Syntax Literate : Jurnal Ilmiah Indonesia – ISSN : 2541-0849
e-ISSN : 2548-1398
Vol. 3, No 7 Juli 2018

PENYUSUNAN KEBIJAKAN KEAMANAN TEKNOLOGI INFORMASI PADA TRANSAKSI ELECTRONIC BANKING PERBANKAN UMUM BERDASARKAN PERATURAN BANK INDONESIA NOMOR 9/15/PBI/2007 DENGAN MENGGUNAKAN MATRIKS COBIT 4.1 DAN ISO/IEC 27000

R. Irman Hariman
Universitas Kebangsaan Bandung
Email: irmanhariman@gmail.com

Abstrak

Layanan informasi dan transaksi elektronik merupakan aset yang paling bernilai bagi sebuah bank umum. Sumberdaya berupa teknologi keamanan transaksi elektronik harus mampu mendukung jalannya layanan prima tersebut. Namun teknologi keamanan informasi yang digunakan untuk menunjang layanan tersebut masih belum memadai jika kebijakan pimpinan yang berisikan kebijakan pengamanan transaksi elektronik dan mengatur pelaksanaannya bahkan menjadi panduan pelaksanaannya masih lemah bahkan belum tersusun. Kebijakan keamanan teknologi informasi terutama dalam pelayanan transaksi elektronik perbankan (e-banking), harus disusun berdasarkan standar keamanan yang sudah ada yaitu ISO/IEC seri 27000. Bahkan untuk melakukan audit keamanan teknologi informasi pun seharusnya sudah memiliki panduan yang sudah standar, sehingga perbankan umum memiliki standar penyusunan kebijakan dan memiliki panduan untuk melakukan audit internal keamanan teknologi informasi pada layanan transaksi elektronik (e-banking). Penyusunan kebijakan keamanan transaksi elektronik ini memiliki objektifitas berupa standar susunan kebijakan yang harus ada dalam penyelenggaraan teknologi keamanan sebagai dukungan terhadap layanan transaksi elektronik sebuah bank umum. Pendekatan yang digunakan untuk menghasilkan standar penyusunan kebijakan ini adalah dengan menggunakan matriks 2 dimensi yang berisikan domain kontrol atau klausul ISO/IEC 27000 yang memiliki 11 klausul dengan Cobit 4.1 pada domain kontrol atau klausul Delivery and Support, yaitu DS-5 (Ensure System Security) yang memiliki 11 klausul, sehingga menghasilkan 11 klausul baru yang akan dipetakan pada Peraturan Bank Indonesia No. 9/15/PBI/2007, tentang Penerapan Manajemen Resiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum.

Kata Kunci *: ISO/IEC 27000, Cobit 4.1, Bank Umum, Transaksi Elektronik, e-Banking, Kebijakan Keamanan*

Pendahuluan

Penggunaan dan pemanfaatan teknologi informasi saat ini telah membawa perubahan dalam kegiatan operasional serta pengelolaan data transaksi suatu bank sehingga dapat dilakukan secara lebih efektif dan efisien serta memberikan informasi secara lebih cepat dan akurat serta tepat waktu. Perkembangan teknologi informasi pada sistem perbankan yang harus selalu kreatif dan penuh inovatif dalam memberikan layanan maksimal pada masyarakat yang menjadi nasabahnya guna memenuhi kepuasan para nasabah sehingga dapat meningkatkan *market shared* dan *value* lainnya. Perkembangan produk perbankan berbasis teknologi diantaranya berupa *Electronic Banking (e-Banking)* ditujukan untuk memudahkan nasabah dalam melakukan transaksi perbankan secara *non cash* setiap saat melalui jaringan elektronik perbankan tersebut. Penggunaan jasa layanan pihak ketiga dalam penyediaan sistem transaksi dan pelayanan bank semakin meningkat pula.

Pelaksanaan transaksi keuangan antar perbankan diseluruh dunia dapat dilakukan, sehingga nasabah memerlukan kenyamanan dan keamanan saat transakasi dilakukan. Berbagai manfaat dan keunggulan yang dapat diperoleh dari penggunaan teknologi informasi dalam kegiatan operasional bank, terdapat pula resiko-resiko yang mungkin dapat merugikan bank serta nasabahnya diantaranya risiko operasional, risiko hukum, dan risiko reputasi selain risiko perbankan lainnya seperti risiko likuiditas dan risiko kredit. Mengingat bahwa penggunaan teknologi informasi merupakan aset yang sangat penting dalam operasional karena dapat meningkatkan nilai tambah dan daya saing bank, sementara penyelenggaraannya mengandung berbagai risiko, maka perbankan perlu menerapkan *IT Governance* yang didukung segenap fasilitas keamanan teknologi informasi dengan menerapkan kebijakan manajemen bidang keamanan yang dilengkapi dengan prosedur dan mekanisme.

Keberhasilan penerapan *IT Security Governance* pada perbankan akan sangat bergantung pada komitmen seluruh unit kerja (*stake holder*) di bank tersebut, baik penyelenggara maupun pengguna teknologi informasi. Penerapan *IT Security Governance* disuatu perbankan dilakukan melalui penyelarasan Rencana Strategis Teknologi Informasi dengan strategi bisnis bank tersebut, optimalisasi pengelolaan sumber daya, pemanfaatan teknologi informasi (*IT value delivery),* pengukuran kinerja

dan penerapan manajemen risiko yang efektif. Untuk dapat menerapkan manajemen risiko yang efektif maka diperlukan :

1. Keterlibatan dan pengawasan Dewan Komisaris dan Direksi.
2. Penyusunan dan penerapan kebijakan dan prosedur terkait teknologi informasi.
3. Proses identifikasi, pengukuran, pemantauan dan pengendalian risiko yang berkesinambungan.

Bank dituntut pula untuk mengantisipasi kebutuhan akan infrastruktur teknologi informasi yang memadai dalam rangka menghadapi implementasi *Basel II. B*ank diharapkan mampu mengelola resiko yang dihadapi secara efektif dalam seluruh aktivitas operasional yang didukung dengan pemanfaatan teknologi informasi. Permasalahan yang terjadi pada sistem transaksi elektronik perbankan akan menyebabkan inkonsistensi pada transaksi yang akan sangat merugikan nasabah secara materil, bahkan efek terbesar terjadi pada perbankan adalah adanya *rush* sehingga perbankan akan mengalami *collapse*.

Sehingga pada akhirnya sistem keamanan transaksi elektronik pada perbankan umum tersebut memenuhi aspek keamanan yang dipersyaratkan dalam seperti *authentication, confidentiality/privacy, non-repundiation* dan *availability* serta sesuai dengan kebijakan-kebijakan yang diisyaratkan Peraturan Bank Indonesia melalui Peraturan Bank Indonesia No. 9/15/PBI/2007, tentang Penerapan Manajemen Resiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum.

Metode Penelitian

Penelitian yang digunakan adalah kualitatif, dengan menggunakan studi literatur yang kemudian digunakan dalam mendefinisikan hal-hal yang diperlukan selama melakukan penelitian dan membentuk paradigma baru pada sistem tersebut dan dimaksudkan untuk mendapatkan model yang sesuai dalam menetukan tahapan penyusunan keamanan transaksi electronik pada bank umum. Hal ini dilakukan dengan cara mengkobinasikan 2 metodologi, yaitu dengan menggunakan COBIT 4.1 khususnya pada salah satu domainnya yaitu domain kontrol DS-5 *Ensure System Security* dan ISO/IEC 27000 dengan data primer berdasarkan Peraturan Bank Indonesia No. 9/15/PBI/2007.

Berikut perangkat-perangkat tersebut yang terdiri dari :

a. COBIT 4.1 dengan DS-5 (*Ensure system security*)

Cobit 4.1 bukanlah parameter khusus keamanan teknologi informasi namun Cobit memiliki satu klausul yang secara khusus menekankan pada bagian keamanan teknologi informasi. Klausul yang akan digunakan adalah *klausul Delivery and Support* (DS-5) yang memiliki 11 kontrol objektiv, digunakan untuk memperoleh parameter tambahan yang lebih komfrehensif dalam menentukan sistem keamanan teknologi informasi khusunya pada sistem keamanan transaksi elektronik suatu bank sehingga dapat dijadikan alat untuk melakukan audit kemanan teknologi informasi terhadap fasilitas dan layanan transaksi elektronik dengan berdasarkan PBI no 9/15/PBI/2007 yang merupakan standar yang sudah dijalankan pada bank umum.

b. ISO/IEC 27000

Standar ISO/IEC 27000 memiliki 11 domain / kalusul keamanan yang menjadi pedoman dalam penerapan *Information Security Management System* (ISMS), sekaligus *guideline* dalam penyusunan *kebijakan* standar dalam penyelenggaraan keamanan teknologi informasi termasuk teknologi keamanan pada transaksi elektronik bagi seluruh perbankan umum. Penggunaan ISO/IEC 27000 dimaksudkan menjadi parameter utama dalam menerapkan keamanan transaksi elektronik. Sehingga pelaksanaan monitoring, evaluasi keamanan teknologi informasi dalam transaksi elektronik menjadi mudah, bahkan dapat dijadikan pedoman oleh semua bank diseluruh Indonesia.

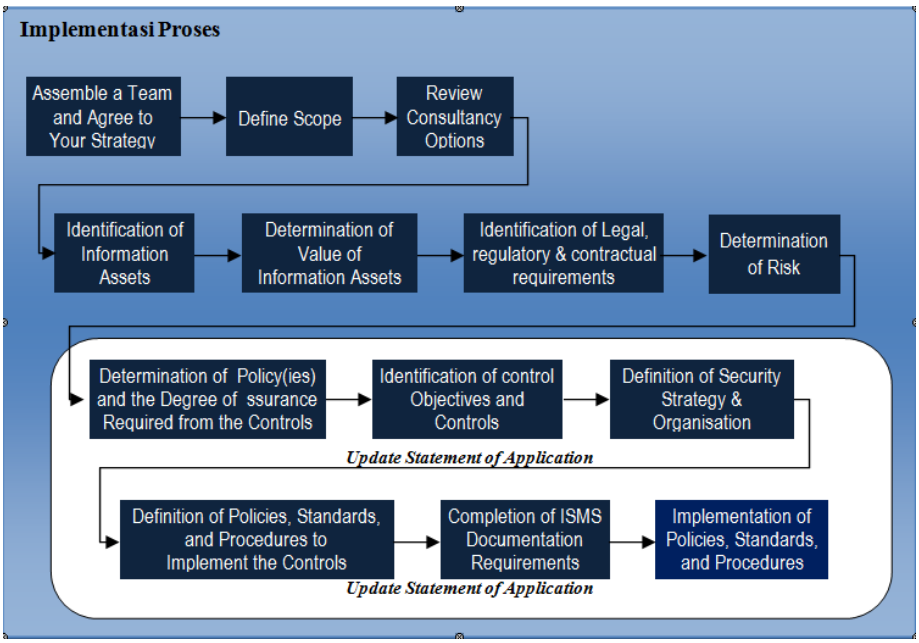
Hasil dan Pembahasan

Analisis yang dilakukan menggunakan *Content Analysis* yang diperoleh melalui data primer Peraturan Bank Indonesia Nomor 9/15/PBI/2007 yang akan dipetakan pada matriks baru yang dihasilkan dari COBIT 4.1 dengan kalusul DS 5 (*Delivery and Support*) yaitu *Ensure Security* dan keseluruh klausul ISO/IEC 27000. Parameter baru yang akan dihasilkan dalam penelitian ini dapat dijadikan sebagai panduan bagi perbankan dalam menjalankan fasilitas sistem keamanan transaksi elektronik bahkan dapat digunakan dalam melakukan evaluasi berupa audit keamanan teknologi informasi

khususnyapada fasilitas, prosedur dan mekanisme transaksi elektronik selain hanya menjadi panduan penyusunan keamanan transaksi elektronik yang sesuai dengan amanat yang terkandung dalam Peraturan Bank Indonesia Nomor 9/15/PBI/2007.

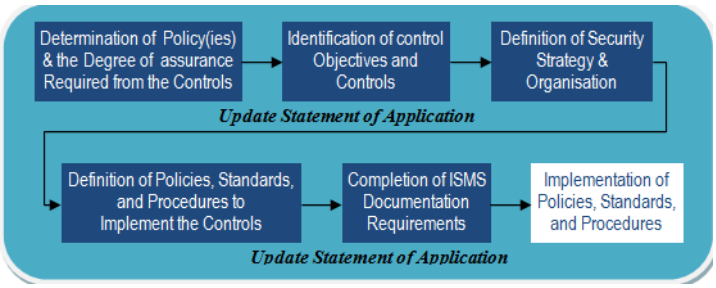
Pelaksanaan sistem keamanan terhadap teknologi informasi khususnya *electronic banking* pada setiap bank umum merupakan upaya yang dilakukan untuk menciptakan layanan perbankan yang aman berbantukan teknologi informasi. Namun untuk melaksanakan mekanisme pengamanan sistem layanan transaksi elektronik tidak sekedar dipasangnya perangkat-perangkat teknologi keamanan saja tapi perlu regulasi dan kebijakan keamanan dari pimpinan perbankan sehingga sebelumnya perlu dilakukan penyusunan kebijakan keamanan gunas mengetahui segala kekurangan dan kelebihan dari fasilitas keamanan yang ada dalam menunjang layanan transaksi elektronik.

Tahapan penyusunan kebijakan ini dilakukan dengan melalui proses yang sangat panjang mulai dari pembentukan tim sampai menentukan resiko yang ada kemudian baru melangkah pada pendefinisian sampai penerapan kebijakan tersebut bahkan lebih jauh sampai terciptanya *Standard Operational Procedure*. Namun pada penelitian ini tidak akan dibahas seluruh tahapan sebelumnya melainkan lebih difokuskan pada tahapan selanjutnya yaitu mulai dari pendefinisian *kebijakan* sampai penyusunan *kebijakan*.



Gambar 1. Kerangka implementasi proses pelaksanaan keamanan (ISO/IEC 27000)

Sesuai gambar 1 diatas, maka diambilah tahapan berikut ini, yang akan digunakan dalam penyusunan kebijakan yaitu :

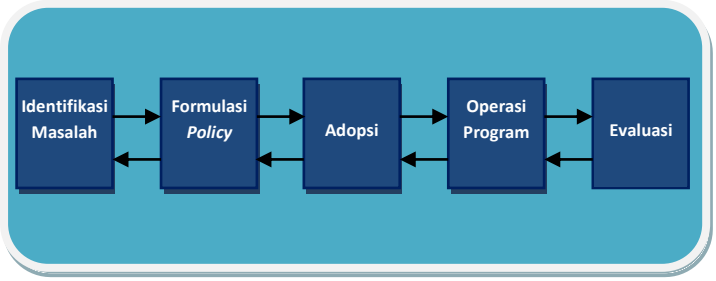


Gambar 2. Penentuan dan penerapan atau pelaksanaannya

Sebelum tahapan diatas (gambar 2) dilakukan, maka perlu diketahui hal-hal apa saja yang harus dipersiapan. Berikut tahapan-tahapan yang perlu diketahui sebelunya :

1. Melakukan inventarisir terhadap resiko yang mungkin terjadi pada sistem keamanan transaksi elektronik.
2. Dari resiko-resiko yang sudah diinventarisir tersebut, maka tahap berikutnya adalah menurunkannya menjadi rancangan (*kebijakan*) sesuai dengan keperluan dan berdasarkan standar yang ada. Untuk mendapatkan formulasi yang diperlukan dibawah ini merupakan hal-hal yang diperlukan selama proses berlangsung.

Berikut dibawah ini akan dilakukan tahapan yang dibutuhkan untuk pembentukan dan formulasi kebijakan berdasarkan permasalahan yang ada dan kerap terjadi pada sistem transaksi elektronik.



Gambar 3. Elemen Proses Pembuatan (*Kebijakan*)

Berikut penjelasan setiap elemen diatas :

1. **Identifikasi Masalah**

   Merupakan identifikasi terhadap peluang yang ada dan dapat mempermudah dalam pembuatan kebijakan, dilakukan pada level eksekutif. Hasilnya berisi masalah-masalah yang harus ditangani serta prioritas penanganan masalah tersebut terutama bidang pengamanan transaksi elektronik.

2. **Formulasi (kebijakan)**

   Melakukan formulasi kebijakan harus mempunyai cara berfikir strategis bagaimana rencana dalam menghadapi masalah yang telah diidentifikasikan, berisikan mengenai tujuan dan merupakan rencana usulan kebijakan yang idealnya dan ingin dicapai dari urutan prioritas tersebut serta alternatif yang dilakukan untuk mencapai tujuan tersebut.

3. **Adopsi**

   Proses ini akan dilihat apakah yang dibuat memungkinkan untuk dilakukan atau bahkan baik untuk diterapkan atau tidak, maksudnya adanya kesesuaian dengan organisasi dan lembaganya atau perusahaannya.

4. **Operasi Program**

   Proses berikutnya yang harus dilakukan adalah melakukan aksi atau kegiatan untuk mewujudkan tujuan yang telah didefinisikan dalam rencana penyusunan kebijakan.

5. **Evaluasi**

   Evaluasi ini digunakan untuk menilai apakan penyusunan kebijakan tersebut akan digunakan sebagai suatu kebijakan keamanan pada fasilitas transaksi elektronik atau bahkan perlu ditinjau ulang.

Setelah melalui tahapan diatas, maka tahapan berikutnya dapat dilakukan dengan :

1. Melakukan identifikasi terhadap kendali objektif dalam pelaksanaan kendali.
2. Mendefinisikan kebutuhan keamanan dan strategi bisnis dan organisasi terkait dengan transaksi elektronik. Melakukan pemeriksaan “kesehatan” sistem dan *benchmark* keamanan teknologi informasi kepada standar sistem yang sudah ada (berdasarkan Peraturan Bank Indonesia No. 9/15/PBI/2007 dan ISO/IEC 27000).

Mendefinisikan yang dibuat secara lebih lengkap dengan dibuatnya Standar dan Prosedurnya untuk mengimplemtasikan sistem kendalinya.

3. Memetakan setiap yang dibuat dengan standar keamanan ISMS (information security management system) dari ISO/IEC 27000 dengan sebelumnya dilakukan kolaborasi dengan Cobit 4.1 khususnya domain kontrol *Ensure System Security* melalui sebuah matriks sederhana, sehingga diperoleh domain baru yang digunakan sebagai kontrol dari yang dibentuk.
4. Dari hasil diatas akan dihasilkan suatu konsep keamanan teknologi informasi pada sistem elektronik banking. Hasil dari konsep keamanan teknologi informasi akan dijadikan sebagai panduan penyusunan keamanan teknologi informasi (*Handbook of Information Technology Security*).

Setelah sebagaian tahapan dilalui maka dengan penyusunan kebijakan keamanan pun dilakukan dengan penggunakan matriks pada tahap *Definition of Policies, Standards, and Procedures toImplement the Controls*, yang dibuat dari kombinasi Cobit 4.1 dengan klausul DS-5 *Delivery and Support* yaitu *Ensure Security* yang memiliki 11 klausul dan ISO/IEC 27000 yang memiliki 11 klausul juga. Klausul baru yang dihasilkan akan dari kombinasi Cobit 4.1 dan ISO/IEC 27000 akan dipetakan sesuai Peraturan Bank Indonesia Nomor 9/15/PBI/2007 tentang Penerapan Manajemen Resiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum.

Setelah dilakukan studi terhadap data primer PBI Nomor 9/15/PBI/2007 ditemukan masih terlalu umum dan agak sulit untuk diterjemahkan kedalam bentuk kebijakan pimpinan terutama mengenai teknologi infornasi. Belum adanya panduan penyusunan kebijakan keamanan teknologi informasi yang dapat dijadikan acuan dalam membuat prosedur dan mekanisme dalam pelaksanaannya sehingga perlunya dibuat tahapan dan perangkat yang mampu untuk dijadikan acuan dalam menyusun kebijakan keamanan teknologi informasi berdasarkan kondisi sebenarnya dari keamanan teknologi informasi yang selama ini diterapkan dan diadopsi perbankan umum, bahkan saat dilakukan audit teknologi informasi.

Berdasarkan pada Peraturan Bank Indonesia Nomor 9/15/PBI/2007 tentang penerapan manajemen resiko transaksi elektronik, belum dijelaskan secara terperinci bagaimana menyusun dan melaksanakan kebijakan keamanan transaksi elektronik perbankan umum. Bahkan kebijakan keamanan transaksi elektronik yang dilakukan

pada setiap perbankan umum diseluruh Indonesia lebih mengacu pada inisiatif pimpinan dan manajemen perbankan itu sendiri (belum ada standar), sehingga memungkinkan setiap bank umum akan memiliki standar yang berbeda untuk menyusun kebijakan keamanan transaksi elektroniknya itu.

Untuk itu diperlukan suatu perangkat berupa metode yang dapat dijadikan rujukan konkrit dalam menyusun kebijakan keamanan pada transaksi elektronik tersebut. Hal ini diperlukan agar perbankan umum memiliki pola dan mekanisme yang baku dalam membuat atau penyusunan kebijakan keamanan transaksi elektronik bahkan penerapannya serta menjadi acuan dalam melakukan revisi terhadap dokumen kebijakan yang sebelumnya ada seperti ketentuan pada PBI Nomor 9/15/PBI/2007 Pasal 33 bahwa ”Bank yang telah memiliki kebijakan, prosedur dalam penggunaan Teknologi Informasi dan pedoman manajemen risiko penggunaan Teknologi Informasi wajib menyesuaikan dan menyempurnakannya paling lambat 12 (dua belas) bulan sejak berlakunya Peraturan Bank Indonesia ini”.

Penyusunan kebijakan keamanan teknologi informasi terutama untuk mendukung kelancaran transaksi elektronik tidaklah mudah, perlu ada tahapan yang. Untuk mendapatkan perangkat dan pedoman yang dapat dijadikan sebagai tahapan yang akan digunakan dalam penyusunan kebijakan keamanan transaksi elektronik ini maka dalam jurnal penelitian ini akan dipergunakan dua metode yang dapat dikolaborasikan yaitu Cobit 4.1 terutama *domain control* DS-5 *Delivery And Support* yang memiliki 11 kontrol objektif dan ISO/IEC 27000 yang sama-sama memiliki 11 kontrol objektif. Cobit 4.1 dan ISO/IEC 2700 yang dijadikan sebagai perangkat utama yang akan dijadikan metodologi dan akan menjadi sangat penting digunakan untuk mendapatkan penilaian yang objektif dari status keamanan transaksi elektronik pada perbankan saat dilakukan *assessment*, terutama dalam penerapan kebijakan keamanan teknologi informasi sistem elektronik banking yang selama ini digunakan.

Cobit 4.1 pada *Domain Control Delivery And Support* (DS-5) dan ISO/IEC 27000 digunakan untuk memperoleh kontrol objektif baru yang lebih handal untuk dijadikan acuan sebagai tahapan penyusunan kebijakan keamanan yang akan dikolaborasikan dengan parameter pada PBI NOMOR : 9/15/PBI/2007. Kontrol objektif baru (Cobit 4.1 dengan DS-5 nya dan ISO/IEC 27000) dihasilkan dengan cara dibuatnya matriks, sehingga akan menghasilkan 11 kontrol objektif baru. Melalui

matriks yang dibuat ini selanjutnya akan digunakan untuk menjadi panduan dalam menyusun dan menentukan kebijakan keamanan yang akan disesuaikan dengan PBI NOMOR : 9/15/PBI/2007. Berdasarkan matriks yang dibuat akan dihasilkan kontrol objektif baru yang bersesuaian diantara keduanya, sehingga 11 kontrol objektif baru pun dihasilkan. Berikut ke-11 kontrol objektif yang dimiliki Cobit 4.1 Domain DS-5 dan ISO/IEC 27000) dapat terlihat pada tabel 4 dibawah ini.

Tabel 1.

Domain pada DS-5 (Cobit 4.1) dan ISO/IEC 27000

No	Kontrol Objektif DS-5 (Cobit 4.1) Ensure System Security	Kontrol Objektif ISO/IEC 27000
1	Management of IT Security	Security Policy
2	Security Plan	Organization of Information Security
3	Identity Management	Asset Management
4	User Account Management	Human Resources Security
5	Security Testing, Surveillance and Monitoring	Physical & Environmental Security
6	Security Incident Definition	Communication & Operation Management
7	Protection of Security Technology	Access Control
8	Cryptographic Key Management	Information Systems Acquisition, Development & Maintenance
9	Malicious Software Prevention, Detection and Correction	Information Security Incident Management
10	Network Security	Business Continuity Management
11	Exchange of Sensitive Data	Compliance

Mekanisme yang dilakukan pada pembuatan matriks ini sederhana, yaitu :

1. Menyusun domain kontrol yang terdapat pada Cobit 4.1 dan ISO/IEC 27000 dan menempatkannya pada suatu matriks dua dimensi (tabel) dengan susunan yang sesuai dengan urutan pada masing-masing metode.
2. Melihat kontrol objektif pada tiap-tiap domain yang dimiliki oleh keduanya kemudian akan dilihat kesamaannya.
3. Mencari bentuk kesamaan yang paling dominan dari domain yang dimiliki masing-masing *tools* dengan menempatkan domain-domain itu sesuai dengan keterurutanya masing-masing, sehingga kontrol objektif yang dihasilkan akan dibuat terurut berdasarkan susunan dari ISO/IEC 27000.

4. Setelah mengetahui kontrol objektif pada setiap domainnya maka tahapan berikutnya adalah menentukan domain-domain yang bersesuaian dari keduanya dengan cara menempatkan c*hecklist* pada domain yang beririsan berdasarkan banyaknya kesamaan atau kemiripan dari domain yang ada.
5. Membentuk domain-domain baru yang sesuai dengan menggunakan istilah baru yang sesuai, namun tetap mempertahankan sebanyak 11 domain kontrol.
6. Kemudian dari ke-11 domain kontrol yang baru tersebut akan dilakukan *mapping* (dipetakan) pada pasal-pasal yang terdapat pada standar PBI NOMOR : 9/15/PBI/2007.
7. Dihasilkan metodologi baru yang sesuai dengan ketentuan PBI NOMOR : 9/15/PBI/2007 dalam melakukan penyusunan dan penerapan kebijakan keamanan transaksi elektronik pada bank umum.

Dari tahapan yang dilakukan diatas maka matriks tersebut akan menghasilkan klausul baru yang lebih sesuai karena dihasilkan dari dua metode yaitu Cobit 4.1 dan ISO/IEC 27000.

Tabel 2.

Klausul Baru Hasil Mapping Cobit 4.1 dengan ISO/IEC 27000

Domain	Kontrol Objektif (Klausul) Baru Hasil Mapping
CISO.1	Perencanaan Kebijakan Keamanan (Security Policy Plan)
CISO.2	Manajemen Organisasi Keamanan TI (Management & Organization of IT Security)
CISO.3	Manajemen Aset dan Proteksi Keamanan (Asset & Protection of Security Management)
CISO.4	Sumber Daya Manusia dan Identitas Manajemen (Human Resource and Identity Management)
CISO.5	Pengawasan Fisikdan Pengujian Keamanan dan Pengawasan (Physical and Environmental Security Testing Surveillance and Monitoring)
CISO.6	Komunikasi dan Pelaksanaan Dengan Manajemen Akun Pengguna (Communication and Operation using User Account Management)
CISO.7	Kendali Akses dan Keamanan Jaringan (Access Control & Network Security)
CISO.8	Akuisisi Sistem Informasi, Pengembangan dan Perlindungan serta Manajemen Penggunaan Kunci Kriptografi (Information Systems Acquisition, Development using Cryptographic Key Management)
CISO.9	Mendefinisikan Perihal Kecelakaan Keamanan Informasi (Information Security Incident Definition)
CISO.10	Kelanjutan Usaha Dan Manajemen Pertukanan Data Sensitif (Business

Domain	Kontrol Objektif (Klausul) Baru Hasil Mapping
	Continuity and Exchange of Sensitive Data Management)
CISO.11	Pelaksanaan Dengan Pendeteksian Dan Perbaikan Dari Perangkat Lunak yang Mengandung Kode Jahat (Compliance and Malicious Software Prevention Detection and Correction)

Kesimpulan

Berdasarkan hasil analisis permasalahan yang ada dan terjadi di perbankan umum dimana masih terdapat berbagai permasalahan terkait dengan pelayanan transaksi elektronik terutama keamanan transaksi yang berbasis teknologi informasi. Bahkan perangkat kebijakan keamanan transakasi elektronik pun masih belum memiliki keseragaman, dikarenakan Bank Indonesia sebagai pemangku kepentingan perbankan di Indonesia hanya membuat rambu-rambunya saja dalam bentuk Peraturan Bank Indonesi Nomor : 9/15/PBI/2007. Untuk itulah laporan ini memiliki harapan agar permasalahan diatas dapat diselesaikan dengan baik, berikut kesimpulan yang dihasilkan dari pembahasan penelitian ini, yaitu :

1. Bahwa kebijakan yang dimiliki oleh perbankan umum cenderung tidak memiliki panduan standar saat dilakukan penyusunannya, sehingga dengan laporan yang diselesaikan ini penyusunan dapat dilakukan dan menjadi panduan yang baik bagi perbankan umum dan menunjang kelancaran pelaksanaan prosedur pengamanan transaksi elektronik. Hal ini dilakukan dengan metode yang digunakannya yaitu matriks CISO yang merupakan kontrol objektif yang dihasilkan dari Cobit 4.1 DS-5 (Ensure System Security) dan ISO/IEC 27000.
2. Penyusunan kontrol objektif berikutnya dilakukan dengan memetakan pada Peraturan Bank Indonesia Nomor 9/15/PBI/2007, sehingga dihasilkan klausul-klausul yang sesuai dengan peraturan Bank Indonesia.
3. Dengan penggunaan Cobit terutama DS-5 maka audit terhadap keamanan teknologi informasi dapat dilakukan dan memperoleh objektifitas karena kontrol objektif yang digunakan sesuai dengan parameter yang digunakan saat audit teknologi informasi
4. Dengan adanya SOP yang dibuat berdasarkan Dokumen Kebijakan, maka departemen IT akan bertindak responsif jika terjadi insiden pada infrastruktur teknologi informasi

BIBLIOGRAFI

Chris Britton. 2001. "*IT Architecture and Middleware: strategies for building largeintegrated systems*," Addison Wesley.

Indocommit (23 Desember 2005), Kepatuhan terhadap Sistem Keamanan Informasi http://www.indocommit.com/index.html?menu=29&idnews=1506&kid=0&PHPSESSID=ac0fa9bf4b764ea21e26b230102b4 ecb.

ISO/IEC 27000 : 2005 Information Technology – *Code of Practice For Information Security Management*, 2005.

ISO/IEC 27000 : 2005 Information Technology – *Information security management systems – requirements,* 2005.

Jacquelin Bisson, CISSP,"Analis Keamanan Informasi, Callio Technologies) & René Saint-Germain (Direktur Utama, Callio Technologies, Mengimplementasi kebijakan keamanan dengan standar BS7799 /ISO17799 untuk pendekatan terhadap informasi keamanan yang lebih baik", White Paper, 2005 http://202.57.1.181/~download/linux_opensource/artikel+tutorial/general_tutorials/ wp_iso_id.pdf.

Jimmy Hannytyo Pinontoan (28/12/2007), "*Manajemen Keamanan Informasi dengan ISO27001 & ISO27002".*

McLeod Jr.R. 1996. *Sistem Informasi* Manajemen, Jilid 1, edisi Bahasa Indonesia. Terjemahan Teguh, H. Prenhallindo, Jakarta.

O'Brien, J.A. 2002. *Introduction To Information System: Essential For The E-Business Enterprise*, 11th edition. McGraw Hill, New York.

Snyder, Lawrence. 2007. *Fluency with Information Technology: Skills, Concepts, and Capabilities (3rd Edition).*