrosesan data dapat terjadi. Untuk mengatasi permasalahan maka dibutuhkan sistem pemrosesan data transaksi yang berbantuan teknologi, dalam hal ini disebut sistem informasi akuntansi terkomputerisasi. Penggunaan teknologi pada sistem informasi akuntansi tetap membutuhkan pengendalian yang memadai, dalam hal ini pengendalian yang dikembangkan dalam sistem informasi akuntansi yang terkomputerisasi menuntut adanya pengendalian yang berbantuan teknologi. Kondisi ini disebabkan untuk mendukung tingkat *relevancy* antara sistem yang ada dengan pengendalian yang dimiliki sistem tersebut. Banyak teknologi yang digunakan dalam *portfolio* mekanisme pengamanan yang dibutuhkan untuk melindungi *physical*

dan *logical asset* dimana teknologi *biometric* merupakan salah satu dari *portfolio* mekanisme yang secara khusus mengarah pada proses *authentication.*

Teknologi *biometric* merupakan teknologi yang digunakan untuk menunjukkan keaslian *(authentication)* dari individu yang melakukan akses terhadap aset organisasi. *Authentication* adalah konsep yang menunjukkan bahwa hanya mereka yang diijinkan saja *(authentic)* yang dapat mempunyai akses terhadap asset organisasi. *Biometric* bukan hanya digunakan dalam sistem informasi akuntansi, aplikasinya cukup luas. Menurut prediksi yang dilakukan oleh International Biometric Group, bahwa industri keamanan *biometric* mendapat peningkatan pemasukan yang cukup besar pada tahun 2007 jika dibandingkan tahun 2003 dapat dilihat pada gambar 1.



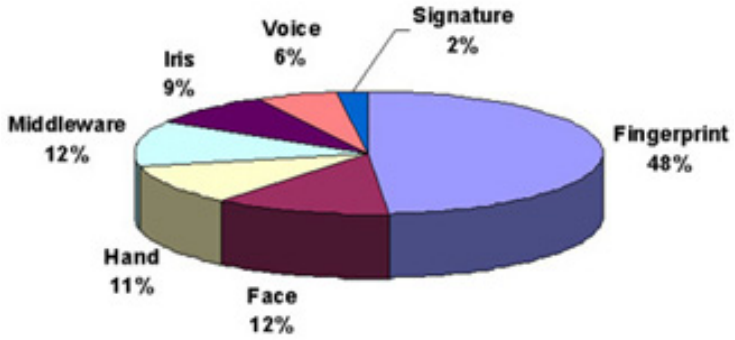
(Sumber: International Biometric Group 2004)

Gambar 1. Grafik Perkiraan Pendapatan pada Industri Biometric Security (dalam jutaan US$)

Memang *forecasting* tidak selalu menjadi kenyataan, namun *forecasting* yang berdasarkan data historis dan perhitungan yang cermat merupakan sesuatu yang perlu diperhitungkan. Gambar 3 akan lebih diperjelas dalam gambar 2, yang berisi informasi mengenai penyebaran pendapatan dalam beberapa teknologi *security* yang merupakan lingkup *biometric security*.

Implementasi *biometric security* juga dilakukan oleh pemerintah Singapura, yang saat ini sedang merencanakan penggunaan paspor *biometric* pada oktober 2005 dan saat ini 9000 penduduk Singapura yang bekerja di *airlines* telah bersedia untuk melakukan uji coba paspor *biometric* selama 6 bulan. Paspor ini memuat data-data pribadi pemiliknya, seperti bentuk muka, sidik jari, dan bahkan pola selaput pelangi mata atau iris. Semua data ini, akan disimpan dalam sebuah *chip* memori yang termuat dalam paspor *biometric.* Hal yang lebih menarik lagi adalah ketika para pemilik paspor lama tidak perlu mengganti jika paspor tersebut sudah kadaluarsa, yang perlu dilakukan hanya menambahkan

chip ini ke dalam paspor yang sekarang dimiliki. Penggunaan paspor teknologi *biometric* ini dilakukan oleh pemerintah Singapura sebagai respon untuk meningkatkan keamanan dalam negeri (Radio Singapore International 2004). Kondisi ini bukan hanya terjadi di Singapura, IBM sebagai industri yang bergerak dalam bidang produsen *notebook* juga berencana akan menerapkan teknologi *biometric* sebagai salah satu pengamanan notebook terbaru *(notebook thinkpad)* yang akan dikeluarkan oleh perusahaan ini (SPI 18: 2005)



(Sumber: International Biometric Group 2004)

Gambar 2. Penyebaran Pendapatan diantara Biometric Security

Penerapan teknologi *biometric* ini ternyata juga bukan hanya digunakan di luar negeri, di Indonesia ternyata fenomena ini sudah kelihatan, contohnya PT Legoso Securinfo dan juga PT. DataSript yang sudah menawarkan penerapan teknologi *biometric* pada sistem absensi, dengan menggunakan *fingerprint*. Hal ini juga diikuti dengan munculnya tas *biometric* yang dirancang oleh Universitas Indonesia khusus untuk tas wanita (jawapos.com).

Pembahasan dalam tulisan ini akan diarahkan pada elemen *security*, sebagai salah satu elemen yang harus dimiliki oleh sebuah sistem yang *reliable*. Dalam pendekatan *security* ini akan diperkenalkan teknologi *biometric*, sebagai alternatif teknologi yang dapat digunakan sebagai pengendalian dalam sebuah sistem informasi akuntansi.

PENGENDALIAN PADA SISTEM INFORMASI AKUNTANSI TERKOMPUTERISASI

Sistem informasi akuntansi yang terkomputerisasi, tentu saja tidak bisa dilepaskan dari aspek teknologi informasi yang mempengaruhi sistem informasi akuntansi. Sistem informasi akuntansi yang terkomputerisasi semakin banyak digunakan pada kondisi sekarang karena biaya *hardware* dan *software* yang sudah mulai dapat dijangkau oleh organisasi, bahkan sistem informasi akuntansi yang terkomputerisasi juga dapat diperoleh melalui *web browser*. Sistem informasi akuntansi yang berbasis *web*, seperti yang ditawarkan oleh NetLedger dapat diakses dari seluruh dunia. Tiga keuntungan sistem informasi akuntansi yang terkomputerisasi dibandingkan sistem manual (Warren 2005:250), yaitu: (1)

Menyederhanakan proses pencatatan dan penyimpanan data. Transasksi dicatat secara elektronik dan pada waktu bersamaan diposting secara elektronik ke buku besar dan buku besar pembantu (2) Sistem komputerisasi biasanya lebih akurat dibandingkan sistem manual (3) Sistem komputeriasi menyediakan informasi bagi manajemen dengan informasi saldo akun yang *realtime,* hal ini disebabkan posting yang dilakukan secara langsung dari jurnal ke buku besar pada saat yang bersamaan.

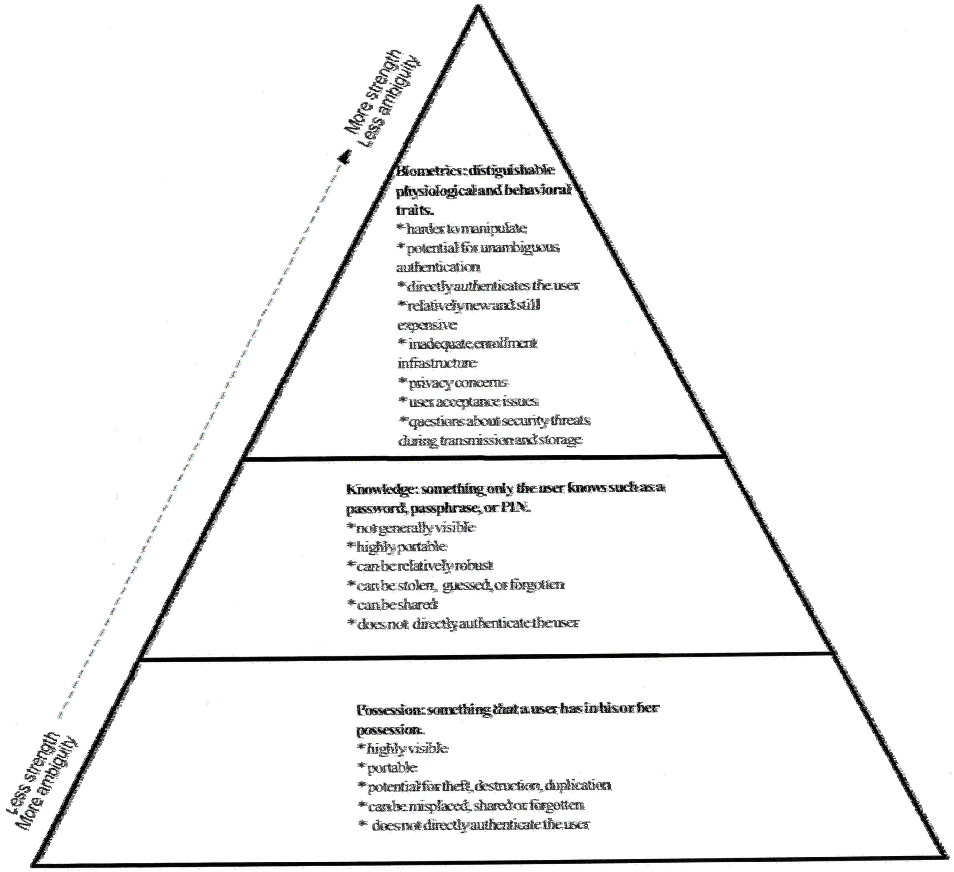
Pengendalian yang dibutuhkan pada kondisi sistem informasi akuntansi terkomputerisasi tentu saja akan berbeda dengan sistem informasi akuntansi manual, sehingga dalam konteks sistem informasi akuntansi yang berbantuan teknologi juga akan membutuhkan pengendalian yang berbantuan teknologi. Dalam memenuhi kebutuhan ini, maka teknologi *biometric security* merupakan alternatif yang dapat dipertimbangkan dalam pengendalian sistem informasi akuntansi yang terkomputerisasi. Teknologi *biometric security* merupakan pengendalian yang dibutuhkan dalam sistem informasi terkomputerisasi, dalam konteks menentukan *authentication*. Konsep *something you are* yang dikembangkan menjadi teknologi *biometric* merupakan model *authentication* yang paling akurat dibandingkan kedua model *authentication* yang ada. (Chandra and Calderon 2003:54).

Organisasi profesi dalam bidang akuntansi sebenarnya telah banyak memberikan kontribusi dalam memunculkan ide terhadap kerangka dan standar yang berkenaan dengan pengendalian dalam suatu *business process* dan lebih khusus pada sistem informasi akuntansi. Struktur Pengendalian Internal (SPI) yang terdiri dari lima komponen pengendalian yang ada sekarang, merupakan hasil pengembangan yang dilakukan oleh COSO (Committee of Sponsoring Organizations) yang merupakan aliansi dari beberapa organisasi profesi akuntansi, seperti American of Accounting Association (AAA), American Institute Certified Public Accountant (AICPA), Institute of Internal Auditor (IIA), Institute of Management Accountants (IMA) dan Financial Executive Institute. Selain SPI juga dikembangkan pengendalian yang digunakan untuk sistem komputerisasi, yaitu COBIT (Control Objective for Information and Related Technology) yang dikembangkan oleh Information System Audit and Control Foundation (ISACF). Merupakan hal yang sangat tidak mungkin jika sebuah organisasi dapat melakukan *business process* tanpa adanya pengendalian yang ada dalam organisasi itu sendiri. Pengendalian itu merupakan sebuah sistem yang mencegah, mendeteksi dan melakukan perbaikan terhadap tindakan yang tidak sesuai dengan hukum yang ada (Weber 1999:35). Dua hal yang perlu diperhatikan dari definisi pengendalian tersebut, yang pertama berkenaan dengan kata sistem. Pengertian dari sistem adalah, seperangkat komponen yang berelasi antara satu elemen dengan elemen yang lain untuk mencapai satu tujuan (Romney and Steinbart 2003:2). Hal yang perlu diperhatikan disini adalah *password* maupun teknologi *biometric security* tidak bisa dikatakan sebagai pengendalian, jika password dan teknologi *biometric security* tersebut berdiri sendiri (Weber 1999:35). Namun jika Password dan teknologi *biometric security* tersebut berelasi dengan komponen yang lain untuk mencapai satu tujuan yakni; mencegah, mendeteksi dan melakukan perbaikan terhadap tindakan diluar hukum, maka password dan

biometric security dikatakan sebagai pengendalian. Jika berbicara mengenai teknologi *biometric security* maka *biometric security* merupakan komponen *information technology infrastructure* yang berperan sebagai teknologi pendukung dalam sistem. Hal kedua yang perlu digaris bawahi berkenaan dengan pengertian pengendalian adalah kata di luar hukum. Weber (1999:35), mendefinisikan di luar hukum ini sebagai tindakan yang *unauthorized, inaccurate, incomplete, redundant, ineffective* atau *inefficiient* ketika melakukan akses terhadap aset atau fasilitas dalam organisasi.

TEKNOLOGI *BIOMETRIC SECURITY*

Secara umum ada tiga model *authentication* yang digunakan dalam mengamankan aset sebuah organisasi (Liu & Silverman 2004) yaitu: (1) *Something you have (possession):* kunci atau kartu identitas (2) *Something you know (knowledge):* password, PIN atau kata kunci yang digunakan untuk melakukan suatu akses kedalam asset organisasi (3) *Something you are (biometric):* teknologi *biometric security*. Ketiga model tersebut dapat dilihat pada gambar 3

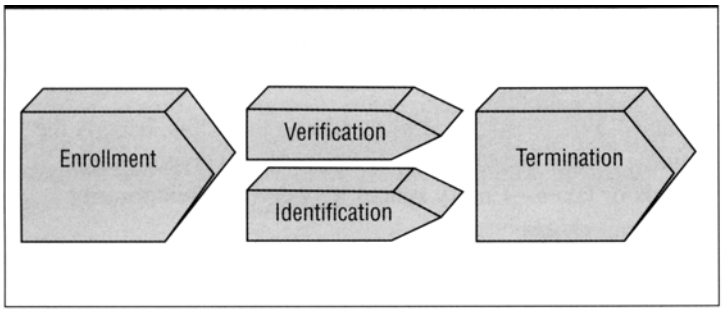


(Sumber: Chandra and Calderon 2003:54)

Gambar 3. *Authentication* Model

Gambar 3 menjelaskan tiga jenis model *authentication*, dimana teknologi *biometric* yang merupakan pendekatan *something you are* merupakan pendekatan *authentication* yang paling akurat, hal ini disebabkan karena keunggulan *biometric* diantara *model authentication* yang lain (Chandra and Calderon 2003:54, Ax-S Biometric 2005). Keunggulan tersebut adalah: (1) Sulit untuk dimanipulasi karena menggunakan konsep *something you are* (2) Memungkinkan dilakukan *audit trial* terhadap setiap kejadian yang ada, dimana melalui *biometric security* dapat diketahui: siapa yang melakukan akses terhadap aset organisasi *(who)*, dimana *(where)* dan kapan *(when)* individu tersebut melakukannya (3) Mencegah individu yang tidak mempunyai otorisasi untuk melakukan akses terhadap aset organisasi. Kondisi sangat memungkinkan terjadi kebocoran, jika menggunakan *password (something you know)* atau kartu *(something you have)*, dimana kartu yang dimiliki individu dapat dipinjamkan kepada individu yang lain atau hilang dan ditemukan oleh individu yang tidak mempunyai otorisasi (4) Sebagai solusi untuk kelemahan konsep *something you know,* yaitu adanya kemungkinan individu tidak dapat mengingat kembali *password* atau PIN untuk melakukan akses.

Biometric merupakan sistem yang membaca bagian tubuh manusia untuk mengenali keaslian *(authentication)*, dimana teknologi ini menggunakan bagian yang unik dan tetap dari tubuh manusia seperti sidik jari, selaput pelangi mata/ iris maupun wajah yang disimpan dalam database teknologi *biometric* (Liu & Silverman). Mekanisme kerja dari teknologi ini adalah mencocokkan antara data yang diterima melalui *biometric reader* dengan apa yang ada dalam database sistem *biometric* atau dengan kata lain membandingkan data yang sudah didefinisikan *(predifined data)* dengan data sekarang *(presented data)*. Dari perspektif dana investasi, teknologi *biometric security* tidak lagi tergolong investasi yang mahal, karena harga aplikasi *biometric* sudah mulai terjangkau oleh hampir semua lapisan organisasi, jika dibandingkan beberapa tahun sebelumnya (Byrne 2003:44), sehingga dalam hal ini teknologi *biometric security* dapat dipertimbangkan sebagai salah satu alternatif sebagai pengendalian dalam sistem informasi akuntansi.



(Sumber: Wallhoff 2003:39)

Gambar 4. *Biometric Process*

Tahapan yang terjadi dalam sistem pengendalian teknologi *biometric* terbagi dalam 4 tahap, yaitu: *enrollment, verification, identification* dan *termination* (gambar 4). Tahap *enrollment* merupakan tahap pengambilan *(capturing)* data oleh sistem melalui *biometric reader*. *Biometric reader* yang dipakai untuk *finger print* akan berbeda dengan dengan *biometric reader* untuk retina, namun untuk mekanisme kerja yang terjadi pada sistem yang ada tetap sama. Dalam *verification* dan *identification,* sistem akan mengambil data yang dimiliki oleh individu *(data presented)* dan membandingkannya dengan data yang terdapat pada *template (predefined data)*. Istilah *template* disini, merupakan data individu yang telah disetujui untuk melakukan akses terhadap aset atau fasilitas organisasi, dimana data tersebut disimpan dalam database sistem *biometric* atau data individu yang disimpan dalam *chip*. Pada tahap terakhir yakni tahap *termination,* sistem akan memutuskan, apakah individu tersebut merupakan individu yang *athentication* atau *non-athentication*. Aplikasi yang paling sering digunakan dalam *biometric security* adalah sidik jari *(fingerprint)* karena lebih ekonomis dan lebih komersial.

JENIS TEKNOLOGI *BIOMETRIC*

Penemuan pada berbagai jenis *biometric security* telah membuat adanya alternatif pilihan yang dapat dimplementasikan oleh organisasi. Beberapa teknologi *biometric security* yang ada dapat dilihat pada tabel 1, yang menunjukkan aplikasi penggunaan berbagai macam teknologi *biometric*, kelebihan yang dimiliki oleh *biometric security* dan beberapa kendala yang perlu diperhatikan dalam setiap aplikasi teknologi yang ada. Yang perlu diperhatikan adalah penyajian berbagai macam teknolgi *biometric security* tersebut bukan berbicara mengenai pemilihan teknologi *biometric* terbaik, namun lebih cenderung kearah bagaimana pemilihan organisasi terhadap *biometric security* yang lebih sesuai dengan kondisi organisasi. Penerapan teknologi *biometric* yang diaplikasikan pada suatu organisasi belum tentu menjadi pengendalian yang memadai bagi organisasi yang lain.

Tabel 1. Jenis Teknologi *Biometric Security*

Technology	***Description***
Hand Geometry	***Features:*** *evaluate the shape curves of the hand, some use three dimensional perspective, suitable for large database, infrequent usage and less disciplined users.* *Prospective: easy to use, good balance of performance features, high accuracy, flexible performance tuning and configuration, ease of integration into other systems* *Constraint: not many applications develop, still in infancy* *Applications: used at airports, legislative buildings in some foreign countries, daycare centers, hospitals, prisons and immigration facilities.*

	Examples: can be found at home page of the biometric consortium (2003b)
Signature Scan	*Features: traditional device, a behavioral device, it checks the way a person sign his/ her name and writes letters.* *Prospective: fairly accurate* *Constraint: age effect change pattern, not as accurate as other biometric.* *Applications: a crude non-automated version used in retailers' point-of-sale systems; also used to secure PDA devices* *Examples: can be found at home page of the biometric consortium (2003b)*
Finger print	*Features: matches the minutiae, pattern, ultrasonic or moire fringe imprint; most common of all devices, works well in controlled environment.* *Prospective: good accuracy, low false acceptance, low cost, small size, ease of integration* *Constraint: usage errors, high false rejection with large database* *Applications: most widely used in industry for a wide range of applications; used in biometric mouse and other similar device to secure desktop and mobile computers; used for authentication in distributed networks.* *Examples: can be found at home page of the biometric consortium (2003b)*
Voice Scan	*Feature: measure the wavelengths and frequencies of the voice* *Prospective: amplitude and frequency modulations provide high accuracy* *Constraint: variability of traducers and local acoustics, complicated enrollment procedure, user-unfriendly, age and hardware cause variability* *Applications: show strong potential for use in securing mobile computers, PDAs and other similar devices, employed by many large companies to protect computer, office, lab and vault access.* *Examples: can be found at home page of the biometric consortium (2003b)*
Iris Scan	*Features: scan the iris of the eye and digitizes a pattern for matching purpose, works well in identification mode* *Prospective: less intrusive than retina scan, higher matching performance, works well with glasses, across ethnic groups* *Constraint: difficult to use and integrate with other systems* *Application: welfare fraud prevention in Illions; beginning used in ATM machines; used to enable single sign-on distributed networks; used in smart cards, workforce management, network security and authentication.* *Examples: can be found at home page of the biometric consortium (2003b)*
Retina Scan	*Feature: a digital image of the retina of the eye is created to match the pattern against a live sample, scanning done by low-intensity light via an optical coupler* *Prospective: highly accurate* *Constraint: problems with glasses, intrusive* *Applications: welfare fraud prevention in Illions; used to enable single sign-on in distributed networks* *Examples: can be found at home page of the biometric consortium (2003b)*
Facial Scan	*Features: measure the curves on the cheeks and the lips to ascertain the identity* *Prospective: larger number of variables can be studied* *Constraint: difficult to use, limited success in applications*

	Applications: used at several airports and other public locations since 09/11/01
	Examples: can be found at home page of the biometric consortium (2003b)
Keystroke Scan	*Feature: a behavioral biometric device. It measures the force applied and the pattern used to push keys on a keyboard*
	Prospective: very convenient with little intrusion
	Constraint: possible interference of noise, caused by hands movement, not associated with actual keystroke
	Applications: not widely used; has good potential for continuous authentication
	Examples: can be found at home page of the biometric consortium (2003b)

(Sumber: Chandra and Calderon 2003:55)

APLIKASI TEKNOLOGI *BIOMETRIC* TERHADAP SISTEM INFORMASI AKUNTANSI

Weber (1999:34) membedakan antara pengendalian *(control)* dengan pengamanan *(security)* dengan baik sekali. Dijelaskan oleh Weber (1999:35) bahwa teknologi *biometric security* tidak akan dinamakan sebagai pengendalian jika teknologi *biometric security* berdiri sendiri, namun ketika teknologi *biometric security* digunakan sebagai teknologi yang mendukung dalam sistem informasi akuntansi, maka teknologi *biometric security* dinamakan sebagai salah satu pengendalian dalam sistem informasi akuntansi. Hal yang sama juga dikatakan oleh Byrne (2003:44), bahwa teknologi *biometric security* sebagai salah satu teknologi dalam *identity management* seharusnya tidak berdiri sendiri hanya sebagai teknologi sendiri, seharusnya teknologi *biometric security* merupakan salah satu komponen dalam sistem informasi akuntansi yang ada. Berdasarkan komponen sistem informasi akuntansi maka posisi teknologi *biometric security* dalam sistem informasi akuntansi tentu saja sebagai *information technology infrastructured* (Romney and Steinbart 2003:2). Konsep Byrne sebenarnya dapat dikembangkan menjadi suatu *integrated system*, yaitu penggunaan teknologi *biometric security* secara komprehensif dalam lingkup yang lebih besar, yakni dalam lingkup sistem informasi manajemen. Pengendalian *biometric security* digunakan untuk mendukung implementasi sistem informasi manajemen, bukan hanya pada sistem informasi akuntansi. Namun kembali lagi harus dikritisi bahwa tidak setiap organisasi akan menerapkan solusi yang sama dalam mengimplementasikan *biometric security*. Ada beberapa organisasi yang hanya menerapkan *biometric security* pada tingkat solusi sistem informasi akuntansi dan sementara organisasi yang lain langsung pada tingkat solusi manajemen. Implementasi teknologi *biometric security* cukup luas dalam hal pengendalian dalam sistem informasi akuntansi, diantaranya: (1) *Physical access*. Penggunaaan teknologi *biometric security* sudah cukup banyak digunakan dalam hal *physical access*. Aplikasi ini digunakan dalam hal melindungi aset organisasi berupa aset fisik, baik berupa akses kedalam ruangan maupun akses kedalam aset organisasi. Penggunaan *biometric security* akan lebih optimal penggunaannya ketika digunakan untuk jumlah *user* yang besar. Sebagai contoh penggunaan *biometric*

security untuk 65.000 orang pada Olympiade tahun 1996. Hal ini dilanjutkan oleh Disney World dengan menggunakan *fingerprint* pada sistem parkir Disney World. International Air Transport Association juga mempunyai program untuk mengimplementasikan sistem *biometric security* dalam bentuk *Eye Ticket*, dimana bandara North Carolina dan Flughafen Frankfurt akan menjadi *file project* dari program ini. Dalam penerapan untuk sistem informasi akuntansi, teknologi *biometric security* dapat digunakan untuk mencegah *inventory fraud* (Chandra and Calderon 2003:26). Kondisi ini akan memungkinkan hanya setiap individu yang sudah diotorisasi oleh sistem yang dapat mempunyai akses terhadap *inventory* yang dimiliki organisasi (2) *Virtual Access*. Weber (1999:224), membagi *information system assets* menjadi dua, yakni *physical asset* dan *logical asset*. *Virtual access* termasuk aplikasi *biometric security* untuk melindungi *logical asset* yang berupa data maupun *software. Virtual access* ini lebih banyak digunakan dalam menjaga keamanan data dalam jaringan. Umumnya data yang ada dalam jaringan, dilindungi dengan menggunakan password atau PIN. PIN atau *password* tidak dapat menjamin akses yang dilakukan oleh individu yang diluar otorisasi karena merupakan hal yang sangat memungkinkan jika nomer PIN atau *password* tersebut dapat diketahui oleh individu lain. Sebagaimana dikemukakan oleh Ernst & Young, bahwa 84% dari *fraud* yang terjadi pada organisasi komersial, disebabkan oleh pemberitahuan password atau PIN kepada individu lain (Byrne 2003:42). Teknologi *biometric security* memungkinkan bahwa data yang ada dalam jaringan tersebut hanya diakses oleh individu-individu yang benar-benar diijinkan *(authentication),* sehingga prinsip *data integrity* dalam sistem informasi akuntansi dapat dijaga dalam konteks ini (3) *E-commerce applications*. Aplikasi teknologi *biometric security* dalam hal *e-commerce* mulai diperhitungkan oleh para ahli teknologi informasi di bidang *cybercommerce.* Mekanisme dari aplikasi ini memang masih membutuhkan *biometric device* yang berfungsi sebagai *biometric reader* pada setiap tempat transaksi *e-commerce.* Jika transaksi *e-commerce* dilakukan melalui rumah ataupun kantor maka kondisi ini mengharuskan adanya *biometric reader* yang dimiliki oleh individu yang melakukan transaksi *e-commerce.* Namun pada kondisi perkembangan teknologi yang demikian pesat, sangat memungkinkan penggunaan layar komputer sebagai *biometric reader,* sehingga tidak memerlukan *biometric device* yang berfungsi sebagai *biometric reader* lagi. Sebagai buktinya Nuance communication mulai mengembangkan media telepon yang berfungsi sebagai perantara *biometric reader* yang dapat digunakan ketika ingin melakukan proses *authentication* yang berupa gelombang suara pada transaksi *e-commerce.* Implementasi *biometric security* pada *e-commerce* dilatarbelakangi karena fenomena penipuan melalui *e-commerce* menjadi sesuatu yang sangat diwaspadai oleh para pelaku yang menjual produknya melalui *on-line shopping*. Dalam konteks ini *biometric security* berperan sebagai pengendalian dalam salah satu *accounting subsystems,* yakni *revenue cycle*. Pengendalian dalam *revenue cycle* untuk *e-commerce* merupakan sesuatu yang harus menjadi prioritas bagi organisasi yang terlibat dalam *e-commerce*. Hal ini sesuai dengan survei yang dilakukan oleh Clear Commerce yang menyatakan bahwa tingkat penipuan melalui *on-line shopping* sangat tinggi, hal ini terutama terjadi pada kondisi ketika individu-individu dari negara-negara

berkembang bertindak sebagai pembeli. Survei ini juga menyatakan negara Indonesia merupakan negara kedua setelah Ukraina sebagai *country of orign* kejahatan yang menggunakan *credit card* sampai tahun 2003 (Ahmadjayadi dan Cahyana 2004). Untuk mengatasi permasalahan ini, MasterCard sedang mengmbangkan implementasi teknologi security dalam *e-commerce*, dimana MasterCard memperkirakan bahwa penggunaan teknologi *biometric* dalam *e-commerce* akan mengurangi penipuan hingga 80%, ditinjau dari sisi keunggulan yang dimiliki teknologi *biometric security* (Liu and Silverman 2004) (4) *Covert surveillance. Covert surveillance* merupakan topik yang masih jarang diteliti dan merupakan aplikasi yang sulit untuk diimplementasikan (Liu and Silverman 2004). Hal ini dapat dipahami, karena aplikasi teknologi *biometric* membutuhkan dukungan dan komitmen dari pemerintah sebagai elemen yang memegang peranan yang sangat penting dalam hal infrastruktur untuk implementasi teknologi *biometric security*, khususnya aplikasi *covert surveillance. Covert surveillance* digunakan pada gedung-gedung milik umum atau fasilitas-fasilitas umum yang memungkinkan semua orang melakukan akses. Tujuan dari aplikasi ini sebenarnya bukan pada proses *authentication*, namun lebih kearah proses *capturing data* atas semua individu yang melakukan akses terhadap gedung-gedung maupun fasilitas umum, sehingga proses ini memungkinkan dilakukannya pemantauan atas identitas pengunjung fasilitas milik umum, dalam hal inilah yang membuat aplikasi ini disebut sebagai *covert surveillance* atau pengamatan secara sembunyi-sembunyi. Kemungkinan ide ini muncul, ketika serangan teroris dalam bentuk bom yang terjadi pada gedung-gedung dan fasilitas umum. Melalui teknologi *biometric security*, data dari semua pengunjung dan pengguna fasilitas dan gedung tersebut dapat dilacak secara cepat. Namun aplikasi ini juga dapat digunakan pada perusahaan-perusahaan, misalnya pada ruangan-ruangan maupun fasilitas yang ada pada perusahaan, sehingga akan diketahui semua data individu yang melakukan akses. Jika pada konsep *physical access,* teknologi *biometric* hanya berperan sebagai pengendalian, agar individu yang memiliki otorisasi saja yang mempunyai akses terhadap aset organisasi. Teknologi *covert surveillance* memungkinkan organisasi memiliki data individu yang melakukan akses terhadap aset organisasi, sehingga dapat dilakukan pengendalian dan evaluasi atas akses individu terhadap aset organisasi. Tidak semua teknologi *biometric security* dikondisikan untuk menyimpan data individu yang melakukan proses *authentication* hal ini disesuaikan juga dengan kebutuhan organisasi. Maksudnya, kondisi ini akan berpengaruh pada kapasitas database dari teknologi *biometric security* yang akhirnya mempengaruhi sisi *cost* yang harus dikeluarkan organisasi untuk mengimplementasikan teknologi ini.

IMPLEMENTASI TEKNOLOGI *BIOMETRIC* SEBAGAI SALAH SATU SISTEM PENGENDALAIAN

Sistem informasi dan pengendalian yang diimplementasikan dalam sebuah organisasi tentu saja harus sesuai dengan strategi organisasi, (Romney and Steinbart 2003: 226). Untuk mengimplementasikan sebuah sistem yang baru, dapat menghabiskan waktu lebih dari satu tahun. Prinsip ini sama dengan implementasi teknologi *biometric* dalam sistem informasi akuntansi. Namun

sebelum sebuah organisasi mengunakan teknologi *biometric*, menjadi suatu kewajiban bagi organisasi untuk melakukan *feasibility study*, apakah organisasi memang harus mengadopsi teknologi ini atau tidak, jika organisasi tetap memutuskan untuk melakukannya, maka organisasi juga memutuskan teknologi yang mana yang akan diadopsi dari beberapa pilihan yang ada pada teknologi *biometric* (Tongia and Jain 2003: 27). Tiga tahapan yang harus dilakukan sebuah organisasi dalam mengimplementasikan pengendalian atas sistem informasi akuntansi, yaitu: (1) *Strategic planning and budgeting.* Tahap ini lebih banyak mengarah kedalam unsur strategi dari implementasi pengendalian yang dilakukan oleh organisasi, dengan kata lain tahap ini merupakan peta dari implementasi pengendalian yang dilakukan organisasi, dalam hal ini implementasi teknologi *biometric.* Dalam peta strategi organisasi tersebut dapat dilihat penjelasan mengenai rencana jangka panjang yang dimiliki oleh organisasi dalam mengimplementasikan pengendalian yang ada. Untuk dapat menyusun strategi perencanaan ini, tentu saja organisasi harus melakukan penelitian dan survei, baik sifatnya internal perusahaan maupun eksternal *(benchmarking).* Penelitian dan survei yang dilakukan oleh organisasi akan diarahkan pada *hardware*, *software*, sumber daya manusia dan infrastruktur yang dibutuhkan. Rencana yang telah disusun ini harus dievaluasi secara berkesinambungan oleh organisasi, sehingga dapat diketahui hambatan-hambatan yang ada, solusi dan kesempatan yang bisa dikembangkan oleh organisasi. Jika pola ini dilakukan maka akan melahirkan *continous improvement* yang akan membawa hasil yang optimal bagi organisasi (2) *Developing a system reliability plan.*

Romney and Steinbart (2003: 228), mengungkapkan seringkali permasalahan yang dihadapi organisasi dalam implementasi sebuah sistem pengendalian adalah permasalahan yang berkenaan dengan *monitoring* dan perencanaan pengembangan. Jika tahap *strategic planning and budgeting* lebih banyak menekankan mengenai implementasi sistem pada tahap awal, maka tahap ini lebih banyak berhubungan dengan tahap sesudah implementasi, yakni *controlling* yang dilakukan organisasi terhadap implementasi pengendalian yang dilakukan oleh organisasi. Hal berikutnya dari tahap *developing a system reliability plan* adalah rencana pengembangan dari implementasi yang dilakukan, termasuk didalamnya *upgrade* atau *update software* sistem pengendalian. Seiring perjalanan waktu, pengendalian yang diterapkan oleh organisasi dapat kehilangan tingkat *relevancy*-nya dengan perkembangan tingkat ancaman maupun resiko yang ada dalam lingkungan pengendalian (3) *Documentation.* Jika berbicara mengenai implementasi sistem baru, baik sistem pengendalian maupun sistem informasi akuntansi, maka tahapan yang ada dalam implementasi itu sebenarnya tidak pernah terlepas dari masalah dokumentasi. Dokumentasi merupakan proses mengarsipkan seluruh proses yang dilakukan ketika implementasi *biometric security* pada organisasi pengarsipan yang dilakukan dalam bentuk manual. Dalam sistem yang terkomputerisasi, dokumentasi akan menolong auditor dalam melakukan *review* terhadap sistem yang ada (Weber 1999: 15). Bagi organisasi, dokumentasi memampukan organisasi untuk terus melakukan evaluasi dan *continuous improvement*. Tanpa dokumentasi, tidak mungkin organisasi menerapkan apa yang telah direncanakan organisasi dalam strategi

jangka panjang, karena hal ini berhubungan dengan rotasi yang terjadi dalam posisi jabatan maupun *turnover* karyawan, sehingga ketika terjadi pergantian staf untuk melakukan pengembangan sistem yang telah diimplementasikan, dapat diantisipasi dengan adanya dokumentasi. Tiga jenis dokumentasi digunakan dalam implementasi *biometric security* yaitu: (1) *Administrative documentation.* Tahap ini merupakan dokumentasi yang menjelaskan standar yang digunakan untuk *system analysis.* Survei awal mengenai kebutuhan implementasi *biometric security*, survei mengenai aplikasi *biometric security, feasibility study* dan *system requirement* didokumentasikan dalam *administrative documentation* (2) *Systems documentation.* Pada tahap ini sistem dokumentasi yang ada menjelaskan *input, processing steps, output* dari aplikasi yang ada (3) *Operating documentation.* Dokumentasi ini menjelaskan apa saja yang dibutuhkan untuk menjalankan aplikasi yang ada, seperti spesifikasi dari *hardware* dan *software* beserta penjelasan mengenai spesifikasi kebutuhan sumberdaya manusia.

TANTANGAN TEKNOLOGI *BIOMETRIC*

Teknologi *biometric* memang merupakan alternatif yang perlu dipertimbangkan sebagai pengendalian dalam sistem informasi akuntansi. Memang masih ada beberapa perbaikan-perbaikan yang juga masih harus dilakukan, dalam rangka membuat teknologi *biometric* lebih stabil dan lebih fleksibel. tantangan yang perlu diperhatikan sehubungan dengan teknologi *biometric* adalah: (1) Standarisasi. Industri *biometric* terdiri dari 150 vendor *hardware* dan *software* yang terpisah, dimana masing-masing vendor tersebut mempunyai standar sendiri dalam hal *interface system, algorithma* maupun struktur data (Liu and Silverman 2004). Kondisi ini akan membuat perlu adanya standar antara vendor tersebut, sehingga dapat menghasilkan suatu sistem yang lebih fleksibel dan *applicable* (20 Aplikasi teknologi *hybrid* pada *biometric security.* Konsep ini lebih mengarah pada ide untuk memunculkan teknologi yang baru dengan cara melakukan penggabungan anatara teknologi biometric yang ada atau menggabungkan anatar teknologi biometric *(something you are)* dengan teknlogi *smart card (something you have)* atau password *(something you know)* (3) Manajemen siklus hidup teknologi *biometric*. *Biometric* memang identik dengan konsep *something you are*. Konsep ini menjelaskan bahwa setiap individu merupakan individu yang unik, sehingga akan memiliki karateristik dan spesifikasi yang berbeda. Namun keunikan dan spesifikasi individu tersebut tentu saja tidak statis, dalam hal ini dapat mengalami perubahan (Byrne 2003: 43). Misalnya teknologi *biometric security fingerprint* akan membaca dan mengambil data dari sidik jari setiap individu yang mencoba melakukan akses ataupun *authentication* terhadap sebuah sistem dalam organisasi. Hal yang perlu dikritisi adalah bagaimana jika seorang individu mengalami kecelakan dan mengalami perubahan pada garis-garis jarinya. Tentu saja hal ini mengakibatkan *biometric reader* tidak dapat lagi mengenali garis tangan jari individu tersebut dan akan menolak *authentication* dari individu tersebut. Menurut penelitian yang dilakukan Chandra dan Calderon (2003), beberapa *teknologi biometric reader fingerprint* tidak akan dapat lagi mengenali *authentication* dari garis-garis jari individu, ketika jari individu tersebut kotor, baik disebabkan oleh abu maupun zat yang lainnya.

KESIMPULAN

Implementasi teknologi *biometric security* cukup luas, dalam hal pengendalian pada *physical access, virtual access, e-commerce applications* dan *covert surveillance.* Tahapan yang perlu dilakukan dalam implementasi teknologi *biometric security* adalah *strategic planning and budgeting, developing a system reliability plan* dan *documentation.* Tantangan dalam pengembangan teknologi *biometric* berkaitan dengan standarisasi, aplikasi teknologi *hybrid* dan manajemen siklus hidup pada *biometric security.*

Oleh karena itu teknologi *biometric security* dapat dipertimbangkan sebagai salah satu alternatif pengendalian dalam system informasi akuntansi karena memiliki keuanggulan dibandingkan teknologi lain. *Biometric security* yang merupakan konsep "*something you are*", memiliki *authentication* yang lebih akurat dibandingkan teknologi lain.

Walaupun teknologi *biometric* lebih unggul dibandingkan dengan pengendalian yang lain, tidak semua organisasi harus menerapkan teknologi *biometric security*, jika dilihat dari *cost and benefit* yang dimiliki organisasi tersebut dalam mengimplementasikan teknologi ini.

DAFTAR PUSTAKA

Ahmadjayadi, Cahyana (2004), Konsep Pengamanan dan Perlindungan Infrastruktur Berbasis teknologi Informasi, *Kementrian Komunikasi dan Informasi*, Information System Security Control and Audit Conference 2004.

Ax-S Biometric (2005, 20 Januari). "Biometric Security Risk Assessment", Available: <http://www.ax-sbiometrics.com/Downloads/ PhysicalRiskAssessmentbrief.pdf>

Byrne, Jim (2003), "Large-Scale Biometric Management: A-Centralized, Policy-based Approach to Reducing Organizational Identity Chaos", *Information System Control Journal,* Vol 6, page 41-44

Chandra, Akhilesh & Calderon, Thomas G (Fall 2003), "Toward a Biometric Security Layer in Accounting Systems", *Journal of Information Systems,* page 51-70.

Donny, Cracker: Sebab Akibat dan Kepastian Hukum, *Information and Communication Technology Watch,* Available: <http://free.vlsm.org/v17/com/ictwatch/paper/paper061.htm> (6 Januari 2005)

International Biometric Group, Available: <http://www.biometricgroup.com/reports/public/market_report.html> (2005, 17 Januari). "Biometric Market and Industry Report 2004-2008".

Jawa Pos (2005, 5 Januari) "Tas Berteknologi Biometric", Available: <http://cdc.eng.ui.ac.id>

Liu, Simon & Silverman, Mark, "A Practical Guide to Biometric Security Technology", *Computer Society*, Available: <http:\\www.computer.org> (2005, 5 Januari)

Media Indonesia (04 Juli 2002), "Survei Terhadap 450 CIO-Perencanaan Keamanan Sistem Informasi Lemah.", *Nakertransnet*, Available: <http://www.nakertrans.go.id> (2005, 4 Januari).

Radio Singapore International (19 Oktober 2004). "Lebih Aman Dengan Paspor Biometrik", <http://www.rsi.com.sg> (2005, 4 Januari)

Radio Singapore International, (2005, 4 Januari). "Paspor Singapura Bakal Diganti Paspor Biometrik", Available: <http://www.rsi.com.sg> (1 November 2004).

Romney, Marshall B and Steinbart, Paul John (2003), *Accounting Information Systems,* Ninth Edition, Prentice Hall.

Ross, Steven J (2003), "Who Needs Information Security", *Information System Control Journal,* Vol 6, page 9-10

SP18 (2005, 4 Januari). "IBM Gunakan Pengaman Biometric Untuk Notebook", Available: <http://www.sp18. com>

Tongia, Rahul and Jain, Kanika (2003), "Investing in Security-Do Not Rely on FUD, *Information System Control Journal,* Vol 6, page 27-28

Wallhoff, John (2003), "Enforce Security with a Fingerprint Biometric Solution", *Information System Control Journal*, Vol 4, page 39-43.

Warren, Carl, S., Reeve, James, M. dan Fess, Philip, E. (2005), *Accounting*, 21th edition, Thomson Learning.

Weber, Ron (1999), *Information Systems Control and Audit,* Prentice Hall.